ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МАҚАН ЕСБОЛАТОВ АТЫНДАҒЫ АЛМАТЫ АКАДЕМИЯСЫ

Қазақстан Республикасының ғылым және техникаға еңбек сіңірген қайраткері,
Қазақстан Республикасы ҚЖҒА академигі, з.ғ.д., профессор
Елеген Ізтілеуұлы Қайыржановтың
90 жылдық мерейтойына арналған

ҚОҒАМ МЕН МЕМЛЕКЕТТІ АҚПАРАТТАНДЫРУ ЖӘНЕ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА ҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ

атты халықаралық ғылыми-тәжірибелік конференциясы
(22 қыркүйек 2023 ж.)

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА

международная научно-практическая конференция посвященной 90-летию со дня рождения
заслуженного деятеля науки и техники Республики Казахстан,
академика КАЕН Республики Казахстан, д.ю.н., профессора
Каиржанова Елегена Изтлеуовича
(22 сентября 2023 г.)

Алматы 2023

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МАҚАН ЕСБОЛАТОВ АТЫНДАҒЫ АЛМАТЫ АКАДЕМИЯСЫ

Қазақстан Республикасының ғылым және техникаға еңбек сіңірген қайраткері,
Қазақстан Республикасы ҚЖҒА академигі, з.ғ.д., профессор
Елеген Ізтілеуұлы Қайыржановтың
90 жылдық мерейтойына арналған

ҚОҒАМ МЕН МЕМЛЕКЕТТІ АҚПАРАТТАНДЫРУ ЖӘНЕ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА ҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ

атты халықаралық ғылыми-тәжірибелік конференциясы
(22 қыркүйек 2023 ж.)

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА

международная научно-практическая конференция посвященной 90-летию со дня рождения
заслуженного деятеля науки и техники Республики Казахстан,
академика КАЕН Республики Казахстан, д.ю.н., профессора
Каиржанова Елегена Изтлеуовича
(22 сентября 2023 г.)

Алматы
2023

УДК 343.2/.7
ББК 67.408
Қ 54

Жауапты редактор:
А.М. Сайтбеков – Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының бастығы полиция генерал-майоры, ҚР ҰҒА құрметті мүшесі, профессор, саясаттану ғылымдарының докторы, заң ғылымдарының кандидаты

Редакция алқасы:
Ж.Р. Дильбарханова (з.ғ.д., профессор),
Е.М. Бимолданов (з.ғ.к., қауымдастырылған профессор),
А.Г. Кан (з.ғ.к., қауымдастырылған профессор),
С.А. Сейлханова (з.ғ.к.)

Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл: халықар. ғыл.-тәж. конф. мат-ры (22.09.2023 ж.) = Противодействие преступности в условиях цифровизации и информатизации общества и государства: мат. межд. науч.- практ. конф. (22.09.2023 г.). – Алматы: ҚР ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2023. – 265 б. қазақша, орысша.

ISBN 978-601-360-081-9

Жинақта Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасымен ұйымдастырылған Қазақстан Республикасы ғылым және техникаға еңбек сіңірген қызметкері, ЖҒҚА академигі, заң ғылымдарының докторы, профессор Қайыржанов Елеген Істілеуұлының 90 жылдығына арналған «Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» халықаралық ғылыми-тәжірибелік конференция қатысушыларының ғылыми мақалалары мен баяндамалары ұсынылған.

В сборнике представлены научные статьи и доклады участников Международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства», посвященной 90 годовщине со дня рождения заслуженного деятеля науки и техники Республики Казахстан, академика КАЕН Республики Казахстан, доктора юридических наук, профессора Каиржанова Елегена Изтлеуовича, организованного кафедрой уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова.

Жинаққа енген материалдар автордың редакциясымен берілді.
Материалы, публикуемые в сборнике, даны в авторской редакции

ББК 67.408
УДК 343.2/.7

ISBN 978-601-360-081-9

© Қазақстан Республикасы ІІМ
М. Есболатов атындағы
Алматы академиясы, 2023

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференциясының бағдарламасы

Программа международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»

Күні:	22 қыркүйек 2023 ж.
Дата:	22 сентября 2023 г.
Өткізу орын:	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
Место проведения:	Алматинская академия МВД Республики Казахстан им. М. Есбулатова
Түрі	Offline және Online (ZOOM интернет-платформасын қолдана отырып)
Формат:	Offline и Online (с использованием интернет-платформы ZOOM)
Басталуы	Сағат 10.00-де (Нұр-Сұлтан қ. уақыты бойынша)
Начало:	В 10.00 ч. (по времени г. Нур-Султан)
10.00 - 14.00	Пленарлық отырыс. Конференция жұмысы Пленарное заседание. Работа конференции
14.00	Конференция жұмысын қорытындылау және аяқтау Подведение итогов и завершение работы конференции

10.00 – 10.10	**Сайтбеков А.М.** **Сайтбеков А.М.**	Алғыс сөз Приветственное слово
10.10 – 10.20	**Әбдіров Н.М.** **Абдиров Н.М.**	Алғыс сөз Приветственное слово

1 секция. Қылмысқа қарсы іс-қимылдың цифрлық трансформациясы
Секция 1. Цифровые трансформации противодействия преступности

10.20 – 10.30	**САЙТБЕКОВ Айдар Мүтәлікұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының бастығы полиция генерал-майоры, ҚР ҰҒА құрметті мүшесі, профессор, саясаттану ғылымдарының докторы, заң ғылымдарының кандидаты	Модератор

САЙТБЕКОВ Айдар Муталикович
Начальник Алматинской академии МВД Республики Казахстан им. М. Есбулатова генерал-майор полиции, кандидат юридических наук, доктор политических наук, профессор, почётный член НАН РК

10.30 – 10.40 **ӘБДІРОВ Нұрлан Мәжитұлы** Баяндама
Қазақстан Республикасы Орталық сайлау комиссиясының төрағасы, з.ғ.д., профессор Доклад
«Цифрландыру және электронды дауыс беру: перспективалар мен тәуекелдер»

АБДИРОВ Нурлан Мажитович
Председатель Центральной избирательной комиссии Республики Казахстан д.ю.н., профессор «Цифровизация и электронное голосование: перспективы и риски»

10.40 – 10.50 **СӘРСЕНОВ Сәкен Сейітжаппарұлы** Баяндама
Қазақстан Республикасы Ішкі істер министрінің цифрландыру және байланыс жөніндегі орынбасары Доклад
«ІІО қызметінде цифрлық трансформацияны іске асырудың тиімділігін бағалау ерекшеліктері»

САРСЕНОВ Сакен Сейтжаппарович
Заместитель Министра внутренних дел Республики Казахстан по цифровизации и связи
«Особенности оценки эффективности реализации цифровой трансформации в деятельности ОВД»

10.50 – 11.00 **ТҰРЫСОВ Әсет Нұрланұлы** Баяндама
Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібінің вице-министрі «Мемлекеттік органдарының қызметінде цифрлық технологияларды қолдану» Доклад

ТУРЫСОВ Асет Нурланович
Вице-министр цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
«Применение цифровых технологий в деятельности государственных органов»

11.00 – 11.10	**ШЕСТАКОВ Дмитрий Анатольевич** Санкт-Петербург халықаралық криминологиялық клубының президенті, Ресей Федерациясының еңбек сіңірген ғылым қайраткері, з.ғ.д., профессор «Қауіпсіздік құқығы және сот төрелігін цифрландыру» **ШЕСТАКОВ Дмитрий Анатольевич** Президент Санкт-Петербургского международного криминологического клуба, доктор юридических наук, профессор, заслуженный деятель науки России «Право безопасности и оцифровка правосудия»	Баяндама Доклад
11.10 – 11.20	**ЖАТҚАНБАЕВА Айжан Ержанқызы** Конституциялық Сот судьясы, з.ғ.д., профессор «Конституциялық өндірісте цифрландыру: отандық және шетелдік тәжірибе» **ЖАТКАНБАЕВА Айжан Ержановна** Судья Конституционного Суда, д.ю.н., профессор «Цифровизация в конституционном производстве: отечественный и зарубежный опыт»	Баяндама Доклад

2 секция. Цифрландыру процесінің қазіргі заманға әсері криминологиялық шындығы
Секция 2. Влияние процесса цифровизации на современную криминологическую реальность

11.20 – 11.30	**ӘБДІРОВ Нұрлан Мәжитұлы** Қазақстан Республикасы Орталық сайлау комиссиясының төрағасы, з.ғ.д., профессор **АБДИРОВ Нурлан Мажитович** Председатель Центральной избирательной комиссии Республики Казахстан д.ю.н., профессор	Модератор
11.30 – 11.40	**Доктор Мариус Лауринайтис** (Литва Республикасы) Миколас Ромерис Университетінің Құқықтық технологиялар орталығының (LegalTech) заң факультеті профессоры, Вильнюс (Литва), әлеуметтік ғылымдар докторы, IT-құқық, PhD. «Экономиканы цифрландыру: алғышарттар, үрдістер, перспективалар»	Баяндама Доклад

Доктор Мариус Лауринайтис
(Литовская Республика)
Профессор юридического факультета Центра правовых технологий (LegalTech) Университета Миколаса Ромериса, Вильнюс (Литва), доктор социальных наук, ИТ-право, PhD.
«Цифровизация экономики: предпосылки, тенденции, преспективы»

11.40 – 11.50 **ДЖАНСАРАЕВА Рима Еренатовна** Баяндама
Әл-Фараби атындағы ҚазҰУ қылмыстық құқық, қылмыстық процесс және криминалистика кафедрасының меңгерушісі, з.ғ.д., профессор Доклад
«Қазіргі цифрлық кеңістіктегі қылмысқа қарсы іс-қимыл»

ДЖАНСАРАЕВА Рима Еренатовна
Заведующая кафедрой уголовного права, уголовного процесса и криминалистики КазНУ имени Аль-Фараби, д.ю.н., профессор
«Противодействие преступности в современном цифровом пространстве»

11.50 – 12.00 **Лея Фокс** (Ұлыбритания) Баяндама
Қылмыстық сот төрелігін зерттеу институтының профессоры Портсмут университеті, MAMBA FHEA PhD докторы, Доклад
«Цифрландыруды зерттеу-жаһандық трендтер мониторингі және білім беру жолдары»

Лея Фокс (Великобритания)
Профессор института исследований уголовного правосудия Университета Портсмута, доктор PhD, MA MBA FHEA
«Исследования цифровизации – мониторинг глобальных трендов и тенденции к обучению»

12.00 – 12.10 **БАТРЫШЕВ Дидар Ғалымұлы** Баяндама
ҚБТУ ректорының м. а., PhD докторы, қауымдастырылған профессор (доцент) Доклад
«Өзекті міндеттерді шешуде цифрландыру»

БАТРЫШЕВ Дидар Галымович
И.о. ректора КБТУ, доктор PhD, ассоциированный профессор (доцент)
«Цифровизация в решении актуальных задач»

12.10 – 12.20 **ЖАНӘБІЛОВА Асел Болатқазықызы** Баяндама
Республикалық нотариаттық палатасының төрағасы, заң ғылымдарының магистрі Доклад
«Құқықтық қызметтер саласындағы ақпараттық қауіпсіздік»

ЖАНАБИЛОВА Асель Булатказыевна
Председатель Республиканской нотариальной палаты, магистр юридических наук
«Информационная безопасность в сфере правовых услуг»

12.20 – 12.30 **ҚАЙЫРЖАНОВА Солидат Елегенқызы** Баяндама
Батыс Қазақстан инновациялық-технологиялық университетінің тарих және құқық кафедрасының профессоры, з.ғ.д., доцент Доклад
«Киберқылмыстылық: түсінігі, түрлері және алдын алу»

КАИРЖАНОВА Солидат Елегеновна
Профессор кафедры истории и права Западно-Казахстанского инновационно-технологического университета, д. ю.н., доцент
«Уголовно-правовые отношения в сфере информационного пространства»

3 Секция. Қоғамды ақпараттандыру жағдайында құқық бұзушылықтардың алдын алу
Секция 3. Профилактика правонарушений в условиях информатизации общества

12.30 – 12.40 **БИМОЛДАНОВ Ержан Малаевич** Модератор
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары., қауымдастырылған профессор з.ғ.к., полиция полковнигі

БИМОЛДАНОВ Ержан Малаевич
Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., ассоциированный профессор, полковник полиции

12.40 – 12.50 **КАНАТБЕК Азиз** (Қырғыз Республикасы) Баяндама
Қырғыз Республикасы Президентінің жанындағы Ұлттық стратегиялық зерттеулер институтының директоры, Қырғыз Республикасы Ұлттық ғылым академиясының корреспондент-мүшесі, профессор Доклад
«Ақпараттық кеңістіктегі стратегиялық басқаруды дамытудың негізгі үлгілері»

КАНАТБЕК Азиз (Кыргызская Республика)
Директор Национального института стратегических исследований при Президенте Кыргызской Республики, член-корреспондент Национальной академии наук Кыргызской Республики, профессор
«Основные модели развития стратегического управления в информационном пространстве»

12.50 – 13.00 **КИМ Ёнхо** (Оңтүстік Корея) Баяндама
Кинель университетінің полиция кафедрасының профессоры, Доклад
Корея полиция департаментінің киберқылмыс бойынша кәсіби тергеушісі
«Қазіргі киберқылмыс: мәселелер мен шешу жолдары»

КИМ Ёнхо (Южная Корея)
Профессор кафедры полиции университета Кёниль, профессиональный следователь по киберпреступности
Корейского полицейского управления
«Современная киберпреступность: вопросы и пути решения»

13.00 – 13.10 **ЧУКМАИТОВ Дулат Сламбекович** Баяндама
И. Жансүгіров атындағы Жетісу университеті Доклад
құқық және экономика жоғары мектебінің профессоры, з.ғ.д., профессор
«Сотталғандарды қадағалау мен бақылауда цифрлық және биометриялық технологияларды қолдану»

ЧУКМАИТОВ Дулат Сламбекович
профессор высшей школы Права и экономики НАО Жетысуский университет им. И. Жансугурова д.ю.н., профессор
«Использование цифровых и биометрических технологий в совершенствовании надзора и контроля за осужденными »

13.10 – 13.20 **АКИМЖАНОВ Талгат Курманович** Баяндама
«Құқықтану және халықаралық құқық» Доклад
кафедрасының профессоры, Тұран университетінің құқық ҒЗИ директоры, з.ғ.д., профессор
«Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында жазаны орындаудың жаңа үлгілерін іздеу»

АКИМЖАНОВ Талгат Курманович
Профессор кафедры «Юриспруденция и Международное право», Директора НИИ права Университета Туран, д.ю.н., профессор
«Поиск новой модели исполнения наказания в условиях цифровизации и информатизации общества и государства»

13.20 – 13.30 **РУСТЕМОВА Гаухар Рустембековна** Баяндама
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Құқық қорғау қызметін басқару кафедрасының профессоры, з.ғ.д., профессор Доклад
«Қазақстан Республикасында денсаулық сақтауды цифрландыру туралы»

РУСТЕМОВА Гаухар Рустембековна
Профессор кафедры управления правоохранительной деятельностью Алматинской академии МВД Республики Казахстан им. М. Есбулатова, д.ю.н., профессор
«О цифровизации здравоохранения в Республике Казахстан»

13.30 – 13.40 **СЕРАЛИЕВ Алибек Болатович** Баяндама
Отставкадағы генерал-майор, з.ғ.к., доцент Доклад
«Қазақстан Республикасының ақпараттық қауіпсіздігін қорғауды қамтамасыз ету мәселелері»

СЕРАЛИЕВ Алибек Болатович
Генерал-майор в отставке, к.ю.н., доцент
«Проблемы обеспечения защиты информационной безопасности Республики Казахстан»

13.40 – 13.50 **АЛАУХАНОВ Есберген Оразұлы** Баяндама
Қазақстан Республикасы Президентінің жанындағы Адам құқықтары жөніндегі комиссияның мүшесі, Қазақстанның еңбек сіңірген қайраткері, з.ғ.д., профессор Доклад
«Профессор Е.И. Қайыржановтың қазіргі заманғы ғылыми мұрасы»

АЛАУХАНОВ Есберген Оразович
Член комиссии по правам человека при Президенте Республики Казахстан, заслуженный деятель Казахстана, д.ю.н., профессор
«Научное наследие профессора Каиржанова Е.И. в современных реальностях»

13.50 – 14.00 **БИМОЛДАНОВ Ержан Малаевич**
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары., қауымдастырылған профессор з.ғ.к., полиция полковнигі

Баяндамаларды талқылау және конференция жұмысын қорытындылау
Подведение итогов и завершение работы конференции

БИМОЛДАНОВ Ержан Малаевич
Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ю.н., ассоциированный профессор, полковник полиции

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» халықаралық ғылыми-тәжірибелік конференцияға қатысушылар тізімі

Список участников международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»

№	Аты-жөні Ф.И.О.	Лауазымы Должность
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ОРТАЛЫҚ САЙЛАУ КОМИССИЯСЫ ЦЕНТРАЛЬНАЯ ИЗБИРАТЕЛЬНАЯ КОМИССИЯ РЕСПУБЛИКИ КАЗАХСТАН		
1.	Әбдіров Нұрлан Мәжитұлы Абдиров Нурлан Мажитович	Қазақстан Республикасы Орталық сайлау комиссиясының төрағасы, з.ғ.д., профессор Председатель Центральной избирательной комиссии Республики Казахстан д.ю.н., профессор
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН		
2.	Сәрсенов Сәкен Сейітжаппарұлы Сарсенов Сакен Сейтжаппарович	Қазақстан Республикасы Ішкі істер министрінің цифрландыру және байланыс жөніндегі орынбасары Заместитель Министра внутренних дел Республики Казахстан по цифровизации и связи
3.	Сайтбеков Айдар Мүтәлікұлы Сайтбеков Айдар Муталикович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының бастығы полиция генерал-майоры, ҚР ҰҒА құрметті мүшесі, профессор, саясаттану ғылымдарының докторы, заң ғылымдарының кандидаты Начальник Алматинской академии МВД Республики Казахстан им. М. Есбулатова генерал-майор полиции, кандидат юридических наук, доктор политических наук, профессор, почётный член НАН РК.
4.	Бимолданов Ержан Малаевич Бимолданов Ержан Малаевич	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары, қауымдастырылған профессор, з.ғ.к., полиция полковнигі Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ю.н., ассоциированный профессор, полковник полиции
5.	Қойшыбаев Еркебұлан Ұланұлы Койшибаев Еркебулан Уланович	Алматы қаласы ПД криминалдық полиция басқармасының киберқылмысқа қарсы күрес бөлімінің аса маңызды істер жөніндегі аға жедел уәкілі, полиция подполковнигі Старший оперуполномоченный по особо важным делам отдела по борьбе с киберпреступлениями управления криминальной полиции ДП г. Алматы, подполковник полиции

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН		
6.	Тұрысов Әсет Нұрланұлы Турысов Асет Нурланович	Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібінің вице-министрі Вице-министр цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ КОНСТИТУЦИЯЛЫҚ СОТЫ КОНСТИТУЦИОННЫЙ СУД РЕСПУБЛИКИ КАЗАХСТАН		
7.	Жатқанбаева Айжан Ержанқызы Жатканбаева Айжан Ержановна	Конституциялық Сот судьясы, з.ғ.д., профессор Судья Конституционного Суда, д.ю.н., профессор
РЕСПУБЛИКАЛЫҚ НОТАРИАТТЫҚ ПАЛАТА РЕСПУБЛИКАНСКАЯ НОТАРИАЛЬНАЯ ПАЛАТА		
8.	Жанәбілова Асел Болатқазықызы Жанабилова Асель Булатказыевна	Республикалық нотариаттық палатасының төрағасы, заң ғылымдарының магистрі Председатель Республиканской нотариальной палаты, магистр юридических наук
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПРЕЗИДЕНТІНІҢ ЖАНЫНДАҒЫ АДАМ ҚҰҚЫҚТАРЫ ЖӨНІНДЕГІ КОМИССИЯ КОМИССИЯ ПО ПРАВАМ ЧЕЛОВЕКА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ КАЗАХСТАН		
9.	Есберген Оразұлы Алауханов Алауханов Есберген Оразович	Қазақстан Республикасы Президентінің жанындағы Адам құқықтары жөніндегі комиссияның мүшесі, Қазақстанның еңбек сіңірген қайраткері, з.ғ.д., профессор Член комиссии по правам человека при Президенте Республики Казахстан, заслуженный деятель Казахстана, д.ю.н., профессор
ШЕТЕЛДІК ҒАЛЫМДАР ЗАРУБЕЖНЫЕ УЧЕНЫЕ		
10.	Дмитрий Анатольевич Шестаков Дмитрий Анатольевич Шестаков	Санкт-Петербург халықаралық криминологиялық клубының президенті, Ресей Федерациясының еңбек сіңірген ғылым қайраткері, з.ғ.д., профессор Президент Санкт-Петербургского международного криминологического клуба, доктор юридических наук, профессор, заслуженный деятель науки России
11.	Доктор Мариус Лауринайтис (Литва Республикасы) Доктор Мариус Лауринайтис (Литовская Республика)	Миколас Ромерис Университетінің Құқықтық технологиялар орталығының (LegalTech) заң факультеті профессоры, Вильнюс (Литва), әлеуметтік ғылымдар докторы, PhD. IT-құқық. Профессор юридического факультета Центра правовых технологий (LegalTech) Университета Миколаса Ромериса, Вильнюс (Литва), доктор социальных наук, ИТ-право, PhD..

12.	Лея Фокс (Ұлыбритания) Лея Фокс (Великобритания)	Қылмыстық сот төрелігін зерттеу институтының профессоры Портсмут университеті, MAMBA FHEA PhD докторы Профессор института исследований уголовного правосудия Университета Портсмута, доктор PhD, MA MBA FHEA
13.	Канатбек Азиз (Қырғыз Республикасы) Канатбек Азиз (Кыргызская Республика)	Қырғыз Республикасы Президентінің жанындағы Ұлттық стратегиялық зерттеулер институтының директоры, Қырғыз Республикасы Ұлттық ғылым академиясының корреспондент-мүшесі, профессор Директор Национального института стратегических исследований при Президенте Кыргызской Республики, член-корреспондент Национальной академии наук Кыргызской Республики, профессор
14.	Ким Ёнхо (Оңтүстік Корея) Ким Ёнхо (Южная Корея)	Кинель университетінің полиция кафедрасының профессоры, Корея полиция департаментінің киберқылмыс бойынша кәсіби тергеушісі профессор кафедры полиции университета Кёниль, профессиональный следователь по киберпреступности Корейского полицейского управления
15.	Чжо Санг-Хён (Оңтүстік Корея) Чжо Санг-Хён (Южная Корея)	Оңтүстік Кореядағы Шинхан университетінің полиция бөлімі факультетінің профессоры профессор факультета полицейского управления универсетета Шинхан в Южной Кореи
16.	Розенко Станислав Васильевич Розенко Станислав Васильевич	Құқық Жоғары мектебінің басшысы Югор мемлекеттік университеті, заң ғылымдарының кандидаты, доцент Руководитель Высшей школы права Югорского государственного университета, кандидат юридических наук, доцент
17.	Мұсаев А. И. Мусаев А.И.	Өзбекстан Республикасы қоғамдық қауіпсіздік Университетінің ақпараттық технологиялар кафедрасының доценті Доцент кафедры инфомационных технологий Университета общественной безопасности Республики Узбекистан
18.	Парсиев С.С. Парсиев С.С.	Өзбекстан Республикасы қоғамдық қауіпсіздік Университетінің ақпараттық технологиялар кафедрасының профессоры Профессор кафедры инфомационных технологий Университета общественной безопасности Республики Узбекистан

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. АЛЬ-ФАРАБИ		
19.	Джансараева Рима Еренатовна Джансараева Рима Еренатовна	Әл-Фараби атындағы ҚазҰУ қылмыстық құқық, қылмыстық процесс және криминалистика кафедрасының меңгерушісі, з.ғ.д., профессор Заведующая кафедрой уголовного права, уголовного процесса и криминалистики КазНУ имени Аль-Фараби, д.ю.н., профессор
20.	Баймагамбетова Зульфия Мажитовна Баймагамбетова Зульфия Мажитовна	Халықаралық құқық кафедрасының аға оқытушысы, доктор PhD, Әл-Фараби атындағы Қазақ ұлттық университеті Старший преподаватель кафедры международного права, доктор PhD, Казахский национальный университет им. Аль-Фараби
ҚАЗАҚСТАН-БРИТАН ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ КАЗАХСТАНСКО-БРИТАНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ		
21.	Батрышев Дидар Ғалымұлы Батрышев Дидар Галымович	ҚБТУ ректорының м.а., PhD докторы, қауымдастырылған профессор (доцент) И.о. ректора КБТУ, доктор PhD, ассоциированный профессор (доцент)
22.	Иманбаев Азамат Жанатұлы Иманбаев Азамат Жанатович	Қазақ-Британ техникалық университетінің сениор-лекторы, техника ғылымдарының магистрі Сениор-лектор, Казахско-Британского технического университета, магистр технических наук
23.	Зиро Аасо Араз Зиро Аасо Араз	Қазақ-Британ техникалық университетінің сениор-лекторы, техника ғылымдарының магистрі Сениор-лектор, Казахско-Британского технического университета, магистр технических наук
ОТАНДЫҚ ҒАЛЫМДАР ОТЕЧЕСТВЕННЫЕ УЧЕНЫЕ		
24.	Қайыржанова Солидат Елегенқызы Каиржанова Солидат Елегеновна	Батыс Қазақстан инновациялық-технологиялық университетінің тарих және құқықтану кафедрасының профессоры заң ғылымдарының докторы, доцент кіші әділет кеңесшісі Профессор кафедры История и юриспруденция Западно-Казахстанского инновационного-технологического университета доктор юридических наук, доцент младший советник юстиции
25.	Сағынбекова Гүлнар Мейрханқызы Сагынбекова Гульнар Мейрхановна	Заң ғылымдарының докторы Алматы қ. мамандандырылған ауданаралық экономикалық соты Доктор юридических наук Специализированный межрайонный экономический суд г. Алматы

26.	Акимжанов Талгат Курманович Акимжанов Талгат Курманович	«Құқықтану және халықаралық құқық» кафедрасының профессоры, Тұран университетінің құқық ҒЗИ директоры, з.ғ.д., профессор Профессор кафедры «Юриспруденция и Международное право», Директора НИИ права Университета Туран, доктор юридических наук, профессор
27.	Сералиев Алибек Болатович Сералиев Алибек Болатович	Отставкадағы генерал-майор, з.ғ.к., доцент Генерал-майор в отставке, к.ю.н., доцент
28.	Усенбаева Асемгуль Узакбаевна Усенбаева Асемгуль Узакбаевна	Еуразия технологиялық университеті Құқық мектебінің аға оқытушысы, заң ғылымдарының магистры Старший преподаватель Школы права Евразийского технологического университета, магистр юридических наук
29.	Султанов Салимжан Исаевич Султанов Салимжан Исаевич	Еуразия Технологиялық Университеті Құқық мектебінің қауымдастырылған профессоры, заң ғылымдарының кандидаты Евразийский технологический университет ассоциированный профессор школы права, кандидат юридических наук
30.	Сатыбалдинов Марат Темірғалиұлы Сатыбалдинов Марат Темиргалиевич	Құқық мектебінің аға оқытушысы, Еуразиялық технологиялық университеті, Алматы қ. Старший преподаватель Школы права, Евразийский технологический университет, г. Алматы
31.	Қаратаев Тұрдалы Жақслықұлы Каратаев Турдалы Жакслыкович	Заң ғылымдарының кандидаты Кандидат юридических наук
32.	Ысқақов Әсет Қабділхамитұлы Искаков Асет Кабдылхамитович	Қазақстан Республикасы ІІМ ҚАЖК Оқу орталығының арнайы пәндер циклінің оқытушысы, әділет майоры, заң ғылымдарының магистрі Преподаватель цикла Специальных дисциплин Учебного центра КУИС МВД Республики Казахстан, майор юстиции, магистр юридических наук
33.	Құлажанова Аяжан Нүсіпжановна Кулажанова Аяжан Нусупжановна	Еуразия Технологиялық Университеті, «Құқық» факультетінің аға оқытушысы, заң ғылымдарының магистірі Евразийский технологический университет, старший преподаватель факультета «право», магистр юридических наук

34.	Османова Гүлайна Джалалықызы Османова Гюлайна Джалалыкызы	Абай атындағы ҚазҰПУ, Тарих және құқық институты, «Құқықтану» кафедрасының аға оқытушысы, PhD докторы КазНПУ им. Абая, Институт истории и права, старший преподаватель кафедры «Юриспруденция», доктор PhD
35.	Бижанова Айгүл Рабханқызы Бижанова Айгүл Рабханқызы	Абай атындағы ҚазҰПУ, Тарих және құқық институты, «Құқықтану» кафедрасының қауымдастырылған профессоры, заң ғылымдарының докторы КазНПУ им. Абая, Институт истории и права, ассоциированный профессор кафедры «Юриспруденция», доктор юридических наук
36.	Қыздарбекова Баян Жәкенқызы Кыздарбекова Баян Жакеновна	Қазақстан Республикасы Заңнама және құқықтық ақпарат институтының қылмыстық, қылмыстық-процестік, қылмыстық-атқару заңнамасы бөлімінің жетекші ғылыми қызметкері, з.ғ. к., қауымдастырылған профессор Ведущий научный сотрудник отдела уголовного, уголовно-процессуального, уголовно-исполнительного законодательства Института законодательства и правовой информации Республики Казахстан, к.ю.н., ассоциированный профессор
37.	Шаяхметова Жанна Бекполқызы Шаяхметова Жанна Бекполовна	Х. Досмұхамедов атындағы Атырау университетінің қылмыстық-құқықтық пәндер кафедрасының профессоры, заң ғылымдарының кандидаты, доцент профессор кафедры уголовно-правовых дисциплин Атырауского университета им. Х. Досмухамедова кандидат юридических наук, доцент
38.	Сералиева Әлия Мәжитқызы Сералиева Алия Мажитовна	«Құқықтану» кафедрасының қауымдастырылған профессоры Абай атындағы Қазақ ұлттық педагогикалық университеті, заң ғылымдарының кандидаты, қауымдастырылған профессор (доцент) Ассоциированный профессор кафедры «Юриспруденция» Казахского национального педагогического университета имени Абая, кандидат юридических наук, ассоциированный профессор (доцент)
39.	Шаяхметова Жанна Бекполқызы Шаяхметова Жанна Бекполовна	Х. Досмұхамедов атындағы Атырау университетінің қылмыстық-құқықтық пәндер кафедрасының профессоры, заң ғылымдарының кандидаты, доцент профессор кафедры уголовно-правовых дисциплин Атырауского университета имени Х. Досмухамедова кандидат юридических наук, доцент
40.	Чукмаитов Дулат Сламбекович Чукмаитов Дулат Сламбекович	И. Жансүгіров атындағы Жетісу университеті құқық және экономика жоғары мектебінің профессоры, з.ғ.д., профессор профессор высшей школы Права и экономики НАО Жетысуский университет им. И. Жансугурова д.ю.н., профессор

41.	Бапанова Тоғжан Талғатқызы Бапанова Тогжан Талгаткызы	Алматы қ. ОҚО арнайы пәндер оқытушысы философия докторы (PhD) Преподаватель специальных дисциплин ЮКА г. Алматы доктор (PhD) философии
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПРОКУРАТУРАСЫ		
42.	Аширбеков Марат Есенұлы Аширбеков Марат Еркенович	Бас көлік прокурорының аға көмекшісі әділет кеңесшісі, заң ғылымдарының магистрі Старший помощник Главного транспортного прокурора советник юстиции, магистр юридических наук
43.	Воеводкин Денис Викторович Воеводкин Денис Викторович	Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты, әділет кеңесшісі докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, советник юстиции
44.	Жилхайдарова Баян Аблаевна Жилхайдарова Баян Аблаевна	Құқық қорғау академиясының магистранты Қазақстан Республикасы Бас прокуратурасының жанындағы органдардың, 2-сыныпты заңгер магистрант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан,юрист 2-го класса
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҰЛТТЫҚ ҰЛАН АКАДЕМИЯСЫ		
45.	Садыров Айдос Қайтпергенұлы Садыров Айдос Кайтпергенович	Қазақстан Республикасы Ұлттық ұлан академиясының қару-жарақ және атыс кафедрасының бастығы, полковник Начальник кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, полковник
46.	Волков Борис Витальевич Волков Борис Витальевич	Қазақстан Республикасы Ұлттық ұланы академиясының қару-жарақ және атыс кафедрасының оқытушысы, подполковник, педагогика магистрі преподаватель кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, подполковник, магистр педагогики
47.	Мурталимов Шоқан Рамазанұлы Мурталимов Шокан Рамазанович	Қазақстан Республикасы Ұлттық ұланы академиясының қару-жарақ және атыс кафедрасының оқытушысы, подполковник, магистр Преподаватель кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, подполковник, магистр
48.	Сейтжан Қанат Көшербайұлы Сейітжан Қанат Көшербайұлы	Қазақстан Республикасы Ұлттық ұлан академиясы штабының автоматтандыру бөлімінің аға инженері, аға лейтенант Старший инженер отдела автоматизации штаба Академии Национальной гвардии Республики Казахстан, старший лейтенант

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІІМ Б. БЕЙСЕНОВ АТЫНДАҒЫ ҚАРАҒАНДЫ АКАДЕМИЯСЫ		
49.	Алтайбаев Совет Қапашұлы Алтайбаев Александр Васильевич	Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академисы, Қылмыстық құқық және криминоогия кафедрасының профессоры, заң ғылымдарының кандидаты, қауымдастырылған профессор Карагандинская академия МВД Республики Казахстан имени Б. Бейсенова, Профессор кафедры уголовного права и криминогии, кандидат юридических наук, ассоциированный профессор
50.	Арынова Әсия Нұрланқызы Арынова Асия Нурлановна	Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы,қылмыстық құқық және криминология кафедрасының оқытушысы, құқық магистрі, полиция подполковнигі Карагандинская академия МВД Республики Казахстан им.Б. Бейсенова, преподаватель кафедры уголовного права и криминологии, магистр права, подполковник полиции
51.	Байтеленова Самал Ғалымқызы Байтеленова Самал Галымовна	Қазақстан Республикасы ІІМ Қарағанды академиясы Б. Бейсенов атындағы Ғылыми-зерттеу институтының қылмыстық саясат және қылмыстың алдын алу проблемаларын зерттеу орталығының ғылыми қызметкері. Научный сотрудник Центра по исследованию проблем уголовной политики и профилактики преступности Научно-исследовательского института Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІНІҢ Ш. ҚАБЫЛБАЕВ АТЫНДАҒЫ ҚОСТАНАЙ АКАДЕМИЯСЫ		
52.	Ғалым Ажар Маратқызы Ғалым Ажар Маратқызы	ҚР ІІМ Ш. Қабылбаев атындағы Қостанай академиясы ҚПжК кафедрасының аға оқытушы полиция подполковнигі Старший преподаватель кафедры УПиК Костанайской академии МВД РК имени Ш. Кабылбаева подполковник полиции
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІІМ М. ЕСБОЛАТОВ АТЫНДАҒЫ АЛМАТЫ АКАДЕМИЯСЫ		
53.	Рустемова Гаухар Рустембековна Рустемова Гаухар Рустембековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының құқық қорғау қызметін басқару кафедрасының профессоры, з.ғ.д., профессор Профессор кафедры управления правоохранительной деятельностью Алматинской академии МВД Республики Казахстан им. М. Есбулатова, д.ю.н., профессор
54.	Кегембаева Жанар Аманжанқызы	Заң ғылымдарының докторы, профессор Қазақстан Республикасы ІІМ М. Есболатов ат. Алматы академиясы

	Кегембаева Жанар Аманжановна	Доктор юридических наук, профессор Алматинской академии МВД Республики Казахстан им. М. Есбулатова
55.	Батырбаев Адылхан Кошкенович Батырбаев Адылхан Кошкенович	Қазақстан Республикасы ІІМ М. Есболатов ат. Алматы академиясының қылмыстық құқық және криминология кафедрасының профессоры., з. ғ. к., полиция полковнигі Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ю.н., полковник полиции
56.	Марат Айгүл Маратқызы Марат Айгуль Маратовна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова
57.	Маймаков Айболат Тлеубаевич Маймаков Айболат Тлеубаевич	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедра бастығының орынбасары з.ғ.м., полиция полковнигі Заместитель начальника кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., полковник полиции
58.	Абажанова Асем Зейноллаевна Абажанова Асем Зейноллаевна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова, м.ю.н., подполковник полиции
59.	Әбіжанов Сырым Маратұлы Абижанов Сырым Маратович	Қылмыстық құқық және криминология кафедрасының доценті, PhD докторы, полиция подполковнигі Доцент кафедры уголовного права и криминологии, доктор PhD, подполковник полиции
60.	Жиенгалиева Айгерим Алтынбековна Жиенгалиева Айгерим Алтынбековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Қылмыстық құқық және криминология кафедрасының аға оқытушысы з.ғ.м., полиция майоры Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова, м.ю.н., майор полиции
61.	Бапанов Мағжан Талғатұлы	ҚР ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминологии кафедрасының оқытушысы полиция майоры, з.ғ.м.

	Бапанов Мағжан Талғатұлы	Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД РК им. М. Есбулатова майор полиции, м.ю.н.
62.	Айткеш Айбек Қанатұлы Айткеш Айбек Канатулы	ҚР ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедрасының оқытушысы полиция капитаны, з.ғ.м. Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н, капитан полиции
63.	Тұрғынбаева Альбина Маратқызы Тургунбаева Альбина Маратовна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция капитаны Преподаватель кафедры уголовного права и криминологии Алматинской академия МВД Республики Казахстан им. М. Есбулатова капитан полиции
64.	Бейсеналиев Бауыржан Нұралыұлы Бейсеналиев Бауржан Нуралыулы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасының аға оқытушысы, заң ғылымдарының кандидаты, полиция подполковнигі Старший преподаватель кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова, кандидат юридических наук, подполковник полиции
65.	Сапаров Жансерик Жайшылыкович Сапаров Жансерик Жайылыкович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Ғылыми-зерттеу орталығы, қылмысқа қарсы іс-қимыл және заңнаманы жетілдіру проблемаларын зерттеу бөлімшесінің бастығы, заң ғылымдарының магистрі, полиция подполковнигі Начальник Научно-исследовательского центра отделения по изучению проблем противодействия преступности и совершенствования законодательства, Алматинской академии МВД Республики Казахстан им. М. Есбулатова магистр юридических наук, подполковник полиции
66.	Шидемов А. Г. Шидемов А. Г.	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Ғылыми-зерттеу орталығы аға ғылыми қызметкер полиция майоры Старший научный сотрудник Научно-исследовательского центра Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции

67.	Абикенов Абдулла Нурхатулы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Жоғары оқу орнынан кейінгі факультетінің 2-курс докторанты полиция капитаны, заң ғылымдарының магистрі
	Абикенов Абдулла Нурхатулы	Докторант 2 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции, магистр права
68.	Аманова Диана Турановна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Жоғары оқу орнынан кейінгі факультетінің 2 курс докторанты полиция майоры, ұлттық қауіпсіздік және әскери істер магистрі
	Аманова Диана Турановна	Докторант 2 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова, майор полиции, магистр национальной безопасности и военных дел
69.	Курмангалиева Лаура Жумабековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Жоғары оқу орнынан кейінгі факультетінің 2-курс докторанты полиция капитаны, заң ғылымдарының магистрі
	Курмангалиева Лаура Жумабековна	Докторант 2 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции, магистр права
70.	Нұргүл Байтоққызы Кубанова	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Жоғары оқу орнынан кейінгі факультетінің 2-курс докторанты полиция майоры, заң ғылымдарының магистрі
	Кубанова Нургуль Байтоковна	Докторант 2 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции, магистр права
71.	Сарбасов Алихан Ержанович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Жоғары оқу орнынан кейінгі факультетінің 1-курс докторанты полиция капитаны, заң ғылымдарының магистрі
	Сарбасов Алихан Ержанович	Докторант 1 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции, магистр права
72.	Сабанова Анна Сергеевна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының магистранты, полиция лейтенанты
	Сабанова Анна Сергеевна	Магистрант Алматинской академии МВД Республики Казахстан им. М. Есбулатова, лейтенант полиции

АБДИРОВ Нурлан Мажитович
Председатель Центральной избирательной комиссии Республики Казахстан,
доктор юридических наук, профессор

ЦИФРОВИЗАЦИЯ И ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ: ПЕРСПЕКТИВЫ И РИСКИ

XXI век входит в историю общемировым трендом на ускоренное продвижение продуктов цифровизации в самые различные сферы деятельности человека, что, безусловно, оказывает определяющее воздействие на технологическое развитие многих государств.

2 сентября 2019 года в Послании народу Президент страны Касым-Жомарт Токаев объявил, что «Казахстан взял курс на развитие цифровой экономики. Правительству предстоит адаптировать законодательство под новые технологические явления: 5G, «Умные города», большие данные, блокчейн, цифровые активы, новые цифровые финансовые инструменты. Казахстан должен стать брендом в качестве открытой юрисдикции для технологического партнерства, строительства и размещения дата-центров, развития транзита данных, участия в глобальном рынке цифровых услуг» [1].

А уже в 2020 году мир столкнулся с невиданным ранее влиянием пандемии коронавируса на экономические, социальные, культурные и политические процессы. Это заставило человечество форсированно войти в новую цифровую реальность, начать быстро к ней приспосабливаться и научиться в ней выживать. Из-за вынужденного запрета на проведение массовых мероприятий и предписаниям по самоизоляции граждан были отменены выборы в большинстве стран, где планировалось их проведение. Отмена традиционных выборов с голосованием на избирательных участках повысила актуальность разработки цифровых сервисов дистанционного голосования.

В целом закономерно, что цифровизация, изменяющая качественный уровень взаимоотношений между государством и обществом, неизбежно, входит и в электоральную сферу. Ведь выборы – это основной институт непосредственного участия граждан в политической жизни страны, гарантированного Конституцией, а доверие населения к процедуре выборов – одна из ключевых составляющих легитимности действующей политической системы в любой стране. Роль избирательной системы и избирательного процесса на протяжении столетий всегда была фундаментальной, ведь выборы придают политической системе устойчивость, а обществу – стабильность.

В связи с этим, все более актуализируется задача по вовлечению общества в электоральный процесс, учитывая разнообразие современных технологий, применяемых в международной избирательной практике.

Условия изменились, когда вектор истории свернул в сторону виртуального пространства, заставив пересмотреть все накопленное в традиционной системе выборов. С рождением цифрового государства родилась и новая их форма – электронные выборы.

От каменного лототрона до перфокарт, от механических машин и компьютеров до прямой электронной записи и онлайн-выборов история автоматизации процедуры голосования насчитывает не один век. Люди всегда стремились сделать процессы удобнее и эффективнее, а выборы – не исключение.

Актуальность оценки потенциала электронного голосования применительно к нашей стране возникла после обращения Президента Касым-Жомарта Токаева к нации с Посланием от 16 марта 2022 года. Во исполнение пункта 12 Общенационального плана мероприятий по его реализации Центральной избирательной комиссией проводится системная работа по изучению мирового опыта внедрения альтернативных форм голосования на выборах (электронное, дистанционное, досрочное, многодневное) [2].

Надо отметить, что на сегодня электоральный транзит от традиционного бумажного к электронному голосованию охватывает все континенты. По состоянию на 2022 год в нем участвуют более 40 государств, где законодательно закреплена возможность применения электронных технологий на выборах и тестируются различные формы дистанционного голосования и электронного голосования на избирательных участках. В 12 странах из их числа законодатели ввели электронное голосование в качестве императивной нормы права. В этих странах электронное голосование стало единственной формой реализации активного избирательного права и применяется на муниципальных, региональных и общенациональных выборах.

При этом государства-операторы электронного голосования существенно отличаются по электоральной культуре, традициям демократии, уровню социально-экономического, культурного, научного развития. Технологическая модернизация процесса голосования на выборах идет по множеству разнонаправленных траекторий. Чтобы убедиться в этом, достаточно сравнить особенности электронного голосования в развивающейся Индии и развитой Швейцарии, в компактной по территории Эстонии и огромной Бразилии. [3, с. 65].

Вопрос же внедрения цифровых сервисов в избирательную практику Казахстана не менее актуален, но возможен только в том случае, если это примет сам избиратель. А этого можно достичь при условии публичного и всестороннего обсуждения, глубоких всесторонних научных исследований. Начать эту работу следует с анализа общественного мнения по вопросу отношения к электронному голосованию.

Не ограничиваясь проведением обзора мировой практики применения электронного голосования, Центральная избирательная комиссия Казахстана полагает целесообразным проведение мониторинга общественных настроений в самой республике с целью определения уровня восприятия обществом упомянутых альтернативных форм голосования, наличия технологических и репутационных барьеров данного формата, пользовательских предпочтений избирателей, а также оценки перспектив их внедрения в будущем.

В целях дальнейшего изучения вопроса уже в текущем году Центризбиркомом было инициировано проведение широкого социологического опроса, который реализуется совместно с Казахстанским институтом стратегических исследований при Президенте РК.

Надо сказать, что повышенный интерес к исследованию новых цифровых технологий в избирательном процессе и их влияния на реализацию гражданами своих избирательных прав нашел отражение в трудах многих зарубежных исследователей. В частности, различные аспекты электронного голосования изучены Р. Альмейдой, Л. Рикки, Л. Камаринхи-Матосом, Р. Альварезом, Т. Холла, Е. Арнольдом, М. Солваком, К. Вассила, Р. Криммером, Д. Дуэнас-Сидом, П. Винкелем, А. Койтмае, Р. Серрано, М. Фрейре, К. Вреде, К. Рибоном, Ш. Энгугардом. Существенный научный задел российских ученых в изучении данной тематики появился только в последние годы, среди которых можно назвать публикации Р.А. Алексеева, А.В. Абрамова, Я.В. Антонова, И.Б. Борисова, А.А. Вешнякова, А.А. Тедеева [4, с. 147-148], В.И. Федорова и др.

В них пристальное внимание вызывают вопросы обеспечения гарантий избирательных прав граждан в условиях цифровизации избирательного процесса, влияния интернет-голосования в разных странах на явку избирателей и градус доверия к государственной власти, проблемы правовой защиты электронного голосования, кибербезопасности и др.

Заслуживают внимания наработки российского исследователя Федорова В.И., издавшего в 2023 году большую монографию «Электронное голосование: российский и зарубежный

опыт», в которой проводится прямая корреляция между применением электронного голосования и уровнем электоральной культуры общества [5]. На материалах 12 стран (Бельгия, Бразилия, Бутан, Венесуэла, Индия, Кыргызстан, Монголия, Намибия, Филиппины, Швейцария, Эстония, Россия), в большинстве из которых в избирательном законодательстве предусмотрено применение электронного голосования на общенациональных выборах на территории всей страны, автор рассмотрел вопросы влияния электронного голосования на явку избирателей и доверие к выборам, определил тенденции развития электронного голосования и факторы, оказывающие влияние на выбор его формы.

Если же обратиться к исследовательскому полю Казахстана, то тема цифровых выборов совершенно обойдена вниманием наших исследователей, что, возможно, связано с направленностью таких выборов на перспективу и отсутствием в текущей политической повестке. Между тем, сложность и многоплановость вопросов, требующих своего качественного решения вряд ли возможно без глубокой, всесторонней их научной проработки уже на данном этапе развития страны.

Оговоримся, что, анализируя разнообразный мировой опыт электронного голосования, приходит понимание, что в большинстве стран мира электронным голосованием считают любую форму волеизъявления граждан, при которой для обработки голосов избирателей, участников референдума используются программно-технические средства.

Формы электронного голосования могут быть разными. Выделяются две большие разновидности: голосование на стационарных избирательных участках и голосование через интернет. В мировой практике развития автоматизированных систем голосования можно выделить три больших этапа эволюции: механический, электронный, дистанционный. Если механический этап завершился в 1960-х годах, то два других – электронный и дистанционный продолжают оставаться актуальными и в наши дни. Одним из проявлений электронной демократии является дистанционное электронное голосование, которое также нередко именуется интернет-голосованием.

Совет Европы в своей Рекомендации «О юридических, оперативных и технических стандартах электронного голосования» использует широкое понятие электронного голосования, которое включает в себя «электронные машины для голосования на избирательных участках, использование оптических сканеров для записи и (или) подсчета бюллетеней и дистанционного электронного голосования» [6]. Таким образом, в широком смысле под ним понимается как дистанционное, так и стационарное электронное голосование.

Дистанционное электронное голосование представляет собой голосование без применения бюллетеня, изготовленного на бумажном носителе, с применением особого программного обеспечения, используемого в рамках процедуры электронного голосования. Данная дефиниция в большой степени схожа с определением электронного голосования. Разница состоит в том, что при дистанционном электронном голосовании применяется особое программное обеспечение, а не технические средства [7, с. 105].

Можно сделать вывод, что сегодня интернет-голосование в основном доступно для голосования за пределами страны, а когда оно используется внутри страны, то в основном ограничивается определенными группами избирателей. Следует отметить, что США разрешают отправлять голоса из-за границы по электронной почте, что не рассматривается как интернет-голосование [8].

Таким образом, дистанционное электронное голосование или интернет-голосование, с одной стороны, пока не слишком широко распространено в качестве официальной формы голосования, с другой – его преимущества стимулируют избирательные органы проводить эксперименты по его внедрению, результаты которых оцениваются неоднозначно.

Кое-кто в Казахстане может помнит, что в 2004 году у нас была запущена автоматизированная информационная система «Сайлау», представляющая собой комплекс, автоматизирующий учет избирателей, процессы подготовки, регистрации и голосования, подведение итогов голосования, подготовку и отображение результатов голосования,

сведения о кандидатах, баллотирующихся на должность Президента Республики Казахстан или в депутаты Парламента Республики Казахстан [9].

Как свидетельствуют прошедшие в то время выборы, избиратели в большинстве своем предпочли воспользоваться традиционным бумажным избирательным бюллетенем, а не электронным. Так, если в 2004 году услугами электронного голосования воспользовались всего 7,2% избирателей, принявших участие в выборах, то в 2005 году – 5,8%, а в 2007-м лишь 2,2% [10].

Происходящие на практике кратковременные перебои в работе системы из-за отключения электроэнергии, перезагрузки компьютеров и т.д. тоже вызвали дополнительные трудности в популяризации системы.

Актуальной была и проблема низкой эффективности использования системы в межэлекторальный период, а также необходимость постоянных финансовых затрат на ее содержание и модернизацию.

Трехлетний опыт применения в избирательном процессе АИС «Сайлау» показал недоверие к ней со стороны казахстанских избирателей. Основные претензии обусловлены выявлением существенных недостатков в системе электронного голосования, на которые обращали внимание эксперты и наблюдатели БДИПЧ/ОБСЕ, политические партии и общественные объединения страны, а также сами избиратели [11].

Вместе с тем, рост доверия к цифровым технологиям в целом постепенно нарастает во всем мире, и Республика Казахстан здесь не является исключением. Достаточно вспомнить онлайн покупки, банковские приложения и сервисы.

Поэтому первыми шагами по реализации поручений, озвученных в Послании Главы государства от 16 марта 2022 года, стали меры, принятые Центризбиркомом Казахстана совместно с заинтересованными органами по созданию единой электронной базы избирателей, в том числе с учетом имеющихся возможностей НАО «Правительство для граждан» и платформы www.egov.kz, ее интеграции с другими информационными системами.

На сегодняшний день международным правовым актом, который определяет стандарты электронного голосования, выступает упомянутая выше Рекомендация Совета по стандартам электронного голосования. В этом документе описаны требования к условиям проведения электронных выборов.

Согласно Рекомендации, для соблюдения основных принципов избирательного права необходимо выполнить ряд условий. В частности, электронная машина для голосования или интернет-сервис должны быть простыми в обращении и доступными для лиц с ограниченными возможностями. Соблюдая принцип всеобщего избирательного права, каждый электронный голос должен быть посчитан только один раз. При голосовании необходимо исключить любое влияние на принятие избирателем решения. Электронная система голосования не должна иметь возможности узнать, как проголосовал избиратель.

Поэтому внедряя электронное голосование, мы должны исходить из сущности института «тайного голосования», которая изложена в статье 8 Закона о выборах в Республике Казахстан, в котором обозначено, что «голосование на выборах ... является тайным, исключающим возможность какого бы то ни было контроля за волеизъявлением избирателей» [12].

Анализ норм действующего законодательства, а также правоприменительной практики позволяет утверждать, что тайна голосования является одной из конституционно защищаемых ценностей. Поэтому ее защита приобретает особое значение в условиях интернет-голосования, которое активно экспериментируется в мире. Подобные практики совершенно обоснованно ставят перед правом вопрос о создании новых или совершенствовании существующих механизмов защиты свободы волеизъявления граждан.

Данная проблема разными зарубежными исследователями рассматривается, но акцент в их исследованиях делается больше на шифровании данных и работе информационных систем. [13, с. 63].

Например, ряд российских ученых, оценивая влияние цифровых технологий на избирательный процесс, отмечают, что тайность голосования обеспечивается анонимизацией и блокчейн технологиями, которые не позволят открыть доступ к результатам голосования

конкретного избирателя после сохранения им заполненного бюллетеня для голосования [14, с. 45]. Однако более значимой является проблема нарушения принципа тайного голосования на этапе голосования в неконтролируемой среде, в которой может находиться избиратель в момент заполнения бюллетеня, поскольку оно привязано к определенной учетной записи гражданина в сети. Кроме того, на голосующего в момент голосования может оказываться административное давление или иной контроль. Гражданину, который голосует на избирательном участке, посредством деятельности членов участковой комиссии, наблюдателей, правоохранительных органов, кабинки для тайного голосования обеспечивается защита его избирательных прав. Отсутствие должной правовой защиты граждан на этой стадии избирательного процесса открывает возможности различного рода манипуляциям и может создать репутационный урон цифровой трансформации выборов и делигитимизировать их результаты [13, с. 63].

Критики также говорят о том, что при проведении дистанционного голосования возникает проблема с идентификацией избирателя, т.к. при наличии необходимой идентифицирующей информации через его компьютер может проголосовать посторонний человек. То есть, возникает вопрос о нарушении принципа личного голосования и свободы волеизъявления в процессе дистанционного голосования.

Международная практика показывает, что к моменту внедрения электронного голосования следует детально отрегламентировать вопрос уголовно-правовой защиты тайного голосования.

Проведенный анализ действующего законодательства позволяет выдвинуть гипотезу, что внедрение цифровых технологий в избирательный процесс приведет к трансформации моделей незаконной деятельности, а это, в свою очередь, потребует принятия адекватных мер конституционно-правовой ответственности.

Очевидно, риск административного давления или подкупа избирателя значительно упростится, что поставит под угрозу институт «тайного голосования». Отсутствие реакции со стороны права на эти угрозы способно привести к делигитимизации избирательного процесса и создать риски нарушения общественной безопасности и причинения вреда правам человека в сфере дистанционного электронного голосования. Российский ученый В.И. Федоров отмечает, что превентивную роль в недопущении негативных последствий и в защите конституционных прав граждан России может сыграть совершенствование института уголовно-правовой защиты тайного голосования [15].

Большим техническим риском дистанционного электронного голосования для нашей страны являются угрозы хакерских атак, взлома электронной системы и подделки IP-адресов. Согласно выводам Ranking.kz, в 2023 году в рейтинге стран по национальному индексу кибербезопасности (глобальный оперативный индекс, измеряющий готовность стран предотвращать киберугрозы и управлять киберинцидентами), сделанному на базе данных международной инициативы NCSI [*https://ncsi.ega.ee/*], Казахстан занял 78-е место из 176 в мире. Индекс РК составил 48,05% (максимально возможный – 100%), уровень цифрового развития населения достиг 60,18% [16].

Именно наличие серьезной угрозы взлома баз данных и внесение в них скрытых изменений является основной причиной осторожного и ограниченного внедрения онлайн-голосования в мире. В самой среде ИТ-специалистов расхожим является мнение, что нельзя доверять любой программе, автором которой ты не являешься.

Также необходима гарантия надежности электронной системы. Любая электронная система потенциально уязвима, и система электронного голосования – не исключение: сбои, недочеты, выход из строя сервисов или какое-либо потенциально неправомерное воздействие на них.

В целом, мы видим тенденцию перехода многих «традиционных» уголовных правонарушений в разряд киберпреступлений: мошенничества с платежными картами, кражи денег с банковских счетов, распространение компьютерных вирусов, онлайн-торговля наркотиками и оружием, похищение информации – и это далеко не полный перечень. К

примеру, с начала года в Республике Казахстан зарегистрировано более 18,5 тысяч мошенничеств, совершенных посредством сети Интернет [17].

При этом к наиболее характерным чертам преступности в сфере высоких информационных технологий можно отнести такие как: высокая техническая вооруженность правонарушителей; высокий уровень латентности; использование в качестве орудий правонарушения информационных телекоммуникационных технологий; электронная среда как место совершения правонарушения; трансграничность; организованный характер [18, с. 303].

Большая опасность кроется в распространении в медийном пространстве провокационного и дискредитирующего контента с использованием различных манипуляторных технологий, что подчеркивает важность обеспечения информационной безопасности граждан.

Кроме того, с распространением технологий «нейросеть» и «deepfake» существует риск вброса в медиапространство ложного видео-, аудиоконтента [19]. Поэтому нельзя не отметить здесь Информационную Доктрину Республики Казахстан, утверждённую Указом Президента Республики Казахстан от 20 марта 2023 года, в которой указывается, что новая реальность в информационной сфере и возникающие угрозы информационной безопасности требуют переосмысления подходов в проведении государственной информационной политики, изменения общей парадигмы взаимоотношений между государственными институтами и другими субъектами общественных отношений в информационной сфере.

Словом, удельный вес киберугроз растет. Эта тенденция по мере развития информационных технологий и их сходимости с технологиями искусственного интеллекта в ближайшее десятилетие, скорее всего, будет усиливаться.

В связи с чем актуальным в ближайшей перспективе являются формирование криминологических основ использования новейших информационных технологий для предотвращения преступности и качественная трансформация в работе субъектов профилактики правонарушений на основе применения высокотехнологичных подходов.

Эти технологии должны помочь в сборе, хранении, анализе криминологически значимой информации, прогнозировании преступности и противодействии процессам ее детерминации, ресоциализации потенциальных преступников.

Применение цифровизации способствовало бы созданию огромного объема информации, который может с успехом использован государством. Так, с момента появления интернета и социальных сетей стали возникать различные электронные следы, оставляемые людьми в сети. Это может быть полезным инструментом для органов правопорядка при расследовании преступлений и выявлении преступников.

На четырнадцатом конгрессе Организации Объединенных Наций по предупреждению преступности и уголовного правосудия (г. Киото, 7-12 марта 2021 г.) была принята Киотская Декларация, очерчивающая пути решения проблем в этих сферах на период до 2030 года.

В Декларации указывается на угрожающие тенденции распространения транснациональной организованной преступности. При этом преступники все чаще используют новейшие технологии для осуществления своей незаконной деятельности. Требуется усиление координации международного сотрудничества по вопросам предотвращения и противодействия киберпреступности и технологического переоснащения субъектов профилактики для повышения уровня предупредительной деятельности [20]. В этих условиях, выбирая продвижение электронного голосования в избирательном процессе, наряду с его перспективами мы должны тщательно исследовать риски и вызовы, потенциально существуюшие не только в казахстанских реалиях, но и в глобальном мире.

Литература

1. Официальный сайт Президента Республики Казахстан [Электронный ресурс]: Режим доступа:

URL: http://akorda.kz›ru/republic of Kazakhstan/president.

2. Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 16 марта 2022 года https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-1623953.

3. Федоров В.И. Электоральная культура как фактор транзита к электронному голосованию // Гражданин. Выборы. Власть. №2(16)/2020, – С. 64-76.

4. Федоров В.И., Ежов Д.А. Эволюция электронного голосования в России: проблемы классификации и периодизации // Вестник МГОУ (электронный журнал). 2021. №1., – С. 146-162. URL: www.evestnik-mgou.ru.

5. Федоров В.И. Электронное голосование: российский и зарубежный опыт, – М: НИЦ ИНФРА-М, 2023, – С. 237.

6. Recommendation CM/Rec (2017) 5 of the Committee of Ministers to member States on standards for e-voting (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies). https://search. coe.

7. Ларин И.Г. Проблема действительности выборов при проведении дистанционного электронного голосования // Юридический вестник Самарского университета. 2022. Т. 8, №1, – С. 104-109.

8. E-VotingMap «ИКТ в выборах»: https://www.idea.int/data-tools/data/icts-elections.

9. сайт РГП «ИТЦ ЦИК РК» https://www.election.gov.kz/rus/rgp/pages/ NASHI%20PROEKTI.php.

10. Сулейменов О. Перспектива электронного выбора // Казахстанская правда, 23 сентября 2010.

11. Отчет Миссии БДИПЧ/ОБСЕ по оценке потребностей 21-24 июня 2004 г. «Республика Казахстан. Парламентские выборы 19 сентября 2004 года. Варшава, 28 июня 2004 года». URL: http://www.osce.org/ru/odihr/elections/37422?download=true.

12. Конституционный закон Республики Казахстан «О выборах в Республике Казахстан». 2023, Астана.

13. Евсиков К.С., Анненков А.Ю., Братчикова Л.Р. Уголовно-правовая защита «тайного голосования» в цифровом государстве // Известия ТулГУ. Экономические и юридические науки. 2022. Вып. 3, – С. 62-76.

14. Лопатин А.И. Цифровизация избирательных действий и процедур в России: вопросы права // Журнал российского права. 2022. №5. – С. 43-55.

15. Федоров В.И. Электронное голосование: идея фикс или основа демократий будущего? // Гражданин. Выборы. Власть. №1-2/2017. – С. 170-185.

16. NCSI URL: https://ranking.kz/rankings/industries-rankings/v-reytinge-stran-po-natsionalnomu-indeksu-kiberbezopasnosti-azahstan-zanyal-78-e-mesto-iz-176.html.

17. Интернет-мошенничества вызвали широкий общественный резонанс. URL: https://profit.kz/news/64128/Internet-moshennichestva-vizvali-shirokij-obschestvennij-rezonans.

18. Бутузов В.М. «Соотношение понятий «компьютерная преступность» и «преступность в сфере высоких информационных технологий». Борьба с организованной преступностью и коррупцией (теория и практика)». 2010. Том 23. – С. 302-307.

19. «Информационная доктринаРеспублики Казахстан» утверждена Указом Президента Республики Казахстан от 20 марта 2023 года №145. URL: https://akorda.kz/ru/ob-utverzhdenii-informacionnoy-doktriny-respubliki-kazahstan-2025248.

20. Киотская декларация «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению повестки дня в области устойчивого развития на период до 2030 года». URL: https://www.unodc.org/documents/commissions/Congress/Kyoto_Declaration_booklet/21-02817_Kyoto_Declaration_ebook_R.pdf.

САРСЕНОВ САКЕН СЕЙТЖАППАРОВИЧ
Заместитель МВД Республики Казахстан по цифровизации и связи

ОСОБЕННОСТИ ОЦЕНКИ ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОВД

Современный мир невозможно представить сегодня без неотъемлемой роли продуктов цифровизации, которые стали неразрывной частью повседневной жизни. Продукты цифровизации представляют собой инновационные информационно-коммуникационные технологии, способствующие улучшению процессов в различных сферах деятельности человека. Эти технологии проникают во все аспекты современного общества, начиная с коммуникации и заканчивая управлением государственными структурами.

Один из наиболее ярких примеров внедрения цифровых технологий – это изменения в области коммуникации. В наше время общение через видеосвязь и мессенджеры стало неотъемлемой частью нашей повседневной жизни. Эти инструменты позволяют людям связываться, даже находясь на разных континентах, и обмениваться информацией в режиме реального времени. Благодаря этим технологиям, мир стал ближе, а границы перестали быть барьером для общения.

Еще одной важной сферой, в которой цифровизация оказала значительное воздействие, является электронный документооборот. Электронные документы стали заменой традиционным бумажным документам во многих организациях. Это позволяет сократить бюрократические процедуры, ускорить обмен информацией и повысить безопасность хранения документов.

Оплата покупок с помощью смартфона. Мобильные платежи стали популярными благодаря удобству и безопасности. Потребители могут совершать покупки, не прибегая к наличным деньгам или банковским картам, а используя свой смартфон. Это способствует эффективности и удобству платежных операций.

Продукты цифровизации играют важную роль в современном обществе, облегчая и улучшая множество аспектов жизни. Они становятся неотъемлемой частью нашей повседневной рутины, преображая способы коммуникации, управления информацией и осуществления финансовых операций. Президент Казахстана Касым-Жомарт Токаев также подчеркивает важность цифровизации для современного общества и поддерживает развитие технологий в Казахстане. На сегодняшний день внедрение современных цифровых технологий проводится во многих областях деятельности полиции. Так расширяется система видеонаблюдения в населенных пунктах, видеокамеры устанавливаются на дорогах и в общественных местах. Данные меры позволяют отслеживать оперативную обстановку в реальном режиме времени и автоматически выявлять нарушителей правил дорожного движения. При этом на смартфон водителю поступает сообщение о наложении штрафа, который он также оплатить онлайн посредством гаджета. Внедрение системы сплошного видеонаблюдения в помещениях полиции и учреждениях уголовно-исполнительной системы является важным шагом в обеспечении общественной безопасности и защите прав граждан. Эта мера привела к существенному снижению количества жалоб со стороны граждан и необоснованных обвинений в действиях полицейских. Системы видеонаблюдения стали неотъемлемой частью мониторинга и контроля в правоохранительных органах.

Современные технологии, включая смартфоны, играют ключевую роль в улучшении доступности государственных услуг. Граждане могут получить необходимые услуги, используя свои мобильные устройства, что способствует удобству и сокращению бюрократических процедур. Этот процесс, известный как «смартфонизация услуг органов внутренних дел» , отражает современные тенденции в развитии общества, где цифровые технологии становятся ключевым инструментом улучшения взаимодействия государства и граждан.

Однако, следует отметить, что с развитием цифровых технологий меняется и форма преступности. Киберпреступники используют интернет, социальные сети и мессенджеры для совершения различных видов преступлений, включая сбыт наркотиков и мошенничество. В ответ на эти вызовы, органы внутренних дел применяют цифровые технологии для борьбы с новыми видами преступности. Например, современные системы мониторинга и аналитики позволяют предотвращать ложные звонки и другие виды мошенничества до их поступления к гражданам.

Следует также отметить, что доступность кредитов и финансовых услуг, упрощенная благодаря цифровым технологиям, несет в себе как позитивные, так и негативные аспекты. Органы внутренних дел принимают на себя задачу защиты граждан от новых рисков, связанных с цифровыми финансовыми операциями и мошенничеством.

В заключение, процесс цифровизации в органах внутренних дел становится все более значимым и актуальным. Новые проекты и идеи способствуют улучшению общественной безопасности и обеспечению прав и интересов граждан. Цель полиции остается неизменной - обеспечение безопасности общества и цифровые технологии играют важную роль в достижении этой цели

Литература

1. Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z030000370_. Дата обращения: 11.09.2023 г.

2. Постановление Правительства Республики Казахстан от 31 октября 2018 года №703 «Об утверждении Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/P1800000703. Дата обращения: 11.09.2023 г.

3. Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года №1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/V1500012864. Дата обращения: 11.09.2023 г.

4. Приказ Министра юстиции Республики Казахстан от 27 апреля 2017 года №484 «Об утверждении Правил организации и производства судебных экспертиз и исследований в органах судебной экспертизы». [Электронный ресурс]. URL:https://adilet.zan.kz/rus/docs/V1700015180. Дата обращения: 11.09.2023 г.

5. Приказ Генерального прокурора Республики Казахстан от 3 января 2018 года №2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/V1800016268. Дата обращения: 11.09.2023 г.

САЙТБЕКОВ АЙДАР МУТАЛИКОВИЧ
Начальник Алматинской академии МВД Республики Казахстан им. М. Есбулатова
генерал-майор полиции, к.ю.н., доктор политических наук,
профессор, почётный член НАН РК

ОСОБЕННОСТИ РАЗВИТИЯ КРИМИНОЛОГИЧЕСКОЙ НАУКИ В РЕСПУБЛИКЕ КАЗАХСТАН В ЭПОХУ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

В сознании наших сограждан складывается такое мнение, что памятные даты, знаменующие основные вехи жизни выдающихся личностей (особенно тех, кого уже нет в живых), всегда оцениваются, главным образом имеющими отношение к их творческому наследию людьми, не только с позиций ценности этих трудов для современников, но, что наиболее важно, для будущих поколений. Именно этим подчеркивается историческая миссия мыслителей прошлого, пытавшихся дойти до сути предмета и оставивших потомкам богатое интеллектуальное наследство, без которого не может быть и речи о прогрессе в любой сфере деятельности.

Подтверждением сказанному является научный талант мастера уголовно-правовой и криминологической науки, *заслуженного деятеля науки и техники Республики Казахстан, академика КАЕН Республики Казахстан, доктора юридических наук, профессора Каиржанова Елегена Изтлеуовича,* 90-летний юбилей которого стал для юридической общественности замечательным поводом не только вспомнить добрым словом этого человека и ученого, но и попытаться вновь переосмыслить его научные творения, оценить значение для развития профессиональных идей и воплощения их в современную правоохранительную практику и юридическую науку настоящими и будущими специалистами.

Профессионалам в сфере юриспруденции хорошо известны труды профессора Е.И. Каиржанова, посвятившего большую часть своей карьеры ученого познанию и решению проблем общего и специального предупреждения преступлений; глубоко изучившего на основе законов диалектики философскую сущность преступления, уголовной ответственности и уголовного наказания. Елеген Изтлеуович существенно развил институт объекта преступления по уголовному праву, его научные основы; обосновал его структуру, показал методологическое значение защищаемого от преступных посягательств объекта (интересы личности, общества и государства) для построения норм Особенной части Уголовного Кодекса. Им впервые в восьмидесятых годах прошлого столетия был проведен системный социологический анализ состояния, структуры и динамики уголовных правонарушений за 1960-1980 годы, результаты которого легли в основу последующих трудов казахстанских ученых по проблемам борьбы с преступностью. Он первым в 1995 году в Казахстане подготовил учебник по криминологии для высших учебных заведений, который был переиздан в 2000 году. Более 45 лет он совмещал научную деятельность с преподавательской деятельностью в ведущих ВУЗах страны. Большое научное наследие он оставил и в уголовно-процессуальном праве, криминалистике, судебной экспертизе, экологическом праве и др.

Нет смысла выделять из этого списка какие-либо более или менее значимые для теории и практики научные достижения, они все значимы для казахстанской юридической науки и на современном этапе.

Для специалиста, ищущего пути решения проблем предупреждения преступлений, любой аналогичный научный поиск, предпринятый авторитетным ученым, каковым, вне всяких сомнений, был и остается профессор Е.И. Каиржанов, является не просто полезным, но и выступает мощным стимулом в развитии собственных мыслей и соизмерения их сути с достигнутыми научными результатами. Криминологическое осмысление в этом контексте идей профессора Е.И. Каиржанова об общем превентивном потенциале уголовного закона и перспективах их воплощения в эпоху глобального технологического развития, в пространстве третьего тысячелетия новой эры, без сомнения, послужит совершенствованию социально-правового контроля над новыми видами преступлений или другими словами – инновационной преступностью, определению места и роли в нем соответствующего инновационного уголовного закона и, соответственно, инновационных уголовно-правовых механизмов предупреждения уголовных правонарушений.

Всем моим современникам, безусловно, известны основные мегатехнологии начала третьего тысячелетия, к которым можно отности – нанотехнологии, биотехнологии, информационные технологии, когнитивные технологии, определяющие процессы трансформации традиционных общественных отношений, активно переводящие их в режим искусственного инновационно-технологического регламента, видоизменяющего, а порой нивелирующего привычные для людей формы живого человеческого общения и поведения. Возможно, все они, предшествуют надвигающемуся над разумом человечества цунами искусственного интеллекта с обеспечивающими его цифровыми ресурсами, разваливают формировавшиеся тысячелетиями человеческой истории характерные для нее системы социально-правового контроля. И именно это предопределяет необходимость соответствующей цифровой трансформации уголовно-правового ресурса, направленного на обеспечение своими средствами предупреждения общественно опасных деяний, развивающихся в новом цифровом пространстве (киберпространстве), такие как – хакерство, крякерство, кардинг, фрикинг, диффамация, спамерство, фишинг, флейминг, киберхулиганство, кибертерроризм и др.

На сегодняшнем этапе развития пересечение и слияние виртуальных (цифровых) и реальных человеческих взаимодействий сформировали новый мир, который отличается возможностью совершения любых обычных для человеческого существования действий, включая криминальные. В результате этого происходит мощная трансформация привычных для нас форм поведения из реальных в виртуальные, эффективный правовой контроль над которыми пока только формируется.

Криминально-ориентированная личность, как правило, в расширяющемся кибернетическом пространстве находит больше возможностей для преступной самореализации, чем в реальном мире, еще подконтрольном существующему порядку правоприменения. При этом, ко всем особенностям нового виртуального мира для киберпреступника добавляется, основной защитный от правоохранительного воздействия эффект, как анонимность противоправного поведения. Если оценивать данный негативный для достижения цели уголовно-правового воздействия аспект, характерный для современной киберпреступности, и, соответственно, снижающий потенциал ее предупреждения, еще раз с благодарностью возвращаешься к большому научному наследию профессора Е.И. Каиржанова и его идеям по уголовно-правовой превенции преступлений.

Здесь необходимо напомнить о безоговорочно поддерживаемом криминологами всех поколений классический правоохранительный постулат известного мыслителя XVIII века Чезаре Беккариа о том, что не в суровости уголовного наказания заключается удерживающий человека от совершения преступления эффект, а в его неотвратимости.

Глубоко анализируя факторы, требующие уголовно-правовой оценки субъективного восприятия возможной для преступника перспективы уголовной ответственности, профессор Е.И. Каиржанов отмечал о дифференцированном подходе в развитии системы общей и специальной профилактики и необходимости соотносительности применения уголовно-

правовых средств общего предупреждения к специфичности объекта такого воздействия – личности преступника. Соглашаясь с этими научными выводами, следует обозначить специфику субъективных особенностей, присущих личности киберпреступника, криминологическая характеристика которой пока в силу своей анонимности представляется весьма малозначительной для формирования дифференцированной общей превенции, не говоря об индивидуальной превенции уголовно-правовыми средствами. И здесь необходимо отметить, что именно малозначительность криминологической информации является самым сильным стимулом для ее активного научного познания и исследования для выработки эффективного уголовно-правового предупредительного потенциала действующего законодательства.

Как известно, специалистами в области правоохранительной деятельности, а также исследователями в сфере уголовно-правовой науки и криминологии вполне обоснованно рассматривают обеспечение информационной безопасности в кибернетическом пространстве от различных криминальных посягательств, в качестве важного и перспективного уголовно-политического приоритета. Важно заметить, что при этом акцентируется внимание на необходимости трансформации основных признаков преступлений, приобретающих в киберпространстве соответствующие инновационно-технологические форматы, не изменяющие, в целом, традиционной содержательной стороны таких уголовно-наказуемых деяний. Другими словами, киберпреступление в значительной части сохраняет в себе привычные для человека стандарты его традиционных изъянов, облаченных в преступные мотивационные стимулы удовлетворения своих преступных (паразитических) потребностей, таких как алчность – воровство, жестокость – насилие, хитроумность – обман, извращенность – сексуальная распущенность, гедонизм – алкоголизация, наркотизация и др. Цифровой ресурс здесь выступает для личности преступника более приемлемым, надежным и безопасным средством достижения криминального результата.

Действующее уголовное законодательство, направленное на традиционные форматы общественно опасных деяний не в полной мере достигает свое назначение и воздействие своим «аналоговым» ресурсом до цифрового (кибер) преступления и тем более киберпреступника. И возможно, вносимые изменения и дополнения в Уголовный кодекс Республики Казахстан, направленные на форматирование в этом своем качестве новые цифровые образы уголовно-наказуемых деяний, не всегда достигают ожидаемой эффективности.

В связи с этим, на наш взгляд, одним из эффективных способов достижения целей уголовного закона в условиях глобальной цифровизации общественных отношений, в том числе, цифровизации преступности, должна стать цифровизация уголовного законодательства, то есть внедрение источников уголовного права в информационно-коммуникационное пространство виртуального мира. Предлагаемая нами уголовно-правовая инновация не будет иметь ничего общего с беспрерывными изменениями уголовного законодательства, критика которых уже стала обычным делом в юридическом сообществе. Здесь мы разделяем мнением некоторых ученых, что частые перемены в уголовном законодательстве, «производимые даже в самых благих намерениях, способны принести больше вреда, чем пользы» [1, с. 121].

Предлагаемый новый информационно-технологический концепт модернизации уголовно-правового ресурса, превентивно нацеленного на киберпреступность, должен, на наш взгляд, включать в себя модернизацию под цифровые стандарты существующих уголовно-правовых форм воздействия на преступность, оставляя в них большей частью классическое уголовно-правовое и криминологическое содержание, адаптированное к уже существующей цифровой реальности. По нашему мнению, наличие осуществляемого в мониторинговом режиме цифрового уголовно-правового контроля над преступностью, включенного в общую систему обеспечения кибербезопасности государства, способна, не только максимально фиксировать уголовные правонарушения, совершаемые в киберпространстве, но, и

одновременно создавать информационную базу для формирования инновационно-технологической системы криминологической кибербезопасности, а вместе с ней и системы инновационно-технологического правосудия. Это можно рассматривать и как одно из важных направлений развития цифровой экосистемы Казахстана.

Наряду с цифровым уголовно-правовым ресурсом, формирование общей инновационно-технологической системы криминологической кибербезопасности должно сопровождаться собственно криминологическими и информационно-коммуникационными технологиями. В комплексе объединения всех этих ресурсов и заложен основной превентивный потенциал криминологической кибербезопасности. Безусловно, его реализация будет способна не только фиксировать совершаемые в кибернетическом (виртуальном) пространстве уголовно наказуемые деяния, но и предупреждать возникающие в нем криминальные риски и минимизировать возможные социально негативные последствия развития каких-либо виртуальных правоотношений, т.е. способствовать укреплению самостоятельного превентивного потенциала и, тем самым, будет достигаться в новых условиях глобальной информатизации общая антикриминогенная превенция.

Литература

1. Марцев А.И., Максимов С.В. Общее предупреждение преступлений и его эффективность. Монография. – Томск: Издательство Томского университета, 1989. – С. 160.

КАНАТБЕК АЗИЗ
Директор Национального института стратегических исследований
при Президенте Кыргызской Республики, член-корреспондент
Национальной академии наук Кыргызской Республики, профессор

ОСНОВНЫЕ МОДЕЛИ РАЗВИТИЯ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Развитие информационного пространства является важной, доминирующей особенностью в состоянии современного общества в рамках глобального экономического развития. Катализатором развития данного процесса является переход существующих ранее моделей социального устройства и развитие общественных отношений к новой модели информационного общества. Основным субъектом данной модели общественных отношений, безусловно, выступают средства массовой информации, которые на сегодняшний день способны направить создание общественных масс в ту или иную сторону. Особую актуальность в данном аспекте, безусловно, представляют формирование грамотной и эффективной информационной политики, которой со стороны государства должен быть обозначен вектор развития информационного общества. В этом смысле сегмент информационного общества образуется за счет информационной политики, которая является своего рода регулятором большинства сфер жизнедеятельности человека. При помощи грамотной и продуманной информационной политики можно направить инициативу и стремление человека как общественного индивида в ту или иную сторону. И практика на самом деле это показы. Стоит заметить, что изучение большого количества аналитических исследований, научных трудов дает нам возможность выстроить следующий вывод, что по своей сути политика государства в информационном пространстве представляет собой некий набор средств и приемов управления информационными потоками со стороны органов государственной власти в процессе доведения их до общественного создания. В процессе исследования и раскрытия сущности данного вопроса можно отметить, что существует ряд основных черт, характеризующих информационную политику, которые состоят в следующем. Первое. На современном этапе общественной жизни все больше возрастает роль информационной политики как средства формирования общественного мнения на то или иное явление. В рамках использования информационной политики существуют две основные приоритетные сферы, к которым можно отнести государственную и общественную. Следует заметить, что современные информационно-коммуникационные технологии постепенно стирают различия между разными секторами информационной индустрии. На постсоветском пространстве стоит заметить, пока еще нет единой точки зрения на содержание государственной информационной политики и на ее роль как важной комплексной задачи государственного управления. Отношение к информационной политике в решающем мере зависит от того, какие конкретные вопросы находятся в сфере личной компетенции профессиональных и политических интересов того или иного государственного деятеля, политика или специалиста. Учитывая, что информация является основным источником энергии для развития общества и государства на сегодняшний день, а информационные

процессы являются важной составляющей частью всех внутриполитических и внешнеполитических процессов жизнедеятельности страны, государственную информационную политику следует рассматривать как совокупность целей, отражающих национальные интересы в информационной сфере, стратегии и тактики управленческих решений и методов их реализации, разрабатываемых и реализуемых государством власти для регламентирования и совершенствования как непосредственно процессов отношений и взаимоотношений во всех сферах жизнедеятельности общества и государства, так и процессов в широком смысле технологического обеспечения такого взаимодействия. Долгосрочной стратегической государственной информационной политике должно стать формирование открытого информационного общества, что с учетом глобальных тенденций развития мирового общества является необходимым для ее социального, культурного и политического развития. Информационное пространство, государство, в котором протекают процессы информационного взаимодействия, а именно информационные процессы, представляет, на мой взгляд, прежде всего, совокупность пересекающихся информационных сфер гражданского общества, государственной власти, ну и само собой местного самоуправления. Исходя из подобной объектной структуры информационного пространства в качестве обобщенных объектов регламентирования информационной политики как инструмента государственного управления, на наш взгляд, нужно выделить следующее. Первое, это, безусловно, информационная сфера гражданского общества, информационная сфера власти, состоящая из информационной сферы государственной власти и вложенные в нее сферы местного самоуправления. Ну и, наконец-то, это область пересечения информационных сфер гражданского общества, государственной власти и местного самоуправления. Мы считаем, что для того, чтобы общество и государство развивалось без социальных взрывов и потрясений, необходимо, чтобы общество адекватно реагировало на прямые регулирующие воздействия власти и спокойно адаптировалось к условиям и правилам развития, определяемыми этими воздействиями. Для формирования соответствующего морально-психологического, нравственного и эмоционального состояния общества вся система органов власти должна постепенно осуществлять дополнительное информационное взаимодействие с обществом, публично разъясняя, к примеру, решения и действия. А общество, его институциональные структуры и отдельные граждане должны иметь возможность открыто выражать власти свое коллективное и личное отношение к ее решениям и действиям. Стоит заметить, что подобную адаптацию к модели государства, как система регулирования с обратной связью, в которой общество является объектом регулирования, а система органам власти, управляющим устройством, должна обеспечить специальный контур регулирования, который можно назвать контуром адаптации. Контур адаптации образуется обобщенным каналом передачи дополнительных, адаптирующих воздействий власти на обществе в форме специально подготовленной и публично распространяемой самой власти информации, объясняющей общие цели и задачи, стратегию и тактику ее деятельности, отношение к текущим внутриполитическим и внешнеполитическим событиям с определенным упреждением, разъясняющий смысл и направленность ее конкретных решений и действий. С другой стороны, обобщенным каналом реагирования общества на решения и действия сферы в форме потока информации, отражающей отношение общества, ее структур и граждан к текущим событиям, включая публично выражаемое через средства массовой информации, общественного мнения, а также коллективные и частные заявления и обращения самих граждан. Заключая свой доклад по обозначенной тематике, я буквально коротко остановлюсь. У компетенции государственной власти, а именно то, что в компетенции государственной власти, как субъекта государственной информационной политики, входит определение ее сути, стратегии, тактики проведения, формирования и развития информационного законодательства как главного инструмента ее реализации. Но вместе с тем, как отмечалось уже ранее, роль государственной власти в проведении информационной политики определяется и другими существенными факторами. Во-первых, информационная сфера

государственной власти входит в важное составное участие в информационное пространство страны, а информационное обеспечение ее деятельности в совокупности с местным самоуправлением является одной из функциональных задач государственной информационной политики. То есть, по-другому говоря, не может быть, что политика государственной информационной сферы должна быть различной от политики, реализуемой в органах местного самоуправления. Иными словами, государственная власть – это, по сути, не только субъект, но и один из основных объектов государственного управления в рамках проводимой информационной политики. Во-вторых, такой принцип демократии, как государство для общества, а не общество для государства, можно реализовать лишь при условии, когда деятельность власти и ее органов и институтов информационно открыта, а приоритеты направлены на предоставление услуг населению, в первую очередь информационных услуг. Это требует, нужно отметить, соответствующей организации информационного обеспечения и деятельности. Следующее. Государственная власть – это наиболее крупный и обеспеченный ресурсами потребитель и заказчик на рынке информационной продукции и услуг, от поведения которого на этом рынке во многом зависит его состояние и перспективы. Таким образом, в силу объективных обстоятельств, государственная власть призвана играть ведущую роль не только в формировании, но и в практической реализации государственной информационной политики как многофункциональной комплексной задачи государственного управления. Учитывая тот факт, что информационная политика затрагивает интересы как всеобщества, его институциональных структур и отдельных граждан, так и различных ветвей уровней отдельных органов власти, влияет на все аспекты ежедневительности внутренней, внешнюю политику государства. Проведение государственной информационной политики, начиная с разработки концепции организации контроля за ее реализацией, должно находиться в видении, непосредственно главы государства, то есть Президентского института, в соответствии с возложными на него основным законом Конституции той или иной страны.

Литература

1. Oxford English Dictionary. URL: http:/ /www. askoxford.com.

2. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: Дис. … канд. юрид. наук. Краснодар, 2009 //[Электронный ресурс] – Режим доступа: https://www.dissercat.com/content/ispolzovanie-spetsialnykh-poznanii-pri- vyyavlenii-i-rassledovanii-prestuplenii-v-sfere-kompy. Document (дата обращения: 12.08.2023).

3. Конвенция о киберпреступлениях принята Советом Европы. Серии европейских договоров. – №185 от 23.10.2001. / [Электронный ресурс] – Режим доступа: https://rm.coe.int/1680081580 (дата обращения: 29.08.2023).

4. Каиржанов Е. Криминология (Общая часть): Учебн. Для юрид. вузов: изд. 2 перераб. и доп. – Алматы: «Оркениет», 2000. – С. 288.

BIMOLDANOV Y.M.,
Deputy Head of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov, candidate of law, associate professor, police colonel

ON THE GROUNDS OF CRIMINAL LIABILITY FOR THE CREATION, USE OR DISTRIBUTION OF MALICIOUS COMPUTER PROGRAMS AND SOFTWARE PRODUCTS

The introduction of a separate chapter «Criminal offenses in the field of informatization and communications» in the Special Part of the Criminal Code of the Republic of Kazakhstan adopted on July 03, 2014, is the necessity that our present requires. The social danger of the criminal offenses considered in this chapter consists, first of all, in that they violate the rights and legitimate interests of citizens and organizations, the interests of society and the state protected by law in the information sphere, damage the confidentiality, integrity, safety and accessibility of information resources, information communication systems and infrastructure.

The twenty-first century is rightly called the century of information technology, almost all spheres of human social activity are somehow related to computerization, and this in turn creates social relations in which certain guaranteed rights and freedoms must also be protected through legislation in accordance with the Constitution of the Republic of Kazakhstan [1] .

According to the disposition of Part 1 of Article 210 of the Criminal Code of the Republic of Kazakhstan, the creation of a computer program, software product or amending an existing program or software product for the purpose of unlawful destruction, blocking, modification, copying, use of information stored on an electronic medium contained in an information system or transmitted information and communication network, malfunctions of a computer, subscriber device, computer program, information system of a system or information and communication network, as well as the deliberate use and / or distribution of such a program or software product – shall be punishable by a fine of up to three thousand monthly calculation indices, or by correctional labor in the same amount, or by restriction of liberty for a term of up to three years, or deprivation of liberty for the same period, with deprivation of the right to occupy certain positions or engage in certain activities for a term of up to three years or without it [2].

Malware refers to programs specifically designed to interfere with the normal functioning of computer programs.

That is, these are various kinds of programs specially created for computers, the purpose of which is to disrupt the normal functioning of computer programs in accordance with their documentation in order to achieve the criminal results specified in the law – knowingly leading to unlawful destruction, blocking, modification, copying, use of information stored on a machine medium contained in an information system or transmitted over an information and communication network, computer malfunction, subscriber device, computer program, information system or information and communication network (computer viruses, scanners, patchers, information management, emulators of electronic security equipment, etc.).

If the operation of the malicious program was a condition for a person to commit another criminal offense, the acts must be qualified in the aggregate, regardless of the severity of the other criminal offense.

Currently, the most common are programs designed to collect information, and programs for unauthorized access to computers or other programs.

«Computer viruses» are programs that can reproduce themselves in several copies, modify (change) the program to which they joined, and thereby disrupt its normal functioning.

«Logical bombs» is a deliberate change in the program code, partially or completely incapacitating a program or computer system under predetermined conditions, for example, a certain time.

The fundamental difference between «logical bombs» and «computer viruses» is that they are initially part of the program and do not go to other programs, and «computer viruses» are dynamic programs and can even spread over computer networks.

On the objective side, this criminal offense constitutes the fact of creating computer programs or making changes to existing programs that obviously lead to unauthorized destruction, blocking, modification, copying, use of information stored on electronic media contained in the information system or transmitted through the information and communication network, disruption of the computer, subscriber device, computer program, information system or information and communication network, as well as the intentional use and (or) distribution of such a program or software product [3].

Under the use of the program refers to the publication, reproduction, distribution and other actions for their introduction into circulation. Use can be carried out by recording the program in the memory of a computer, on a tangible medium, distribution through networks or by other transfer to other persons.

This structure is formal and does not require any consequences, criminal liability arises as a result of the creation of the program, regardless of whether the program was used or not. Within the meaning of the commented article, the presence of the source code of the virus programs is already the basis for bringing to justice. However, it should be borne in mind that in some cases the use of such programs will not be criminally punishable. This applies to the activities of organizations engaged in the development of antivirus programs and licensed to protect information.

The form of committing this crime can only be an action expressed in the form of creating malware for computers, making changes to existing programs, as well as intentional use and / or distribution of such a program or software product. The distribution of electronic media with such programs or software product is fully covered by the term «use».

On the subjective side, a criminal offense under Part 1 of Article 210 of the Criminal Code of the Republic of Kazakhstan can only be committed with direct intent, since this article determines that the creation of malicious programs, knowingly for the creator of the program, should lead to unlawful destruction, blocking of modifications, copying, the use of information stored on electronic media contained in the information system or transmitted over the information and communication network, disruption of the computer, the subscriber's building, computer program, information system or information and communication network. The use or distribution of malware or a software product can also be carried out only intentionally [4].

Part 2 of Article 210 of the Criminal Code of the Republic of Kazakhstan as a qualifying attribute provides for the commission of a criminal offense:

1) by a group of persons by prior conspiracy;

2) using his official position;

3) in relation to national electronic information resources or the national information system.

Part 3 of Article 210 of the Criminal Code of the Republic of Kazakhstan has particularly qualifying features:

1) commission by a criminal group;

2) entailing grave consequences.

The subject of this criminal offense may be a natural sane person who has reached 16 years of age, a special subject is provided for in paragraph 2 of part 2 of article 210 of the Criminal Code of the Republic of Kazakhstan.

In conclusion, it should be noted that in the case of creating a computer program, software product or making changes to an existing program or software product for the purpose of unlawful destruction, blocking, modification, copying, use of information stored on an electronic medium contained in an information system or transmitted via information and communication network, malfunctions of a computer, subscriber device, computer program, information system or information and communication network, as well as the intentional use and / or distribution of such a program or software product was a condition for a person to commit another criminal offense, the acts must be qualified in combination, regardless of the severity of another crime.

References

1. The Constitution of the Republic of Kazakhstan // https://www.akorda.kz/en/official_documents/constitution

2. Уголовный кодекс Республики Казахстан: Практическое пособие. – Алматы: «Издательство «Норма-К», 2015. – С. 240.

3. Бимолданов Е.М., Цой А.Н., Цой О.Р. и др. Уголовные правонарушения в сфере информатизации и связи: Учебное пособие. – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан, 2015. – С. 194.

4. Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (том 2). – Алматы: Жеты жарғы, 2015. – С. 1120.

ШЕСТАКОВ ДМИТРИЙ АНАТОЛЬЕВИЧ
Президент Санкт-Петербургского международного криминологического клуба
Заслуженный деятель науки РФ д.ю.н., профессор, заведующий криминологической лабораторией РГПУ им. А.И. Герцена

«ОЦИФРОВКА» УГОЛОВНОГО ПРАВА В СВЕТЕ БЕЗОПАСНОСТИ

Проблемное поле между компьютерными технологиями, преступностью, уголовным правом, а также законодательством о безопасности. В научной школе преступных подсистем традиционно уделяется внимание разработке проблем безопасности. В разработку этих проблем на площадке Санкт-Петербургского международного криминологического клуба значительный вклад внесён У. Зибером (ФРГ) и Н.В. Щедриным (Российская Федерация). [1; 2; 3. с. 26-35]. Законодательство о безопасности, в том числе международное, в последние два десятилетие множится. Переход от юридического осмысления норм безопасности к *постановке вопроса о праве безопасности* связан с именем немецкого преступностиведа Ханса-Йорга Альбрехта[1]. [4]. В клубе обсуждение преступностиведческой проблемы безопасности, в частности в связке с компьютерной преступностью и компьютерным противодействием ей, ведёт отсчёт времени во всяком случае уже с опубликования в 2009 году в нашем журнале статьи Ульриха Зибера[2] и состоявшейся 3 июня 2010 года беседы с ним. Его доклад назывался «Свобода против безопасности в борьбе с терроризмом и организованной преступностью – международное развитие и германская уголовная политика». Зибер сыграл значимую роль в критическом осмыслении искусственного нагнетания страхов перед преувеличенными угрозами в целях протаскивания чрезвычайных, порой преступных мер безопасности под знаменем «войны с терроризмом».

Зибер полагает, что «развитие информационного общества, рискованного общества… ведёт уголовное право – особенно в контексте нарастающей глобальной уголовной политики – к функциональной границе… и ставит его перед новыми категориальными вызовами». По его мнению, право безопасности требует самоопределения, ибо оно не может вместиться в классические правовые отрасли уголовного, полицейского, военного законодательства. [1. с. 36]. Зибером многое сделано для продвижения компьютерной проблематики применительно к уголовно-правовой области.

Вместе с тем наступление законодательного регулирования «безопасности» на уголовное право, проникновение подходов «безопасности» в уголовное и уголовно-процессуальное законодательство послужило одним из подтверждений своевременности того, что в невско-волжской преступностиведческой школе – в пределах криминологии закона – было введено понятие преступного закона.

Итак, внимание клуба давно привлекает к себе проблемное поле между: 1) уголовным правом; 2) «правом безопасности»; 3) компьютерными технологиями преступной деятельности; и 4) компьютерными технологиями противодействия преступности. Теперь, спустя годы, значение преступностиведческого осмысления данного поля наконец-то

1 Ханс-Йорг Альбрехт – почётный профессор Санкт-Петербургского международного криминологического клуба, экс-директор Института международного и зарубежного уголовного права им. М. Планка, неоднократно выступавший с докладами на беседах клуба.
2 Ульрих Зибер – почётный профессор Санкт-Петербургского международного криминологического клуба, экс-директор Института международного и зарубежного уголовного права им. М. Планка.

начинает пониматься широким кругом специалистов, о чём свидетельствуют публикации и возникающие в России научные подразделения (кафедры вузов, секторы научных учреждений), которые нацелены на освоение вопросов безопасности. Проблематике пределов безопасности в 2017 году в очередной раз было уделено внимание на выездной российско-германской беседе клуба, проведённой на этот раз в Университете им. И. Канта (Калининград). [5. с. 154-162].

С.Я. Лебедев высказывается о необходимости систематизации научного знания о «технологических инновациях преступности и её предупреждения», а также о возникшей потребности в новой отрасли преступностиведения, а именно киберкриминологии. [6. с. 72-73]. Особо следует отметить вклад Х.Д. Аликперова в разработку двух аспектов этой отрасли: во-первых, дистанционный контроль над преступностью посредством чипирования [7. с. 26-33], во-вторых, использование искусственного разума при назначении уголовного наказания.

Шаг в нужном направлении. Как и другие специалисты, занятые вопросами электронной системы определения меры наказания, Лебедев констатирует, что «в условиях глобальной цифровизации речь должна идти об адекватном глобальном и всеобщем правовом технологическом переустройстве системы управления новыми цифровыми социально-правовыми отношениями, в котором уголовно-правовые, криминологические, криминалистические и уголовно-процессуальные инновации должны получить собственное оформление и развитие». Он замечает нарастающее стремление системы правоохранительного контроля к цифровому формату.

Во внедрении информационных технологий в развитие уголовного закона и уголовно-процессуальных практик в современном цифровизированном (оцифрованном?) мире Лебедев усматривает «единственно верную идеологическую, а вместе с ней и информационно-технологическую направленность… обеспечения безопасности личности, общества и государства уголовно-правовыми и криминологическими средствами». При этом остаётся пока интригующей загадкой, какие именно он имеет в виду технологии, помимо представленной Аликперовым в Санкт-Петербургском международном криминологическом клубе электронной матрицы назначения уголовного наказания.

Теперь от науки о преступности ожидается теоретически *увязать уголовно-правовую киберреакцию на преступность с проблемой безопасности*. Российские преступностиведы только-только приближаются к осознанию значимого для нынешнего времени столкновения законодательных норм о «безопасности» с классическим уголовным правом.

Как пишет Йорг Арнольд (Германия), новый импульс дебатам о безопасности дали воздушные нападения террористов 11 сентября 2001 года в Нью-Йорке и Вашингтоне. «С этого времени понятия безопасность и терроризм конкурируют между собой по частоте их использования. Следует признать, – замечает Арнольд, – что отрицать террористическую угрозу… нельзя. Но нельзя и закрывать глаза на то, что она играет роль троянского коня в демонтаже правового государства, причём в общеевропейском измерении». [8. с. 22].

Прикасаясь к проблеме «безопасности» в связи с надвигающимся «цифровым» управлением обществом – в том числе управлением посредством «кибернизации» уголовного права, – нельзя ограничиваться восприятием лишь положительной стороны законодательства безопасности. Долг преступностиведа видеть также отрицательную, в частности криминогенную, сторону этой нормативной отрасли, связанную с ограничением прав человека, нельзя проходить мимо некоторых даже преступных её правил. Следует непрестанно задаваться вопросом: не ведёт ли «оцифровка» уголовного закона и его применения к совершению преступлений и появлению новых видов преступлений? В особенности на глубинных уровнях преступности. Взаимосвязь преступного и противопреступного – вот предмет особого внимания криминолога. При этом нельзя в преступлении просмотреть его *противопреступный* компонент (такое тоже наблюдается… даже в чудовищном преступлении 11 сентября!), а в мере противодействия преступности непростительно было бы не заметить возможную *преступную* составляющую такой меры.

Оцифровка уголовного законодательства и политическая криминология. В 10-е годы текущего столетия важнейшим направлением политической криминологии становится

исследование преступной деятельности той силы, которую в политической криминологии именуют *глобальной олигархической властью (ГОВ)*. Глобальная олигархическая преступность – вот ключевая криминологическая проблема XXI века. [См.: 9. с. 94].

Ещё раз вернёмся к знаковым событиям 11 сентября. Существует мнение, что предпринятые тогда воздушные атаки были искусно проведённой провокацией того, чтобы приблизить установление единого мирового порядка, ограничив для этого права человека. [10]. Так или иначе, в этот трагический день преступники нанесёнными ими ударами целенаправленно или невольно обозначили корень зла, корень глобально организованной преступности. Точнее сказать, было указано направление, в котором уходит корень.

Первые жертвенные самолёты вместе с обречёнными людьми (пассажирами, пилотами, стюардессами и захватившими воздушные суда террористами-самоубийцами) были брошены на Всемирный торговый центр, устроенный в нью-йоркских башнях-близнецах. Это символ не США, а ГОВ (глобальной олигархической власти). Второй удар был нанесён в столице Соединённых Штатов Вашингтоне по Пентагону, символу военщины страны, являющейся проводником воли ГОВ. Готовился ещё третий удар, предположительно по представительной и исполнительной властям США, а именно по Капитолию и Белому дому. Это лишь внешнегосударственный уровень мировой преступности. Основополагающий её уровень – глобальная олигархическая власть.

Сама ГОВ не имеет почтового адреса. Её законспирированность, отсутствие официального статуса, неопределённость и до времени неопределяемость способствуют её неуловимости и безнаказанности. Как Лебедев сопоставил компьютерные технологии уголовного права – этого важного компонента противодействия преступности – с безопасностью, так политической криминологии *безопасность от ГОВ следует связать с «цифровизацией» преступности и противодействия ей*.

Нельзя сказать, что мир не сопротивляется стремлению ГОВ к управлению им посредством информационных технологий. Во всяком случае, Китай уже преуспевает в этом противостоянии. Как отмечает цитируемый Е. Лариной и В. Овчинским австралийский аналитик Саманта Хоффман, Китай не ограничивается оборонительной стратегией превращения страны в высокотехнологичное общество, а стремится преобразовать сначала ближайших соседей, потом ту или иную сферу влияния, и в завершение весь мир по китайским лекалам высокотехнологичного управления, причём на базе традиционных конфуцианских ценностей. Такая глобальная деятельность, обеспеченная технологически, финансово, а также производством серверов, компьютеров, гаджетов, закреплена в решениях партийного и государственного руководства КНР. [См.: 11].

Именно Китай стал той силой, которая может противостоять и уже противостоит глобальной олигархической преступности. Но в этом есть и новая угроза, заслуживающая пристального внимания со стороны политического преступностиведения. Я говорю об угрозе возникновения нового, теперь восточного кратера преступности. Во всяком случае, необходимы дополнения «права безопасности» суверенных государств. Нужны криминологические доводы для обеспечения безопасности производства всего IT-оборудования и IT-технологий.

Защита цифрового суверенитета. В поле зрения политического преступностиведения должна находиться осуществляемая из-за рубежа через Интернет преступная деятельность в области политики. Необходимо отслеживать как факты, так и риски. Понятно, что речь идёт о подготовке и совершении преступлений против общественной безопасности – преступлений террористической направленности и других, а также преступлений против основ конституционного строя и безопасности государства, таких как государственная измена, шпионаж, публичные призывы к осуществлению экстремистской деятельности и др.

Надо иметь в виду также «вмешательство во внутреннюю политику суверенного государства». Это преступление в криминологическом смысле, т. е. общественно опасное деяние, за которое пока специально не установлена уголовная ответственность, хотя мною предложено соответствующий состав ввести в законодательство.

Возникновению и развитию виртуального информационного пространства сопутствовало появление проблем кибератак, кибероружия, боевых действий –

«опосредованных», «гибридных» и совершаемых в так называемой серой зоне. Эти не до конца прояснённые понятия употребляются и военным руководством США. Оцифровка и автоматизация управления вооружением, в том числе ядерным, возможность технического сбоя порождают опасность непреднамеренной войны.

Новым направлением государственно-правовых и, конечно, политкриминологических исследований становится так называемый цифровой суверенитет или, иными словами, национальный суверенитет в киберпространстве. [См.: 12. с. 173]. Именно в связи с этим правовым явлением государственного суверенитета в информационной реальности Россия не присоединяется к Будапештской конвенции Совета Европы «О преступности в сфере компьютерной информации» (ETS N 185). Страну не устраивает в названной конвенции пункт «b» статьи 32 о «трансграничном доступе». Этим пунктом, хотя и с туманными оговорками, допускается возможность спецслужбам одних стран проникать в компьютерные сети стран других и проводить там операции без ведома национальных властей.

Со своей стороны, Россия в 2011 году предложила альтернативный проект конвенции – на этот раз Конвенции ООН – «Об обеспечении международной информационной безопасности». В данный проект заложено обеспечение защиты от действий в информационном пространстве, совершаемых с целью подрыва политической, экономической и социальной систем другого государства, психологической обработки населения, дестабилизирующей общество. [См.: 13. с. 176.]. В проекте сказано: «Каждое государство-участник вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную структуру, расположенную на территории государства-участника или иным образом находящую под его юрисдикцией». [См.: 14. с. 1].

В связи с обострившимся вопросом об охране национального суверенитета в Интернете настала пора (события прямо-таки бегут!) *развить* моё *предложение* об *уголовной ответственности за «вмешательство во внутреннюю политику суверенного государства»*. Как поступить лучше? Ввести ли через запятую конститутивный признак основного состава, сформулировав его так: *«в том числе с использованием электронно-информационного пространства*»? Или учредить соответствующий квалифицированный состав?

Литература

1. Зибер У. Границы уголовного права. Основные положения и призывы новой исследовательской уголовно-правовой программы Института зарубежного и международного уголовного права им. М. Планка / пер. с нем. Д.А. Шестакова // Криминология: вчера, сегодня, завтра. 2009. №1 (16).
2. Н.В. Щедрин Введение в правовую теорию мер безопасности. Красноярск: Изд-во Краснояр. гос. ун-та, 1999.
3. Н.В. Щедрин Концептуально-теоретические основы правового регулирования и применения мер безопасности // Криминология: вчера, сегодня, завтра. 2013. №4 (31).
4. Albrecht H.-J. Kriminalitätsumfang, Opferrisiken und Kriminalitätsfurcht in der Shweiz // Kunz K.-L., Moser R. (Hrsg). Innere Sicherheit und Lenesängste. Bern, Stuttgart, Wien: Haupt, 1997.
5. Arnold J., Shestakov D. Verletzung der staatlichen Souveränität als kriminologisches und strafrechtliches Problem. Ein Kongressbericht // Monatsschrift für Kriminologie und Strafrechtsreform. 2019. Vol. 102. Iss. 2.
6. Д.А. Шестаков, С.У Дикаев., А.П Данилов. Летопись Санкт-Петербургского международного клуба. Год 2014 // Криминология: вчера, сегодня, завтра. 2015. №1 (36).
7. Х.Д. Аликперов. Глобальный дистанционный контроль над преступностью: допустимость, возможности, издержки // Криминология: вчера, сегодня, завтра. 2016. №4 (42).
8. Й.К. Арнольд соотношению (уголовного) права, безопасности и свободы ввиду трансформаций безопасности, понятия «лицо, представляющее угрозу», а также судебной практики Федерального Конституционного Суда, имеющей отношение к понятию «свобода» // Криминология: вчера, сегодня, завтра. 2018. №3 (50).
9. А.П. Данилов. Криминология: Россия и мир. СПб., 2018.
10. Л. Ивашов 11 сентября – это глобальная провокация // www.fondsk.ru/articl (дата обращения: 19.11.2019).

ДОКТОР МАРИУС ЛАУРИНАЙТИС
Профессор юридического факультета Центра правовых технологий (LegalTech) Университета Миколаса Ромериса, Вильнюс (Литва), доктор социальных наук, ИТ-право, PhD

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ: ПРЕДПОССЫЛКИ, ТЕНДЕНЦИИ, ПРЕСПЕКТИВЫ

Неоспоримо, что в нашем быстро изменяющемся мире прогнозирование становится сложной задачей, особенно в свете быстрого развития технологий. Тем не менее, мы можем попытаться выделить ключевые аспекты, которые могут определить будущее в этой области.

Первым важным аспектом является изменение технологической парадигмы. Мы наблюдаем постоянное развитие информационных технологий, и это создает новые возможности для киберпреступников. Производители технологий также активно работают над разработкой новых продуктов и сервисов, что открывает двери для как потенциальных киберпреступников, так и специалистов по кибербезопасности.

Вторым важным аспектом является скорость внедрения этих технологий в нашу повседневную жизнь. Технологии используются в государственных учреждениях, корпорациях и даже обычными гражданами. Это расширяет атакованный цифровой ландшафт и создает новые уязвимости. Угрозы в этой области не только потенциальные, они уже сегодня актуальны и реальны.

Следующим важным аспектом является необходимость анализа и оценки существующего правового регулирования. Структуры и нормативы, разработанные для традиционных видов преступности, могут быть недостаточными для борьбы с киберпреступностью. Важно понять, нужно ли нам разрабатывать новые юридические нормы, специфически ориентированные на киберпреступность, или следует адаптировать существующее законодательство к новым вызовам. Это критически важно, чтобы обеспечить эффективное пресечение и наказание киберпреступников.

Будущее находится в процессе развития, и эти процессы уже сегодня затрагивают множество сфер, от правоохранительных органов до научного сообщества. Нашей задачей является идентификация угроз, а также разработка эффективных стратегий для их пресечения и управления. Мы должны внимательно анализировать технологические изменения, строить эффективные правовые механизмы и сотрудничать для обеспечения кибербезопасности в нашем быстро меняющемся мире.

В 2024 году кибератаки приобретут ключевое значение в сфере безопасности и угроз, исходящих из киберпространства. Это следствие не только постоянной эволюции технологий, но и изменяющегося характера преступности в целом. Географические границы становятся несущественными в цифровом пространстве, что создает особые вызовы и возможности.

Анонимность играет критическую роль в эффективности киберпреступности. Хотя полная анонимность в интернете не существует, она все же обеспечивает преступникам значительное преимущество. Они могут действовать издалека, избегая физического риска, и таким образом, они остаются вне правового поля.

Значительным аспектом будущих атак будет изменение вектора атаки. Киберпреступники будут совершать более сложные и утонченные атаки, направленные не только на финансовую выгоду или хактивизм, но и на национальную и корпоративную

безопасность. Государства также активно включаются в киберпространство, стремясь контролировать информацию и даже нарушать работу критической инфраструктуры.

Важно подчеркнуть, что сфера права и регулирования не успевает за быстрыми изменениями в киберпространстве. Нормативные каркасы разработаны для традиционных видов преступности и не всегда применимы к киберпреступности. Это поднимает важные вопросы о необходимости создания новых юридических норм и механизмов для борьбы с новыми вызовами.

Национальная безопасность становится приоритетом для каждого государства, и стратегии кибербезопасности становятся важными документами в политике безопасности. Научное и практическое сообщество должны активно сотрудничать, чтобы идентифицировать угрозы, разрабатывать стратегии кибербезопасности и создавать адекватные юридические и технические решения.

Каждое государство стремится обеспечивать безопасность не только критической инфраструктуры, но и всей инфраструктуры, оказывающей влияние на повседневную жизнь общества. В данном контексте необходимо обратить внимание на технологии, их уязвимости и прогнозирование будущих событий. Важно заранее идентифицировать потенциальные угрозы, не ожидая момента, когда ситуация станет критической и требует немедленных действий.

Интернет вещей (IoT) является одной из наиболее актуальных и распространенных технологий в современном мире. Умные устройства, объединяющие в себе компьютерную мощность и подключение к сети, стали частью повседневной жизни многих людей. Эти устройства могут быть удаленно управляемыми и подключены к сети из разных мест, что создает дополнительные возможности и удобство для пользователей.

Однако стоит заметить, что многие из этих устройств имеют низкую стоимость и, зачастую, пользователи не всегда полностью понимают, как они работают и какие риски они несут. Создание, разработка и управление этими технологиями часто разделяются между различными структурами и поставщиками. Компоненты могут быть подключены через облачные системы, и физическое местонахождение облака и вопросы доступа к данным остаются часто недоступными для конечного пользователя.

Многие из нас используют умные устройства для автоматизации домашней среды, управления освещением и другими функциями. Несмотря на популярность и удобство, не каждый осознает, что эти устройства также могут представлять опасность. Это не означает, что их следует избегать, но важно задавать вопросы о том, как обрабатываются и хранятся данные, собираемые устройствами.

Одной из потенциальных опасностей является возможность использования IoT-устройств для масштабных атак, таких как DDoS-атаки. Ранее для таких атак требовался доступ к большим дата-центрам и множество компьютеров, но в наши дни достаточно иметь доступ к множеству устройств IoT, чтобы организовать атаку. Эти устройства могут быть подключены к различным сетям, включая энергетические и сетевые системы. При этом их используют не только физические лица, но и компании и даже государственные органы.

Важно отметить, что внутри IoT-устройств могут содержаться логические бомбы, способные автономно выполнять разрушительные действия без предварительной команды. Эти устройства могут нарушать установленный порядок и представлять угрозу для общества. Однако, существует недостаток эффективного регулирования и надзора за IoT-устройствами.

Необходимо признать, что рост использования IoT-технологий предоставляет множество преимуществ, но также вызывает серьезные вопросы в области безопасности. Государства, компании и общество в целом должны совместно работать над разработкой и внедрением стратегий по обеспечению безопасности в сфере IoT, чтобы предотвратить потенциальные угрозы и минимизировать риски для инфраструктуры и общества в целом.

С развитием блокчейн-технологии она начинает внедряться в различные области, не ограничиваясь только криптовалютами и финансовыми транзакциями. Эта технология теперь используется для создания умных контрактов и рассматривается как инструмент для улучшения работы государственных реестров и регистров. Децентрализация, привносимая блокчейном, становится все более ценным преимуществом, особенно в ситуациях, когда

централизованные системы сталкиваются с проблемами координации, доступности и надежности.

Государства стремятся использовать децентрализацию блокчейн-технологии, и это подразумевает необходимость физического размещения данных. Эта проблема может быть особенно актуальной для небольших государств, которые должны обеспечить резервное хранение данных в случае катастрофы или других чрезвычайных событий. Государства должны принимать во внимание факторы безопасности и надежности в выборе места для хранения данных, чтобы обеспечить непрерывное функционирование своих информационных систем.

С развитием новых сетей, таких как следующее поколение сетей 5G и спутниковый интернет (например, Starlink), становится все более важным обеспечивать доступ к сети в различных уголках мира. Гарантированный доступ к сети становится ключевым фактором для обеспечения бесперебойной работы различных сервисов и коммуникаций.

Мобильные устройства и небольшие смарт-устройства играют все более значимую роль в нашей повседневной жизни. Эти устройства собирают и обрабатывают огромное количество данных, что делает их важными в контексте безопасности и конфиденциальности. Поэтому необходимо обращать особое внимание к защите данных, хранящихся и передаваемых через такие устройства, и принимать меры для обеспечения их безопасности.

Блокчейн-технология становится более широко применяемой и внедряется в различные сферы деятельности. Децентрализация и физическое размещение данных становятся ключевыми вопросами для государств. Новые сети и устройства требуют повышенного внимания к безопасности и доступности.

В современном мире практически каждый гражданин обладает мобильными устройствами, такими как смартфоны, и это стало неотъемлемой частью нашей повседневной жизни. Государства и организации всё чаще выбирают путь цифровой трансформации и переносят предоставление государственных услуг в онлайн-пространство, что обеспечивает более быстрый и удобный доступ граждан к необходимым сервисам.

Телефоны стали ключевыми устройствами, которые мы постоянно носим с собой и о которых заботимся. В них хранятся не только контакты и личные сообщения, но и целый спектр цифровых идентификаторов, таких как сертификаты, электронные подписи, банковские данные, а также информация для доступа к облачным сервисам и управления интернетом вещей.

С ростом цифровизации все больше наших личных данных и устройств подвергаются риску преступных действий. Преступники всё чаще обращают внимание на мобильные устройства, так как они содержат множество чувствительной информации. Все, начиная от наших личных идентификационных данных, и заканчивая информацией о финансах, настройках умных устройств, автомобилях, домах, и приватной коммуникации, находится внутри этих мобильных устройств. Это создает серьезные угрозы для нашей личной жизни и безопасности.

Важно понимать, что в эпоху цифровой трансформации и всемирной сети интернет, концепция абсолютной приватности становится парадоксом. Многие люди утверждают, что им важна личная жизнь и их усилия направлены на её защиту, но одновременно размещают множество личных данных в интернете и цифровом пространстве. Поэтому существует несоответствие между заявлениями о желании сохранить приватность и реальными действиями в цифровом мире.

В заключение, рост цифровизации и расширение доступа к личным данным через мобильные устройства создают важные вопросы о безопасности и приватности. Государства, организации и каждый человек должны более серьезно подходить к вопросам защиты личных данных и безопасности мобильных устройств. Это требует более глубокого понимания рисков и эффективных мер по их уменьшению.

Литература

1. Golla S.J., Muhlen N. Der Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei:Zur Legitimation

ЛЕЯ ФОКС
Профессор института исследований уголовного правосудия Университета Портсмута (Великобритания), доктор PhD, MA MBA FHEA

ИССЛЕДОВАНИЯ ЦИФРОВИЗАЦИИ – МОНИТОРИНГ ГЛОБАЛЬНЫХ ТРЕНДОВ И ТЕНДЕНЦИИ К ОБУЧЕНИЮ

Научная тема, имеющая первостепенное значение для современных правоохранительных органов и области исследований, связанной с цифровизацией, мониторингом глобальных тенденций и подходов к обучению, представляет собой одну из ключевых задач сотрудничества между Центром киберпреступности и экономической преступности в университете Портсмута (Великобритания). Этот центр, основанный в 2022 году, является важным организационным элементом для интеграции знаний и расширения исследований, преподавания и инноваций в областях киберпреступности и экономической преступности.

Главной целью этого центра является координация и развитие опыта в области киберпреступности и экономической преступности на разных факультетах университета. В частности, на факультете криминологии и уголовного правосудия, факультете гуманитарных и социальных наук, факультете вычислительной техники, факультете психологии, а также факультете бизнеса и права. Центр способствует более тесному взаимодействию и междисциплинарному сотрудничеству между различными областями интересов, связанными с киберпреступностью и экономической преступностью как внутри университета, так и за его пределами.

Центр киберпреступности и экономической преступности играет важную роль в исследованиях и понимании проблем, связанных с этими видами преступности, и представляет собой одну из крупнейших групп активных исследований в Великобритании по этой тематике. Сотрудники центра находятся на передовой в исследованиях и разработках, направленных на борьбу с киберпреступностью, что является важным вкладом в современную правоприменительную деятельность и обеспечение общественной безопасности.

Исследования в области цифровизации, мониторинга глобальных тенденций и подходов к обучению играют решающую роль в современной правоохранительной деятельности. Эти исследования способствуют поиску инновационных решений, направленных на устранение рисков и повышение социальной и организационной безопасности и устойчивости в отраслях, связанных с борьбой с кибер- и экономической преступностью.

Центр, в рамках которого осуществляются эти исследования, также включает в себя Центр исследований по борьбе с мошенничеством и клинику по борьбе с кибермошенничеством. Эти подразделения являются ключевыми компонентами для обеспечения эффективной борьбы с современными видами преступности.

В современном быстро развивающемся мире – цифровизация оказывает огромное влияние на правоохранительную деятельность. Важно, чтобы правоохранительные органы и их сотрудники оставались в курсе этих изменений и адаптировались к новым вызовам

вовремя. Глобальные тенденции в исследованиях цифровизации включают в себя несколько ключевых аспектов.

Первым из них является взрывной рост объема данных. Цифровая эпоха привела к тому, что данные стали всеобщим ресурсом, доступным как для обычных граждан, так и для правоохранительных органов. Исследования в этой области фокусируются на эффективном управлении и анализе данных, а также на обеспечении их безопасности и конфиденциальности.

Еще одной важной тенденцией является использование искусственного интеллекта и машинного обучения. Эти технологии революционизируют работу правоохранительных органов, позволяя им прогнозировать преступления, автоматизировать анализ цифровых доказательств и распознавание лиц. Эти исследования помогают повысить эффективность предотвращения и расследования преступлений, что является критически важным аспектом в современной борьбе с преступностью.

Исследования в области цифровизации, мониторинга глобальных тенденций и разработки эффективных подходов к обучению сотрудников правоохранительных органов играют ключевую роль в обеспечении безопасности и устойчивости общества. Эти исследования позволяют правоохранительным органам адаптироваться к изменяющимся условиям и более эффективно бороться с современными видами преступности.

Третья тенденция, которая выделяется в контексте исследований цифровизации и её влияния на правоохранительную деятельность, связана с проблемами кибербезопасности. С развитием цифровых технологий увеличивается число киберугроз, таких как фишинговые атаки и программы-вымогатели. Исследования в этой области имеют решающее значение для понимания и борьбы с преступностью. Правоохранительные органы должны быть оснащены современными знаниями и инструментами, необходимыми для эффективного противодействия этим угрозам.

Четвертая тенденция, связанная с цифровой этикой, поднимает важные этические вопросы, такие как нарушение конфиденциальности и предвзятость в алгоритмах искусственного интеллекта. Цифровизация выявляет этические дилеммы, которые могут возникать при использовании цифровых технологий в правоохранительной деятельности. Исследователи занимаются изучением этических последствий и разрабатывают рекомендации по ответственному использованию цифровых технологий в правоохранительных операциях.

Исходя из вышеупомянутых тенденций, следует рассмотреть подходы к обучению сотрудников правоохранительных органов.

Первым важным аспектом является обучение цифровой грамотности. Сотрудники правоохранительных органов должны обладать навыками и знаниями в области цифровой безопасности, анализа данных и эффективного использования цифровых инструментов. Это включает в себя осведомленность в сфере кибербезопасности, понимание технических аспектов работы цифровых технологий и способность ответственно обращаться с данными. Постоянное обучение и повышение квалификации в этой области являются важными компонентами обучения сотрудников правоохранительных органов.

Вторым подходом, который следует рассмотреть, является междисциплинарное обучение. Учитывая многомерный характер цифровизации, обучение сотрудников правоохранительных органов должно быть междисциплинарным. Сотрудничество между различными областями, такими как правоохранительные органы, компьютерные науки и юриспруденция, становится необходимым. Это позволит разработать комплексные подходы к решению сложных проблем, связанных с цифровой безопасностью и борьбой с киберпреступностью.

В итоге, эти подходы к обучению обеспечат сотрудников правоохранительных органов современными знаниями и навыками, необходимыми для эффективной борьбы с цифровыми угрозами и этическими вызовами, связанными с цифровой эпохой.

В рамках данного научного выступления рассматриваются различные подходы и перспективы в обучении сотрудников правоохранительных органов для эффективной адаптации к вызовам, связанным с цифровой трансформацией. Современное общество сталкивается с быстрыми и глубокими изменениями в сфере цифровых технологий, и правоохранительные органы должны активно адаптироваться к этим изменениям для обеспечения безопасности и соблюдения законов.

Первый из рассматриваемых подходов – междисциплинарные перспективы. Эти перспективы предполагают, что сотрудники правоохранительных органов должны обучаться и работать в сотрудничестве с представителями различных областей знаний. Это важно, поскольку цифровая трансформация влияет на различные аспекты общества, включая технологии, право и этику. Междисциплинарное обучение позволяет сотрудникам правоохранительных органов лучше понимать и реагировать на сложные вызовы, представляемые цифровыми технологиями.

Второй подход – обучение на основе сценариев. Этот метод обучения использует практические сценарии, основанные на реальных цифровых угрозах и расследованиях. Это позволяет специалистам развивать навыки критического мышления и принятия решений, необходимые для реагирования на цифровые угрозы. Симуляционные упражнения и тематические исследования могут значительно улучшить подготовку сотрудников правоохранительных органов.

Третий подход - обучение по этике и праву. В условиях цифровой эпохи соблюдение этических норм и законов становится критически важным. Сотрудники правоохранительных органов должны быть осведомлены о этических ограничениях и правовых аспектах, регулирующих использование цифровых технологий в своей деятельности. Обучение по этой тематике помогает предотвратить нарушения прав и обеспечить соблюдение законов при проведении цифровых расследований.

Четвертый подход – международное сотрудничество. В сфере цифровой безопасности и борьбы с киберпреступностью границы становятся относительными. Международное сотрудничество в области исследований и обучения позволяет обмениваться передовым опытом и совместно решать транснациональные цифровые проблемы. Этот подход подразумевает активное сотрудничество между правоохранительными органами разных стран. И, наконец, непрерывное обучение – пятый подход. Цифровизация – это непрерывный процесс, и обучение в этой области также должно быть постоянным. Сотрудники правоохранительных органов должны посещать семинары, конференции, участвовать в онлайн-курсах и постоянно обновлять свои знания и навыки. Это также включает в себя программы наставничества, которые объединяют опытных профессионалов с новичками в области цифровой безопасности.

В заключение, цифровизация правоохранительных органов – это фундаментальный сдвиг, требующий постоянной адаптации. Обучение с использованием вышеупомянутых подходов и перспектив позволяет сотрудникам правоохранительных органов быть в авангарде цифровых инноваций, соблюдая при этом этические стандарты и верховенство закона. Мы должны продолжать исследования, сотрудничество и постоянное образование, чтобы успешно справляться с вызовами цифровой эпохи.

Литература

1. Solove D.J.ldentity Theft, Privacy, and the Architecture of Vulnerability// Hastings Law Journal .-2003.-Vol 54,no 4

2. Trost J.The lmpostor Rule and ldentity Theft in America// Law and Hastings Law Lournal.-2017-Vol 35.no 2.

РУСТЕМОВА ГАУХАР РУСТЕМБЕКОВНА
Профессор кафедры управления правоохранительной деятельностью Алматинской академии МВД Республики Казахстан имени М. Есбулатова, д.ю.н., профессор

О ЦИФРОВИЗАЦИИ ЗДРАВООХРАНЕНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

Цифровое здоровье является частью современного медицинского прогресса. Внедрение информационных технологий и высокая ценность медицинских услуг, такие, как повышение доступности медицинской помощи, улучшение диагностики и лечения, а также улучшение процессов управления эффективностью учреждений соответствуют требованиям времени. Однако в совокупности с возросшими масштабами загрязнения и новыми правовыми рисками, связанными с обработкой и защитой от загрязнений, необходимы новейшие технологии.

Право на здоровье, право на наивысший уровень здоровья является правом человека, признаваемым международным правом. В Международном пакте об экономических, социальных и культурных правах, являющимся общепризнанным центральным механизмом по защите права на здоровье, признается «право каждого человека на наивысший достижимый уровень физического и психического здоровья» (ст.12. п.1).

В отношении права на здоровье, Комитет по экономическим, социальным и культурным правам определил, что государства обязаны предоставить следующее:

–Право доступа к учреждениям здравоохранения, товарам и услугам на *основании принципа недискриминации,* особенно для уязвимых или маргинализированных групп;

–Доступ к *минимальному набору продуктов питания первой необходимости,* содержащему питательных веществ и безопасному для здоровья;

– Доступ к *убежищу, жилищу и санитарным услугам* и достаточному количеству безопасной питьевой воды;

–Обеспечение *лекарствами первой необходимости*;

–*Справедливое распределение* всех учреждений, товаров и услуг здравоохранения» (Право на здоровье. Изложение фактов №31, с.27-28) [1].

Поэтому важным является глубоко и правильно осмыслить достижения науки в области охраны здоровья человека.

Центральным элементом IV-ой технологической революции является цифровая трансформация. Многие отрасли экономики и социальной сферы проходят сейчас этап глубоких преобразований, что в конченом итоге должно привести к их высокой технологичности. Сама цифровая трансформация является сложным, не всегда предсказуемым процессом, затрагивает многие сферы жизни. Она применима в ведущих странах лишь к тем отраслям экономики, что достигли уже высокого уровня так называемой цифровой зрелости.

После известных печальных январских событий прошлого года в Казахстане в стране наступила пора пересмотра всего законодательства. Продолжается конституционная реформа, ожидается принятия ряда новых законов и НПА. Продолжается курс на индустриализацию, важнейшей составляющей и неотъемлемой частью развития Казахстана является цифровая трансформация экономики. Она предполагает внедрение ИКТ (информационно-коммуникативных технологий) и ИИ (искусственного интеллекта), которые изменяют повседневную жизнь не только граждан, их бытие, но и всего общества. Республика Казахстан внедрила цифровое здравоохранение в числе одних из первых в СНГ. Вместе с тем,

Генеральный секретарь ООН Антониу Гутерриш отмечал, что необходимо обратить внимание на темную сторону цифровизации, ведь новые технологии развиваются до такой степени стремительно, что мы не успеваем не только отреагировать на них, но даже иногда осознать их сущность и ту агентность, которую они в себе заключают. Помимо того, что цифровые технологии и искусственный интеллект несут колоссальные преимущества, они становятся инструментом тотального контроля, вмешательства в частную жизнь, подстрекательства, распространения ложной информации, эксплуатации людей, а также совершения правонарушений.

Нам представляется, что стремительная трансформация цифрового здравоохранения в стране также несет определенные правовые риски, как в гражданском, уголовном праве, так и здравоохранительном (медицинском) праве. При этом мы не берем во внимание медицинские риски, т.к. это предмет изучения самих медицинских работников, научных сотрудников НИИ МЗ РК.

В этой связи возникла необходимость изучения специфики и опыта отечественного и зарубежного правового регулирования, разработки, использования и развития систем искусственного интеллекта в государственном управлении, коммерческой и частной жизни, в том числе и здравоохранении. Выявление правовых рисков и существующей неопределённости, связанных с развитием цифровых инноваций и имеющие существенное значение для принятия законодательства в рассматриваемой области, способствуют обеспечению безопасности и защиты прав и интересов личности, общества и государства.

В Казахстане можем отметить немногие отрасли готовых к цифровой трансформации. Между тем, заметим, что процесс распространения новых ИКТ и цифровизация различных сфер экономики, социальной сферы и общественной жизни непосредственно затрагивает совершенствование здравоохранения. Наблюдается цифровизация её, все элементы системы здравоохранения охвачены цифровой революцией. Цифровые продукты для здоровья человека стали неотъемлемой частью профилактики, диагностики, лечения и контроля состояния как общественного здоровья, так и каждого человека.

Для обеспечения гражданам конституционных прав на здоровье и охрану здоровья, в существующей в настоящее время модели системы казахстанского здравоохранения уже используются такие используемые элементы «цифрового здравоохранения», как современное диагностическое оборудование, ангиография, лапароскопия, медицинская статистика, которая позволяет собирать и обрабатывать большие объемы данных (*big data*) для принятия оптимальных решений.

Переход на ЦЗ (цифровое здравоохранение) предполагает преемственность лечения, т.е. использование данных прошлых исследований пациента (больного) в динамике, при этом снижаются затраты на повторные анализы, имеется доступ к данным об аллергиях, непереносимости тех или иных лекарственных средств и т.д. Кроме того, повышается доступность и качество самого лечения, цифровизация здравоохранения способствует быстрому прохождению диспансеризации (первый этап проходит в режиме единого коридора в поликлиниках), профилактике заболеваний через систему напоминаний. Доступность и упрощение получения медицинских услуг за счёт электронных сервисов, переход на единый номер записи на приём к врачу (от районных кол-центров или самой поликлиники) – всё это удобно для пациентов (больных). Посредством ЦЗ улучшается управление системой и контроль в реальном режиме.

Первые результаты ЦЗ наблюдаются в электронной записи на приём к врачу, выписке электронных больничных листков, создании личного кабинета пациента (запись к врачу, результаты лабораторных исследований), т.е. электронная медкарта жителя города, района – в лучшем случае.

Новая область цифровой медицины (ЦМ) зародилась примерно в 2007 г. благодаря появлению смартфонов. Связь мобильных устройств с глобальной сетью Интернет позволила создавать такие технологические платформы, которые объединили информацию с разнообразных устройств и датчиков (специальных сенсоров). Современные носимые устройства способны отслеживать состояние почти всех физиологических систем человеческого тела. Внедрение новых инновационных технологий в разных странах

продвигается по-разному, но это способствует развитию превентивной персонализированной медицины, облегчает принятие управленческих решений.

Сегодня первостепенное значение имеют подготовка кадров, обладающих достаточной квалификацией для осуществления цифровой трансформации в отраслях экономики и социальной сферы, стимулирование распространения передовых институтов и развитие регулирования, формирующего благоприятные условия цифровой трансформации [2].

Важнейшее значение для ЦМ имеют все данные о результатах медицинских исследований, различных манипуляций, мониторинга показателей заболеваний человека и т.п. Но сами по себе эти данные бесполезны, необходимо их обработать, проанализировать и интерпретировать. А это всё возможно при использовании ИИ (искусственный интеллект). Применение ИИ в медицине стадо возможным благодаря современным технологиям сбора, хранения и обработки большого массива данных, ростом вычислительных мощностей и появлением облачных хранилищ.

Эти технологии используются на трёх уровнях:

– врачами –для быстрой и очной интерпретации изображений;

– системами здравоохранения – для улучшения рабочего процесса и возможности сокращения медицинских ошибок;

– пациентами – для обработки собственных данных и укрепления здоровья [3].

Пандемия COVID-19 высветила ряд хронических проблем рассматриваемой отрасли, которые ранее повсеместно маскировались на всех уровнях. В период пандемии страховая медицина оказалась в настоящем коллапсе. Бюджетно-страховая медицина показала свою слабость в протекающих экономических условиях, неспособность решать основные проблемы по охране здоровья, которые связаны с привлечением финансовых потоков в медицину. Проблемы с разработкой и внедрением в отечественное здравоохранение своих современных медицинских технологий остаются по сей день . Как отмечается в литературе, «на всех начальных этапах жизненного

цикла новых технологий (биологических, генетических, информационных и др.) имеются организационные, правовые и этические проблемы» [4].

Таким образом, мы исследуем вопросы цифровизации в здравоохранении и медицине, применение ИИ, правовые риски, что присутствуют в этом процессе. Сегодня в центре правовой науки и культуры должен стоять человек, но уже с новейшими глобальными цифровыми правами [5].

Цифровые права человека – это отдельная тема для изучения, поэтому мы на них не останавливаемся, нет единой устоявшейся точки зрения, а в Казахстане на них только обращают нужное внимание. Но их изучение и место в системе современных прав человека – новое направление в науке и требует самого пристального внимания для понимания цифровизации в целом и роли человека и ИИ в нем.

Литература

1. https://biblioclub.ru /index.php?pade=bookkid=120004 (дата обращения: 04.07.2023:15.33)

2. Цифровая трансформация отраслей: стартовые условия и приоритеты. Доклад НИУ ВШЭ. – М.: Издательский дом высшей школы экономики, 2021. – С. 239.

3. Topol, E.J. High-perfomance medicine: the convergence of human and artificial intelligence //Nature medicine-2019b.-Voe.25.-P.44-56. – URL: https: //doi.org/10.1038/S41591-018-0300-7 (дата обращения: 28.01.2023).

4. Биленко А.И. Российский рынок медицинских услуг: правовые проблемы обеспечения конкуренции: автореф. дис…канд. юрид. наук. – М., 2022. – 22с. (дата обращения:31.07.2023:01.02).

5. Бурьянов М.С. Глобальные цифровые права человека в контексте рисков цифровизации //Век глобализации. 3/2020-54-70 (дата обращения: 03.12.2022:18.01).

ЧУКМАИТОВ ДУЛАТ СЛАМБЕКОВИЧ
профессор высшей школы Права и экономики НАО Жетысуский университет
им. И. Жансугурова д.ю.н., профессор

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ И БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ В СОВЕРШЕНСТВОВАНИИ НАДЗОРА И КОНТРОЛЯ ЗА ОСУЖДЕННЫМИ

Не принижая значения уголовно-правовой борьбы с преступностью, следует всегда констатировать приоритет в ее предупреждении. Один из основоположников казахстанской криминологии Е.И. Каиржанов подчеркивал: «… надо признать, что уголовные наказания выступают лишь одной из специальных мер предупреждения преступности, разработкой которых в целом занимается криминология.

Цель криминологии по сравнению с уголовным правом представляется более широкой – исследование эффективности всех возможных (в том числе и уголовно-правовых) методов и средств борьбы с преступностью и разработка системы (включая и уголовно-правовые) методов и мер, направленной на предупреждение преступности» [1, с.14].

Сама система мер предупреждения преступности это сложный комплекс идеологических, правовых, экономических, культурно-воспитательных, технических, других средств и методов воздействия, а также социального, охранительного, технического контроля [2, с. 384-388]. Причем система динамична и зависит от многих параметров, например, от уровня миграции, количества молодежи в составе населения, уровня жизни и безработицы, уровня алкогольной и наркотической зависимости населения и так далее. Кроме того на глазах меняется социальная среда, влияние глобальной сети интернета, а урбанизация снижает социальные связи и социальный контроль. Мир стремительно меняется благодаря техническому прогрессу, то, что вчера казалось фантастикой сегодня доступно широким слоям населения. Это влияет и на структуру преступности, В корыстных преступлениях все больше деяний с использованием компьютерных сетей и возможностей мобильной сотовой связи.

Бурное развитие современных технологий не может не влиять на методы и средства борьбы с преступностью. МВД РК не должно упустить моменты своевременного прикладного внедрения в практику деятельности передовых инструментов выявления, раскрытия, расследования и предупреждения преступности.

Сегодня необходимо иметь в своей штатной структуре подразделения по установлению источников хакерских атак через взаимодействие с центрами антивирусной защиты компьютерных сетей, а также специалистов по выявлению и процессуальной фиксации деятельности мошенников во взаимодействии с операторами сотовой связи, выработке предложений по совершенствованию уголовно-правовой, уголовно-процессуальной и уголовно-исполнительной борьбы с подобными общественно-опасными деяниями.

Большое подспорье в борьбе с преступностью могут оказать биометрические технологии, особенно в борьбе с рецидивной преступностью [3, с. 219].

Уголовно-исполнительная система как подсистема общего противостояния преступности должна также идти в ногу с современным техническим прогрессом. В условиях дефицита штатного расписания и некомплекта, производительность труда службы пробации может быть достигнута с помощью использования не только электронных браслетов, но и организацией надзора и контроля с помощью биометрических технологий. Необходима постановка технического задания разработчикам в области искусственного интеллекта за соблюдением установленного порядка отбывания наказания. Фантастические сроки внедрения технических новшеств должны учитываться службами МВД, нельзя допускать отставания в техническом перевооружении подразделений. Например, несмотря на бурное развитие дронов и другой малой авиации, она по-прежнему слабо используется в патрулировании дорожного движения, охране объектов подконтрольных национальной гвардии, использовании криминалистическими подразделениями в осмотре места происшествия и так далее [4, с. 219].

Своевременно должно обновляться и техническое оснащение учреждений исполняющих лишение свободы. Цифровизация в первую очередь должна коснуться системы учета и перемещения лиц осужденных к лишению свободы. Специальные части исполнительных учреждений должны быть соединены в единую информационную сеть, необходимо предусмотреть и хранение их биометрических данных. Цифровое личное дело лица осужденного к лишению свободы должно содержать всю уголовно-исполнительную характеристику и с ее учетом уметь выдавать ориентировку уголовному розыску, рекомендовать сроки возможного применения гуманных актов, своевременно выдавать сообщения о необходимости представления материалов в суд и предоставлять объективную информацию для подготовки этих материалов.

Средства видеонаблюдения в учреждении должны позволять идентифицировать цифровое изображение с биометрическими данными осужденных лиц. В перспективе искусственный интеллект должен распознавать признаки агрессивного и другого противоправного поведения и информировать об этом соответствующие службы. Необходима разработка мер защиты технических средств надзора и контроля от попыток вывести их из строя.

Таким образом, современные методы и средства борьбы с преступностью должны базироваться на мерах ее предупреждения, опираться на достижения научно-технического прогресса, темпы которого уже не кажутся столь фантастичными.

Литература

1. Каиржанов Е.И. Криминология. Общая часть, – Алматы, Оркениет, 2000. – С. 180.

2. Чукмаитов Д.С. Проблемы предупреждения индивидуального преступного поведения// Сборник статей по материалам Международной научно-практической конференции «Актуальные вопросы правоохранительной деятельности», посвященной памяти прокурора Казахской ССР Утегена Сеитовича Сеитова / Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2022. – С. 420.

3. Чукмаитов Д.С. Развитие биометрических технологий в условиях правового государства Материалы конференции «Наука и ее роль в современном мире», Карагандинский университет «Болашак», 2010 г. – С. 252.

4. Чукмаитов Д.С. Использование информации о личности правонарушителя в противодействии преступлениям// Сборник материалов научного мероприяти «Учет особенностей личности преступника в предупреждении отдельных видов преступлений: проблемы теории и практики» Материалы Международного научно-практического круглого стола 27.05.2022 г. Қосшы, 2022. – С. 230.

АКИМЖАНОВ ТАЛГАТ КУРМАНОВИЧ
Директор НИИ права при университете «Туран», научный сотрудник НИЦ Алматинской Академии МВД РК им. М. Есбулатова, д.ю.н., профессор, полковник юстиции в отставке, заслуженный работник МВД РК, почетный работник образования РК

ПОИСК НОВЫХ ПУТЕЙ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА

В Республике Казахстан проблеме противодействия преступности уделяется со стороны государства достаточно внимания. Имеется правовая основа противодействия преступности, достаточно мобильная правоохранительная система, и самое главное – сформировано у большей части населения негативное отношение к криминальным проявлениям в обществе.

По мнению известного ученого криминолога В.Н. Кудрявцева, в современном обществе наблюдается серьезное противоборство между преступностью и государством. [1, с. 29]

Причем чем совершеннее становятся формы и методы преступной деятельности, тем активнее наблюдается деятельность правоохранительных органов.

Однако, как свидетельствует правоприменительная практика, ощутимого превосходства в данном противоборстве указанных сторон, по объективным и субъективным причинам, достичь в полном объеме пока не представляется возможным.

Об этом могут сказать любой руководитель правоохранительного органа или научного подразделения занимающегося исследованием проблем противодействия преступности, отдельно взятый представитель гражданского общества, а также регистрируемая стастистика самой преступности.

Как известно, благодаря исследованиям ученых-криминологов, современная преступность развивается и видоизменяется вместе с самим обществом, которое ее и порождает и представляет собой большую угрозу и опасность для самого общества, поскольку не только мешает его нормальному функционированию и существованию, но и опосредованно посягает на его национальную безопасность.

По справедливому замечанию О.В. Дамаскина происхождение преступности связывается с периодом возникновения государства, права, социальным, имущественным и классовым расслоением человеческого общества. [2, с. 84]

Неслучайно, Законом Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 26 июля 2016 года) преступность, наряду с другими факторами, отнесена к основным угрозам национальной безопасности государства. [3, с. 58]

Среди многих причин отставания процесса противодействия преступности от развития самой преступности является постоянное ее изменение и развитие, приспособление к новым реалиям жизни, которые направлены на совершенствование форм и методов преступной деятельности, чтобы они были более эффективными, недосягаемыми до правоохранительных органов и приносили при этом большую прибыль.

Поэтому все процессы, которые происходят в общественном развитии находят свое отражение и в содержании самой преступности.

И не случайно, что одной из причин изменение сущности современной преступности является происходящий процесс цифровизации и информатизации общества и государства.

В самом общем понимании цифровизация предполагает использование цифровых технологий для автоматизации бизнес-процессов, улучшения уровня качества услуг, оптимизации производства и повышения эффективности работы организаций и предприятий в целом.

В результате проводимой цифровизации, меняется и общественная жизнь, повышается ее качество, у человека появляется электронный доступ к информации и услугам, происходит совершенствование систем здравоохранения, образования и других сфер жизни общества.

То есть не выходя из дома или из служебного кабинета, любой гражданин может в условиях цифровизации выполнять какие-либо действия, которые приходилось ранее для осуществления преодолевать определенные расстояния и тратить драгоценное свое время.

Поэтому и криминальный мир стал использовать преимущества цифровизации, однако, не на благо общества, а напротив во вред ему путем нанесения ущерба совершаемыми преступлениями.

Данное обстоятельство требует от государства поиск новых подходов противодействия преступности, которые должны составить основу новой модели борьбы с преступностью.

У нас в стране сложились предпосылки для разработки новых идей по противодействию преступности.

С 2021 года вступила в силу новая Концепция правовой политики Республики Казахстан до 2030 года, утвержденная указом Президента РК от 15 октября 2021 года №674. [4]

По нашему мнению, концептуальная проработка противодействия преступности должна охватить следующие четыре основные направления:

– первое направление – это совершенствование правовой базы противодействия преступности,

– второе направление –это деятельность самой правоохранительной системы, то есть основных субъектов противодействия,

– третье направление – это научное обеспечение процесса борьбы с преступностью и ее исследования,

– четвертое направление – это цифровизация всего процесса противодействия преступности.

В условиях всеобщей цифровизации, мировое сообщество осознало, что самой главной задачей для человечества в третьем тысячелетии является обеспечение информационной безопасности как части национальной безопасности в отдельно взятом государстве и, в целом, на всем мировом пространстве.

В ст. 4 Закона Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 28 декабря 2018 года) к одному из видов национальной безопасности на ряду с общественной безопасностью, военной безопасностью, политической безопасностью, экономической безопасностью, экологической безопасностью отнесена информационная безопасность – как состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека, гражданина , общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная безопасность страны. [4, с. 52]

Роль информационной безопасности трудно переоценить. По мнению ученых, современный период развития можно охарактеризовать как переход от постиндустриального общества к информационному. Его невозможно сегодня представить без интенсивных информационных обменов и развивающихся информационных систем. Информационные

потоки постепенно становятся рычагами управления информационными процессами. [5, с. 13]

Более детальную характеристику процессов, происходящих в информационном пространстве дают ученые-криминологи. По их мнению, современный мир характеризуется стремительным развитием информационных отношений, информационно-телекоммуникационных систем, компьютерных устройств, социальных сетей, появлением новых средств создания, хранения, обработки и распространения электронно-цифровой информации, расширением киберпространства и тотальной компьютеризацией человеческого общества. [6, с. 383]

Чтобы полнее раскрыть содержание информационной безопасности как вида национальной безопасности, рассмотрим понятие самой национальной безопасности – как состояние защищенности национальных интересов Республики Казахстан от реальных и потенциальных угроз, обеспечивающих динамическое развитие человека и гражданина, общества и государства.[3, с. 50]

Казахстан, являясь частью мирового сообщества, вносит большой вклад в решение данного вопроса. Развитие казахстанского общества на современном этапе тесно связано с возрастанием количества условий и обстоятельств, угрожающих жизни и здоровью людей, интересам общества и государства и достигло такого уровня существования, когда обеспечение безопасности, самосохранения, выживания, как отдельного человека, так и мирового сообщества в целом превращается в проблему, необходимость решения которой не оставляет сомнений.

Заслуживает внимания описанная известным ученым криминологом В.Н. Кудрявцевым в своей книге «Стратегия борьбы с преступностью» – стратегия безопасности. Цитируемый автор предлагает меры безопасности определять как предпринимаемые в целях защиты людей, промышленных, военных, научных и иных объектов от преступных посягательств неустановленных (неопределенных) лиц.

При этом центр тяжести перемещается с превентивной и поэтому незаконны репрессии в отношении «подозреваемых» или «неблагонадежных» элементов на осуществление мер по охране и защите государственных и общественных объектов, а также граждан от возможных преступных посягательств. По сути, речь идет об устранении условий, способствующих совершению преступлений.[1, с. 307]

В свою очередь будет интересным исследование общей дефиниции безопасности, в структуру которого входит и само понятие национальной безопасности.

Как известно, понятие безопасности с позиции различных наук, как правило, трактуется неоднозначно. Наука психология безопасность представляет как ощущение, восприятие и переживание необходимости в защите жизненных (духовных и материальных) потребностей и интересов людей. Философия и социология рассматривают безопасность как состояние, тенденции развития и условия жизнедеятельности общества, его структур, институтов и порядков, при которых обеспечивается сохранение оптимального соотношения различных категорий и противоположностей. С позиций юридических наук безопасность рассматривается как система установления правовых гарантий защищенности личности и общества, обеспечения их нормальной жизнедеятельности, прав и свобод.

Например, по мнению С.В. Степашина безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно обусловленными инновациями в ней и свободное, соответствующее собственной природе и ею, определяемой функционирование.[7, с. 23]

Н.Д. Казаков определяет безопасность как «динамически устойчивое состояние по отношению к неблагоприятным воздействиям и деятельность по защите от внутренних и внешних угроз, по обеспечению таких внутренних и внешних условий существования

государства, которые гарантируют возможность стабильного всестороннего прогресса общества и его граждан».[8, с. 62]

М.А. Лесков безопасность рассматривает как явление, тождественное гомеостазису системы, «под которым принято понимать тип динамического равновесия, характерный для сложных саморегулирующихся систем и состояний в поддержании существенно важных для сохранения системы параметров в допустимых пределах».[9, с. 66]

Митрохин В.И., считает, что безопасность есть мера защищенности среды жизнебытия, чести, достоинства, ценностей личности, социальных групп, государства, общества, цивилизации в целом.[10, с. 22-40]

Обобщая приведенные выше дефиниции безопасности, можно сделать обобщенный вывод, что безопасность есть результат социальной деятельности по обеспечению безопасности личности, общества, государства.

В качестве предмета деятельности выступают конкретные угрозы опасности (информационные, экологические, военные, политические, экономические и пр.), а также отдельные материальные носители этих угроз (природные и социально-общественные явления и т.д.).

По мнению российских ученых С.В. Степашина и В.С. Комисарова, *угрозы* могут классифицироваться по различным основаниям.[7, с. 19;11, с. 10]

В ст. 6 Закона Республики Казахстан «О национальной безопасности Республики Казахстан» закреплен перечень основных угроз национальной безопасности, среди которых применительно к рассматриваемой нами проблеме информационной безопасности относятся: п. 16) снижение уровня защищенности информационного пространства страны, а также национальных информационных ресурсов от несанкционированного доступа, а также п.17)информационное воздействие на общественное и индивидуальное сознание, связанное с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности. [3, с. 54]

Как нам представляется информационная безопасность должна охватывать следующие основные направления деятельности.

Первое. Это всеобщая цифровизация. Создание информационной базы о всех направлениях развития современного общества. Только наличие желаемого информационного пространства того или иного государства, может обеспечить его поступательное и развитие и безопасность.

Второе. Это обеспечение доступа граждан к любой интересующей их информации открытого характера. В ч. 3 ст. 18 Конституции Республики Казахстан закреплена норма, что государственные органы, общественные объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации. [12, с. 8]

Третья. Обеспечение безопасности всех источников информации, в том числе и отдельных граждан, имеющейся в Республике Казахстан, то есть информационной базы. Когда обеспечена полная информационная безопасность в обществе, можно говорить о состоянии защищенности данного общества и его граждан.

Следует отметить, что информатизация, кроме позитивного имеет и негативные свойства. Так, по мнению ученых, информационные технологии – это своеобразный «ящик Пандоры», который несет обществу не только блага, но и различные трудности, проблемы, испытания. Расплатой за «технологические блага» стали изменения в социальной культуре людей: информационная сеть Интернет заменила большинству театры , филармонии, консерватории, библиотеки, музеи, книги; общение в социальных сетях – «Живое» общение со знакомыми, друзьями, родственниками и другими людьми, люди становятся психологически интернет-зависимыми. [6, с. 383]

Кроме этого, негативные свойства цифровизации связаны напрямую с преступной деятельностью, то есть с криминальным миром.

Так, по мнению известного российского ученого криминолога В.С. Овчинского стратегия информационного общества понимает само это общество в широком смысле – как общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.[13, с. 22].

Данные процессы стали иметь место в настоящее время и в Республике Казахстан, так как по мнению ученых-криминологов, переход многих развитых стран мира, в том числе и Казахстана к цифровизации способствовал активизации преступности цифрового мира, особенно ее организованных форм.

По мнению известных ученых криминологов в современном обществе наметилась новая тенденция в развитии криминала – это его цифровизация, процесс и тенденции которого описан достаточно подробно и убедительно известным российским ученым В.С. Овчинским в своих последних фундаментальных работах как «Криминология цифрового мира» [13] и « Киберполиция XXI века. Мировой опыт» [14.], «Кибермафия. Мировые тенденции и международное противодействие : монография».[15]

В современной научной литературе и публицистике, в официальных документах и нормативных актах, посвященных противостоянию преступности, используются разнообразный понятийный аппарат и терминология. Они заимствованы из различных областей научных знаний и призваны по возможности наиболее емко выражать сущность данной деятельности. Это и уголовная политика, и борьба (война) с преступностью (с ее концепциями и стратегиями), и контроль над преступностью, реагирование, воздействие на нее, противодействие преступности и т.п. Однако, с позиции угроз национальной безопасности, в том числе и информационной безопасности, преступность самостоятельно не рассматривалась.

Разграничение различных терминов и понятий, обозначающих определенный вид деятельности, имеет не только теоретическое, но и прикладное значение, в особенности для нормотворчества, для организации работы по противостоянию преступности, разграничению компетенции субъектов, осуществляющих эту задачу, по устранению их смешения и дублирования их функций.

Поэтому казахстанский законодатель предвидя цифровизацию криминального мира при разработке нового УК РК 2014 года предусмотрел новую главу 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК [16, с. 119-123], в которую включил наиболее опасные виды посягательств на эти отношения:

а) неправомерный доступ к информации, в информационную систему или сеть телекоммуникации (ст. 205 УК РК);

б) неправомерное уничтожение или модификация информации (ст. 206 УК РК);

в) нарушение работы информационной системы или сетей телекоммуникации (ст. 207 УК РК);

г) неправомерное завладение информацией (ст. 208 УК РК);

д) принуждение к передаче информации (ст. 209 УК РК);

е) создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК);

ж) неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК РК);

з) предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК РК);

и) неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК РК).

По мнению казахстанских и российских ученых, все уголовные правонарушения, входящие в Главу 7 УК РК можно классифицировать на группы:

а) уголовные правонарушения, посягающие на конфиденциальность, целостность и доступность охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникативной сети (ст.с.205-211 УК РК);

б)иные виды уголовных правонарушений в сфере информатизации и связи (ст.ст. 212 и 213 УК РК). [17, с. 302]

И так, подводя итог рассмотрению изложенной пробоемы связанную с противодействием современной преступности в период ее цифровизации, посягающей на информационную безопасность как одного из видов национальной безопасност, и можно сделать следующие выводы.

Первое. В связи с всеобщей информатизацией всех жизненноважных и жизненно обеспечивающих процессов, как нам представляется, информационной безопасности по праву принадлежит в настоящее время ведущее место, среди других видов национальной безопасности.

Второе. Обеспечение информационной безопасности направлено на охрану конституционных прав граждан, общественных организаций, государственных органов и, в целом, всего государства.

Третье. В связи с активной цифровизацией криминального мира, информационная безопасность должна охватить деятельность всех правоохранительных и специальных органов Республики Казахстан, призванных обеспечивать правопорядок и общественную безопасность в Республике Казахстан.

С учетом вышеперечисленных обстоятельств можно констатировать, что обеспечение информационной безопасности в стране – есть мера по укреплению правопорядка, общественной безопасности, стабильности в обществе, а также обеспечению прав и законных интересов граждан страны.

Такая стратегия исходит из определенной политической идеологии и предполагает наличие общей концепции, определение не только ближайших, но и отдаленных целей и способов их достижения, разнообразных мер различных субъектов антикриминального воздействия, пригодных для применения в различных, изменяющихся условиях.

При этом дальнейшее развитие информационной безопасности в Республике Казахстан должна предполагать планирование и осуществление научно обоснованной системы антикриминальных мероприятий на всех уровнях социальной организации и найти свое достойное место в проводимой уголовной политики государства, вытекаюшей из положений новой Концепции правовой политики Республики Казахстан на период с до о 2030 года, утвержденной Указом Президента РК № 674 от 15 октября 2021 года.[4]

Литература

1. Кудрявцев В.Н. Стратегии борьбы с преступностью. – М.: Юристъ, 2003. – С. 352.

2. Дамаскин О.В. Криминологические аспекты противодействия преступности: научн.-прак. Пособие. – М.: Юрлитинформ, 2017. – С. 264.

3. Правоохранительные органы: Сборник законодательных актов. – Алматы: Юрист, 2019. – 256.

4. Об утверждении Концепции правовой политики Республики Казахстан до 2030 года. Указ Президента Республики Казахстан от 15 октября 2021 года №674

5. Информационное право: учебник для бакалавров // отв. Ред. И.М. Рассолов, – Москва: Проспект, 2016. – С. 352.

6. Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / П.В. Агапов, Г.В. Антонов-Романовский, В.К. Артеменков [и др.]; под общ. Ред. Р.В. Журбина; Академия Генеральной прокуратуры Российской Федерации. – Москва: Проспект, 2018. – С. 656.

7. Степашин С.В. Безопасность человека и общества (политико-правовые вопросы): Монография. СПб: СПб ЮИ МВД России, 1994.

8. Казаков НД. Безопасность и синергетика (опыт философского осмысления)//Безопасность. Информационный сборник Фонда национальной и международной безопасности. 1994. №4.

9. Лесков МА. Гомеостатические процессы и теория безопасности // Безопасность. Информационный сборник. 1994. №4 (20).

10.Митрохин В.И. Концептуальные основы стратегии национальной безопасности России // Социально-политический журнал. 1995. №6, – С. 22-40.

11.Комиссаров В.С. Преступления, нарушающие общие правила безопасности (понятия, система, общая характеристика): Автореферат. дис. …д-ра юрид. наук. – М. МГУ. 1997. – С. 50.

12.Конституция Республики Казахстан. Практическое пособие. – Алматы: ТОО «Издательство «Норма-К», 2023. – С. 44.

13.Овчинский В.С. Криминология цифрового мира : учебник для магистратуры // В.С. Овчинский. – М: Норма: ИНФРА М, 2018. – С. 352.

14.Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. – М: Международные отношения, 2020. – С. 288.

15.15.Жданов Ю.Н., Кузнецов С.К., Овчинский В.С. Кибермафия. Мировые тенденции и международное противодействие: монография // Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский; вступ. ст. О.В. Храмова. – Москва: Норма, 2022. – С. 184.

16.Уголовный кодекс Республики Казахстан: Практическое пособие. – Алматы: «Издательство «Норма-К», 2023. – С. 276.

17.Уголовное право Республики Казахстан: Особенная частьв 2-т.: Учебник для вузов. Отв. Ред. И.И. Рогов, К.Ж. Балтабаев, А.И. Коробеев. – Алматы: Жеті Жарғы, 2016. – С. 540.

БЕЙСЕНАЛИЕВ БАУРЖАН НУРАЛЫУЛЫ
старший преподаватель кафедры
оперативно-розыскной деятельности Алматинской
академии МВД Республики Казахстан
им. М. Есбулатова, к.ю.н. Кыргызской Республики,
подполковник полиции

СЕРАЛИЕВА АЛИЯ МАЖИТОВНА
ассоциированный профессор кафедры
«Юриспруденция» Казахского национального
педагогического университета им. Абая,
к.ю.н., ассоциированный профессор (доцент)

КАИРЖАНОВА СОЛИДАТ ЕЛЕГЕНОВНА
профессор кафедры «История и юриспруденция»
Западно-Казахстанского инновационно-
технологического университета д.ю.н., доцент
младший советник юстиции

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ВИДЫ И ПРЕДУПРЕЖДЕНИЕ

Защита от киберпреступлений – это постоянный процесс. Нам нужно быть внимательными и готовыми к новым угрозам (Клиффорд Столл).

Проблема использования достижений науки и техники в преступных целях связана с одним из важнейших направлений интеграционных процессов: созданием по сути международной и глобальной по форме сети Интернет, объединившей миллионы компьютеров, расположенных в разных уголках земли. Всемирная паутина, открывшая широчайшие возможности для получения информации и обмена ею, развивается очень быстрыми темпами [1, с.71]. Для этого киберпреступники используют свой арсенал информационного оружия, представляющий собой совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения.

Таблица 1. К основным видам информационного оружия относят следующие:

№	Название	Какой вред причиняет?
1	Бэкдор	данный инструмент предполагает скрытый метод в системе, который позволяет получить доступ к защищенной области.
2	Компьютерные вирусы	специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, «вирусы» способны самостоятельно размножаться.

3	«Логические бомбы»	программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие
4	Программное вредоносное обеспечение	программы или утилиты, которые после установки выполняет незаявленные функции в фоновом режиме.
5	Нейтрализаторы тестовых программ	обеспечивают сохранение естественных и искусственных недостатков программного обеспечения.
6	Анализаторы трафика (sniffer)	программы или устройства, которые контролируют данные, передаваемые по сети. Традиционно используемые для законных функций сетевого управления, они могут применяться и во время кибератак с целью кражи информации.
7	DDos-атаки	предназначены для нарушения доступа к сети, как правило, при помощи выполнения миллионов запросов каждую секунду в результате чего доступ к сети затрудняется или нарушается.
8	Киберпреступления, совершаемые с помощью e-mail	это метод отправки электронной почты с подменой источника, используется для того, чтобы заставить получателя предоставить конфиденциальную информацию.
9	Keylogger	представляет собой программное или аппаратное средство, предназначенное для контроля нажатия клавиш на клавиатуре компьютера, для получения пароля, пин-кода или другой информации.
Примечание* – составлено автором на основании источника Глотина И.М. Киберпреступность: Основные проявления и экономические последствия //Вопросы экономики и права. – 2014. – №8. – 12 с.		

В отечественных и зарубежных научных кругах преступления, совершаемые в компьютерных и телекоммуникационных системах, именуются по-разному: компьютерные преступления [2,3], высоко-технологичные преступления [4], киберпреступления [5], преступления в области компьютерной безопасности [6,7], компьютерные преступления в сфере информации [8] и т.д.

Термин «киберпреступность» в настоящее время часто используется в сочетании с термином «компьютерная преступность», и часто эти термины используются как синонимы. В литературе наибольшее предпочтение отдается термину «компьютерная преступность». Возможно, это потому, что большинство исследований проводится на криминалистическом или процессуальном уровне. Кроме того, глава 7 УК РК «Уголовные правонарушения в сфере информационной связи», предусматривает ответственность за правонарушения, объектом которых является информация и информационные системы [9].

На самом деле эти термины очень близки друг к другу, но еще не являются синонимами. На наш взгляд, понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computercrime) и более точно отражает сущность такого явления, как преступность в информационном пространстве. Так, Оксфордский словарь определяет приставку «cyber-» как составную часть сложного слова. Его значение «относится к информационным технологиям, Интернету, виртуальной реальности» [10].

Таким образом, «киберпреступность» – это преступление, связанное как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей [11].

Таблица 2. Характерные особенности киберпреступлений

№	Описание
1	высокая скрытость, достигаемая с использованием возможностей инфокоммуникационных сетей, средств обеспечения анонимности, маскировки, шифрования и т.д.;
2	трансграничный характер большинства серьезных киберпреступлений: преступник (члены преступной группы), объект посягательства, потерпевший (потерпевшие) могут географически находиться на территориях различных государств);
3	высокий интеллектуальный уровень подготовки, организации и реализации преступных деяний;
4	высокий уровень профессиональной подготовки преступников;
5	нестандартность подходов, сложность реализации, многообразие и постоянное обновление способов и методов совершения преступлений, а также применяемых специальных технических и программных средств;
6	во многих случаях неосведомленность потерпевших о совершении против них преступных действиях в виртуальной среде, а также нанесенном ущербе;
7	дистанционный характер преступных действий, отсутствие физического контакта преступника, объекта преступления и потерпевшего;
8	низкая эффективность традиционных подходов и методов профилактики, предотвращения, пресечения и расследования компьютерных преступлений;
9	высокая сложность сбора и подготовки юридически значимой доказательственной базы совершения преступлений в виртуальной среде.
Примечание* – составлено автором на основании источника https://www.google.com/search?q=%D1%82%	

Существуют различные виды киберпреступлений, которые постоянно видоизменяются, в связи с латентностью и достижением научнотехнического прогресса.

Самой распространенной является классификация, которая приводится Конвенцией Совета Европы о киберпреступности (англ.: Council of Europe Convention on Cybercrime). В ней указаны четыре типа правонарушений и позже был принят дополнительный протокол, и теперь их пять:

−преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;

−преступления, связанные с применением компьютеров;

−преступления, связанные с контентом;

−преступления, связанные с нарушением авторских и смежных прав;

−пятая группа – преступления, посягающие на общественную безопасность. В эту категорию входят такие виды деятельности, как *кибертерроризм и использование киберпространства в террористических целях* (например, участие в террористических преступлениях или содействие им) [12].

В Казахстане самым распространенными киберпреступлениями являются *фишинг и банковские киберпреступления.* Дело в том, что весь сплав экономической преступности питается и функционирует благодаря финансовым средствам, которые регулируются учреждениями банковской системы [13, с.6]. При этом отмечается именно увеличение электронных атак на информационные ресурсы банковских структур с целью хищения денег или получения конфиденциальных сведений, необходимых для совершения подобных действий [14].

По статистике каждый 12-й звонок – это спам или кибератака. Можно проследить, что количество преступлений растет, но при этом их раскрываемость уменьшается. Как отмечает

адвокат в сфере киберправа С. Дарбинян, «огромное количество реально совершенных преступлений остается за бортом. Например, ситуации, когда у пользователя угоняют «танчик» (танк в многопользовательской онлайн-игре World of Tanks) ценой в несколько тысяч долларов или с помощью вирусов похищают личные пароли от криптокошельков и уводят затем Etherium или Bitcoin. О таких преступлениях не заявляют, их количество никто не отслеживает, по ним не возбуждаются уголовные дела» [15].

Основная цель фишинга – это получение доступа к конфиденциальной информации пользователя, логину, паролю, счету и т. п., то есть определенный вид мошенничества. Жертвой может быть каждый, как работники финансовых учреждений, так и их клиенты. Под страхом потерять все свои денежные средства на карте, жертвы зачастую не думают о негативных последствиях, добровольно предоставляют фишеру личные свои данные, так как их ввели в заблуждение, представляясь работниками финансовых сфер.

Виды фишинга: почтовый – в виде рассылки по электронным адресам, онлайновым – в виде копирования известных сайтов, с изменением буквально одной буквы в адресе страницы, так и комбинированный – сочетающим в себе несколько способов. Сложность в раскрытии фишинга является то, что преступники постоянно меняют свои дислокации, способы совершения, то есть сложно определить имя мошенника, его адрес, местонахождение и т.д.

Что касается банковской киберпреступности, здесь основной целью злоумышленников является хищения денег. В 2022 году в Казахстане было выявлено 5 тыс. случаев оформления фиктивных банковских займов, сообщают в Агентстве РК по развитию и регулированию финансового рынка (АРРФР) [16]. В истории уголовных дел есть случаи, когда сотрудники известных банков сами предоставляли информацию о владельце банковской карты, его паспортные данные и остальной перечень сведений, необходимых для перечисления денежных средств на счет мошенника. Вопрос, который волнует всех жертв этой финансовой махинации, заключается в том, кто же те самые киберпреступники, которые могут так умело выводить миллиарды тенге со счетов жертв. Ответ на этот вопрос весьма нетривиален. Это могут быть заключенные – те, с чьих номеров, чаще всего звонят. При обыске одного из мест отбывания наказания в камерах заключенных были обнаружены телефоны, роутеры, зарядные устройства, наушники, а также записные книжки с фамилиями последующих жертв [17].

Поэтому в тюрьмах нужно установить приборы, способные заглушить телефонную связь на территории тюрьмы.

Юридически абоненты сами добровольно передают киберпреступникам реквизиты своих личных карт, что еще больше усложняет возврат средств. В заключение следует отметить, что человеческая халатность и безграмотность способствуют увеличению количества украденных средств. *Для снижения количества правонарушений в этой сфере следует проводить мероприятия по повышению финансовой грамотности населения, а также информировать старшее поколение о наличии данной проблемы, которое в большей степени подвержено психологическому воздействию киберпреступников.*

Правонарушения, совершаемые в этой сфере, чаще всего относятся к п. 4 ч. 2 ст. 190 УК РК, максимальное наказание по которой составляет четыре года лишения свободы. На данный момент в Уголовном кодексе РК нет статьи, которая бы касалась конкретных преступлений в сфере хищения денежных средств с банковских карт путем предоставления и распоряжения сотрудником банка заведомо ложных сведений. *Единственным способом ограничить тенденцию развития преступности в этой сфере является введение правовых норм, решающих эту проблему.*

Для раскрытия киберпреступлений в банковской сфере Генеральной прокуратурой РК реализован проект «Универсальный сервис СИОПСО» в части направления запросов на наличие банковских счетов и остатка денежных средств, с соблюдением процедуры санкционирования запросов. Это позволило ускорить обмен информацией и изобличить по горячим следам 10 преступных групп кибермошенников. К примеру, в Шымкенте группа злоумышленников из пяти человек, представляясь сотрудниками банков, оформляла

на граждан кредиты и с использованием программ удаленного доступа похищала денежные средства. Совместно с Агентством по финансовому мониторингу внедрен механизм раннего выявления потенциальных финансовых пирамид, приняты организационно-разъяснительные и превентивные меры, позволяющие не допустить массового вовлечения в них граждан. Банки ориентированы на усиленный мониторинг операций и разрыв деловых отношений с подозрительными клиентами. Прекращено и отказано в установлении деловых отношений со 179 подобными лицами. Для профилактики этих видов правонарушения в СМИ опубликовано свыше четырех тысяч материалов, постов и видеороликов, а также проведены SMS-оповещения населения. В регионах проведены выездные акции «Заң керуені», в ходе которых сотрудники прокуратуры и полиции в доступной форме довели до населения информацию о мерах предосторожности от финансовых пирамид и мошенничеств. Принятые меры позволили значительно сократить количество этих преступлений. В 2022 году число совершенных интернет-мошенничеств снизилось на 4%, мошенничеств, связанных с выдачей микрокредитов посредством сети интернет – на 28%, факты создания и руководства финансовыми пирамидами сократились на 27% [18].

В целях профилактических мероприятий постановлением Правительства РК №407 от 30 июня 2017 года была утверждена Концепция Кибербезопасности («Киберщит Казахстана») в рамках которой были усовершенствованы и законодательно закреплены нормы сферы информационной безопасности [19].

В стране также был определен уполномоченный орган в сфере защиты персональных данных – Комитет по информационной безопасности МЦРИАП РК.

Начиная с 2018 года для апробации механизмов реагирования на киберугрозы в рамках Национального антикризисного плана реагирования на инциденты информационной безопасности, проводятся командно-штабные учения с участием представителей заинтересованных государственных органов.

В 2018 г. Комитетом национальной безопасности Республики Казахстан был создан и начал работу Национальный координационный центр информационной безопасности (НКЦИБ), обеспечивающий защиту информационных ресурсов государственных органов и критически важной информационной инфраструктуры от кибератак и киберинцидентов [20].

В 2020 г. утверждены правила сбора и обработки персональных данных, которыми определен порядок и требования к обращению с персональными данными от стадии сбора до стадии их уничтожения.

В 2020 г. начата правоприменительная практика по привлечению к ответственности за нарушение требований по защите персональных данных на ЭИР (проверка в отношении оператора связи, субъектов частного предпринимательства) и законодательства об электронном документе и ЭЦП.

По мнению профессора Каиржанова Е.И. «Главным направлением в борьбе с преступностью является ее предупреждение. В криминологии предупреждение преступности рассматривается как многоуровневая система государственных и общественных мер, направленных на устранение, ослабление или нейтрализацию причин и условий преступности. Разработка мер предупреждения преступности – конечный результат и показатель эффективности всех криминологических исследований [21, с. 168-169].

Поэтому, мы считаем, что для борьбы с киберпреступностью необходимы новые подходы, основанные на широком использовании успехов науки и техники, международного сотрудничества в данной сфере с целью обеспечения безопасности и правопорядка, а также подготовка сотрудников нового поколения, в совершенстве владеющих навыками компьютерных технологий.

Противодействие киберпреступностьи, является глобальной проблемой в силу того, что данный вид преступления носит трансграничный характер. Поэтому для эффективной борьбы с киберпреступлениями считаем, необходимо не только принятие соответствующих нормативно-правовых норм на национальном уровне, но и выработка единых международных

стандартов, таких как определение круга деяний, подлежащих криминализации, выработка единого понятийного аппарата и единой терминологии, пересмотр существующих уголовно-правовых норм с учетом стандартов, установленных международно-правовыми документами.

Литература

1. Сералиева А.М. Киберпреступность: понятие, причины и предупреждение // ВЕСТНИК Серия «Юриспруденция» №4 (70), 2022. – С. 70-78.
2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. – С. 496.
3. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: Дис. … канд. юрид. наук. Красноярск, 2010 //[Электронный ресурс] – Режим доступа: https://www.dissercat.com/content/kompyuternye-prestupleniya-kak-raznovidnost-prestuplenii-informatsionnogo-kharaktera. Document (дата обращения: 11.08.23).
4. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: Дис. … канд. юрид. наук. Краснодар, 2009 //[Электронный ресурс] – Режим доступа: https://www.dissercat.com/content/ispolzovanie-spetsialnykh-poznanii-pri- vyyavlenii-i-rassledovanii-prestuplenii-v-sfere-kompy. Document (дата обращения: 12.08.2023).
5. Суслопаров А.В. Информационные преступления: Дис. … канд. юрид. наук. Красноярск, 2008 // [Электронный ресурс] – Режим доступа: https://www.dissercat.com/content/informatsionnye-prestupleniya. Document (дата обращения: 13.09.2023).
6. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис… канд. юрид. наук. Владивосток, 2005 // [Электронный ресурс] – Режим доступа: https://www.dissercat.com/content /kiberprestupnost-ponyatie-sostoyanie- golovno-pravovye-mery-borby. Document (дата обращения: 20.08.2023).
7. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: Дис. … канд. юрид. наук. М., 2013 // [Электронный ресурс] – Режим доступа: https://www.dissercat.com/content /kriminologicheskoe-i-ugolovno-pravovoe-obespechenie-preduprezhdeniya-kiberprestupnosti. Document (дата обращения: 22.08.2023).
8. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: Сравнительный анализ: Дис. … канд. юрид. наук. М., 2005 //[Электронный ресурс] – Режим доступа: //https://www.dissercat.com/content/prestupleniya-v-sfere-bezopasnosti-obrashcheniya-kompyuternoi-informatsii-sravnitelnyi-anali. Document (дата обращения: 23.08.2023).
9. Уголовный кодекс Республики Казахстан от 3.07.2014 № 226-v (с изм. и доп. по сост. на 12.09.2023) // [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document (дата обращения: 28.08.2023).
10. Oxford English Dictionary. URL: http:/ /www. askoxford.com.
11. Тропина Т.Л. Киберпреступность. – Владивосток, 2009. – С. 45-55.
12. Конвенция о киберпреступлениях принята Советом Европы. Серии европейских договоров. – № 185 от 23.10.2001. / [Электронный ресурс] – Режим доступа: https://rm.coe.int/1680081580 (дата обращения: 29.08.2023).
13. Каиржанова С.Е. Преступность в сфере банковской деятельности: Монография. – Алматы: Экономика, 2006. – С. 241.
14. МВД объявило охоту на хакеров // «Он и она». 2006. – №7.
15. Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия //Социально-политические науки. 2018. №1. – С. 135-137.
16. Курманова А. Требования к безопасности приложений финорганизаций ужесточат. 29.05.2023 · 16:15. //[Электронный ресурс] – Режим доступа: https://kapital.kz/gosudarstvo/116014/trebovaniya-k-bezopasnosti-prilozheniy-finorganizatsiy (дата обращения:29.08.2023).
17. Звонок из банка обернулся двумя кредитами для Петропавловца // [Электронный ресурс] – Режим доступа: https://news.mail.ru/incident

КЕГЕМБАЕВА ЖАНАР АМАНЖАНҚЫЗЫ
з.ғ.д., профессор
Қазақстан Республикасы ІІМ
М. Есболатов атындағы Алматы академиясы

САҒЫНБЕКОВА ГҮЛНАР МЕЙРХАНҚЫЗЫ
з.ғ.д., Алматы қ. мамандандырылған
ауданаралық экономикалық соты

ОТБАСЫЛЫҚ-ТҰРМЫСТЫҚ САЛАДАҒЫ ЗОРЛЫҚ-ЗОМБЫЛЫҚТЫ АЛДЫН АЛУДЫҢ КЕЙБІР МӘСЕЛЕЛЕРІ

Қазақстан Республикасы адам құқықтарын қорғаудың халықаралық стандарттарына қосыла отырып, отбасылық-тұрмыстық зорлық-зомбылық деңгейін жеке адамға қарсы елеулі құқық бұзушылық ретінде қарастыра отырып, оны төмендету бойынша белсенді қадамдар жасауда.

Қазақстан Республикасының Президенті Қ.-Ж. Тоқаев «Жаңа Қазақстан: жаңару мен жаңғыру жолы» Жолдауында «қоғамдағы зорлық-зомбылық деңгейін төмендету үшін жүйелі шаралар қабылдау керек. Бұл ретте, отбасылық-тұрмыстық қатынастар саласындағы құқық бұзушылықтарға тиімді қарсы тұру маңызды рөл атқарады. Бүгінде азаматтар мен қоғам белсенділері әйелдерге және балаларға зорлық-зомбылық көрсеткендердің жазасын қатайту қажеттігін жиі айтып жүр. Бұл мәселені жан-жақты зерделеп, біржола шешуді тапсырамын», – деп айтты [1].

Қазіргі заманғы отбасы көптеген қолайсыз, кейде тіпті криминогендік факторлардың аясында дағдарысты басынан кешіп отыр. Үйдегі (отбасылық-тұрмыстық) зорлық-зомбылық күш қолданудың басқа түрлерінен ерекшеленеді, өйткені жәбірленуші ол үшін тірек және ең жақын болуы керек адамдар тарапынан зорлық-зомбылыққа ұшырайды. Жәбірленуші ретінде туыстық немесе неке байланыстары бар, бірге тұратын, ортақ тұрғын үйі, мүлкі, өмір сүру құралдары бар адамдар, олар материалдық және моральдық жағынан тәуелді болып, өздеріне қарсы жасалған зорлық-зомбылық актілеріне әрдайым жауап бермейді. Осылайша олар зорлық-зомбылық жасаушының өз әрекеттері үшін жазасыздық сезімін дамытуға және заңсыз әрекеттерін жалғастыруға ықпал етеді.

Мұның бәрі кейбір жағдайларда тұрмыстық зорлық-зомбылық субъектісінің жәбірленушінің денсаулығына ауыр зиян келтіру немесе өлтірумен байланысты қылмыстарды жасауға әкеледі.

Тұрмыстық зорлық-зомбылық әртүрлі жағдайда күш көрсету, моральдық, сексуалдық, психологиялық, экономикалық түрде болуы мүмкін. Сондықтан зорлық-зомбылық жасаған тұлға мен жәбірленушінің арасындағы жасалған қатынастарды табиғатына қарай бөліп қарастыру қажет.

Тұрмыстағы зорлық-зомбылық іс-әрекеттерін келесідей жіктеуге болады:

1) ерлі-зайыптылар арасындағы зорлық-зомбылық;
2) балаларға немесе ортақ балаларға қатысты жасалған зорлық-зомбылық;
3) балалар тарапынан қарт туыстарына қатысты жасалған зорлық-зомбылық;
4) жынысына қарамастан бірге тұратын немесе бірге тұрған адамдар арасындағы зорлық-зомбылық;
5) отбасының жасы үлкен мүшелерінің кіші мүшелеріне қатыстыжасалған зорлық-зомбылық [2, 207 б.].

Кейбір зерттеушілер отбасылық-тұрмыстық қатынастарға қатысушылардың шеңберін кеңірек қарастырады. Мысалы, С.М. Рахметов отбасылық-тұрмыстық қатынастар отбасылық

және тұрмыстық қатынастарды қамтитынын негіздеп, көрсетеді. Мысалы, көршілер бір-бірімен тұрмыстық қатынастарда болады. Тиісінше, бір көршінің екіншісіне қатысты жасалынған зорлық-зомбылық отбасылық-тұрмыстық құқық бұзушылықтарға жатады [3, 207 б.].

Зорлық-зомбылықтың ұғымында адамдардың жоғары бір билікке иелену, талпыну, үстем болу, игеру немесе күрес жүргізу сияқты түсінік жатыр. Физикалық және психикалық ұғымдар тар мағынада денеге жарақат келтіру дептүсінсек, кең мағынада адамға келтірілген зиян (психикалық, идеологиялық, физикалық т.б.) немесе басқа бір жеке адамдарға не әлеуметтік топтарға қарсы жасалған мәжбүрлеудің кез келген шарасы деп түсінуге болады. Отбасылық-тұрмыстық саладағы құқық бұзушылықтардың сәтті алдын алу үшін, қолданыстағы терминдер нақты әрі бір мәнді болуы қажет.

Іс жүзіндегі заңнама келесідей анықтаманы береді: «Тұрмыстық зорлық-зомбылық – отбасы-тұрмыстық қатынастар аясында бір адамның басқаға (басқаларға) қатысты дене зардабын және (немесе) психикалық зардап келтіретін немесе келтіру қаупі бар құқыққа қарсы қасақана әрекеті (іс-әрекеті немесе әрекетсіздігі)» [4].

Сондай-ақ, осы Заңда араларында отбасылық-тұрмыстық қатынастар туындайтын адамдар нақты көрсетілгенін атап өткен жөн. Қазақстан Республикасының 2009 жылғы 4 желтоқсандағы «Тұрмыстық зорлық-зомбылық профилактикасы туралы» Заңының 1б. 2) тармағына сәйкес, мұндай адамдардың шеңберіне көршілер кірмейді. Сондықтан біз тек заңдастырылған отбасылық қатынастары бар немесе сол сияқты қалыптасқан, бірақ ресми заңдастырылмаған қатынастары бар адамдарды қарастырамыз.

Отбасылық байланыстар ең берік және отбасылық өмірге сырттан, соның ішінде қоғамдық институттар тарапынан шабуыл көп жағдайда жағымсыз деп қабылданады. Дегенмен, мұндай жақындықтың оң және теріс жағы бар. Сондықтан, көптеген зерттеушілер назар аударғандай, әдетте, отбасындағы зорлық-зомбылық қоғам үшін ең жасырын құбылыс болып қала береді [5].

Отбасылық-тұрмыстық қатынастар саласында ең қауіпті және жиі қолданылатын зорлық-зомбылықтың түрі – бұл физикалық зорлық-зомбылық. Бұл бір адамның отбасылық және тұрмыстық қатынастардағы басқа адамның анатомиялық және физиологиялық тұтастығына заңсыз, әлеуметтік қауіпті, кінәлі әсерінен тұрады. Физикалық зорлық-зомбылық заттарды қолдана отырып немесе жәбірленушімен тікелей байланыста бола отырып, дене жарақаты, ұрып-соғу, шапалақтау түрінде көрінеді. Физикалық зорлық-зомбылықтың салдары адам денсаулығына зиян келтіруге немесе физикалық ауырсынуға, сондай-ақ адам өліміне әкелуі мүмкін. Зорлық-зомбылық тек жәбірленушілердің құқықтарын бұзып қана қоймай, өскелең ұрпақ үшін теріс үлгі болып келеді.

Қазақстан Республикасының Қылмыстық кодексіне сәйкес үйдегі зорлық-зомбылықпен тікелей байланысты не уәжі мұндай зорлық-зомбылық болып табылатын жеке адамға қарсы қылмыстарға адам өлтіру (ҚК 99-бабы); аффект жағдайында жасалған адам өлтіру (ҚК 101-бабы); абайсызда қазаға ұшырату (ҚК 104-бабы); денсаулыққа қасақана ауыр немесе ауырлығы орташа зиян келтіру (ҚК 106, 107-баптары); қинау (ҚК 110-бабы); қажетті қорғаныс шегінен шығу кезінде денсаулыққа ауыр зиян келтіру (ҚК 112-бабы); денсаулыққа абайсызда зиян келтіру (ҚК 114-бабы); қорқыту (ҚК 115-бабы); зорлау (ҚК 120-бабы); сексуалдық сипаттағы зорлық-зомбылық әрекеттері (ҚК 121-бабы); он алты жасқа толмаған адаммен жыныстық қатынас және сексуалдық сипаттағы өзге де әрекеттер жасау (ҚК 122-бабы); жыныстық қатынас жасауға, еркек пен еркектің жыныстық қатынас жасауына, әйел мен әйелдің жыныстық қатынас жасауына немесе сексуалдық сипаттағы өзге де әрекеттерге мәжбүрету (ҚК 123-бабы); жас балаларды азғындық жолға түсіру (ҚК 124-бабы); бас бостандығынан заңсыз айыру (ҚК 126-бабы) және басқалары жатқызылуы мүмкін [6].

Статистика бойынша зорлық-зомбылық көбінесе әйел адамдар мен балаларға қатысты жасалады. Қазақстанда жыл сайын 400-ден астам әйел зорлық-зомбылықтан қаза табады, әрбір үшінші қылмыс әйелдерге қарсы жасалған (37,8%). Сонымен қатар, қазақстандық әйелдердің 15%-ы күйеуі әйеліне қол көтеруге құқылы деп есептейді. Ал ауылда әрбір бесінші әйел тұрмыстық зорлық-зомбылықты қалыпты деп санайды [7].

Отбасылық-тұрмыстық зорлық-зомбылықтың алдын алу мәселелеріне мемлекеттік деңгейде үлкен көңіл бөлінеді. Жоғарыда Аталған «Тұрмыстық зорлық-зомбылық профилактикасы туралы» Заң 3-ші тарауда жеке профилактика шараларын егжей тегжейлі реттеп, белгілеген.

Жеке профилактика шараларының мақсаты – тұрмыстық зорлық-зомбылыққа кінәлі адам тарапынан жаңа құқық бұзушылықтардың алдын алу, сондай-ақ оның құрбандарының қауіпсіздігін қамтамасыз ету болып табылады. К.Х. Рахимбердин мен М.Р. Гета атап өткендей, мұнда, өкінішке орай, тұрмыстық зорлық-зомбылыққа кінәлі адамның мінез-құлқының оң өзгеруі; оның зардап шеккендердің бұзылған құқықтары мен мүдделерін қалпына келтіруге қатысуын қамтамасыз ету; жәбірленушілерге оларды оңалту кезінде әлеуметтік, құқықтық, психологиялық және өзге де көмек көрсету сияқты мақсаттар айтылмаған [8, 67 б.].

Отбасылық-тұрмыстық зорлық-зомбылық қазіргі қоғамдағы ең өзекті мәселелердің бірі болып табылады.

Отбасылық-тұрмыстық зорлық-зомбылықтың алдын алудың бірінші және маңызды аспектісі – бұл мәселені түсіну және оны қоғамда жариялау. Мұндай зорлық-зомбылықтың зияны мен салдары туралы адамдарға оның белгілерін танып, оның пайда болуын болдырмау үшін шаралар қабылдау үшін хабарлау қажет.

Алдын алудың екінші аспектісі – отбасылық және тұрмыстық зорлық-зомбылық құрбандарына құқықтық және әлеуметтік қолдау көрсету. Жәбірленушілер қорықпай және оларға қолдау мен қорғаныс берілетініне сенімді болып, көмек сұрай алатындай тиімді қорғаныс және көмек жүйелерін құру маңызды.

Профилактиканың үшінші аспектісі – жанжалды шешу және эмоцияларды басқару дағдыларын дамыту үшін білім беру және тренингтер өткізу. Зорлық-зомбылық көбінесе отбасындағы қақтығыстарды шеше алмауынан туындайды. Арнайы тренингтер проблемаларды шешудің балама әдістерін ынталандыруға, агрессивтілікті азайтуға және салауатты қарым-қатынас орнатуды үйренуге көмектеседі.

Профилактиканың төртінші аспектісі – барлық мүдделі тараптардың – Үкіметтің, қоғамдық ұйымдардың, медициналық және білім беру мекемелерінің, отбасылардың және әр адамның жеке ынтымақтастығы. Тек бірлескен күш-жігермен ғана отбасылық-тұрмыстық зорлық-зомбылықтың алдын алуда елеулі прогреске қол жеткізуге болады.

Отбасылық-тұрмыстық зорлық-зомбылықтың алдын алудың маңызды аспектісі – зорлық-зомбылыққа ықпал етуі мүмкін әлеуметтік нормалар мен құндылықтардың өзгеруі. Қауіпсіздік пен үйлесімділік атмосферасын құру үшін қоғамдағы гендерлік теңдікті, сыйластықты, төзімділікті және эмпатияны насихаттау қажет.

Жалпы, отбасылық-тұрмыстық зорлық-зомбылықтың алдын алу кешенді тәсілді қажет етеді. Ол осы мәселе туралы хабардарлықты арттыруға, жәбірленушілерген қолдау көрсетуге, жанжалды шешу дағдыларын дамытуға арналған білім мен тренингтерге, барлық мүдделі тараптардың ынтымақтастығына және қоғамдық нормалар мен құндылықтарды өзгертуге негізделуі керек.

Әдебиет

1. «Жаңа Қазақстан: жаңару мен жаңғыру жолы»: Мемлекет басшысы Қ.-Ж. Тоқаевтың 2022 жылғы 16 наурыздағы Қазақстан халқына Жолдауы // https://adilet.zan.kz/kaz/docs/K22002022_1

2. Акимжанов Е.С. Правовая характеристика бытового насилия в Республике Казахстан //Государственная служба и кадры. – 2021. – №3. – 206-209 бб.

3. Рахметов С.М. Проблемы совершенствования законодательства Республики Казахстан по противодействию семейно-бытовому насилию // ҚР Заңнама және құқықтық ақпарат институтының жаршысы. – 2020. – №5 (63). – 127-134 бб.

4. Қазақстан Республикасының 2009 жылғы 4 желтоқсандағы №214-IV «Тұрмыстық зорлық-зомбылық профилактикасы туралы» Заңы //https://adilet.zan.kz/kaz/docs/Z090000214_

5. Әбдәлі А.А., Жұмашев М.А. Отбасылық-тұрмыстық қатынастар аясында жасалатын құқық бұзушылықтар // Мир закона, 2021: https://mir-zakona.kz/

6. Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілдедегі №226-V ҚРЗ // https://adilet.zan.kz/kaz/docs/K14000002266.

ОСМАНОВА ГҮЛАЙНА ЖАЛАЛЫҚЫЗЫ
Абай атындағы ҚазҰПУ, Тарих және құқық институты, «Құқықтану» кафедрасының аға оқытушысы, PhD докторы

БИЖАНОВА АЙГҮЛ РАБХАНҚЫЗЫ
Абай атындағы ҚазҰПУ, Тарих және құқық институты, «Құқықтану» кафедрасының қауымдастырылған профессоры, з.ғ.д.

БАС БОСТАНДЫҒЫНАН АЙЫРУ ТҮРІНДЕГІ ЖАЗАНЫҢ ӘЛЕУМЕТТІК САЛДАРЫ

Адамдардың белгілі бір қоғамдық қатынастар шеңберіндегі саналы іс-әрекеттері әрқашан мақсат қоюға, белгілі бір мақсаттарға жетуге бағытталады. Мұнда құқықтық нормалармен реттелетін қатынастар, әсіресе қылмыстық-құқықтық қатынастар ерекше орын алады деуге болады. Себебі, қылмыстық құқықтық қатынастардың мақсаты айқын. Отандық қылмыстық заңнамада заң шығарушы жазаның мақсатын нақтылап береді: әлеуметтік әділеттілікті қалпына келтіру, сотталған адамның және басқа адамдардың жаңа қылмыстық құқық бұзушылықтардың алдын алу, сотталған адамды түзеу.

Ғылыми еңбектерде қылмыстық-құқықтық аспектідегі әлеуметтік әділеттілік категориясы және оның мақсатқа жетудегі әсері толық зерттелмеген. Бұл ретте, жасалған қылмыстық құқық бұзушылықтар динамикасында әлі де болса жағымсыз тенденциялар байқалып отырғанын атап өткен жөн. Мысалы, Қазақстанда өткен жылы сотталғандар саны туралы ресми мәліметтер бойынша (N10 нысан) сотталғандар саны 27 061 (оның ішінде 443 кәмелетке толмағандар), 23 665 адам қылмыс жасағаны үшін сотталған, 3366 қылмыстық теріс қылық жасағаны үшін сотталушылар тіркелген [1].

Деректерге сүйенсек, елімізде қылмыс жасағаны үшін бас бостандығынан айыру жиі қолданылады және ол азаймай отыр. Қылмыстық-атқару жүйесі мекемелерінде 2022 жылы 34 473 адам ұсталса, 2023 жылдың 1 қаңтарындағы жағдай бойынша бас бостандығынан айыру орындарында 34 355 сотталушы жазасын өтеуде [2].

Соңғы жылдардағы пенитенциарлық реформаларға тоқталатын болсақ, сотталғандарды қылмыстық атқару мекемелерінде ұзақ уақыт оқшаулаудың қоғам мен азаматтар үшін маңызы шамалы екенін жиі естиміз. Бұл ретте сотталғандарға бас бостандығынан айыру жазасы қылмыстық заңдағы жазаның мақсатына жетуді қанша мерзімге қамтамасыз етеді деген сұраққа нақты жауап беру қиын. Сондықтан бұл арақатынасты бас бостандығынан айыру сияқты жаза түрін қысқарту және адамды қоғамнан оқшаулаумен байланысты емес жаза түрін көбейту арқылы өзгерту керек, оның үстіне бұл ұғымнан туындайтынын атап өткен жөн.

Сондай-ақ, ҚР Президентінің 2021 жылғы 15 қазандағы Жарлығымен бекітілген Қазақстан Республикасының 2030 жылға дейінгі құқықтық саясат тұжырымдамасында мемлекеттің қылмысқа қарсы іс-қимыл саласындағы саясаты – құқық бұзушылықтың маңызды бағыты екені атап көрсетілген. құқықтық саясат [3].

Қылмыстық құқық бұзушылық жасаған адам белгілі бір қиыншылықтарға немесе азаптауға ұшырауы мүмкін және бұл заңсыз және қоғамға қауіпті әрекетке мемлекет тарапынан орынды жауаптар болатыны сөзсіз.

Мұнда сот сотталған адамға жаза тағайындау арқылы жеке адамның, қоғамның немесе мемлекеттің мүдделеріне қылмыспен келтірілген зиянды ішінара немесе толық өтеуге мүмкіндік береді. Көп жағдайда жаза қолдану арқылы келтірілген зиянды толық өтеу мүмкін емес. Мысалы, адамның өлімі мен жарақатының орнын ешқандай материалдық құралдар өтей алмайды.

Әрине, қылмыстан зардап шеккен орындардың барлығы бірдей оңалтуға жатпайды. Қылмыстың салдарынан адам өлімі мен денсаулығын жоғалту жағдайларын ешбір жазамен жою мүмкін емес екені сөзсіз.

Қазақстандық ғалым Б.Шнарбаев: «Қылмыстық жаза әлі де болса онша ауыр емес қылмыстармен күресте кек алудың негізгі түрлерінің бірі болып қала береді. Сол себепті қылмыстар үшін қылмыстық жазаның шарасын таңдауда ойластырылған және сараланған көзқарастың болуы маңызды» [4, 65 б.].

Қасақана адам өлтіру үшін қылмыстық жазаның қалпына келтіру функциялары мүліктік аспектілерді жоққа шығармайды. Мысалы, С.В. Бородин, біздің ойымызша, аталған қылмыс үшін бас бостандығынан айыру түріндегі дәстүрлі жазаға қосымша айыппұл белгілеуді әділетті түрде ұсынады. Ол Ресей заңнамасына сүйене отырып, қасақана адам өлтірді деп айыпталушыны қайтыс болған адамның туыстарына материалдық және моральдық шығынды өтеуге міндетті етуді ұсынады [5, 95 б.].

Неліктен заң шығарушы қылмыстық жазаның мақсаты ретінде әлеуметтік әділеттілікті қалпына келтіруді енгізгені түсінікті. Әділ қылмыстық жаза жеке адам мен қоғам арасындағы қайшылықты шешудің өткір құралы және қоғамдағы ең маңызды, өмірлік маңызды қатынастарды барлық азаматтар үшін түсінікті және дұрыс бағалау бола отырып, қоғамға қазіргі құндылықтар жүйесін тез және анық көрсете алады. Керісінше, әділетсіз жаза жеткілікті түрде кең тараған кезде, ол бүкіл құндылықтар жүйесін тез деформациялауы мүмкін, сол арқылы қоғамның өзін өзгертеді. Бұл қылмыс жасалғанда ұсынылады. Қауіптілігі төмен қылмыстар үшін де бас бостандығынан айыру орынды, бірақ ол қылмыскердің жеке басына әсер ете алуы қажет. Қылмыскердің жеке басын ескеретін болсақ, онда оған жеткілікті жаза мөлшері бірқатар факторларға байланысты: сана деңгейіне, оның мәдениетіне, отбасы мен қоғамдағы орнына, ойлау тәсіліне және т.б. [6, 156 б.].

Қылмыстық жазаларды орындау тәжірибесі көрсетіп отырғандай, бас бостандығынан айыруға сотталғандардың түзелуінің негізгі өлшемі жазаны өтеу кезінде (пенитенциарлық қылмыс) немесе босатылғаннан кейін жаңа қылмыстық құқық бұзушылық жасау немесе жасамау фактісі (қылмыстық қылмыстың рецидиві) болып табылады.

Мемлекеттің міндеті, бір жағынан, жасалған қылмыстар үшін жазаның бұлтартпастығын қамтамасыз ету, ал екінші жағынан, сотталған адамды қоғамнан алшақтатпай, жазаны барынша әділ және тиімді ету, сотталған адам, сондай-ақ жалпы мемлекет үшін әлеуметтік зардаптарды барынша азайту болмақ.

Екіншіден, мекемеге орналастыру, ең алдымен, сотталғанды физикалық оқшаулауды білдіреді және репрессивтілікті арттырады, өйткені сотталғанға белгілі және маңызды заңдық шектеулер (еркін жүріп-тұру, жұмыс түрін таңдау мүмкіндігі, жұмыс және демалыс уақыты, туыстарымен қарым-қатынас және достар, т.б. шектеулер) қояды.

Үшіншіден, бас бостандығынан айыру жазасы сотталғанның өзіне ғана емес (қоғамнан оқшаулану, достарымен, әріптестерімен, тіпті туыстарымен байланысын үзу және басқалардың теріс бағалауы), сонымен қатар оның жақын туыстары мен достарына да қайғы-қасірет тудырады (көршілеріне, әріптестеріне, жұбайларына, балалардың сыныптастарына).

Төртіншіден, бас бостандығынан айыру түріндегі жазаның өзі белгілі бір жағымсыз салдарларды тудырады, көбінесе құқық қорғау органдарына тәуелсіз, нәтижесінде сотталушы тұлғасының елеулі деформациясы болады.

Бесіншіден, мекемелерде сотталғандардың болуы қоғамды қылмыстандыруға ықпал етеді.

Алтыншыдан, үкімдерді орындау мемлекет үшін өте қымбат.

2021 жылы Қазақстан Республикасының ҚАЖ мекемелерінде 33 217 сотталған жазасын өтеді, оның ішінде 15 505 адам, яғни 54%, бірінші рет сотталғандар; 13 204 адам немесе 46 пайызы бұрын сотталғандар.

Қылмыстық құқық бұзушылықтың теріс салдарын адамның жасаған қоғамға қауіпті іс-әрекеті үшін кінәлі ретінде жою түзеу мақсатының мазмұнына кірмегенімен, оны бейтараптандыру әсерін де көрсетуі керек. Бұл зардаптарды бейтараптандыру заңмен қорғалатын объектілерге келтірілген залалды жою арқылы мүмкін болады.

Біздің ойымызша, қылмыстық саясат жазалау бағытында емес, қылмыстық құқық бұзушылық жасаған адамның құқықтары мен заңды мүдделерін қалпына келтіру кепілдіктерін қамтамасыз ету бағытында дамуы керек. Сондықтан жаза тағайындау кезінде кінәлінің қылмыстық әрекетінен келтірілген зиянның көлемі мен деңгейін ескеру қажет. Осылайша біз жазаның әділдігіне жақындаймыз.

Бас бостандығынан айыру – қылмыс жасағаны үшін ғана тағайындалатын және сотталған адамды қоғамнан оқшаулайтын жазаның ең ауыр түрлерінің бірі.

Бас бостандығынан айыру қауіптілігі жоғары және қоғамнан оқшауланбай түзелмейтін қылмыс жасаған адамдарға қатысты.

Бас бостандығынан айыру – қылмыстық заңға белгілі ең ауыр жазалардың бірі. Осыған байланысты бұл жазаны оның басқа түрлерін пайдалана отырып, сотталушыны түзеу және жазаның мақсатына жету мүмкін болмаған жағдайда ғана қолдану керек [7, 264 б.].

Сотталғандарды түзеу және бостандықтағы қалыпты өмір сүру жағдайларына бейімдеу арқылы қылмыстық жазаларды жүзеге асырудың тиімділігін арттыруға болады.

Бас бостандығынан айыру түріндегі жазасын өтеген және осыған байланысты қажетті әлеуметтік байланыстарынан толық немесе ішінара айырылған сотталғандар қоғамда көптеген қиындықтарға тап болады. Олардың себептерін келесі жағдайлармен байланыстыруға болады: біріншіден, мұндай адамдардың біліктілігі төмен (олар өндіріске қызығушылық танытпайды және бұрынғы соттылығы туралы теріс имидждің қалыптасуы); екіншіден, меншік нысанына қарамастан кәсіпорындар мен ұйымдардың басшылары осы санаттағы адамдарды жұмысқа алуға мүдделі емес (экономикалық пайданың болмауы); үшіншіден, бұрынғы сотталғандар үшін дайындалған бос жұмыс орындарының төмен жалақысы, бұл соңғыларды қоғамдық өндірістен тыс жеңіл пайда іздеуге итермелейді; төртіншіден, олардың жеке басының терең моральдық-құқықтық деформациясы, сондай-ақ қылмыстық субмәдениет элементтерінің ықпалы және жазалау кезінде алынған тиісті мінез-құлық нормалары және басқалары оларға әсер етеді.

Ұзақ «түрмеде» отырудың жағымсыз салдары арасында мыналарды атап өтуге болады:

1) әлеуметтік (әлеуметтік байланыстардың жоғалуы, отбасының ыдырау қаупі, «әлеуметтік паразитизмнің» қалыптасуының бұрынғы дағдылары мен дағдыларын жоғалту);

2) экономикалық (Қазақстанда қылмыстық-атқару жүйесіне жұмсалған шығындар 10 жыл ішінде 4,5 есе өсті және 2013 жылы 47,5 млрд теңгені құрады. Бір тұтқынды ұстау мемлекетке жылына 613 мың теңге шығын әкеледі);

3) қылмыстық (түрме – қылмыс «фабрикасы», қылмыстық субмәдениеттің таралуы, қоғамның криминализациясы).

Бас бостандығынан айыру жазасының әлеуметтік салдары туралы мәселені толықтыра түссек:

Біріншіден, түзеу мекемесіне орналастыру, ең алдымен, сотталғанды өзіне таныс қоғамнан физикалық оқшаулауды білдіреді (бұл, әрине, бірінші рет бас бостандығынан айыруға сотталған адамдарға қатысты). Сонымен қатар, бас бостандығынан айыру өте репрессивті сипатқа ие, өйткені ол сотталғанға еркін жүріп-тұру, жұмыс түрін, жұмыс және демалыс уақытын таңдау мүмкіндігі, туыстарымен қарым-қатынас жасау сияқты белгілі және елеулі заңдық шектеулер қоюмен байланысты және т.б. Сот үкімімен бас бостандығынан айыру орындарындағы азаматтардың сайлауға және сайлануға құқығы жоқ (ҚР Конституциясының 33-бабы, 3-бап).

Екіншіден, бас бостандығынан айыру сотталғанның өзіне ғана емес (қоғамнан оқшаулану, достарымен, әріптестерімен, тіпті туыстарымен байланысын үзу), сонымен қатар оның жақын туыстары мен достарына (көршілеріне, әріптестеріне, жұбайларына, балаларының сыныптастарына және т.б. теріс. бағалаулар) да зардап шегуде.

Үшіншіден, ғалымдардың пікірінше, бас бостандығынан айыру қылмыскерге оң ықпал ету құралы бола отырып, көбінесе құқық қорғау органдарына тәуелді емес белгілі бір жағымсыз салдарларды тудырады. Яғни, оның түзеу мекемесінде болуы кезінде әртүрлі факторлардың әсерінен сотталғанның жеке басының елеулі деформациясы орын алады.

Белгілі ғалым В.Н. Кудрявцев адамдарды бас бостандығынан айыру орындарында оқшаулаудың парадоксының бірі олардың қылмыстар мен түзеу үшін орналастырылуы, жаңа қылмыстар, кейде онша ауыр емес қылмыстар жасауы екенін атап көрсетті. Бұл деректер, ғалымның айтуынша, қылмыскерлерді қоғамнан оқшаулау арқылы түзеу жұмыстарының тиімсіздігі мен әлсіздігін тағы бір рет көрсетеді. Одан әрі В.Н. Кудрявцев қылмыскерді қоғамнан оқшаулау стратегиясы ескірген дейді [8, 196 б.]

Төртіншіден, түзеу мекемелерінде адамдардың болуы, әдетте, сотталған адамның жеке басының нашарлауына, оған субмәдениеттің әсер етуіне және тұтастай алғанда қоғамның криминализациялануына ықпал етеді. Осылайша, еліміздің тәуелсіз даму жылдарында қылмыстық-атқару жүйесі мекемелерінен бір жарым миллионнан астам адам өтті. Сондықтан қолданыстағы қылмыстық заңнамаға жаза түрлері бойынша өзгерістер енгізу кезінде түзеу мекемелеріне жіберілетін адамдардың санын мүмкіндігінше шектеу мүмкіндігіне назар аудару қажет. Қылмыстық сот ісін жүргізуге азаматтардың тартылуын азайту, қоғамнан оқшаулаумен байланысты емес қылмыстық-құқықтық шараларды кеңінен қолдану үшін жағдай жасау туралы айтылады.

Бесіншіден, сотталғандардың көптігі ел беделіне кері әсер етеді. 1998 жылға дейін Қазақстан түрмедегі саны бойынша әлемде АҚШ пен Ресейден кейінгі үшінші орында тұрған.

Алтыншыдан, бас бостандығынан айыру сияқты жазаның бұл түрін белсенді қолдану экономикалық зардаптарға әкеледі. Егер аталған мәселені қарастыратын болсақ, онда бас бостандығынан айыру сияқты жазаның бұл түрін жүзеге асыру үшін мемлекеттің тікелей шығындары өте үлкен екенін ескерген жөн.

Қорыта келгенде, бас бостандығынан айыру орындарынан босатылған және пробациядағы азаматтарды әлеуметтік оңалту мынадай бағыттар бойынша жүргізілгені абзал:

– Қазақстан халқының саны аз және аумағы үлкен болған жағдайда мемлекет қылмыстық құқық бұзушылық жасағаны үшін сотталған және бас бостандығынан айыруға сотталған әрбір азаматы үшін күреседі және оларды қоғам мен мемлекетке ең аз шығынмен қызмет етуге қайтаруға тырысады;

– бас бостандығынан айыру түріндегі жазаны орындау тәртібін қайта қарастыру арқылы жаңа үлгі жасау;

– сотталғандарды жұмысқа орналастыру және оқыту мәселелерін қайта қарау керек.

Өндірістік қатынастар жүйесін жазаны орындаудың прогрессивті жүйесімен, сондай-ақ шартты түрде мерзімінен бұрын босату шарттарымен байланыстыру орынды болады, ал бұл қылмыстық жазаның мақсаттарын жүзеге асырудың тиімділігіне оң әсер етеді.

Үкімді орындаудың тағы бір маңызды құрамдас бөлігі – бас бостандығынан айыру түріндегі жазаны өтеу.

Үкімді орындау кезіндегі тәрбие сотталған адамды түзеудің маңызды құралы ғана емес, сонымен қатар сотталған адамға оларды еңбекпен қамтамасыз ету және еркін өмір сүруге бейімдеу үшін қажетті дағдыларды меңгеруге мүмкіндік береді.

Сотталғандарды түзетудің басқа негізгі құралдарына қарағанда тәрбиенің басымдығы қандай?

Біріншіден, білім беру сотталғандарды жұмысқа орналастыру мәселесін шешуді қамтамасыз етеді.

Екіншіден, жазаны өтеу кезінде және бостандыққа шыққаннан кейін ғана емес, қылмыстық-атқару жүйесі жағдайында білім алу тек жұмысқа орналасу (еңбек ретінде оқу) сияқты маңызды мәселені шешуге көмектеседі.

Үшіншіден, тәрбие жүйесі арқылы мекеме әкімшілігі сотталғандармен тиімді тәрбие жұмысын жүргізе алады, себебі сотталғандармен дұрыс ұйымдастырылған тәрбиелік іс-шаралар барысында заңға бағыну мінез-құлқын қалыптастыруға бағытталған тәрбие жұмыстары да жүргізіледі.

Сотталғандарды орта білімнен кейінгі және жоғары білім беру бағдарламалары бойынша оқытуды, сондай-ақ жеке жұмысшы кәсіптері бойынша оқытуды және қайта даярлауды енгізу қажет. Оқытудың әртүрлі формалары болуы мүмкін, яғни күндізгі, сырттай және қашықтықтан оқыту.

ҚР ҚК-нің 123-бабының 2-бөлігінде білім беру мәселелері бойынша жергілікті атқарушы органдармен өзара іс-қимыл жасау қажеттігі көрсетілген. Осылайша, сотталғандарға техникалық және кәсіптік білім беруді ұйымдастыру бойынша кәсіптер мен мамандықтардың тізбесін еңбек нарығының мониторингін ескере отырып, жергілікті атқарушы органдармен келісім бойынша мекеме әкімшілігі қалыптастыратыны көрсетілген.

Төртіншіден, бас бостандығынан айыруға сотталғандардың көші-қонының жоғары болуын ескере отырып (жыл сайын ҚАЖ мекемелеріне 5-10 мыңға жуық сотталғандар келіп-кетеді), мекемелерде оқытуды дұрыс ұйымдастыру адамдардың үлкен тобын қамтуға мүмкіндік береді.

Бесіншіден, мекемелерде сотталғандарды тәрбиелеу мәселелерін тиімді ұйымдастыру мақсатында мемлекет сотталғандарды қолдаудың және оқу-тәрбие процесін ынталандырудың материалдық нысандарын қамтамасыз етеді. Яғни, сотталғандарды мекемелерде оқытуды қоғамдық пайдалы еңбектің міндетті түрлерінің біріне айналдыруға болады, өйткені қылмыстық-атқару жүйесі мекемесінде оқу арқылы сотталған адам өзіне ғана емес, бүкіл мемлекетке де пайдалы болады.

Әдебиет

1. Құқықтық статистика деректері // https://qamqor.gov.kz/crimestat/.
2. Бейнебақылау тұтқынды да, бақылаушыны да тәртіпке келтіреді. 19 сәуір, 2021 жыл. - [Электрондық ресурс]. https://kznews.kz/zhanalyqtar/bejnebaqylau-qamaudagyny-da-qadagalaushyny-da-tartipke-keltiredi/ Жүгінген күні: 11.01.2023 ж.
3. Қазақстан Республикасы Президентінің 2021 жылғы 15 қазандағы No 674 Жарлығы. Қазақстан Республикасының 2030 жылға дейінгі құқықтық саясат тұжырымдамасы: 2021 жылғы 15 қазанда бекітілген No 674 // https://adilet. zan.kz/kaz/docs/U2100000674.
4. Шнарбаев Б.К. Преступления небольшой тяжести и уголовные проступки: монография. – Костанай: Костанайский филиал ФГБОУ ВО «Челябинский государственный университет», 2018. – С. 202.
5. Бородин С.В. Вопрос о возмещении ущерба за умышленные преступления // Государство и право. – 1994. №4. – С. 95.
6. Османова Г.Ж. Бас бостандығынан айыру түріндегі жаза ұғымына заманауи теориялық көзқарас // Қазақстан ғылымы және өмірі. – 2020. – No 12/2 (148). – 155-159 б.
7. Османова Г.Ж. Бас бостандығынан айыру түріндегі жазаның қылмыстық-құқықтық сипаттамасы // Инновационно-предпринимательское образование в контексте повышения качества жизни: матер. Междунар. науч.-практ. конф. 12 декабря 2018 г. – Алматы, 2019. – Б. 263-266.
8. Кудрявцев В.Н. Стратегии борьбы с преступностью. – М.: Юрист, 2003. – С. 349.

КЫЗДАРБЕКОВА БАЯН ЖАКЕНОВНА
Ведущий научный сотрудник отдела уголовного, уголовно-процессуального, уголовно-исполнительного законодательства Института законодательства и правовой информации Республики Казахстан, к.ю.н., ассоциированный профессор

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРЕСТУПНЫХ ЦЕЛЯХ: ПОСТАНОВКА ПРОБЛЕМЫ И ПРЕДПОСЫЛКИ ВВЕДЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Концепцией правовой политики Республики Казахстан до 2030 года, утверждённой Указом Президента Республики Казахстан от 15 октября 2021 года №674, предусмотрено совершенствование уголовного законодательства с учетом современных вызовов и угроз, в том числе с использованием IT-технологий, «включительно путем введения отдельного состава правонарушения, предусматривающего ответственность за применение искусственного интеллекта в преступных целях». Заданное Концепцией направление является подтверждением признания казахстанским обществом угроз, которые стали нарастать с поступательным развитием технологий искусственного интеллекта *(далее – ИИ)*. Это, в свою очередь, ставит перед уголовно-правовой наукой задачу выработки теоретически выверенных подходов в криминализации поведенческих актов, совершенных с применением ИИ.

Несмотря на злободневность проблемы уголовно-правовых рисков, связанных с применением ИИ, она не получила достаточного освещения в отечественной юридической литературе. В последние годы повышенный интерес к ней проявляют российские ученые-юристы, анализ работ которых позволяет обозначить определенные парадигмы и подходы к: определению круга деяний с использованием ИИ, требующих уголовно-правового реагирования; роли, которую играет ИИ в составе уголовного правонарушения: субъекта, предмета и потерпевшего. Наиболее важные из них, с нашей точки зрения, могут быть взяты за основу при разработке единой теоретической модели уголовно-правовой защиты указанной области общественных отношений в Казахстане.

Современные исследователи в области уголовного права, заявляющие о необходимости разрешения вопросов уголовно-правовой ответственности за вред, причиненный системами ИИ и робототехники, справедливо утверждают, что решение этого вопроса невозможно без уяснения оснований к их криминализации. По справедливому утверждению И.А. Филипповой, наблюдаемая распространенность случаев использования ИИ для совершения преступлений, в том числе посягательств на программное обеспечение беспилотника, являются основанием для уголовно-правового регулирования этой относительно новой группы общественных отношений [1]. Аналогичное мнение высказывается и другими учеными [2].

Указывая на наличие всех предпосылок к криминализации новых деяний с применением ИИ, ученые-юристы, тем не менее, придерживаются разных позиций в таких вопросах, как: круг деяний в рассматриваемой сфере, ответственность за которые следует криминализировать; кто должен выступать субъектом преступления.

Как показал анализ норм действующего УК РК, использование технологий (систем) ИИ в совершении уголовного правонарушения не отнесено ни к отягчающим обстоятельствам, ни к квалифицированным видам уголовных правонарушений. Отсутствуют также и специальные уголовно-правовые нормы, посвященные ИИ.

Вместе с тем эксперты в области уголовного права отмечают, что технологии ИИ могут быть использованы в качестве инструмента для облегчения совершения общественно опасного деяния либо в качестве орудия преступной деятельности: для совершения киберпреступлений (кибератаки с применением вирусных программ, программ шпионов и т.п.; применении роботов-дронов с алгоритмами ИИ в целях совершения террористических преступлений, доставки наркотических средств и других запрещенных предметов – оружия, взрывчатых веществ, взрывных устройств [3]. Кроме этого, они могут быть использованы для вторжения в частную жизнь человека, совершения убийства, а также многих других деяний: против собственности, общественной, военной безопасности и т.д. Также практике известны случаи, когда ИИ выступал в качестве средства совершения преступления. Например, использование синтезированной речи для того, чтобы выдать себя за другого человека.

Одним из наиболее популярных способов использования технологий (систем) ИИ в криминальных целях являются дипфейки, представляющие собой синтезированные с помощью ИИ видео, аудио или изображения, которые могут выглядеть очень реалистично и создаются путем объединения и смешивания существующего контента. Хотя дипфейки имеют потенциально полезные применения, такие, как создание спецэффектов в фильмах или улучшение видеосвязи, они также могут быть использованы для преступных целей. Дипфейки могут использоваться для создания и распространения: видео или аудио сценариев, чтобы обмануть людей, выдавая их за других, и затем попросить их предоставить финансовую информацию или совершить денежные переводы; ложной информации - видео с фальшивой информацией о политиках, знаменитостях или других публичных личностях с целью влиять на общественное мнение или создания дезинформации; поддельных компрометирующих видео или фотографий и распространения их в интернете; поддельных видео или аудио, чтобы представить себя в виде другой личности и получить доступ к защищенной информации или взаимодействовать с целью шпионажа; видео или аудио, в которых изображается человек, совершающий угрозы или шантажирующий других с целью вымогательства.

В юридической литературе вопрос о том, какие уголовные правонарушения совершаются при помощи ИИ, решается по-разному. Одни указывают довольно узкий круг ситуаций, в которых использование ИИ повлекло за собой вред объектам уголовно-правовой охраны, а другие, предлагая довольно широкий перечень, не обосновывают необходимость их криминализации в достаточной мере. Так, И.Р. Бегишев полагает, что общественно опасными являются следующие деяния: «конструирование робота-убийцы специально для совершения правонарушения; отключение программных и аппаратных функций, блокирующих возможность причинения вреда человеку; конструирование робота, способного причинить вред человеку; конструирование робота без осознания того, что он может быть использован для причинения вреда человеку» [2].

По нашему мнению, выделение в качестве самостоятельных деяний таких, как конструирование робота-убийцы специально для совершения правонарушения и конструирование робота, способного причинить вред человеку, является излишним. Поскольку оба этих деяний посягают на личность, правильнее было бы их не разделять.

И.Р. Бегишевым приводятся также примеры, в которых использование ИИ повлекло за собой причинение вреда человеку по неосторожности: «… наезд на пешехода беспилотным транспортным средством; столкновение с беспилотным летательным аппаратом; сбой в работе промышленного робота, повлекший несчастный случай с работником; отказ в работе той или иной системы медицинского робота, повлекший смерть пациента или серьезное нарушение функционирования организма человека» [2]. Несмотря на то, что автору удалось смоделировать ряд возможных ситуаций причинения вреда охраняемым уголовным законом

общественных отношений при эксплуатации ИИ с умышленной и неосторожной формах вины, тем не менее, им не предлагаются конкретные пути решения проблемных вопросов.

Характерно, что в статье, написанной И.Р. Бегишевым совместно с З.И. Хисамовой «Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты», представлен более широкий перечень ситуаций, требующих уголовно-правового регулирования: «при создании системы ИИ была допущена ошибка, приведшая к последствиям; в систему ИИ был осуществлен неправомерный доступ, повлекший повреждение или модификацию его функций, вследствие чего было совершено преступление; ИИ, обладающий способностью к самообучению, принял решение о совершении действий/бездействий, квалифицируемых как преступление; ИИ был создан преступниками для совершения преступлений» [4].

Допуская все описываемые в литературе ситуации, при которых ИИ причиняется вред объектам уголовно-правовой охраны, особо хотелось бы остановиться на двух из них: 1) когда лицо неправомерно воздействуют на систему ИИ путем повреждения и модификации его функций, в результате чего совершено уголовное правонарушение; 2) когда ИИ специально создан для совершения уголовных правонарушений. Как нам представляется, эти ситуации являются схожими и разница между ними только в том, что в первом случае преступники вносят изменения в уже созданную программу ИИ, в то время как во втором случае система ИИ изначально разрабатывается для совершения уголовных правонарушений. То есть и в первой, и во второй ситуации ИИ используется в качестве средства или орудия совершения уголовного правонарушения. Это означает, что к уголовной ответственности в данных случаях должно подлежать лицо, использовавшее ИИ в преступных целях.

В подтверждение этого можно привести следующие примеры из практики стран, в которых беспилотные дроны введены в официальную эксплуатацию: лицо оснащает дрон программой, чтобы причинить конкретный вред человеку; использование беспилотных летательных аппаратов (далее - БПЛА) для совершения террористического акта (в 2018 г. в Ингушетии была задержана организованная группа, занимавшаяся подготовкой взрывов зданий территориальных подразделений МВД и ФСБ с помощью БПЛА) [5] и покушение на людей [6]; беспилотник следит за тем, как люди вводят ПИН-код банкомата [6]; беспилотник используется для передачи наркотических или психотропных веществ; для съемки чужой частной жизни [6] и т.д. Также практике известны случаи, когда ИИ выступал в качестве средства совершения преступления. Например, использование ботов для производства фейковых видеоклипов с целью политических манипуляций; использование синтезированной речи для того, чтобы выдать себя за кого-то» [7].

Из вышеизложенного следует, что использование технологий (систем) ИИ характерно для довольно обширного круга уголовных правонарушений. Их повышенная опасность заключается в том, что действия виновного лица, использовавшего высокотехнологичный способ, причиняют или могут причинить больший вред гражданам и обществу по сравнению с вредом от совершения деяния без их применения. Поэтому прав М. Брандидж, утверждающий, что полный спектр воздействия ИИ на безопасность огромен – «… будь то на уровне преступников, которые настроят машины на взлом или фишинг информации у отдельных лиц, или же это будет внедрение в частную жизнь путем слежения, профилирования личности и дальнейших репрессий» [7]. В дополнение хотелось бы добавить, что ИИ значительно облегчает совершение уголовных правонарушений, снижая риск разоблачения людей, которые в отдельных случаях могут формировать и задавать им криминальные цели и задачи.

В вопросе криминализации деяний, совершаемых с использованием ИИ, важным является поиск ответа на вопрос о том, кто должен признаваться субъектом уголовного правонарушения тогда, когда деяние совершено в результате допущенной ошибки в системе ИИ или самообучаемой программой. Как справедливо отмечается в литературе, разработчики и обладатели ИИ не стремятся причинить какой-либо вред, а самообучаемость программ

может привести к неожиданной деятельности, наносящей какой-либо вред, даже если разработчиками такой вариант развития событий специально не предусматривался и не учитывался.

Поскольку ИИ не может являться субъектом уголовного правонарушения, важным является установление причинно-следственной связи между деятельностью ИИ и действиями (бездействиями) производителя, пользователя или иного лица, незаконно вмешавшегося в работу ИИ. Для этого сначала нужно установить сам факт причинения вреда действиями (бездействиями) ИИ, а уже затем выяснять наличие либо отсутствие причинно-следственной связи между действиями (бездействиями) программиста, производителя, пользователя, иного лица и причинившими вред действиями (бездействиями) ИИ. Безусловно, что если причиной наступивших последствий от действий (бездействий) ИИ явилась ошибка программиста, производителя, то квалифицироваться они должны как деяния, совершенные по неосторожности. Ответственность в зависимости от последствий в этих случаях может быть предусмотрена гражданским, административным и уголовным законодательством.

Вместе с тем на создателей и пользователей ИИ необходимо возложить обязанность по предупреждению и минимизации рисков наступления негативных последствий его использования. В последние годы участились случаи, когда ИИ причинен вред охраняемым законом отношениям ввиду недостаточной компетентности или необоснованного риска человека (программиста, производителя, пользователя) либо неправомерного вмешательства постороннего лица. Так, в СМИ описываются ситуации, в которых говорится о предложенных ИИ некорректных методах лечения, повлекших за собой последствия в виде вреда здоровью различной степени тяжести или смерть [8] и др. Большинство авторов высказывают убежденность в том, что в этих случаях ответственность должна быть возложена на производителя, продавца или пользователя продукции, оснащенной ИИ; иные лица [9, с. 461]. Указывается, что самостоятельность ИИ и самообучаемых нейронных сетей относительна, поскольку алгоритм их действий создается человеком [10, с. 51]. Однако по справедливому утверждению отдельных ученых, «разработчики и обладатели ИИ не стремятся причинить какой-либо вред… самообучаемость программ может привести к неожиданной деятельности, наносящий какой-либо вред, даже если разработчиками такой вариант развития событий специально не предусматривался и не учитывался» [11].

Так, к примеру, если авария с участием беспилотного автомобиля, повлекшая вред здоровью или смерть человеку, явилась следствием ошибок в программном обеспечении, то ответственность в этом случае будет возложена на разработчика программы или производителя, при условии наличия вины в форме неосторожности. Ответственность разработчика или производителя здесь может наступить по статье 306 «Выпуск или продажа товаров, выполнение работ либо оказание услуг, не отвечающих требованиям безопасности» УК РК.

Также существует точка зрения, в соответствии с которой субъектом преступления может быть признан сам ИИ [12]. Данную позицию мы не разделяем в силу следующего. Во-первых, уголовная ответственность в нынешней ее конструкции никак не может быть приспособлена для применения в отношении технологии, наделенной ИИ. Так, в соответствии с ч. 1 ст. 15 УК РК уголовной ответственности подлежит физическое лицо. Во-вторых, даже если законодательно закрепить за технологией (системой) ИИ права и обязанности и предусмотреть для них соответствующую уголовную ответственность, то непонятно, каким образом под нее будет переустроен механизм достижения целей уголовного наказания. В-третьих, тезис о том, что ИИ, в систему которого была введена задача причинения вреда охраняемым объектам уголовно-правовой охраны, не может рассматриваться как субъект уголовного правонарушения, подтверждается также и тем, что компьютерная программа не обладает психикой и сознанием, являющимися обязательными при установлении вменяемости и вины.

Примечательно, что в зарубежной литературе по этому вопросу также приводятся диаметральные мнения. По мнению одних ученых, признание ИИ субъектом преступления невозможно вследствие того, что преступное поведение и ментальный элемент (внутренняя сторона), являющиеся обязательными элементами преступления, никак не характерны для ИИ [13, с. 178]. Другие же не только допускают привлечение ИИ к уголовной ответственности, но предлагают предусмотреть для них такие виды наказания, как деактивация, перепрограммирование или наделение статусом преступника привлечения роботов и ИИ к уголовной ответственности. Аргументом в пользу подобного подхода выступает усложнение, децентрализация, автономизация технологий ИИ, которые создают ряд проблем для человека, осуществляющего контроль над такими технологиями: человек, даже управляющий системой ИИ, не всегда способен полностью контролировать все действия и реакции системы, а тем более предугадать её поведение [14, с. 99].

Принимая доводы первой группы ученых, мы подвергаем сомнению состоятельность выдвигаемых решений о необходимости отнесения ИИ к субъектам уголовного правонарушения. Даже с учетом автономности и децентрализованности некоторых современных систем ИИ, нельзя не принимать во внимание тот факт, что принцип субъективного вменения, закрепленный в действующем уголовном праве, может касаться только физических лиц. В качестве дополнительного аргумента против критикуемой позиции мы также хотели бы обратить внимание на отмечаемое многими экспертами такое свойство системы ИИ, как непрозрачность, т.е. неясность, каким образом система производит выбор того или иного решения [15, с. 99].

Не вдаваясь в полемику по вопросу о том, кто должен нести ответственность за вред, причиненный в результате применения ИИ, отметим, что мы разделяем широко распространенное мнение о необходимости признания таковыми *разработчика, оператора, владельца либо лицо, ответственное за его эксплуатацию.* В то же время нельзя забывать, что в настоящее время уголовная ответственность предусмотрена только для физических лиц, т.е. рассматривать разработчика ИИ в качестве субъекта данных деяний мы можем, как уже отмечали ранее, только в рамках статьи 306 «Выпуск или продажа товаров, выполнение работ либо оказание услуг, не отвечающих требованиям безопасности» УК РК. Поэтому данное обстоятельство выступает дополнительным аргументом в пользу рассмотрения вопроса о введении уголовной ответственности юридических лиц.

Таким образом, появление и развитие новых интеллектуальных компьютерных систем не только качественно меняет сферы общественной жизни, но и приводит к использованию их в преступных целях. Основанием криминализации деяний с применением технологий (систем) ИИ является достаточный уровень их общественной опасности (причиняют вред или создают опасность его причинения), обусловленный, прежде всего: объектом посягательств, причинением реального ущерба или созданием возможности его причинения.

Литература

1. Филипова И.А. Правовое регулирование искусственного интеллекта: учебное пособие [Электронный ресурс] // URL: http://old.lib.unn.ru/students/src/2836.pdf (дата обращения: 21.07.2023).

2. Бегишев И.Р. Социальная обусловленность уголовно-правового регулирования общественных отношений, связанных с робототехникой и киберфизическими системами [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/sotsialnaya-obuslovlennost-ugolovno-pravovogo-regulirovaniya-obschestvennyh-otnosheniy-svyazannyh-s-robototehnikoy-i (дата обращения: 21.07.2023).

3. Антонова Е.Ю. Технологии искусственного интеллекта - субъект преступления или орудие / средство совершения преступления? [Электронный ресурс] // URL: https://elibrary.ru/item.asp?id=47918676i (дата обращения: 21.07.2023).

4. Хисамова З.И., Бегишев И.Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты [Электронный ресурс] // URL: file:///C:/Users/user%204/Downloads/23051.pdf (дата обращения: 21.07.2023).

5. Террокоптер: как бандиты с помощью дрона хотели взорвать МВД и ФСБ [Электронный ресурс] / URL: https://ria.ru/20180207/1514160209.html (дата обращения: 21.07.2023).

6. 25 преступлений с использованием дронов Электронный ресурс] // URL: https://formaxfun.com/top-25-prestuplenij-s-ispolzovaniem-dronov/ (дата обращения: 21.07.2023).

7. Три угрозы человечеству, которые несет искусственный интеллект [Электронный ресурс] // URL: https://www.bbc.com/russian/features-43139404 (дата обращения: 21.07.2023).

8. Коленов С. ИИ-онколога IBM Watson уличили во врачебных ошибках 27 июля [Электронный ресурс] // URL: URL: https://hightech.plus/2018/07/27/ii-onkologa-ibm-watson-ulichili-vo-vrachebnih-oshibkah (дата обращения: 21.07.2023).

9. Мосечкин И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник СПбГУ. Право. – 2019. – Т. 10. – Вып. 3. – С. 461-476.

10. Васильев, А. А. Правовое регулирование робототехники и искусственного интеллекта в Европейском Союзе // Российско-азиатский правовой журнал. – 2019. – № 1. – С. 50-54.

11. Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования [Электронный ресурс] // URL: http://vestnik43.ru/assets/mgr/docs/ /mosechkin-maket-itog.pdfl дата обращения: 21.07.2023).

12. Аверинская С.А. Создание искусственного интеллекта с целью злонамеренного использования в уголовном праве Российской Федерации [Электронный ресурс] // URL: http://vestnik43.ru/assets/mgr/docs/ /mosechkin-maket-itog.pdfl (дата обращения: 21.07.2023).

13. Hallevy G. The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control / G. Hallevy // Akron Intellectual Property Journal. – 2010. –Vol. 4, iss. 2. – P. 171-201.

14. Хисамова, З. И. Сущность искусственного интеллекта и проблема определения правосубъектности // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2020. – № 2. – С.96–106.

15. Искусственный интеллект – непрозрачность алгоритмов беспокоит экспертов [Электронный ресурс] // URL: https://rossaprimavera.ru/news/867e30a6 (дата обращения: 21.07.2023).

РОЗЕНКО СТАНИСЛАВ ВАСИЛЬЕВИЧ
Руководитель Высшей школы права Югорского государственного университета,
к.ю.н., доцент

УГОЛОВНОЕ ПРАВО, НАКАЗАНИЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ

Актуальность проблематики исследования взаимодействия уголовного права и кардинально развивающегося искусственного интеллекта обоснована тем, что данный фундаментальный вопрос в науке уголовного права нуждается в новом осмыслении, потому что развитие информационных и цифровых технологий в настоящее время позволяет утверждать, что появились не только количественные, но и качественные преобразования в области информации, которые нуждаются в соразмерной уголовно-правовой охране, а также следует учитывать те обстоятельства, которые обуславливают неизбежные и кардинальные изменения в уголовном праве, базирующиеся на развитии феномена искусственного интеллекта.

На текущий момент, примерно 77% жителей планеты используют услугу и устройство с искусственным интеллектом, который стал повседневной реальностью для представителей человеческого сообщества. Генезис цифровых технологий определяет изменения наиболее важных областей человечества. Искусственный интеллект – это вызов для государства, поскольку оно не может в полной мере осуществлять правовое регулирование цифровых технологий, а также для общества, которое получило субъект, задача которого содействовать жизнедеятельности людей, что постепенно превращается в функцию ограничения и контроля. Поскольку ИИ вносит в развитие человеческой цивилизации кардинальные перемены, то уголовное право как инструмент защиты должно быть готово предложить выверенные правовые конструкции правовой охраны, с учётом будущих изменений.

Человечество в виде ИИ создаёт себе помощника, но всякое благо может быть использовано по разному, в том числе и во зло. Поэтому ИИ это данность, а каким он станет, зависит от нас, но изначально, это не враг, а инструмент.

В этой связи, есть о чем думать, есть о чем рассуждать, и есть что предложить. Мы должны реагировать на процесс генезиса ИИ в области уголовного права, поскольку в этой случае возможные революционные преобразования и необходимо предупредить отрицательные последствия.

Мы живем в период мобилизационного управления, когда технологии и информация быстро меняются. В качестве одного из последствий данных процессов является то, что уголовное законодательство переживает многочисленные изменения и дополнения. Без доступа к информации жить сложнее, но тогда необходимо обсудить проблематику уголовного наказания, где будет применяться лишение доступа лица к определённой информации, а также создание модели усиленного контроля лица, совершившего преступление.

Развитие искусственного интеллекта (далее – ИИ) – это не только новое явление в правовом регулировании, но и вызов в преодолении консервативности уголовного права. ИИ как новое самостоятельное явление в государственной и общественной жизнедеятельности

сейчас обладает примерно 10% человеческого мышления, но пределы его вмешательства будут изменяться. Искусственный интеллект нашел применение во многих прикладных сферах человеческой жизнедеятельности, но это не человеческий разум в его понимании настоящего времени, а технология, которая реализуется в нескольких направлениях: обработка естественного языка, большие данные, совместные системы, анализ изображений, робототехника в приложениях, вычислительный социальный выбор и др. Цели искусственного интеллекта и цели человечества на текущий момент совпадают, и не противоречат друг другу, так как интеллект первого не превосходит интеллект человеческий, но это не значит, что искусственный интеллект не может быть использован в чьих-то корыстных или иных противоправных (преступных) целях. В значительной мере, значение ИИ представляется по фантастическим произведениям, что не совсем точно показывает сложившуюся ситуацию. ИИ на настоящий момент, представлен отдельными цифровыми инструментами. Но ожидается кардинальное развитие технологий, которые обеспечат ИИ качественное подобие человеческому интеллекту, что обеспечит ему самостоятельность в решении задач.

«Исследования в области ИИ ведутся достаточно активно, однако однозначное суждение исследователей, касающееся возможно построить ИИ, способный реализовать функции интеллекта человека, отсутствует. Соответственно, открытым остается вопрос, возможна ли в принципе машинная имитация человеческого интеллекта» [Бегишев, Хисамова, 2022: 12]. Если подобное случится и качественный скачок произойдет, то «псевдоразум» (новый разум, новоинтеллект, сверхразум) также должен подлежать уголовной ответственности и наказанию, поскольку как самостоятельный субъект мыслительной деятельности он возможно сможет совершать преступления. Но, тогда требуется ответить и на другой вопрос, а может ли быть искусственный интеллект объектом или предметом преступления. Как информационная технология быть предметом преступного посягательства он несомненно может, но в первом случае однозначный ответ найти гораздо сложнее. Если человеческое сообщество, люди могут выступать в качестве объекта преступления, то почему не может быть объектом искусственный разум, достигший, например уровня 95%, аналогичный человеческому, пусть и созданный людьми?

Закрепление понятия искусственного интеллекта в российском праве осуществлено сравнительно недавно, в Национальной стратегии развития искусственного интеллекта до 2030 года, определение ИИ является сложносоставным, комплексным (включает технологии, продукты деятельности, программное обеспечение, информацию и т.д.) и включает в себя разные подходы исследователей, так как существует значительное количество описания характеристик и признаков искусственного интеллекта: это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Данное определение следует признать условным, так как является многозначным компромиссом.

Необходимо уточнить, что искусственный интеллект и робототехника выступают различными самостоятельными как технологическими и программными явлениями (продуктами), так и правовыми терминами, что предопределено приоритетом в ИИ информационных технологий, а в робототехнике – внешней аппаратной реализации и самостоятельности перемещения.

Уголовное право далеко от футурологии, скорее наоборот, оно крайне консервативно [Жалинский, 2009], а с другой стороны, – стремительное изменение общественных отношений предопределяет необходимость обширных изменений и дополнений российского уголовного

законодательства, поскольку в определенных сферах правового регулирования оно сильно отстает.

Искусственный интеллект сочетает в себе большие возможности и трудно прогнозируемые в настоящее время угрозы, так как характеризуется способностью к самообучению и осознанной, активно-волевой деятельности, но его мыслительная деятельность на текущий момент не аналогична человеческой. Но, этот процесс качественного преодоления в отставании интеллектуального развития, только вопрос времени. Развитие информационных технологий может сопровождаться и деградацией отдельных сфер человека.

Одним из значимых инструментов в области взаимодействия информационных технологий и уголовного права следует признать искусственный интеллект, который можно анализировать в нескольких уголовно-правовых значениях, как:

1. Как часть объекта уголовно-правовой охраны, поскольку его можно рассматривать и как информацию, и как технологию, в отношении которых может быть совершено преступное посягательство;
2. Орудие и средство совершения преступления;
3. Как общеопасный способ совершения преступного посягательства;
4. Уникальный предмет преступления;

Инструмент уголовно-правового механизма, позволяющий классифицировать отдельные деяния как преступления (правонарушения). Например, Роскомнадзор ввел в эксплуатацию систему «Окулус», которая направлена на поиск нарушений российского законодательства в изображениях, видеороликах, текстах в сети интернет, где речь может идти о экстремизме, идеологии терроризма, расизме и т.п.

Поскольку не все цифровые технологии входят в сферу правового регулирования, так и отдельные элементы искусственного интеллекта не будут входить в область уголовно-правовой защиты.

В последующем, ИИ можно позиционировать как обязательный элемент уголовного законотворчества.

Использование ИИ предопределяет доступность, надежность и истинность уголовно-правовой информации.

Искусственный интеллект может быть использован при проектировании уголовного законодательства, в частности, идеальной модели Уголовного кодекса РФ.

По нашему мнению, появление феномена ИИ требует изменение данного подхода, так как когда изменяются технологии в результате преступного посягательства это традиционно, но когда будут проявляться последствия в области информации, ситуация будет усложняться тем, что в сфере виртуальной реальности сам искусственный интеллект будет формировать последующие последствия различного характера, поскольку обладает саморазвитием и автономной самостоятельностью.

В целом, следует сделать вывод о том, что появление феномена «искусственный интеллект» обусловило необходимость исследования проблем не только уголовно-правовой охраны этого явления, но системного взаимодействия, так как понятий аппарат и конструкции в уголовном законодательстве будут дополняться.

Векторами развития уголовного права в эпоху ИИ могут быть следующие:

Ограничение в пользовании технологиями ИИ отдельными категориями лиц (например, управление автомобилем и т.п.);

1. Формулирование новых видов уголовных наказаний (чипирование, электронный контроль);
2. Восстановление прежних видов наказаний, которые возможно применять с помощью технологий ИИ (ссылка, высылка);
3. Создание электронных паспортов осужденных лиц, где возможно контролировать доходы, расходы, осуществлять контроль перемещения;
4. ИИ позволяет фиксировать ежедневное поведение лица;

5. Уголовное право будет учитывать развитие цифровых технологий.
6. Модернизация исполнения лишения свободы на определенный срок.

Современная ситуация развития информационного общества позволяет по новому взглянуть на один из самых сложных и консервативных институтов уголовного права - наказания. И имеются серьёзные основания для последующей теоретико-правовой деятельности в науке уголовного права. А значит у уголовного права есть будущее! ИИ, который в настоящее время создается и развивается, не является противником, а инструментом развития человеческого сообщества. Угрозу видят прежде всего в самостоятельности ИИ и возможности появления у него функций управления. Саморазвитие ИИ необходимо учитывать. Он может быть использован при назначении и исполнении наказания. И доступ к нему может быть ограничен как лишение привилегии.

Уголовное право ожидают перемены, но это не новая для него ситуация. Подобное имело место быть и в прошлых столетиях, когда промышленная революция, научно-технический прогресс и т.п., способствовали качественным изменениям в данной отрасли права. Уголовное право традиционно было далеко от футурологии, но в настоящее время, необходимо анализировать тенденции его будущего развития, так как оно должно соответствовать требованиям соответствующего периода времени.

И возникает интересный вопрос, если ИИ достигнет нового качества в своем развитии - новоинтеллекта, который близок или тождественен человеческому, то в случае совершения им преступления, возможно ли назначение наказания?

Литература

1. Бегишев И.Р., Хисамова З.И. Искусственный интеллект и уголовный закон: монография. – Москва: Проспект, 2022. – С. 192.
2. Жалинский А.Э. Уголовное право в ожидании перемен: теоретико-инструментальный анализ. -2 изд., перераб. и доп. – М.: Проспект, 2009. – С. 400.

ШАЯХМЕТОВА ЖАННА БЕКПОЛОВНА
Профессор кафедры уголовно-правовых дисциплин
Атырауского университета им. Х. Досмухамедова к.ю.н., доцент

СРАВНИТЕЛЬНО-ПРАВОВОЙ АСПЕКТ УГОЛОВНОЙ ЗАЩИТЫ ЦИФРОВОЙ ЛИЧНОСТИ

О недостаточной теоретической разработанности темы, в частности, свидетельствует отсутствие корректного разграничения таких категорий англосаксонской правовой системы , как «использование идентификационных данных лица » («identity theft ») и «мошенничество с использованием личных данных » («identity theft »). В научных исследованиях отмечается непоследовательность использования данных терминов на международном и национальном уровнях.Анализ доктринальных источников и нормативных правовых актов показал , что рассматриваемые категории нередко используются в качестве синонимов.

В отечественной правовой доктрине феномен использования идентификационных данных лица («identity theft ») именуется » «кражей личности », «хищением» личных данных или «кражей идентичности »,что также не совсем корректно. Некоторые американские и немецкие правоведы справедливо утверждают ,что термин «кража личности »неточен и неуместен с правовой точки зрения. Если кража вещи влечет ее изъятие из фактического обладания собственника, то «кража»злоумышленником личных данных , как правило, не лишает потерпевшего возможности их использования. Соответственно, личность не может быть «украдена».

Существует еще один недостаток обозначения термином « кража» неправомерного завладения личными данными. Так, в случаях кражи в традиционном понимании собственник имущества выступает единственным потерпевшим, однака зачастую помимо лица, личная информация которого незаконно используется , нарушаются права и законные интересы третьих лиц , вступающих в правоотношения со злоумышленником, а также различных финансовых учреждений , оказывающих последнему те или иные услуги. При этом термин « мошенничество с использованием личных данных » также адекватно не отражает рассматриваемое явление, поскольку мотивация преступников, незаконно получающих личные данные,не обязательно является корыстной.

Л. Лопуки утверждает, что рассматриваемое преступление имеет как минимум двух потерпевших:физическое или юридическое лицо,вступающее в правовые отношения со злоумышленником ,выдающим себя за другое лицо, а также лицо ,чьи личные данные незаконно используются. И.Д. Солвей заключает, что проблема «кражи»личных данных является социальной проблемой, затрагивающей не только конкретных потерпевших. «Кража» личных данных ослабляет безопасность всего общества. Террористы, в частности незаконно используют личные данные в целях облегчения своей деятельности. Рассматриваемое преступное явление наносит ущерб кредиторам, финансовым учреждениям и компаниям,и эти потери накладываются на потребителей в виде более высоких процентных ставок, цен и сборов.

Действительно, понятие «кража» личных данных имеет отмеченные выше неточности.Представляется ,что рассматриваемые преступные деяния более корректно называть «незаконным использованием идентификационных (личных)данных лица»

Помимо рассмотренной терминологической несогласованности , необходимо обратить внимание и на отсутствие единства мнений ученых практиков и экспертов в области защиты данных относительно уголовно-правовой природы указанного преступного деяния. Отсутствие общепризнанного понимания «использования идентификационных данных лица» затрудняет статистические сравнительно-правовые исследования.

«Масштабы » «кражи» личных данных могут быть скрыты, если рассматриваемое преступное явление не считать самостоятельным преступлением, или, наоборот, преувеличены, если отождествлять указанную преступную деятельность с мошенничеством»

Можно ли рассматривать «использование идентификационных данных лица» как самостоятельное преступление ,даже если «украденные » личные данные не используются для совершения иных преступлений ?Или же «использование идентификационных данных лица » лишь облегчает совершение иных преступлений? Исследование зарубежной правовой доктрины позволило выделить два основных подхода к установлению природы рассматриваемого преступления.

Первый подход определяет «использование идентификационных данных лица» как способ совершения конкретного преступления, который поглощается при квалификации иным преступным деянием.Согласно второму подходу «использование идентификационных данных лица» – это самостоятельное преступление, которое следует отличать от преступныхпосягательств,совершаемых посредством незаконного использования личных данных третьих лиц.

При этом правоведы,придерживающиеся второго подхода, по-разному определяют объем криминализации рассматриваемого преступного деяния.Так, существует точка зрения согласно которой «использование идентификационных данных лица имеет место в случае получения злоумышленником личных данных или документов с целью выдачи себя за потерпевшего».В этом случае из объема криминализации выпадают в частности случаи продажи данных на черном рынке или создания фейковых аккаунтов в социальных сетях с целью причинения ущерба репутации потерпевшего.

Основное различие вышеуказанных подходов состоит в том наделяется ли самостоятельной либо комплементарной ролью неправомерное использование личных данных. Вместе с тем использование идентификационных данных лица следует понимать в широком и узком смысле .Согласно узкому подходу преступное использование личных данных «identity theft» совершается из корыстных побуждений ,а именно для получения злоумышленником товаров, услуг или привилегий материального характера или избавления от материальных затрат посредством выдачи себя за потерпевшего, данные которого украдены. Можно выделить следующие основные виды указанного преступного деяния в узком смысле в зависимости от сферы, на которую посягает злоумышленник.

1. Использование финансовых данных личности. Это наиболее распространенная форма незаконного использования личных данных. Виновный от имени потерпевшего открывает новые кредитные или банковские счета, оформляет ипотеку а также выводит средства с существующих счетов.

2. Использование медицинских данных личности .Оцифровка медицинских данных привела к тому ,что они стали доступны злоумышленникам.Этот вид преступления связанс использованием имени потерпевшего и информации,содержащейся в карте медицинского страхования.

В качестве последствий такого преступления выступает имущественный ущерб,а также потенциальный вред здоровью потерпевшего. Из-за использования злоумышленниками медицинских данных потерпевшему ставится неправильный диагназ,или назначается неверное лечение,оно откладывается иза непонимания того,какая информация в их

медицинской карте является действительной. П. Диксон приводит случай из судебной практики ,проживающий в штате Пенсильвания, обнаружил что самозванец незаконно использовал его данные в целях получения лечения в пяти разных больницах на сумму более 100 000 долларов.

3. Использование налоговых данных личности. Например,житель Лас-Вегаса подал ложные налоговые декларации с использованием «украденных»личных данных с целью получения налоговых вычетов.

Широкий подход определяет «использование идентификационных данных лица» «identity theft» как несанкционированное использование личных данных,:

b) причинения ущерба чести и достоинству потерпевшего посредством создания фейковых аккаунтов в социальных сетях или иных действий, совершаемых от имени потерпевшего;

c) выдачи злоумышленником себя за потерпевшего (за исключением присвоения личности в корыстных целях). Например, злоумышленник, живущий от имени другого лица, может преследовать цель сокрытия от правосудия.

Литература

1. Богданова Д.А.О некоторых последствиях кражи идентичности//Новые информационные технологии в образовании науке:Материалы X международной научно-практической конференции.

2. Генкин А.С., Путинцева И.К. Хищение личных данных в США:масштабы проблемы ,финансовые,правовые и репутационные риски// Страховое дело.-2016.-№9

3. Матюхина Е.Н. Российское и германское законодательство о персональных данных: сравнительный анализ подходов и практики применения//Lex russica.-2019.-№4

4. Golla S.J., Muhlen N. Der Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei:Zur Legitimation

5. Hoofnagle C.J.Identity Theft:Making the Known Unknowns Known//Harvard Journal of law and Technology.-2007.-Vol.21, no.1.

6. Koops B.J.,Leenes R.ldentity theft,identity froud and /or identity-related crime//Datenschutz und Datensicherheit.-2006-Vol.30,no.9.

7. Solove D.J.ldentity Theft, Privacy, and the Architecture of Vulnerability// Hastings Law Journal .-2003.-Vol 54,no 4

8. Trost J.The lmpostor Rule and ldentity Theft in America// Law and Hastings Law Lournal.-2017-Vol 35.no 2

САДЫРОВ АЙДОС КАЙТПЕРГЕНОВИЧ
Начальник кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, полковник

СОВРЕМЕННЫЕ СПОСОБЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Будущее борьбы с преступностью определяется во многом теми же технологиями, которые революционизируют бизнес и другие сферы жизни. Искусственный интеллект (ИИ), автоматизация, большие данные, расширенная реальность и все наиболее важные тенденции, которые мы выявляем в других секторах, в равной степени оставляют свой след в полицейской деятельности.

Эти технологии дают полицейским и спецслужбам беспрецедентные полномочия по борьбе с преступной деятельностью, когда они пытаются обеспечить нашу безопасность. Они также помогают бороться с новыми формами преступности, которые появляются по мере того, как преступники становятся все более изобретательными в использовании технологий и данных.

Итак, вот взгляд на некоторые из последних разработок в области технологий, которые на мой взгляд, будут играть ключевую роль в полицейской деятельности сегодня и в ближайшем будущем.

Данные смарт-устройств

Объем генерируемых данных стремительно растет, и многие из этих данных потенциально могут быть полезны, когда речь идет о борьбе с преступностью. Устройства Интернета вещей (IoT), такие как видеодомофоны и голосовые помощники, с их способностью фиксировать случайные события, происходящие в их среде, все чаще становятся ценными источниками информации для офицеров и детективов, ищущих улики. Данные с умной колонки Alexa были использованы судом в США для оказания помощи в деле о двойном убийстве. А данные фитнес-трекеров Fitbit использовались в нескольких случаях, в том числе недавно в деле мужчины, обвиняемого в убийстве своей жены.

Более 400 полицейских сотрудничают с производителем видеодомофонов Ring для доступа к данным, снятым с их устройств (с разрешения владельцев устройств). Кроме того, инфраструктура умного города будет все чаще создаваться с функциями для предотвращения и раскрытия преступлений, такими как управление светофорами, чтобы помочь полиции и бригадам скорой помощи быстро добраться до места преступлений или несчастных случаев.

Одной из сетей устройств, специально созданных для борьбы с преступностью, является ShotSpotter. Он состоит из массива микрофонов, подключенных к городской инфраструктуре, таких как уличные фонари, которые улавливают звуки выстрелов. Затем он выдает оповещения в режиме реального времени сотрудникам правоохранительных органов, которые могут реагировать быстрее, чем если бы им приходилось ждать сообщений от свидетелей. Технология существует уже некоторое время, но становится все более распространенной.

Компьютерное зрение

Компьютерное зрение имеет несколько важных вариантов использования в полицейской деятельности. Возможно, чаще всего он используется для автоматического распознавания

номерных знаков (ALPR), чтобы камеры могли идентифицировать транспортные средства и их водителей. Более недавним приложением является распознавание лиц, которое также оказалось спорным, поскольку было установлено, что одно полицейское подразделение в Великобритании использует его незаконно. Это было связано с тем, что он использовался «без разбора» и без учета ограничения расовых или гендерных предрассудков.

Тем не менее, полиция все чаще использует эту технологию – недавние развертывания в США включают выявление лиц, причастных к нападениям на Капитолий 6 января и беспорядкам Black Lives Matter в 2020 году.

Компьютерное зрение также используется в новом поколении детекторов лжи, которые работают, анализируя микроскопические движения глаз и лица субъекта. Одна из таких систем под названием EyeDetect добровольно использовалась на подозреваемых, а также использовалась работодателями на собеседованиях при приеме на работу.

Компьютерное зрение вскоре может быть использовано даже для упреждающего обнаружения преступлений до того, как они произойдут. Продолжаются исследования по применению машинного обучения к видеоданным с целью создания алгоритмов прогнозирования, которые могут подсказать, где могут произойти преступления, на основе скопления людей в окружающей среде, трафика, погоды и объектов, которые могут быть обнаружены в окружающей среде. Это могут быть данные, снятые с камер видеонаблюдения, или даже кадры с дронов.

Робототехника

Роботы явно полезны в правоохранительных органах из-за их способности попадать в опасные ситуации. В то время как общество и технологии, вероятно, не совсем готовы к Робокопу общего назначения, автономные мобильные подразделения будут играть все более важную роль в ряде специализированных ролей в ближайшие годы.

Одним из наиболее важных является утилизация бомб, подозрительных пакетов и других подозрительных и потенциально опасных предметов. Они существуют с 1970-х годов, но последнее поколение управляется с помощью гарнитур в стиле VR, а также способно работать с гораздо большей степенью автономии, чем более ранние модели. Также были разработаны роботы, которые могут подниматься по лестнице и даже перепрыгивать через стены, чтобы избежать необходимости для людей-операторов вручную размещать их рядом с предполагаемой бомбой, прежде чем они смогут приступить к работе.

Роботы также используются службами безопасности и правоохранительными органами для наблюдения. Робособака, созданная Boston Dynamics, перемещается с помощью радара и оснащена тепловизионными камерами для обнаружения злоумышленников даже в темноте. Кроме того, были разработаны планы, позволяющие использовать их в сценариях переговоров о захвате заложников.

Прогнозируется, что рынок роботов в правоохранительных органах достигнет 5,7 миллиарда долларов в 2023 году, поэтому мы можем быть уверены, что появится еще много интересных вариантов использования.

Цифровые двойники

Цифровой двойник – это компьютерная модель любого реального объекта, системы или процесса. Он получает информацию от данных - благодаря технологии IoT и датчикам – что позволяет ему точно моделировать то, что он является двойником. В провинции Гуандун, Китай, временное полицейское управление сотрудничало с городскими властями для создания карты города в режиме реального времени, показывающей, где происходят инциденты, а также картографирования общественных взаимодействий, звонков, использования полицейских ресурсов и предполагаемых или потенциальных угроз. Каналы из 10 отдельных правительственных ведомств консолидированы в модели, что дает полиции полный обзор в режиме реального времени с помощью платформы визуального анализа данных. Это означает, что полиция может моделировать и оценивать свою реакцию на что угодно, от общегородских

чрезвычайных ситуаций до распределения ресурсов, чтобы решать повседневные проблемы, такие как уличные грабежи и общественные беспорядки.

Виртуальная реальность (VR) и дополненная реальность (AR)

VR и AR обладают большим захватывающим потенциалом, который, как мы уже видим, используется для облегчения обучения и повседневной работы полицейских. Одна система, разработанная Axom, предназначена для обучения полиции целому ряду навыков, включая деэскалацию потенциально насильственных ситуаций и работу с представителями общественности, когда могут быть осложняющие факторы, такие как нарушение слуха или болезнь Альцгеймера.

В США полицейские в Оклахоме используют другую систему под названием Apex Officer, которая помогает научиться реагировать на звонки, когда психическое здоровье является проблемой. Другие системы используют 360-градусные видеостены, которые окружают обучаемого, вместо того, чтобы требовать от него ношения гарнитуры.

Вдали от тренировок и в полевых условиях AR полезен, поскольку позволяет офицерам оставаться в курсе того, что происходит в их окрестностях, расширяя свое понимание ситуации с помощью наложенной компьютерной графики. В Китае полицейские используют AR-очки, которые могут идентифицировать подозреваемых и тех, кто разыскивается для допроса. Очки, созданные стартапом Xloong Technology, позволяют полиции получать доступ к функциям распознавания лиц и номерных знаков в режиме реального времени. Хотя проблемы конфиденциальности означают, что эта технология вряд ли будет принята западными полицейскими силами в ближайшее время, это интересный взгляд на то, куда может двигаться будущее технологий правоохранительных органов.

Литература

1. Марр Б. 5 крупнейших технологических тенденций в полиции и правоохранительных органах // Forbes journal URL: https://www.forbes.com/sites/bernardmarr/2022/03/08/the-5-biggest-tech-trends-in-policing-and-law-enforcement/?sh=323d0dec3840

АЛТАЙБАЕВ СОВЕТ ҚАПАШҰЛЫ
Қазақстан Республикасы ІІМ Б.Бейсенов атындағы Қарағанды академисы қылмыстық құқық және криминология кафедрасының профессоры, з.ғ.к., қауымдастырылған профессор

БАС БОСТАНДЫҒЫНАН АЙЫРУ ЖАЗАСЫ – АДАМДЫ ҚОҒАМНАН ОҚШАУЛАУДЫҢ БІР ТҮРІ

Халықтың өмірі мен денсаулығын, құқықтық тәртібін қамтамасыз ету мақсатында мемлекет адамдардың белгілі санатын оқшаулау түрінде мәжбүрлеуді қолдануға міндетті. Аталған шара қоғамға қауіпті тұлғалар санатына: психикалық немесе жұқпалы аурулармен ауыратын құқық бұзушыларға қатысты қолданылуы мүмкін.

Ғылыми әдебиеттерде «бас бостандығынан айыру» түсінігінің яғни сотталғанды оқшаулаудың негізгі белгісін толық түсіндірілуі қазіргі уақытқа дейін берілмегені айтылған. Құқық ғылымында мұндай жағдай, біріншіден белгілі мерзімге бас бостандығынан айыру, өмір бойы бас бостандығынан айыру және қамауға алу сияқты жаза түрлерінің заңды көрсетілуін қиындатады. Екіншіден, бас бостандығынан айыруды қауіпсіздігі аралас мекемелерде өтеумен, еркіндікті шектеу, тәртіптік әскери бөлімде ұстау сияқты жазаларды жіктеу бойынша теориялық дау шығарады. Үшіншіден, «оқшаулау», «режим», «күзет», «қадағалау» түсініктерін байланыстырмайды. Төртіншіден, бас бостандығынан айыру белгісі сияқты «оқшаулау» түсінігінің жеткіліксіз теориялық-құқықтық бағасы, мекемелер қызметінде адам құқығын қамтамасыз ету деңгейін көтеру бойынша тиісті шаралар қолдануға мүмкіндік бермейді.

Сот төрелігі механизмінің элементі, мемлекеттік мәжбүрлеу түрі сияқты оқшаулаудың құқықтық көрініс мәселесінің болуы, бас бостандығынан айыру жерлерінен босаған тұлғалар және сотталғандармен әлеуметтендіру жұмысында сабақтастық механизмін құруға, Қазақстан Республикасында қазіргі бас бостандығынан айыру мекемелерінің жұмыс істеуінің құқықтық және ұйымдастыру негіздерін жетілдіру бойынша қылмыстық және қылмыстық-атқару саясаты дамуын жетілдіру үстінде.

Бас бостандығынан айырудағы оқшаулаудың мәнін түсіну үшін, оқшаулаумен байланысты мемлекеттік мәжбүрлеудің басқа түрлерінде қарастырып бағалау керек, сонымен қатар қоғамдағы адамның қалыпты әлеуметтік байланыстарын бұзатын, оның еркіндікке құқығын жүзеге асыруын шектейтін мәжбүрлі және мәжбүрлі емес шараларды қарастырып бағалау керек.

Оқшаулау (франц. isolation – оқшаулау, жекелеу) – қоршаған ортамен байланыстан айыру, кімді немесе нені оқшаулау, жекелеу [1].

Біздің ойымызша, мемлекеттік мәжбүрлеу түрлері сияқты оқшаулаудың заңды түрлеріне құқықтық табиғатын көрсететін авторлардың дәлелдері негізделген болып көрінеді. Бұл дұрыс, өйткені мемлекеттік мәжбүрлеу конституцияға қарсы, яғни заңсыз болуы мүмкін емес. Қазақстан Республикасы Конституциясының 12-бабының мағынасы бойынша Қазақстан Республикасында Конституцияға сәйкес адам құқықтары мен бостандықтары танылады және оларға кепілдік беріледі. Адам құқықтары мен бостандықтары әркімге тумысынан жазылған, олар абсолютті деп танылады, олардан ешкім айыра алмайды, заңдар мен өзге де нормативтік

құқықтық актілердің мазмұны мен қолданылуы осыған қарай анықталады. Республиканың азаматы өзінің азаматтығына орай құқықтарға ие болып, міндеттер атқарады.

Құқықтық санат сияқты оқшаулауға нақты анықтауды Р.С. Маковик берді: «мәжбүрлі, мемлекет атынан жасалатын құзыретті орган белгілеген, мақсатын заң анықтаған, мемлекет арнайы белгіленген және жабдықталған жерлерде, оны бұрын қоршаған қоғамдық және табиғи тіршілік ортамен тұлғаның әлеуметтік байланыстарын уақытша құқықтық шектеуі» [2, 43] – дейді.

Тұрақты әлеуметтік байланыстардың уақытша бұзылуымен және ажыратуымен байланысты тұлғаның оқшаулауы (оның түріне және құқықтық негізіне тәуелсіз), барлық жағдайда оның қоғамда бейімсіздігіне әкеледі. Сонымен қатар адам және қоғам арақатынасында қайшылық деңгейі және қауіптілік шегі жоғарлайды. Осындай қайшылықтар өткірлігі негізінде адамның әлеуметтік және жеке бастамаларына бағытталған.

Мұндай адам бір уақыт қоғамнан бөліну (оқшаулау) жағдайында болады. Оқшаулаудың әлеуметтік түрін дамуын бағаламауға болмайды, өйткені ол мемлекеттің әлеуметтік саясатын тиімсіздігі және өмірдің жайсыздығының ішкі қарама-қайшылығынан пайда болады. Әлеуметтік оқшаулау тұлғаның оң белсенділігін тоқтатады. Ол селқостықтың себебі болады және жағымсыз тәуелділігі пайда болуына әкеледі, ол адамның азғындауына, заңсыз және қылмыстық мінез-құлыққа әкеледі. Әлеуметтік оқшаулау адамды бас бостандығынан айыру түріндегі қылмыстық-құқықтық оқшаулауға әкеледі.

Құқық көзқарасынан адамды оқшаулау заңды және заңсызға бөлінеді. Адамды оқшаулаудың заңды түрлеріне: әкімшілік қамау, қамауға алу түрінде бұлтартпау шарасы, қамау, бас бостандығынан айыру және өмір бойы бас бостандығынан айыру сияқты қылмыстық жазалар, қылмыстық-құқықтық сипатты шаралар: жабық типті арнайы оқу-тәртіптік мекемеге кәмелетке толмаған адамды орналастыру, медициналық мәжбүрлеу шараларды қолдану жатады. Бұл мемлекеттік және арнайы мәжбүрлеудің әртүрлі шаралары.

Қылмыстық заң: адамды ұрлау (ҚР ҚК 125-б.), бас бостандығынан заңсыз айыру (ҚР ҚК 126-б.), психиатриялық стационарға заңсыз орналастыру (ҚР ҚК 127-б.), адамды кепілге алу (ҚР ҚК 261-б.), көрінеу заңсыз ұстап алу, күзетпен қамауға алу немесе күзетпен ұстау (ҚР ҚК 414-б.), яғни адамды оның еркіне қарсы кез келген жерде ұстауға бағытталған кез келген әрекеттерді бас бостандығынан айырудың заңсыз түрлеріне жатқызады. Барлық осы құрамдарды, олардың объективті жағы жалпы бірдейлігі біріктіреді және адамды мәжбүрлеп оқшаулауында және еркіндікке және қол сұқпаушылыққа өз құқығын іске асыруға бөгет жасауда көрінеді. Қол сұғушылықтың осы түрлерінің себептері және мақсаттары әртүрлі болуы мүмкін, олар жауапкершіліктің деңгейіне және әрекеттің саралауына әсер етеді.

Әскери іс-қимылдарды жүргізу жағдайында әскери қызметкерлерді тұтқындау және бейбіт халықты депортациялау оқшаулаудың (бас бостандығынан айырудың) ерекше түрлері болып табылады. Тұтқындау – жаудың соғысқа жарамдылығын төмендету және оған тиімді шығуды жоспарлау мақсатында, жедел және стратегиялық ақпаратқа иеленген тұлғалар немесе басшылық құрам тұлғаларын ұстау бойынша арнайы шараларды өткізгенде немесе ұрыс кезінде жаудың тірі күшіне зиян келтіру. Депортация (лат. *deportatio* – шығару) – мемлекеттен тұлғаны мәжбүрлеп шығару. Депортация жиі басқа бір мемлекетке шығып кеткен шетел азаматтарына немесе азаматтығы жоқ адамдарға қатысты қолданылады [3] (1949 ж. 12 тамыздағы «Соғыс кезіндегі бейбіт азаматтарды қорғау туралы» Конвенцияның 49-б.) [4].

Адамды құқыққа қарсы бас бостандығынан айыруға болмайды және заңмен қудаланады.

Осы зерттеуде бас бостандығынан айыруда жаза белгісі сияқты оқшаулауды бағалау үшін жаза шарасы ретінде құқық бұзушыларға оқшаулаудың заңды қолданудың талдауын жасау орынды.

Бас бостандығынан айырудың түрлері мақсаттар және оларды қолданудың құқықтық негіздері бойынша, құқықтық шектеудің мазмұны және орындаудың нормативты реттеуі бойынша, оқшаулауға ұшыраған адамдардың құқықтық жағдайы бойынша, қолдану

субъектілері бойынша, оларды орындау органдары мен мекемелер бойынша, осындай шараларды қолданудың салдары және оқшаулау деңгейі бойынша бөлінеді.

Әкімшілік қамауға алу сот қолданатын әкімшілік ең қатаң жаза болып табылады. Ол жасаған құқықбұзушылық туралы іс бойынша қаулымен белгіленген мерзімге кінәліні қоғамнан оқшаулауы болып табылады.

Әкімшілік тәртіпке тарту сияқты қамауға алу ерекше жағдайларда белгіленеді және қолданылады. Жалпы ереже бойынша мұндай әкімшілік қамаққа алу мерзімі – отыз тәулікке дейінгі, ал төтенше жағдайлар режимі талаптарын бұзғаны үшін қырық бес тәулікке дейінгі мерзімге белгіленеді [5].

Әкімшілік қамаққа алу туралы қаулыны қолдану тәртібі, осы жазаны өтеу, әкімшілік тұтқындауға алынған тұлғалардың мәселелері Қазақстан Республикасының әкімшілік құқық бұзушылық туралы кодексінің 913-бабының нормаларымен реттелген.

Әрине мемлекет мәжбүрлеу шарасы ретінде оқшаулауды қолданып, осындай шараға ұшыраған тұлғаларға арнайы мекемелерде өркениетті жағдай жасау міндетті, өйткені адамның қадірін қорлаудан қорғау ҚР Конституциясының 17-бабы 2-т. кепілдендірілген – Ешкімді азаптауға, оған зорлық-зомбылық жасауға, басқадай қатыгездік немесе адамдық қадір-қасиетін қорлайтындай жәбір көрсетуге не жазалауға болмайды, оған барлық адамдарды азаптан және басқада қатыгез немесе адамның қадірін қорлайтын жаза түрлерінен қорғау туралы Декларацияның 4-б. талаптары бағыттайды [6].

Мемлекет осындай тұлға амалсыз «қамқорлықта» болуы фактісінен шығатын мәселелер кешенін шешуге міндетті. Бұл тұрмыс жағдайы, ұстаудың қауіпсіздік жағдайлары, денсаулықты қорғау, персоналмен дұрыс қатынас, сотталғандарды және қамауға алынғандарды еңбекке тарту мәселелері.

Қамауға алу арнайы мекемеде сотталғанның оқшаулауымен байланысты жазаның жаңа түрі болып табылады (ҚР ҚК 45-б.). Жазаның осы түрі осы жаза жүйесіне қосылғаннан кейін заң шығарушы оны «кейінге қалдырылған» санатына қосты. Қазіргі уақытта ҚР ҚК жазалар жүйесіне оны қайта қосқан болса да, бірақ оған баға беру қажет, өйткені жазаның осы түрінің мәні сотталғанды оқшаулау түрінде қолданумен белгіленеді. Қамауды бас бостандығынан айырудан сотталғандарды оқшаулау деңгейі, ұстау қысқа мерзімі, оны орындау үшін мекеменің арнайы түрі болуы сияқты белгілері ерекшелейді.

Егер бас бостандығынан айыруда оқшаулау деңгейі қауіпсіздігі аралас мекемелердегі жартылай еркіндіктен түрмедегі қатаң оқшаулауға дейін құбылса, қамауға алу түрмедегі орташа қауіпсіз мекемелерге теңестірілген, өтеу шарттарымен сотталғанның қатаң оқшаулауын қарастырады (ҚР ҚАК 85-б.). Қамауға алу он тәуліктен елу тәулікке дейінгі мерзімге белгіленеді (ҚР ҚК 45-б. 1-б.) және сотталғандар қамаққа алу түріндегі жазасын сотталған жердегі арнаулы қабылдау орындарында өтейді (ҚР ҚАК 63-б. 1-б). Өзінің мәні бойынша, ол қысқа мерзімге бас бостандығынан айыру болып табылады.

Заң шығарушы қылмыстық теріс қылық жасағаны үшін қамауға алуды қарастырған. ҚР Қылмыстық кодексі нормаларының талдауы заң шығарушы біздің ойымызша соттармен қамауға алуды және бас бостандығынан айыруды қолдану шарттарын толық шектемегенін көрсетті. Бұл оларды қолданудың қалыпты тәжірибесін қалыптастыруға әсер ете ме? Қылмыстар құрамының бірқатар санкциялары жазалар баламасында қамауға алу және бас бостандығынан айыруда бар.

Қамауға алу және бас бостандығынан айыру ұқсас емес, өйткені заң шығарушы біріншіні екіншіге қарағанда жазаның жеңіл түрі деп анықтаған, жазалау жүйесінде олардың тиісті орындарын бекіткен (ҚР ҚК 40-б.) – қылмыстық теріс қылық жасағаны үшін кінәлі деп танылған адамға - қамаққа алу, ал, қылмыс жасағаны үшін кінәлі деп танылған адамға – бас бостандығынан айыру қолданылуы мүмкін. Олардың әртүрлі жазалау қасиеттері қамаудың ұзақ мерзімі елу тәуліктен аспайды, ал қамау үйіндегі оқшаулау деңгейі түрме режиміне теңестірілумен сипатталады. Біздің ойымызша қамауға алу оқшаулау элементтері бар естен тану күйі жаза сияқты қысқа мерзімді бас бостандығынан айырудың бір түрі болуы мүмкін. Екінші жағынан, қамау үйлері жаңа аймақтық кіші түрмелер жүйесін білдіреді немесе тергеу изоляторларында және бас бостандығынан айыру мекемелерінде арнайы қамау жайларды білдіреді. Әлеуметтік әлеуеті шектелген (белгілі бір тұрғылықты жері және жұмысы жоқ,

еңбекке жарамсыз тұлғалар) қысқа мерзімді – сотталғандарға қатысты қамауға алу әсерлі болар еді. Әрине, қатаң оқшаулау жағдайында және әлеуметтендіру сипатты шаралар аз қолданумен 50 тәулік бойы ұстау негізсіз, өйткені осы тұлғаларды түзету мақсатымен сәйкес келмейді. Құқық бұзушыларды оқшаулау түрі сияқты әкімшілік қамауға алуды заң шығарушы 30 тәулікке дейін, ал төтенше жағдайлар режимі талаптарын бұзғаны үшін қырық бес тәулікке дейінгі белгілегенін ескерсек, қамауға алу түрінде қылмыстық жаза санкцияның төменгі белгісі бір айдан кем болмау керек. Мұндай жағдайдан қолайлы шешім ұсынылды: қамауға алудың жоғарғы ұзақ мерзімін 1 айға дейін қысқарту керек. Осындай мерзімдермен қамауға алу сотталғанның әлеуметтік пайдалы қатынастарына теріс әсер етпейді, сонымен қатар қамауда ең бастысы - оның ұзақтығы емес деген ереже сақталады. Жазаның осы түрінің жазалау әсері қатаң және қысқа мерзімді үйлесуі болу керек. Тұтқындау қылмыстың санатына және сипатына сәйкес болу керек, ал қысқа мерзімдігі – оны түрме қамауына ауыстырмау керек.

Біздің ойымызша, қамауға алудан қылмыстық жаза түрінде сияқты толық бас тартуға болмайды, өйткені оны қолдану үшін материалдық және ұйымдастыру негізін құру үшін қомақты қаржы қаражат керек. Біздің ойымызша, осыған дейін айтылып келе жатқандай ББАМ (бас бостандығынан айыру мекемесі) қамау үйлер және тиісті ғимараттарды құру – ол ББАМ жүйесін толығымен реформалау жолы. Мекемелерді режимнің негізгі түрі және режимнің басқа түрлерінің мамандандырылған учаскелері бар түзету кешендерге түрлендіруі қылмыстық-атқару заңнама талаптары негіздерінде орын алды (ҚР ҚАК 89-б.).

Мемлекеттік мәжбүрлеу түрі және әлеуметтік құбылыс сияқты тұлғаны оқшаулау мәселесі біздің ойымызша «тұлғаның еркіндігі», «қоғамдық қауіпсіздігі», «құқық тәртібі», «мемлекеттік мәжбүрлеу» түсініктерінің құқықтық білдіру тұрғыдан бағаланады. Мұндай тәсіл келесідей қорытындыларға әкеледі:

1. Сот төрелігі механизмінің элементі, мемлекеттік мәжбүрлеу түрі сияқты тұлғаны оқшаулаудың құқықтық көрінісі мәселесінің жеткіліксіз зерттеуі, оны қолдану және іске асырудың нәтижелі құқықтық және ұйымдастыру негіздерін әзірлеуде мемлекеттік саясаттың қалып қоюына әкелуі мүмкін.

2. Әлеуметтік даму тұлғаның еркіндігін қылмыстық-құқықтық құралдар арқылы қорғауға жататын ерекше маңызды құндылыққа айналдырды. Сонымен қатар, тұлға еркіндігі құқықтық қатынастар жиынтығы сияқты әртүрлі өмірлік жағдайларға және адамдардың қылықтары әсіресе олардың құқыққа қарсы мінездеріне байланысты құқықтық шектеу объектісі ретінде көрінуі мүмкін.

3. Сотталғандарды оқшаулау құқықтық институт болып табылады, ал оны орындау процессінде күрделі әлеуметтік, саяси-заңдық, және психологиялық-педагогикалық мазмұны бар. Сондықтан құқықтық құбылыс сияқты «сотталғанды оқшаулау» түсінігі теориялық негіздемесі қылмыстық-атқару құқықтық қатынастарда мемлекеттің рөлін бір жағынан, қылмыстық-атқару саясатын қалыптастыру және іске асыру екінші жағынан түзету мекемесі және сотталғанның құқықтық дәрежесін анықтау үшін маңызды мәні бар.

Әдебиет

1. Маковик Р.С. Изоляция как правовая категория // Человек: преступление и наказание. 1994. №1. – С. 43.

2. Орысша-қазақша түсіндірме сөздік: Әлеуметтану және саясаттану бойынша / Жалпы редакциясын басқарған э.ғ.д., профессор Е. Арын – Павлодар: «ЭКО» ҒӨФ. 2006. – 569 б.

3. Международное право в документах. – М., 1982. – С. 734-794.

4. Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі 2014 жылғы 5 шілдедегі №235-V ҚРЗ.

5. Қазақстан Республикасының Конституциясы 1997 ж. (өзгерту, толықтыруларымен).

БИЯТОВ ТАЛГАТ КОРГАНБЕКОВИЧ
доцент кафедры права Костанайского филиала
ФГБОУ ВО «Челябинский государственный университет», к.ю.н.

ОСОБЕННОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ ГРАЖДАН РЕСПУБЛИКИ КАЗАХСТАН

Уголовная ответственность несовершеннолетних граждан – это важная и сложная тема, требующая серьезного исследования. В Республике Казахстан есть ряд особенностей, которые отличают уголовную ответственность несовершеннолетних от ответственности взрослых. Данные особенности связаны с возрастом, психологическим и физиологическим развитием несовершеннолетних, а также с целью реабилитации и социализации этих граждан.

Создание суда по делам несовершеннолетних является значимым шагом в развитии системы ювенальной юстиции в Казахстане, началом процесса гуманизации системы правосудия и междисциплинарного подхода среди специалистов разных направлений. С 12 августа 1994 года Республика Казахстан является стороной Международной Конвенции ООН о правах ребенка. Одним из руководящих принципов Конвенции является принцип наилучшего обеспечения интересов ребенка.

Конвенция признает право каждого ребенка, обвиненного в нарушении закона, на «принятие решения по рассматриваемому вопросу независимым компетентным и беспристрастным органом».

В целях реализации указанной Конвенции в 2002 году принят Закон Республики Казахстан «О защите прав ребенка».

В 2003-2006 годах реализован международный проект «Ювенальная юстиция в Казахстане», в рамках которого Указом Главы государства Республики Казахстан от 23 августа 2007 года в городах Астана и Алматы образованы первые экспериментальные ювенальные суды.

В ходе реализации проекта «Ювенальная юстиция в Казахстане» были изучены международные нормы, мировая практика, соответствие национального законодательства существующим международным стандартам в сфере ювенальной юстиции.

По результатам проекта внесены предложения по совершенствованию действующего законодательства, внедрению мировых методик, созданию органов ювенальной юстиции.

В последующем, Указом Главы государства от 19 августа 2008 года одобрена Концепция развития системы ювенальной юстиции в Республике Казахстан на 2009-2011 годы, которая определила, что ювенальный суд является наиболее важным звеном системы ювенальной юстиции.

С учетом положительного опыта деятельности пилотных ювенальных судов, Указом Главы государства от 4 февраля 2012 года такие суды образованы во всех областных центрах и некоторых крупных городах республики.

В Казахстане – единственном из стран Центральной Азии на сегодня успешно функционируют 19 ювенальных судов [1].

В Уголовном кодексе Республики Казахстан есть отдельный раздел, который выделяет особенности уголовной ответственности и наказания для несовершеннолетних. Это сделано в

соответствии с принципами гуманизма и справедливости. Несовершеннолетними УК РК признает лиц, которым во время совершения уголовного правонарушения исполнилось четырнадцать, но не исполнилось восемнадцати лет [2].

Рассматривая мировую практику о возрасте и наказание несовершеннолетних Бенюмов К. отметил, что на сегодняшний день Шотландия – страна с одним из самых низких в Европе порогом достижения возраста уголовной ответственности. Осуждены могут дети от восьми лет. Для сравнения: в Англии и Уэльсе к уголовной ответственности могут привлекаться дети от десяти лет, в большинстве стран ЕС возраст варьируется от 13 до 18 лет.

В Европе, Великобритании и странах Содружества дела несовершеннолетних преступников (в большинстве стран – до 18 лет или до 21 года) рассматривают специальные комиссии и суды. Не допускается, чтобы несовершеннолетние преступники содержались в тех же исправительных учреждениях, что и взрослые. Правда, несмотря на то что лишение свободы применяется к несовершеннолетним только в особенно серьезных случаях, в Великобритании в детских исправительных учреждениях содержится более 3 тыс. человек. Для сравнения: в европейских странах этот показатель вдвое ниже. В Финляндии детей заключенных и вовсе трое.

В Иране за мальчиками и девочками закреплен разный минимальный возраст уголовной ответственности: для девочек – 9 лет, для мальчиков – 15. По достижении этого возраста граждане Исламской Республики могут быть приговорены к любому наказанию вплоть до смертной казни. Ежегодно здесь погибают десятки несовершеннолетних преступников. По данным Amnesty International, на Иран приходится 80% казней несовершеннолетних в мире. Сейчас исполнения смертного приговора ожидают как минимум 130 несовершеннолетних иранцев. И это при том, что Исламская Республика Иран ратифицировала все международные договоренности о правах несовершеннолетних, что делает казни юных преступников прямым нарушением международных обязательств. [3].

В США действует принцип «Взрослое преступление – взрослый срок». Вплоть до 2005 года, когда Верховный суд счел неконституционным приговаривать к смерти несовершеннолетних преступников, этот принцип распространялся даже на смертную казнь. Так, в штате Техас с момента возвращения смертной казни в 1987 году власти приговорили к смерти 12 детей-убийц.

Правда, несовершеннолетних в США никогда не казнили – подростки в возрасте от 12 до 17 лет, совершившие тяжкие преступления, должны были находиться под стражей до достижения совершеннолетия. На момент отмены смертной казни для несовершеннолетних преступников исполнения приговора в американских тюрьмах ждало более 70 смертников.

На сегодняшний день пожизненные сроки в американских тюрьмах отбывает почти 2,5 тыс. несовершеннолетних заключенных, причем чаще всего они осуждены без права освобождения по амнистии.

В мире всего два государства, до сих пор не подписавших Конвенцию ООН по правам ребенка, которая запрещает казнить несовершеннолетних. Одно из них США. Второе – Сомали. [3].

Состояние преступности несовершеннолетних в Республике Казахстан вызывает обоснованную тревогу в обществе. Согласно статистическим данным Комитета правовой статистики и специальных учетов Генеральной Прокуратуры Республики Казахстан (по оконченным уголовным делам) за последние 5 лет по стране в среднем более 2000 уголовных правонарушений совершается несовершеннолетними, так в 2017 году таковых – 3148 деяний, а в 2021 году – 1529. Как видно, общая преступность характеризуется тенденцией снижения, но в тоже время категория тяжких преступлений характеризуются значительным ростом, так в 2018 году их совершено 487, то в 2020 году составило 702 факта [4].

Важно обратить внимание на то, что преступные действия, совершенные несовершеннолетними гражданами, характеризуется зачастую насилием и жестокостью.

Подростки при совершении преступлений в неудачных обстоятельствах совершают убийства, наносят тяжкие телесные повреждения и совершают разбойные нападения.

Общей тенденцией можно назвать снижение возраста преступников-несовершеннолетних и омоложение «пьяной» преступности: каждое пятое преступление совершается несовершеннолетним в состоянии алкогольного или наркотического опьянения. Существует также заметный рост преступности среди девочек-подростков.

Привлечение несовершеннолетних к уголовной ответственности помогает разрешить конфликтные ситуации, возникающие в уголовно-правовых отношениях, что в конечном итоге должно способствовать восстановлению и укреплению правопорядка.

В соответствии с законодательством Республики Казахстан, несовершеннолетние граждане в возрасте от 14 до 18 лет считаются несовершеннолетними и признаются пригодными для уголовной ответственности. Однако возраст уголовной ответственности может быть снижен до 16 лет в особых случаях, таких как особая жестокость или опасность преступления. Это делается для защиты несовершеннолетних от совершения серьезных преступлений.

Несовершеннолетние вменяемые в возрасте от четырнадцати до шестнадцати лет привлекаются к уголовной ответственности только за те преступления, которые с исчерпывающей полнотой перечислены в уголовном законе. Согласно мнению, когда дети достигают этого возраста, они обладают достаточным пониманием реальной природы своих поступков, их общественной опасности и способны контролировать их [5].

Преступления, за которые к уголовной ответственности и наказанию могут привлекаться несовершеннолетние в возрасте от четырнадцати до шестнадцати лет, относятся к умышленным, а по степени общественной опасности относятся к категории средней тяжести (девять составов), а остальные к тяжким или особо тяжким преступлениям

Важно отметить, что еще одной особенностью уголовной ответственности несовершеннолетних граждан в Казахстане является то, что при назначении уголовного наказания суд учитывает возраст, психологическое состояние и индивидуальные особенности несовершеннолетнего, а также его возможность реализовать свой социально-правовой статус. Если несовершеннолетний достиг возраста уголовной ответственности, но из-за отставания в психическом развитии, которое не связано с психическим расстройством, он не в полной мере осознает фактический характер и общественную опасность своих действий (бездействия) или не может контролировать их, то он не несет уголовной ответственности. В таком случае, уголовное преследование этого несовершеннолетнего может быть прекращено в уголовном досудебном процессе или в судебном процессе.

Кроме того, специальные органы занимаются рассмотрением уголовных дел несовершеннолетних. Несовершеннолетние имеют право на защиту своих прав и интересов, включая право на адвоката, а также возможность подачи апелляций и жалоб на решения суда.

Согласно части 1 ст.81 УК РК видами наказаний, назначаемых несовершеннолетним, являются:

1) лишение права заниматься определенной деятельностью;
2) штраф;
3) исправительные работы;
4) привлечение к общественным работам;
5) ограничение свободы;
6) лишение свободы.

В комментируемой статье законодателем дан исчерпывающий перечень видов наказаний, назначаемых несовершеннолетним. Как можно заметить, Уголовный кодекс не предусматривает специфических видов наказаний, применяемых только к несовершеннолетним

Остановимся отдельно на таких видах наказаний, как штрафы и лишение свободы, рассмотрим особенности их назначения.

Несовершеннолетним, у которых есть самостоятельный заработок или имущество, на которое можно наложить взыскание, будет назначен штраф размером от пяти до ста месячных расчетных показателей (МРП).

Лишение свободы несовершеннолетним может быть назначено на срок не более десяти лет. Однако, если дело связано с убийством при отягчающих обстоятельствах или с актом терроризма, либо если у несовершеннолетнего есть несколько уголовных правонарушений, одно из которых является убийством или актом терроризма, то срок лишения свободы может составить до двенадцати лет.

Несовершеннолетним, совершившим преступление небольшой или средней тяжести, не связанное с причинением смерти, лишение свободы не будет назначено.

В статье 53 УК прописано, что несовершеннолетие виновного считается фактором, смягчающим уголовную ответственность и наказание. Это следует учитывать в процессе судебного рассмотрения дела.

Отметим, что определение возраста лица, привлекаемого к уголовной ответственности, регулируется Нормативным постановлением Верховного Суда Республики Казахстан от 11 апреля 2002 года N 6 «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий». Согласно пункту 2 этого Постановления, орган, ведущий уголовный процесс, должен принять меры для установления точной даты рождения лица, привлекаемого к ответственности. В то же время, лицо считается досягаемым определенного возраста начиная со следующего дня после дня рождения [5].

Если отсутствуют документы, подтверждающие возраст, или есть сомнения в их достоверности, то в соответствии с частью 1 статьи 271 Уголовно-процессуального Кодекса Республики Казахстан необходимо провести экспертизу. В таких случаях последний день того года, который указали эксперты, считается днем рождения. Если эксперты указали возраст в диапазоне (например, от 14 до 15 лет), выбирается минимальный возраст.

Как уже ранее говорилось, суд при избрании наказания несовершеннолетнему обращает внимание на его возраст, психологическое развитие, однако не будем забывать, что на становлении психики подростка влияют внешние факторы, исходящие, в первую очередь, из семьи. Поэтому согласно пункту 17 Нормативного постановления Верховного Суда РК от 11.04.2002 г. №6 при назначении наказания несовершеннолетним суды обязаны помимо обстоятельств, указанных в части 3 статьи 52 УК РК, учитывать условия их жизни и воспитания (неблагополучная обстановка в семье, грубое, порой жестокое отношение к подросткам со стороны родителей, близких родственников и т.д.), уровень психического развития, особенности личности (наличие психического расстройства, неуравновешенность, вспыльчивость и т.д.), мотивы совершения преступлений (детское озорство, «за компанию», зависть, мстительность и т.д.), влияние на подростка старших по возрасту лиц [6].

Согласно Уголовно-исполнительному кодексу Республики Казахстан, несовершеннолетние, которые осуждены к лишению свободы, отбывают наказание в учреждениях средней безопасности для содержания несовершеннолетних. Также в этом же учреждении могут отбывать наказание совершеннолетние граждане, оставленные там до достижения 21 года и пробывшие там не менее одного года. Особенности отбывания наказания в виде лишения свободы для несовершеннолетних регулируются главой 24 Уголовно-исполнительного кодекса.

Несовершеннолетними лицами являются граждане, которые на время совершения преступления было четырнадцать полных лет, но не исполнилось 18 лет. Необходимо отметить, что допрос несовершеннолетнего лица, является законным только в присутствии его законного представителя.

Мы должны уяснить, что несовершеннолетним лицам не назначаются наказания в виде лишения свободы и казни. Но законодательством определено, что им налагается ограничение свободы не более двух лет. Но исключением могут быть случаи, когда деяние могло совершиться во время террористического акта. В таких случаях могут назначить срок до 12 лет.

Наказания в виде штрафа, налагаются только в случаях, когда у несовершеннолетнего лица есть самостоятельный заработок. То есть, во время досудебного разбирательства должностные лица должны проверить нет ли у него самостоятельного заработка.

Уголовная ответственность – вид правовой ответственности; итог правового преступления – которая выражается в наказании преступника и является видом государственного принуждения.

Таким образом, особенности уголовной ответственности несовершеннолетних граждан в Республике Казахстан направлены на защиту и реабилитацию несовершеннолетних, признавая их особый статус и потребности. Этот подход основан на международных стандартах и стремлении общества создать условия для социальной адаптации и воспитания несовершеннолетних. Однако, несмотря на все особенности, несовершеннолетние граждане все равно несут уголовную ответственность за свои деяния. Так реализуется конституционный принцип равенства всех перед законом и судом.

Очевидно, что дети вполне способны совершать тяжкие преступления. Другое дело, что при рассмотрении таких случаев суды должны учитывать особенности несформировавшейся личности. Ребенку труднее противостоять дурному влиянию среды, совершенное им злодеяние может быть трагической, но случайной ошибкой. В этом смысле несовершеннолетнего преступника проще поставить на путь исправления. Итоговая задача ювенальной юстиции – защита детей и подростков защита от всякого вида насилия, которые могут получить несовершеннолетние со стороны взрослых.

Делая сравнительный анализ ювенальной юстиции стран Европы, Азии, Латинской Америки, Канады и США политолог КазНПУ им. Абая Задерий В. отмечает, что на данные момент в Казахстане существует и развивается собственная ювенальная система, высшим звеном которой является ювенальный суд. И данная система отвечает всем современным мировым стандартам ювенальной юстиции.

В стране существует государственная концепция развития системы ювенальной юстиции которая объединяет в себе социальных работников, психологов, ювенальных адвокатов, ювенальную полицию и ювенальную прокуратуру, суд. Ювенальные суды рассматривают уголовные, гражданские и административные дела, касающиеся детей. В этой связи отмечается суды стали меньше применять в качестве меры наказания лишение свободы, в частности, к лицам, впервые совершившим преступления, преступления небольшой и средней тяжести. На сегодняшний день в Казахстане действует только одно закрытое учреждение для осужденных несовершеннолетних, расположенное в городе Алматы. Ранние в Казахстане действовало пять закрытых учреждений.

При этом Задерей В. отмечает, что заслуживают более детального рассмотрения следующие аспекты: предпочтительность воспитательных мер перед наказанием, карательными мерами; глубокое знакомство с психологией, с личностью несовершеннолетнего правонарушителя, трудоустройство их и обучение.

Действительно, на основании вышеизложенного можно сделать вывод о том, что для привлечения несовершеннолетнего лица к уголовной ответственности нужно учитывать все аспекты. То есть, знать его возраст, характер содеянного преступления, имеет ли заработок и его права в соответствии законодательством Республики Казахстан.

Одним из проявлений повышенного внимания к защите прав несовершеннолетних в уголовных делах является двойное представление их интересов в уголовном процессе. В нем участвует адвокат и законный представитель. Один из родителей, усыновители, опекуны, попечители или уполномоченный представитель учреждения или организации, уполномоченный в качестве законного представителя несовершеннолетнего обвиняемого.

Предлагается обязательное проведение комплексной судебной психолого-психиатрической экспертизы на определение патологических психических проявлений, так и составление психологического и эмоционального портрета личности несовершеннолетнего правонарушителя.

Согласно части 1 ст.81 УК РК видами наказаний, назначаемых несовершеннолетним, являются: лишение права заниматься определенной деятельностью; штраф; исправительные работы; привлечение к общественным работам; ограничение свободы; лишение свободы.

Уголовный кодекс РК не предусматривает специальных (отдельных) видов наказаний для несовершеннолетних.

С учетом сказанного предлагается в целях обозначения особенности ювенального судопроизводства судебные приговоры по уголовным делам в отношение несовершеннолетних в Уголовном кодексе РК отдельными статьями прописать названия окончательных судебных решений (постановление или приговор) выносимые ювенальными судами а именно:

1.Ювенальное судебное постановление. В виде ПОСТАНОВЛЕНИЯ ювенальный суд выносит окончательное судебные решения с назначения наказанием не связанные с лишением свободы. Которые указаны в часть 1 ст.81 УК РК, а именно: лишение права заниматься определенной деятельностью, штраф, исправительные работы, привлечение к общественным работам, ограничение свободы.

2.Ювенальный судебный приговор. В виде ПРИГОВОРА ювенальный суд выносит окончательное судебные решения с назначением наказанием в виде лишение свободы. Которые указаны в часть 1 ст.81 УК РК.

С учетом особенности привлекаемого лица предлагается в отношение несовершеннолетнего лица, отбывавшего наказание по ювенальному судебному ПОСТАНОВЛЕНИЮ (судебные решения не связанные с лишением свободы), в последующем при отсутствие повторности, рецидива уже не признавать как уголовную судимость и не отмечать об этом решение в государственных органах судебной и правовой статистики.

Литература

1. Акпар Р.М. Как работают ювенальные суды в Казахстане//Защита прав и законных интересов несовершеннолетних является одним из приоритетных направлений государственной социально-правовой политики республики. 26 сентября 2017г., сайт: Zakon.kz -https://www.zakon.kz/redaktsiia-zakonkz/4879865-kak-rabotayut-yuvenalnye-sudy-v.html (Дата обращения 31.10.23.);
2. Уголовный кодекс Республики Казахстан https://adilet.zan.kz/rus/docs/K1400000226 (Дата обращения 19.10.23.);
3. Бенюмов К. Детство в клеточку//Журнал «Коммерсантъ Власть» АО «Коммерсантъ». 123112, Москва.
4. Аралбаев С.С. Уголовная ответственность несовершеннолетних. Учебно-методическое пособие // С.С.Аралбаев – Костанай: КРУ им.А.Байтурсынова, 2022. https://ksu.edu.kz/files/TB/book/jur/posobie_ 7_nesovershen_ 2022.pdf (Дата обращения 19.10.23.);
5. Мамонтов Н.И. Особенности уголовной ответственности несовершеннолетних и освобождения их условно-досрочно от не отбытого наказания – https://online.zakon.kz/Document/?doc_id=38375883&pos=6;-124#pos=6;-124 (Дата обращения 19.10.23.);
6. Нормативное постановление Верховного Суда Республики Казахстан от 11 апреля 2002 года N 6 «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий» – https://adilet.zan.kz/rus/docs/P02000006S_ (Дата обращения 19.10.23.);
7. В. Задерий, кандидат политических наук, Казахский национальный педагогический университет им. Абая Ювенальная юстиция в правовой практике ряда стран Европы, Азии, Латинской Америки, Канады и США, журнал «Юрист», №12, 2012г.

НАСЫРОВА Э.М.
Начальник отделения Научно-исследовательского центра Алматинской академии МВД Республики Казахстан им. М. Есбулатова
подполковник полиции, PhD

ЛИМ В.В.
Старший преподаватель Международного транспортно-гуманитарного университета
кафедры социальных наук и права

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

В современных условиях преступность приобрела интернациональный и мобильный характер. Правоохранительные органы многих стран адекватно реагируют на эти процессы, осуществляя переход к новым методам работы. Международный опыт показывает, что нашими коллегами внедряются новые превентивные приемы воздействия на преступность и расследования правонарушений, которые основаны на инновационных технологиях.

Успех этой работы зависит от межведомственного взаимодействия, координации и слаженности действий уполномоченных органов и наличия объективной информации о происходящих событиях. В Казахстане органам прокуратуры, помимо высшей надзорной функции, отведена роль «ядра» правоохранительной системы и координации деятельности правоохранительных органов. В силу такого статуса и функционала прокуратура внедрила несколько видов систем информационного взаимообмена и оперативного реагирования между правоохранительными, специальными и заинтересованными государственными органами.

Оператором этих систем выступает Комитет по правовой статистике и специальным учетам, который образован в структуре Генеральной прокуратуры в 1995 г. [1]. Его статус, задачи и функции, а также принципы ведения всей правовой статистики определены отдельным законом. В этом ведомстве автоматизированном режиме аккумулируются сведения о преступности, результатах судебных процессов, прокурорских проверках, рассмотрении обращений граждан и другая правовая информация.

Весь этот массив содержится в пяти информационных системах, к которым предоставлен удаленный доступ всем заинтересованным государственным и правоохранительным органам.

Самым обширным ресурсом является Система информационного обмена правоохранительных и специальных органов (далее – Система), разработанная Генеральной прокуратурой.

Доступ к Системе сотрудникам правоохранительных органов обеспечивается через защищенный канал связи посредством использования специального электронного ключа. Он именной, за счет чего администратор Системы может отслеживать действия каждого сотрудника в ней.

Система объединила 76 баз данных всех государственных органов страны. К примеру, следователь, используя Систему в рамках расследуемого уголовного, дела без бумажного запроса может оперативно получить сведения об объектах недвижимости у субъекта, наличии у него земельных участков, всех видов транспорта, обременений на них, оружия, судимости,

уплате налогов и штрафов, исполнительных документах о взыскании долга, выдаче паспортов, водительских удостоверений, полученных лицензиях, оказанных ему государственных услугах, выплате заработной платы, пенсий, пособий, выездах за пределы страны и многое другое. Прокурор, не выходя из кабинета, может получать в электронном режиме все необходимые для него данные по расследованию конкретного дела, то есть вести так называемый электронный прокурорский надзор.

Сотрудник дорожной полиции или участковый инспектор может оперативно узнать о наличии сведений по прошлым фактам привлечения проверяемого лица к ответственности, нахождении его в розыске, неуплате им алиментов и иную информацию [2].

В рамках общенадзорной деятельности для прокурора хорошим помощником выступает сервис «Взаимосвязанные лица». Работая с сервисом электронных государственных закупок, можно сопоставить данные по различным тендерам, провести сверку цен на услуги и товары, выявить взаимосвязи участников закупок. С подключением базы данных миграционной полиции, судов и пограничной службы стал прозрачным контроль за выдворением незаконных мигрантов.

К примеру, в ходе выборочного мониторинга выявлены 600 лиц, подлежащих по решениям судов депортации, но не выдворенных из страны. Другой мониторинг данных выявил порядка 60 лиц, совершивших ДТП в состоянии алкогольного опьянения, в отношении которых прекращены дела за примирением сторон, однако вопрос о лишении водительских прав остался не решенным. В необходимых случаях этот сервис позволяет выявить всех владельцев движимого и недвижимого имущества, начиная с самого первого. Можно отследить работников, чьи пенсионные отчисления идут от одного работодателя; участников групповых нотариальных действий и нотариусов; попутчиков на железнодорожном и авиатранспорте.

Необходимо отметить, что Система оправдала себя и при розыске преступников. Теперь информация обо всех операциях, произведенных разыскиваемыми лицами, собирается в один объем и Система автоматически сигнализирует правоохранительному органу о них.

К примеру, Система показала, что гражданин Т., находившийся в розыске за совершение изнасилования на юге Казахстана, устроился на работу на западе страны. На его имя работодателем отчислялись пенсионные выплаты. Благодаря электронным ресурсам Системы пенсионные поступления, их локализация были отслежены, а сам преступник был задержан. Применяя подобную схему поиска, а также и по другим видам государственных услуг (документирование, прописка, оплата сборов и штрафов).

Для повышения оперативности расследования реализуется механизм выдачи требований о судимости в электронном виде. Схема его проста: сотрудник органа уголовного преследования может оформить электронное требование в Системе информационного обмена, а судья или прокурор может проверить его через сайт. Теперь время исполнения такого запроса занимает не более 3 минут, тогда как раньше на это требовалось от 3 до 5 дней. Разработана и мобильная версия портала Системы информационного обмена. Благодаря этому полицейские уже в пути следования на место происшествия с помощью мобильного устройства могут получить первичную информацию (анкетные данные потерпевшего, возможного подозреваемого, сведения о наличии оружия, автотранспорта, психических расстройств, судимости и другие данные, имеющие значение).

Благодаря принятым мерам и предусмотренной возможности ведения онлайн контроля достигнуты прозрачность и оперативность рассмотрения заявлений о преступлениях. Данный ресурс позволяет сейчас рассматривать до 92% заявлений от их общего количества в оперативные 3-х дневные сроки. Кроме того, граждане имеют возможность знать о текущем состоянии общественной безопасности по географической Карте преступности. Интерактивная карта предусматривает данные о совершаемых преступлениях, вплоть до улиц и домов, по времени суток и сезонности. Сведения на карту передаются из ЕРДР. Граждане наглядно могут видеть криминогенные места, могут выбрать наиболее безопасные районы для

проживания, полиция – выстраивать маршруты патрулирования, а исполнительные органы – принимать меры по благоустройству и обеспечению общественной безопасности. Эта карта в первую очередь полезна органам полиции, которые оперативно реагируют на очаги преступности и принимают профилактические меры (камеры наблюдения, автопатрули и прочее). Граждане также могут подключить свои мобильные аппараты, задать интересуемый радиус, после чего им будут приходить данные о преступлениях в конкретном месте [3].

Это также позволяет общественности не только контролировать работу правоохранительных и других государственных органов по профилактике преступности, но и принимать активное участие в обеспечении правопорядка.

Такой же принцип использован при разработке карты дорожно-транспортных происшествий, которая доступна на сайте Генеральной прокуратуры. Данные учета дорожно-транспортных происшествий, а также пострадавших в них теперь отражаются на карте с детализацией по трассам, населенным пунктам, перекресткам и улицам.

Эта статистика не означает, что граждане стали меньше соблюдать правопорядок и больше совершать правонарушения. Повсеместное внедрение средств видеофиксации явилось одним из эффективных инструментов для соблюдения принципа «неотвратимости наказания». Нарушения незамедлительно попадают в процессинговый центр ЕРАП для обработки и оформления предписания о необходимости уплаты штрафа с автоматическим направлением SMS-уведомления о порядке сокращенного производства.

Информационная система ЕРАП «Единый реестр административных производств», комитет также оцифровывал весь процесс привлечения к административной ответственности.

Поэтапная автоматизация процессов вывела из тени скрытые правонарушения, которые раньше не фиксировались. Если в 2010 году по стране регистрировалось около трех миллионов правонарушений, то к 2015 году их количество возросло до четырех миллионов, а по итогам 2021 года и 10 месяцев 2022 года – свыше семи миллионов административных правонарушений.

В ЕРАП интегрированы 19 банков второго уровня и Казпочта. Это дало возможность реализовать в мобильных приложениях банков второго уровня функционал по оплате административных штрафов. В целом уполномоченными органами в электронном формате административное производство ведется по 88% правонарушений.

В рамках государственном программы «Цифровой Казахстан» Комитет по правовой статистике и специальным учетам Генеральной прокуратуры страны запустил информационную систему «Единый реестр административных правонарушений». Данная система позволяет автоматически идентифицировать правонарушителя, правильно определять квалификацию деяния, определять размер наложенного взыскания. Сам ЕРАП в себе заключает уже более 67 интегрированных государственных органов, которые уполномочены возбуждать административные производства. Также, в этой системе регистрируются все правонарушения государственных органов.

Кроме того, в информационную систему ЕРАП интегрировали базы данных судебных исполнителей. А еще к ней подключены 19 банков второго уровня и Казпочта. Это было сделано, чтобы правонарушители могли в более удобном формате оплачивать административные штрафы. В информационную систему ЕРАП автоматически приходят данные о правонарушениях с установленных видеокамер.

Благодаря цифровизации стало менее затратным как по времени, так и по процедурам фиксировать правонарушения. Если ранее сотрудник дорожной полиции, остановив автолюбителя за нарушение Правил дорожного движения, оформлял это нарушение полчаса, то сейчас на это затрачивается 5-7 минут. Все действия производятся на планшете, и при этом гражданин может сразу оплатить штраф в сокращенном порядке с 50-процентной скидкой. И сотруднику полиции, и гражданину удобно.

Все это способствовало повышению исполняемости уплаты штрафов и повышению правовой дисциплины в обществе. Если в 2010 году штраф платил один из четырех правонарушителей, то сейчас – уже трое из четырех. В суммарном выражении взыскиваемость штрафов выросла с 27% до 70%.

Внедрение проекта «Электронное обращение» (единая платформа для работы с обращениями граждан) позволила всем государственным органам от центра до сельских регионов работать с обращениями в единой информационной среде. Автоматизация процессов в информационной системе (регистрация, порядок проведения процедур и принятия решений) ориентирована на требования нового Административного процедурно-процессуального кодекса, вступившего в действие с 1 июля 2021 года.

Следует отметить, в соответствии с законодательством комитет оказывает информационно-справочное обслуживание граждан. То есть главная задача – это информирование человека, гражданина и общества о правовых процессах в стране, как в целом, так и индивидуально каждой личности.

Во-первых, это общая безопасность общества. Если каждый будет знать о криминогенной ситуации в стране, районе или месте своего проживания, то человек уже будет защищен, так как может не только потребовать от госорганов принятия мер, но и сам принять усилия по собственной защищенности.

Во-вторых, лица, вовлеченные в уголовный процесс, зная, что делается по их заявлению или как расследуется уголовное дело в отношении них, могут отстаивать свои права и требовать выполнения прямых обязанностей от органов расследования. Для этого мы обеспечиваем достоверность сведений ЕРДР от начала и до завершения расследования, вплоть до вынесения приговора судом и его исполнения. В этих же целях сотрудники комитета на постоянной основе проводят проверки соблюдения учетно-регистрационной дисциплины со стороны органов досудебного расследования. Принимаются меры, чтобы все заявления граждан рассматривались в установленные сроки, по ним принимались законные решения и не укрывались преступления. И от того, насколько правильными и достоверными будут сведения, зависят интересы людей, вовлеченных в орбиту уголовного процесса. В рамках цифровизации для участников уголовного или административного производства создана возможность в онлайн-режиме иметь доступ не только к сведениям, но и процессуальным документам по электронным делам через «Публичный сектор» ЕРДР, который доступен всем гражданам на портале «Информационный сервис» (Qamqor.gov.kz) [4].

В-третьих, это оказание государственных услуг. В основном граждане ранее знали комитет как орган, выдающий справки о наличии либо отсутствии судимости. Данная государственная услуга «Выдача справки о наличии либо отсутствии судимости» ранее предоставлялась территориальными органами комитета при личном обращении гражданина с выдачей бумажной справки. После 2014 года данная государственная услуга была автоматизирована. Сейчас справки выдаются автоматически в течение 10 минут, если для этого не требуется дополнительная проверка. В целом комитетом ежегодно выдаются более 3,5 миллиона справок о наличии либо отсутствии судимости в рамках оказания государственной услуги.

Еще одной государственной услугой, оказываемой комитетом является апостилирование официальных документов, исходящих из органов прокуратуры, органов следствия и дознания. Сейчас гражданин имеет возможность, не выходя из дома, подать одно заявление онлайн и получить справку с апостилем в любом выбранном им городе страны.

Кроме того, на портале Информационный сервис (Qamqor.gov.kz) комитета реализована возможность подать заявление в полицию в режиме онлайн, не выходя из дома, а также можно узнать о своих штрафах и своевременно их оплатить, получить информацию о ходе рассмотрения своих обращений по уникальному номеру талона, который выдается государственными органами, и другую интересную правовую информацию.

Тем самым правовая информация стала открытой и доступной для физических и юридических лиц.

Помимо сферы уголовного процесса прокуратурой внедрен электронный проект под названием «Айкын» (прозрачность). Уникальность этого проекта состоит в том, что сами граждане могут узнать о ходе рассмотрения обращений в государственных органах через Интернет, отслеживая не только их продвижение по инстанции, но и принятие решения, а также контролировать сроки рассмотрения. Для этого заявителям выдается талон с индивидуальным номером, предназначенным для входа в автоматизированную систему.

Также с 1 января 2016 года полностью автоматизирован процесс передачи данных из информационных систем государственных органов всех уровней в информационную систему «Единый учет обращений лиц».

Это позволило полномасштабно реализовать проект «Айкын», целью которого является установление прозрачности процедуры прохождения документов, предоставление доступа гражданам к сведениям о ходе рассмотрения их обращений, а также исключение личного контакта чиновников и граждан, как предпосылки к коррупционным действиям. Для этого заявителям при обращении в государственный орган выдается талон с уникальным 18-значным номером. По номеру талона граждане посредством информационного сервиса Комитета по правовой статистике и специальным учетам могут отследить ход рассмотрения своего обращения и получить сведения о регистрации и результатах рассмотрения, а также ознакомиться с ответом еще до получения его по почте.

Кроме того, при направлении гражданами обращения заказным письмом, государственный орган вносит в информационную систему указанный на конверте почтовый идентификатор и добавляет к нему символы «55555». Введя этот номер на информационном сервисе граждане также могут получить данные по своему обращению.

Кроме того, в целях установления обратной связи с населением и оперативного разрешения возникающих вопросов на веб-сайте Комитета ведет работу онлайн-консультант. Пользователи имеют возможность задать интересующие их вопросы, связанные с правовой статистикой и специальными учетами, использованием информационных сервисов, в том числе, касательно рассмотрения обращений в государственные органы, и получить ответы в режиме реального времени. В нерабочее время вопросы принимаются по электронной почте, ответы на которые направляются на электронный адрес пользователя.

Представляется, что это послужит прочной основой к построению современного формата правоохранительной системы, повышению уровня доверия населения к ней и обеспечению прав граждан.

Перечень информационных систем КПСиСУ ГП РК

1. «Единая унифицированная статистическая система» (ЕУСС) обеспечивает формирование статистических отчетов и аналитических сведений в сфере уголовной, гражданской и административной правовой статистики.

2. «Специальные учеты» (АИС СУ) – это банк данных всех видов учетов, в том числе учетов лиц, привлеченных к уголовной ответственности, осужденных, разыскиваемых, признанных судом недееспособными и ограниченно дееспособными, уволенных по отрицательным мотивам с государственной службы, экстремистов и террористов.

3. «Автоматизированная дактилоскопическая информационная система» (АДИС) – это банк, который позволяет установить личность по отпечаткам пальцев. Содержит сведения о состоящих на дактилоскопическом учете лицах, задержанных без определенного места жительства и документов, удостоверяющих личность, арестованных и осужденных за совершение уголовных преступлений.

4. «Единый учет обращений лиц» (ЕУОЛ) – это база данных всех обращений физических и юридических лиц в государственные органы, их движение и результат рассмотрения.

5. «Централизованный банк данных должников «Шектеу» (ЦБДД «Шектеу») содержит данные обо всех физических и юридических лицах, имеющих долговые обязательства перед государством, сведения о наличии предусмотренных законодательством ограничений и принятых судебных актов об ограничении выезда должника за пределы Республики Казахстан, временном запрещении выдачи лицензий и разрешений, приостановлении действий, ранее выданных должнику лицензий и разрешений.

6. «Информационный сервис» (http://qamqor.gov.kz) предоставляет заинтересованным государственным органам удаленный доступ к вышеуказанным информационным базам Комитета (ЕУСС, АИС СУ, ЕУОЛ, «Шектеу») для обеспечения своевременной, полной и достоверной информацией, находящейся в ведении правовой статистики и специальных учетов.

7. «Система информационного обмена правоохранительных, специальных государственных и иных органов» (СИО ПСО) – портал для получения необходимой

информации правоохранительными и специальными органами из баз данных государственных органов в электронном виде (в on-line режиме), для оперативного реагирования и использования информации в служебных целях.

8. «Единый реестр досудебных расследований» (ИС ЕРДР) – автоматизированная база данных, предназначенная для регистрации уголовных правонарушений, расследования уголовных дел (в том числе в электронном формате), прокурорского надзора за ходом досудебного расследования и направления уголовных дел в суд.

9. «Единый реестр административных правонарушений» (ИС ЕРАП) – автоматизированная база данных, предназначенная для автоматической идентификации правонарушителя, правильного определения квалификации деяния, определение размера наложенного взыскания.

10. Информационно-аналитическая система судебных органов «Төрелік».

11. Автоматизированная информационная система «Интегрированная аналитическая составляющая информационных систем КПСиСУ ГП РК» («Oracle Bi») – информационная аналитическая система, являющаяся аналитическим инструментом, который позволяет формировать любые запросы и отчеты на основании электронных информационных учетных документов, содержащихся в информационных системах Комитета.

Правовая статистика и отчетность по преступности, ее видам, категориям, масштабам, а также по субъектам и другим критериям формируется в автоматическом режиме. Что значительно повышает оперативность уголовного судопроизводства.

Таким образом, информация является одним из важнейших инструментов государственного управления. Деятельность органов государственной статистики Республики Казахстан направлена на обеспечение органов управления достоверной и полной информацией. Она строится на принципах методологического единства и централизации. Безусловно, все это играет серьезную роль в улучшении работы этих органов, а также в деле изучения и предупреждения преступности.

Литература

1. https://www.gov.kz/memleket/entities/pravstatlang=kk
2. Закон Республики Казахстан от 19 марта 2010 года №257-IV «О государственной статистике» (с изменениями и дополнениями по состоянию на 02.01.2023 г.)
3. Закон Республики Казахстан от 22 декабря 2003 года №510 «О государственной правовой статистике и специальных учетах»
4. Интернет – ресурс https://qamqor.gov.kz/crimestat/indicators
5. Приказ Генерального прокурора Республики Казахстан от 27 сентября 2022 года №191 «О внесении изменений и дополнений в некоторые приказы Генерального Прокурора Республики Казахстан в сфере правовой статистики и специальных учетов»
6. Закон Республики Казахстан от 6 января 2011 года №380-IV «О правоохранительной службе» (с изменениями и дополнениями по состоянию на 11.09.2022 г.)
7. Якимов И.Н. Современные положения регистрации преступников // Рабоче-крестьянская милиция. – 1923. http://www.juristlib.ru/book_10432.html (Интернет-ресурс).
8. О Концепции правовой политики Республики Казахстан до 2030 года: Указ Президента Республики Казахстан от 15 октября 2021 года №674.

СЕРАЛИЕВА А.М.,
Құқықтану кафедрасының
қауымдастырылған профессоры,
заң ғылымдарының кандидаты,
(Абай атындағы Қазақ ұлттық
педагогикалық университеті)

БАЙМАГАМБЕТОВА З.М.
халықаралық құқық кафедрасының аға
оқытушысы, доктор PhD
Әл-Фараби атындағы Қазақ ұлттық
университеті

ОТБАСЫНДАҒЫ ТҰРМЫСТЫҚ ЗОРЛЫҚ-ЗОРЛЫҚТЫҢ ҰҒЫМДАРЫ МЕН ФОРМАЛАРЫ

Соңғы кездері отбасындағы тұрмыстық зорлық-зомбылық мәселесі отбасы мүшелерінің ішкі ісі болып табылатын тұлға аралық жанжал ретінде ғана емес, адам құқықтарын бұзу ретінде қарастырылғандықтан отбасындағы тұрмыстық зорлық-зомбылық мәселесі ерекше өзекті бола бастады.

Халықаралық деңгейде тұрмыстық зорлық-зомбылық көбінесе әйелдерге қатысты зорлық-зомбылық контекстінде қарастырылады. ҚР Президенті жанындағы Әйелдер істері және отбасылық-демографиялық саясат жөніндегі ұлттық комиссияның мәліметі бойынша соңғы бес жылда елімізде әйелдерге қатысты ауыр қылмыстар саны 153 пайызға, тұрмыстық салада екі еседен астамға өскен [1].

Тұрмыстық зорлық-зомбылықты әлеуметтік құбылыс ретінде анықтау кезінде келесі ұғымдар қолданылады: отбасылық зорлық-зомбылық, тұрмыстық зорлық-зомбылық. «Тұрмыстық зорлық-зомбылық» термині зорлық-зомбылық әрекеттері жасалатын жер ретінде үй аумағын білдіреді. Криминологиядағы тұрмыстық (отбасылық) зорлық-зомбылықты «тұрмыстық» немесе «отбасылық-тұрмыстық» деп те атайды. Ол құқықтық немесе нақты қатынастарда тұратын отбасының бір мүшесінің немесе оған теңестірілген адамның екінші адамға қайталанатын қатыгездік қарым-қатынас жасауынан қалыптасады [2]. Тұрмыстық зорлық-зомбылық – бұл бір адамның жақын қарым-қатынастағы серіктесін бақылауға және үстемдік етуге тырысуы. Бұл физикалық, моральдық және жыныстық қорлау және қаржылық жағдайды теріс пайдалану арқылы көрсетілуі мүмкін. Көп жағдайда мұны ерлер әйелдерге қатысты жасайды. Кез келген үйде кез-келген әйел осындай жағдайға ұшырауы мүмкін. Сіздің серіктесіңіздің тарапынан сізді қорлап жатқанын көрсететін ескерту белгілері болуы мүмкін [3, 115-116 б.].

Отбасындағы қылмыстық тұрмыстық зорлық-зомбылық бірқатар факторларға байланысты айтарлықтай ерекшелікке ие.

1. Отбасындағы зорлық-зомбылық қылмыстылық, қылмыскер мен жәбірленуші арасындағы қарым-қатынастың ерекшелігіне байланысты, латенттіліктің жоғары деңгейімен сипатталады. Яғни, жәбірленушілер мен отбасының басқа мүшелері құқық қорғау органдарына жүгіну стигмасына байланысты көмекке жүгінбейді және өз мәселелерін өздері шешеді.

2. Отбасындағы тұрмыстық зорлық-зомбылыққа байланысты құқық бұзушылықтар бүкіл әлемде жиі кездеседі. Құқық бұзушылықтың субъектісі мен жәбірленуші бір-бірін танитын, бірге өмір сүретін, қарым-қатынас жасайтындықтан олар жеке сипатта болады.

3. Отбасылық өмір – адам тіршілігінің жеке саласы, сондықтан ол құқықтық реттеуге нашар ұшырайды және отбасындағы қарым-қатынастың өзі көбінесе құқықтық нормаларға негізделмейді, бірақ тәрбиелік әсерге ие (мысалы, арқасынан шапалақпен ұру, белдікпен ұру және т.б.).

Тұрмыстық зорлық-зомбылық физикалық, психологиялық, жыныстық және (немесе) экономикалық зорлық-зомбылық түрінде көрсетілуі мүмкін [4, 4-бап, 1-тармақ].

Физикалық зорлық-зомбылық – физикалық күш қолдану және физикалық ауырсыну арқылы денсаулыққа қасақана зиян келтіру [4, 4-бап, 2-тармақ].

Л.Д. Гаухман «физикалық зорлық-зомбылық басқа адамның денесіне оның еркінен тыс қоғамдық қауіпті құқыққа қарсы әсер ету» деп есептейді [5, 6 б.]. Физикалық зорлық-зомбылық әрқашан әрекет болып табылады және әрекетсіздік арқылы жүзеге асырылмайды [6]. Физикалық зорлық-зомбылық жәбірленушінің физикалық ауырсынуын, денсаулығына әртүрлі ауырлықтағы зиян келтіру немесе өлім түрінде әртүрлі салдарға әкелуі мүмкін. Физикалық мәжбүрлеу адам ағзасының анатомиялық тұтастығын бұзуға (ұрып-соғу, қару қолдану және т.б.), басқа физиологиялық процестерге (күшті дәрілік, есірткі және психотроптық препараттарды, антипсихотиктерді қолдану, тамақтан айыру, ұйқы және т.б.) және мәжбүрлі адамның физикалық еркіндігін шектеуге (ұстау, байланыстыру және т.б.) әсер етуі мүмкін. [7, 38 б.].

Психикалық зорлық-зомбылыққа келетін болсақ, ол жәбірленушіні физикалық зорлық-зомбылықпен қорқыту, қорқыту құралы ретінде бірқатар қылмыстар жасау кезінде қолданылады, көбінесе белгілі бір ауызша мәлімдемелер, ишаралар, қару-жарақ немесе басқа заттардың көмегімен сөзсіз қырғын-сүргін тудыру әсерін қалдырады [8].

Психикалық зорлық-зомбылық – адамның психикасына қасақана әсер ету, қорқыту, қорлау, бопсалау немесе өмірге немесе денсаулыққа қауіп төндіретін, сондай-ақ психикалық, физикалық және жеке дамудың бұзылуына әкелетін құқық бұзушылықтар немесе әрекеттер жасауға мәжбүрлеу арқылы ар-намыс пен қадір-қасиетті қорлау [4, 4-баптың 3-тармағы].

Р.А. Левертованың пікірінше, «қорқыту – психикалық зорлық-зомбылықты білдірудің жалғыз түрі» [9, 6 б.]. Психикалық зорлық-зомбылық тек физикалық зорлық-зомбылық, моральдық және мүліктік зиян келтіру қаупімен ғана емес, сонымен қатар жәбірленушіге немесе оның жақындарына беделін түсіретін мәліметтерді таратумен және т. б. байланысты деп санаймыз.

Е.Г. Веселов психикалық зорлық-зомбылықтың формалары туралы мәселеге сәл өзгеше көзқараспен қарайды: психикалық зорлық – зомбылық деп ол «адам психикасына кез-келген мақсатты деструктивті әсер ету: қорлау, адамның қадір-қасиетін жүйелі түрде қорлау, қиянат, гипноз, есірткі немесе психотроптық заттарды мәжбүрлеп енгізу, оның ішінде оның өміріне немесе денсаулығына зиян келтіру қаупі» деп түсінеді [10]. Бұл есірткі немесе психотроптық заттарды мәжбүрлеп енгізу деп жәбірленушінің денесіне оның еркіне қарсы (күштеп) енгізу түсіндіріледі. Есірткі немесе психотроптық заттарды ерікті түрде қолдану зорлық-зомбылық ретінде қарастырылмайды.

Қорқытудың негізгі объектісі адам психикасы болып табылады. Зорлық-зомбылықпен қорқыту психикаға әсер етеді, ол қорқыту, жәбірленушіге физикалық күш қолдану арқылы қорқыту арқылы жүзеге асады.

Ұсынылған психикалық зорлық-зомбылық анықтамаларының жалпы тізімі оның бірқатар ортақ белгілерін анықтауға мүмкіндік береді:

– психикалық зорлық-зомбылық сыртқы ортада көрініс табады;

– ол адам мінез-құлқының нақты саналы әрекеттерінде көрінеді;

– белгілі бір нысандарда көрсетіледі (әдетте, ол жәбірленушіге ақпаратты түрде әсер етеді);

– тікелей (жәбірленушіге бағытталған) және жанама (оның туыстарына, мүлкіне қарсы, болашаққа бағытталған және т.б.) сипатта болуы мүмкін;

– нақты адресаты бар;

– белгілі бір мақсаттарды көздейді (физикалық, материалдық немесе моральдық зиян келтіру, ерік бостандығын шектеу); қылмыс жасау құралы ретінде әрекет етеді; белгілі бір салдар туғызады [11, 29 б.].

Бұл жәбірленушіні қылмыстық талаптарға бағынуға, оның еркін басуға мәжбүрлеуге бағытталған психикаға әсер ету құралы болып табылады. Қорқытуды білдіру тәсілдері әртүрлі болуы мүмкін: сөздік нысан, қаруды көрсету, ым-ишара, құқық бұзушылықтың жасалу жағдайы және т.б. Қорқыту кінәлі тарапынан адамға тікелей айтылуы мүмкін немесе үшінші тараптар арқылы берілуі мүмкін [12].

Психологиялық зорлық-зомбылық қорлауға, мазақ етуге бағытталған әрекеттер арқылы жүзеге асырылуы мүмкін. Психикалық зорлық-зомбылық ұғымы жәбірленушіге оның еркіне қарсы (немесе одан тыс) заңсыз психикалық әсер етудің кез келген түрін қамтуы мүмкін. Демек, психикалық зорлық-зомбылық құқық бұзушылық жасау тәсілі немесе құралы бола алады, сондай-ақ жасалған әрекеттің жағдайын сипаттай алады, бұл олардың жиынтығында жасалған қоғамдық қауіпті әрекетті дұрыс саралауға әсер етеді.

Қылмыстық құқық ғылымында жыныстық зорлық-зомбылықтың бұл түрі өздігінен дербес бөлінбейді. Алайда, қылмыстық заңда жыныстық сипаттағы зорлық-зомбылық әрекеттерін жасағаны үшін жауапкершілікті белгілейтін норманың пайда болуымен (ҚР ҚК 121-бабы) зорлық-зомбылықтың осы түрін заңнамалық тұрғыдан бөліп көрсету туралы айтуға болады (дегенмен «жыныстық зорлық-зомбылық» термині ҚР ҚК-де қолданылмайды [12]. Бірақ бұл термин ҚР «Тұрмыстық зорлық-зомбылықтың профилактикасы туралы» Заңының 4-бабының 4-тармағында қолданылады: «жыныстық зорлық – зомбылық – адамның жыныстың тиіспеушілігіне немесе жыныстық еркіндігіне қауіп төндіретін құқыққа қарсы қасақана іс-әрекет, сондай-ақ кәмелетке толмағандарға қатысты сексуалдық сипаттағы іс-әрекеттер». Жыныстық зорлық-зомбылық – бұл басқа адамның көмегімен жыныстық қанағаттану, бірақ оның қалауына қарсы болады. Серіктестік/ерлі-зайыптылық қатынастардағы жыныстық зорлық-зомбылықтың келесі көріністері бар: жыныстық зорлық-зомбылық, жыныстық мәжбүрлеу, қудалау, физикалық күшті, қорқытуды қолдану арқылы жыныстық қатынасқа түсу, ұрып-соғудан кейін жыныстық қатынасты күштеп жасау, жыныстық қатынасты қорлау құралы ретінде пайдалану [13]. Жыныстық зорлық-зомбылық отбасында жиі кездеседі және жоғары латенттілікке ие. Жәбірленуші агрессордың әрекетіне физикалық немесе психологиялық тұрғыдан қарсы тұра алмайды немесе өзінің даму ерекшеліктеріне байланысты агрессордың іс-әрекетінің сипатын түсінбейді.

Экономикалық зорлық-зомбылыққа келетін болсақ, бұл адамды тұрғын үйден, тамақтан, киім-кешектен, мүліктен, заңда көзделген құқығы бар қаражаттан қасақана айыру. Ерлі-зайыптылардың/серіктестердің қарым-қатынасындағы зорлық-зомбылықтың экономикалық түрі отбасы жүйесіндегі ресурстардың біркелкі бөлінбеуіне негізделген. Бұл нысанның мынадай көріністері бар: отбасының кәмелетке толған бір мүшесінің екіншісін отбасы бюджетін басқару мүмкіндігінен айыру, қаражатқа ие болу және оларға өз қалауы бойынша билік ету құқығынан айыру әрекеті, балаларды асыраудан бас тарту, оған тікелей жұмыс істеуге тыйым салу, кірісті жасыру, отбасылық қаражатты жұмсау, қаржылық шешімдердің көпшілігін өз бетінше қабылдау, шығындарды барынша қатаң бақылау [14].

Тұрмыстық зорлық-зомбылық субъектілері бойынша: ерлі-зайыптылар арасындағы зорлық-зомбылық, туыстар мен балалар арасындағы зорлық-зомбылық, басқа туыстарға (әжеге, атаға және т.б.) зорлық-зомбылық көрсету болып бөлінеді. Криминологиялық аспекті тұрғысынан мұндай қатынастардың заңды немесе нақты некеден туындауы, сондай-ақ адамдардың бірге тұру немесе бөлек тұру фактісі маңызды емес.

Зорлық-зомбылықтың танымал түрлерінің қатарына айқайлау, қорлау, ұрып-соғу, жала жабу, мүлікті бүлдіру және т.б. атауға болады. Зорлаушы билікке ұмтылады, өзін-өзі растағысы келеді, жәбірленушіні қорлау арқылы өзін жоғарылатқысы келеді. Көбінесе айқайлау мен қорлау ұрып-соғумен бірге жүреді.

Тұрмыстық зорлық-зомбылыққа байланысты алдын алу шараларының жүйесін жалпы сипаттағы (құқық қорғау және мемлекеттік органдардың қызметі және т.б.) және жеке сипаттағы (тұрмыстық зорлық-зомбылық құрбанының мінез-құлқына байланысты) призмадан қарастыруға болады деп санаймыз. Е.С. Қайыржановтың пікірінше, «қылмыс үшін жазалаудан гөрі оның алдын алған дұрыс» [15, 168 б.]. Сондықтан, егер сіз немесе сіздің туыстарыңыз, көршілеріңіз тұрмыстық зорлық-зомбылыққа ұшыраған болса, ешбір жағдайда үндемей қалмауыңыз керек. Осындай жағдай орын алғанда ішкі істер органдарына өтінішпен жүгіну қажет. Сондай-ақ, біз тұрмыстық зорлық-зомбылыққа байланысты құқық бұзушылықтардың алдын алу – бұл осы құқық бұзушылықтарды тудыратын себептер мен жағдайларды жою, бейтараптандыру немесе жою жөніндегі қызмет деген қорытындыға келдік.

Әдебиет

1. Как цифровые технологии помогают защищать жертв домашнего насилия в Казахстане от 21.04.2023// [Электронный ресурс] – Режим доступа //https://news.un.org/ru/story/2023/04/1440112. (Дата обращения: 25.08.2023).
2. ООН: домашнее насилие. //[Электронный ресурс] – Режим доступа: https://caparolsochi.ru/oon-domashnee-nasilie (Дата обращения: 26.08.2023).
3. Рустемова Г.Р., Насырова Э.М. К вопросу о семейно-бытовом насилии// «Бытовое насилие: переосмысление системы противодействия» материалы международной научно-практической конференции (12.09.2022) – Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы, 2022. – С. 115-118.
4. Закон РК от 4.12.2009 № 214-IV «О профилактике бытового насилия» (с изм. и доп. по сост. на 01.07.2023) //[Электронный ресурс] – Режим доступа: // https://online.zakon.kz/Document /?doc_id=30525680&pos=64;-51#pos=64;-51 (Дата обращения: 27.08.2023).
5. Гаухман Л.Д. Борьба с насильственными посягательствами. - М. Изд-во: «Юрид. лит.» 1969. – С. 119.
6. Базаров Р.А. Уголовно-правовая характеристика насилия. Проблемы обеспечения личной безопасности граждан //Труды Академии МВД РФ. – М., 1995. – С. 42-48.
7. Уголовное право России. Практический курс /Под общ. ред. А. И. Бастрыкина; под науч. ред. А. В. Наумова. – М., 2007. – С.176-177.
8. Комментарий к Закону РК «О профилактике бытового насилия» [Электронный ресурс] – Режим доступа: //https://adilet.zan.kz/ rus/docs/T090000214 (Дата обращения: 27.08.2023).
9. Левертова Р.А. Ответственность за психологическое насилие по советскому уголовному праву. – Омск, 1978. – С. 103.
10. Веселов Е.Г. Физическое или психическое принуждение как обстоятельство, исключающее преступность деяния. - Автореф. дис. ... канд. юрид. наук. - Краснодар, 2002.
11. Клоченко Л.Н. Психическое насилие: вопросы уголовно-правовой регламентации и квалификации... дис. на соиск. уч. степ. к.ю.н. – М., 2019. – С. 204.
12. Дубянский С. Правовое понятие насилия от 22.11.2012 [Электронный ресурс] – Режим доступа://https://www.startbase.ru/knowledge/articles/98/ (Дата обращения: 28.08.2023).
13. Ератина Е.А., Ефремова В.А. Психологические особенности женщин с виктимным поведением в семье //Виктимность и виктимологическая профилактика: Материалы круглого стола по дисциплине «Психология отклоняющегося поведения». – Тверь: Твер. гос. ун-т, 2019. – С. 16-21.
14. Даренских С.С. Семейное насилие в отношении женщин //Известия АлтГУ. 2013. №2 (78). Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/semeynoe-nasilie-votnoshenii-zhenschin (Дата обращения: 27.08.2023).
15. Каиржанов Е.И. Криминология (Общая часть). Учебник. 2-е издание, пер. и допол. – Алматы, 2000. – С. 288.

ПАРСИЕВ С.С.
профессор кафедры инфомационных технологий Университета общественной безопасности Республики Узбекистан

МУСАЕВ А.И.
доцент кафедры тнфомационных технологий Университета общественной безопасности Республики Узбекистан

ОБЕСПЕЧЕНИЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИЙ ОБЩЕСТВА И ГОСУДАРСТВА

Цифровизация и информатизация являются важными процессами для развития общества и государства. Они позволяют улучшить качество жизни граждан, повысить эффективность работы государственных органов и бизнеса, а также снизить затраты на производство и потребление.

Обязанностью нашего государства является улучшение жизни общества и повышение уровня жизни населения, а также обеспечения защищенности общества от противозаконных посягательств, социальных и межнациональных конфликтов, чрезвычайных ситуаций и угроз, способствует устойчивому развитию общества и обеспечивает реализацию права, свободы и законных интересов человека;

В этом направлении государством проводится большая практическая работа. Объем государственных услуг, оказываемых населению, постоянно увеличивается. Обеспеченность Интернетом в нашей республике постоянно увеличивается. В июне 2023 года Узбекистан расположился на 85 месте в рейтинге скорости домашнего интернета от Speedtest Global Index.

По сравнению с маем страна поднялась на три позиции. Скорость домашнего интернета в Узбекистане оценивается в 51,25 Мб/с.

Финансовые услуги между банком и гражданами осуществляются полностью онлайн.

В условиях цифровизации и информатизации общества и государства большое значение имеет обеспечение общественной безопасности. Борьба с преступностью и ее профилактика эффективны в обеспечении общественной безопасности. Преступность в обществе – это прежде всего угроза общественной безопасности, она может вызывать тревогу у гражданского населения и, в свою очередь, может приводить к социальным потрясениям, более того, реализация преступности в цифровом мире также является поводом для обоснованных опасений общества. Необходимо учитывать что, созданная на данный момент информационная инфраструктура государств мира позволяет лицам, совершающим преступления, скрывать свою личность используя различные средства анонимайзеров, совершать их на расстоянии из любого места с применением аноноимных и беспроводных сетей, таких как TOR, VPN, и общаться со своими сообщниками прозрачно на международном уровне на мессенджерах [3] и осуществлять финансирование с использованием криптовалют и остаться незамеченными. На основе таких фактов специалисты в области информационных технологий и кибербезопасности отмечают, что «информационное общество» уже не имеет политических, социальных и экономических границ.

Для сбора доказательств, в том числе и на международном уровне, необходимым условием является использование возможностей компьютерных технологий по логированию, особенно по уголовным делам в сфере информационных преступлений. Для борьбы с новыми видами правонарушений, связанными с использованием компьютерной техники, многие государства разработали новое законодательство об ответственности за компьютерные преступления. Эффективное решение проблемы компьютерных преступлений требует согласованных международных действий и сотрудничества, особенно по передаче обезличенной технической информации которые не является передачей персональных данных. Однако это возможно только в том случае, если существует общее понимание проблемы государственными структурами и наличия необходимости рассмотрения таких решений [2].

Для предотвращения правонарушений в обеспечении общественной безопасностб а также для сбора доказательств в основном используются аппаратные устройства и программное обеспечение. В качестве аппаратных устройства мы можем предоставить различные типы камер, радаров и датчиков установленных в различных местах. Программное обеспечение, которое анализирует информацию, предоставленную в открытых источниках в обществе позволяет определить и предотвращать преступность в обществе. А также совместное использование аппаратного и программного обеспечения эффективно предотвращает преступность и киберпреступность.

В профилактике преступности создаются программы прогнозирования потрясений в обществе с использованием технологий искусственного интеллекта. При этом база искусственного интеллекта этого программного обеспечения обрабатывает через нейронную сеть события, повлиявшие на жизнь общества и их влияние на него. В этой нейронной сети рассчитываются индексы социального благополучия населения (душевой доход, газо-, электро- и водоснабжение), а также с помощью искусственного интеллекта обрабатываются сообщения, связанные с общественной жизнью и вызывающие эмоции, распространяемые в социальных сетях. В результате активизируются механизмы общественной безопасности и предотвращаются преступления. А так же искусственный интеллект может использоваться для обнаружения угроз безопасности, таких как кибератаки и мошенничество.

Создание аппаратного и программного обеспечения по определения индекса общественной безопасности на основе общественного мнения публикуемых в открытых ресурсах интернета, медиапространстве и в социальных сетей позволяет эффективно обеспечить общественной безопасности в условиях цифровизации общества и государства.

Литература.

1. Wiener N . Cybernetics or Control and Communication in the Animal and the Machine. – New York: The Technology Press and John Wiley & Sons, Inc. – Paris: Hermann et Cie, 1948.

2. Борьба с преступностью в киберпространстве: проблемы и решения, сборник материалов Республиканской научно-практической конференции, Академия МВД РУ, (24 февраля 2022 г.), Ташкент: MALIK PRINT Co., 2022. – С. 482.

ҚАРАТАЕВ ТҰРДАЛЫ ЖАҚСЫЛЫҚҰЛЫ
заң ғылымдарының кандидаты

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПО ҚЫЗМЕТКЕРЛЕРІНІҢ ДЕНЕ КҮШТЕРІ, АРНАУЛЫ ҚҰРАЛДАРЫ МЕН АТЫС ҚАРУЫН ҚОЛДАНУ ПРОБЛЕМАЛАРЫ

Қазақстан Республикасының Конституциясының 1-бабына сәйкес «Қазақстан Республикасы өзін демократиялық, зайырлы, құқықтық және әлеуметтік мемлекет ретінде орнықтырады, оның ең қымбат қазынасы – адам және адамның өмірі, құқықтары мен бостандықтары» болып табылады. Осы актінің 13-бабының негізінде «Әркімнің құқық субъектісі ретінде танылуына құқығы бар және өзінің құқықтары мен бостандықтарын, қажетті қорғанысты қоса алғанда, заңға қайшы келмейтін барлық тәсілдермен қорғауға хақылы» [1, б.2].

Адамдар мен азаматтардың өмірі мен денсаулығын қорғаудың әдістерінің бірі – мемлекеттік қызметкерлердің дене күштерін, арнаулы құралдарды қызметтік атыс қаруларын қолдану болып табылады.

Қолданыстағы нормативтік-құқықтық актілерге сүйенсек, көптеген мемлекеттік органдарға аталған іс-әрекеттерді жүзеге асыру өкілеттіктері берілген. Қазақстан Республикасының Құқық қорғау [2, б. 3], арнаулы мемлекеттік органдары [3], Қазақстан Республикасы Мемлекеттік күзет қызметі [4] Ұлттық қауіпсіздік органдары [5] Сыртқы барлау [6] Қазақстан Республикасының ІІМ Ұлттық ұлан Комитеті [7] Қазақстан Республикасының қорғанысы және Қарулы Күштері [8] «Қазақстан Республикасының кейбір заңнамалық актілеріне Қазақстан Республикасының арнаулы мемлекеттік органдары мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» Қазақстан Республикасының 2012 жылғы 13 ақпандағы №553-IV Заңы [9] және «Қазақстан Республикасындағы кедендік реттеу туралы» Қазақстан Республикасының Кодексі 2017 жылғы 26 желтоқсандағы №123-VI ҚРЗ 13-бабына сай [10] кеден органдары Қазақстан Республикасының заңнамасына сәйкес дене күші мен арнаулы құралдарды қолдана алады. Қосымша өкілеттіктер «Қазақстан Республикасының Ұлттық қауіпсіздік комитеті Шекара қызметінің мәселелері» Қазақстан Республикасы Президентінің 1999 жылғы 10 желтоқсандағы N 282 [11] және «Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен әскери құралымдарының жалпыәскери жарғыларын бекіту туралы» Қазақстан Республикасы Президентінің 2007 жылғы 5 шілдедегі N 364 Жарлығымен [12] реттеледі.

Соның ішінде ішкі істер органдарының дене күші, арнаулы құралдары мен атыс қаруларын қолдану негіздері мен тәртібіне қатысты сот тәжірибесінде бірқатар қиындықтар кездесіп отыр.

Қазақстан Республикасы аумағындағы 2022 жылы 4-5 қаңтардағы террористік актілер болған оқиға барысында көптеген адамдар қайтыс болды.

Бас прокуратураның есебіне сүйенсек Қазақстанда қаңтардағы оқиғаның салдарынан кемінде 225 адам қаза болған. Қазақстан бойынша 4578 жәбірленуші бар, 4 353-і жараланған. 3393-і – құқық қорғау орган қызметкері. Төтенше жағдай кезінде (5-14 қаңтар аралығында – БП) мәйітханаларға 225 адам жеткізілді. Бір бөлігі – теракті қатысқан қару ұстанған қарақшылар. 19-ы - құқық қорғау орган қызметкері. Өкінішке қарай, терроризм актісінен бейбіт тұрғындар да қаза болған» [13]. Бас прокуратураның мәліметінше 6 қаңтарға дейін

полиция атыс қаруын қолданбаған. 6 қаңтарда Қауіпсіздік кеңесінің шешімімен елде антитеррористік операция жүргізілетіні жарияланды. Осы күннен бастап құқық қорғау органдары мен Қарулы күштер террористерді жою үшін қару қолданылды. 2011 жылы Маңғыстау облысында жанжал барысында 72 адам жараланған, қайтыс болған адамдардың саны 16 құраған.

Ішкі істер органдары аталған құқықты «Қазақстан Республикасының ішкі істер органдары туралы» Қазақстан Республикасының Заңы 2014 жылғы 23 сәуірдегі №199-V ҚРЗ [14] 19-бабын басшылыққа ала отырып жүзеге асыра алады. Онда, «Ішкі істер органдары қызметкерлерінің арнаулы құралдарды, атыс қаруын және өзге де қаруды алып жүруге, сақтауға және қолдануға, дене күшін, оның ішінде жауынгерлік күрес тәсілдерін қолдануға құқығы бар» деп көрсетілген.

Ішкі істер органдарының дене күші, арнаулы құралдары мен атыс қаруларын қолдануда кездесетін мәселелердің бірі – қолданыстағы нормативтік-құқықтық актілердің тиісті деңгейде жетілмеуі деп есептейміз.

«Құқық қорғау қызметі туралы» Қазақстан Республикасының 2011 жылғы 6 қаңтардағы №380-IV Заңының 8 тарауында «Атыс қаруы және өзге де қару, арнаулы құралдар және дене күшін қолдану негіздері мен тәртібі» [2] қаралған.

Аталған заңның 59-бабына байланысты Атыс қаруы және өзге де қару, арнаулы құралдар және дене күші қоғамға қауіпті әрекеттерді тоқтату, құқық бұзушылықтардың сипаты мен нақты ахуалдарды ескере отырып, оларды жасаған адамдарды ұстау және құқық қорғау органдарына жеткізу мақсатында қолданылады.

Қызметкерлердің дене күшін, оның ішінде жауынгерлік күрес тәсілдерін, сондай-ақ арнаулы құралдарды қолданудың негіздеріне келесілерді жатқызуға болады:

– жеке тұлғаларға, қызметкерлерге және қоғамдық тәртіпті қорғау, қоғамдық қауіпсіздікті қамтамасыз ету және қылмыстылыққа қарсы іс-қимыл бойынша қызметтік немесе қоғамдық борышын атқарып жүрген өзге де адамдарға жасалған шабуылды тойтару;

– кепілге алынған адамдарды босату, жаппай тәртіпсіздіктердің және қоғамдық тәртіпті топтасып бұзудың (қылмыстық-атқару жүйесі мекемелерінде ұстаудың белгіленген режимін топтасып бұзушылықтарды), сондай-ақ сотталғандар, күдіктілер және айыпталушылар түзеу мекемелерінен және тергеу изоляторларынан қашқан кездегі немесе қашқандарды ұстау кезіндегі құқыққа қарсы әрекеттердің жолын кесу;

– жеке тұлғаларға, ұйымдарға және мемлекеттік органдарға тиесілі үйлерге, үй-жайларға, ғимараттарға, көлік құралдарына, жер телімдеріне жасалған шабуылды тойтару, сол сияқты оларды басып алудан босату;

– егер құқық бұзушылар (сотталғандар, күдіктілер, айыпталушылар және әкімшілік құқық бұзушылық жасағандар) қызметкерлерге, қоғамдық тәртіпті қорғау, қоғамдық қауіпсіздікті қамтамасыз ету бойынша өздеріне жүктелген міндеттерді атқарып жүрген өзге де адамдарға бағынбаса немесе қарсылық көрсетсе, оларды құқық қорғау органдарына жеткізу үшін ұстау үшін, ұсталған, күзет қойылған адамдарды, сондай-ақ әкімшілік қамауға алынған, сотталған, күдікті және айыпталушы адамдарды, не олардың қашып кетуі немесе айналадағыларға немесе өзіне зиян келтіруі мүмкін деп санауға жеткілікті негіздемелер болса, сондай-ақ қызметкерлердің өздеріне заңмен жүктелген міндеттерді жүзеге асыруына қасақана кедергі келтіретін адамдарға қатысты күзетпен апару және күзету;

– қызметкердің өзін-өзі қорғау немесе өзінің отбасының мүшелерін қорғау мақсатында оған және (немесе) олардың денсаулығына немесе өміріне ауыр зиян келтірудің нақты қаупі төнген кезде шабуылды тойтару;

– қажетті қорғаныс, аса қажеттік;

– егер бұл құқық бұзушылықтың жолын кесу, құқық бұзушының жеке басын анықтау, сондай-ақ егер хаттама жасау міндетті болып табылса, оны сол орында жасау мүмкін болмаған кезде әкімшілік құқық бұзушылық туралы хаттама жасау мақсатында қажет болса, құқық бұзушыларды жеткізу;

– егер жүргізуші қызметкердің тоқтату жөніндегі заңды талаптарына бағынбаса, көлік құралдарына ақау келтіру арқылы оларды тоқтату үшін қолдануға құқығы бар.

Арнаулы құралдарға қол кісендерін, резина таяқтарды, көзден жас ағызатын заттарды, алаңдатып әсер ететін жарық-дыбыс құрылғыларын, үй-жайларды ашуға, көлікті мәжбүрлеп тоқтатуға арналған құрылғыларды, суатқыштарды, қызметтік жануарларды, броньды машиналарды жатқызуға болады. Сонымен қатар аталған тізім «Қоғамға қауіпті іс-әрекеттерді тоқтату, оларды жасаған адамдарды ұстау және ішкі істер органдарына жеткізу мақсатында ішкі істер органдарының қызметкерлері қолданатын арнайы және көлік құралдарының тізбесін бекіту туралы» 2001 жылғы 30 қазандағы Қазақстан Республикасы Үкіметінің N 1375 қаулысымен [15] бекітілген.

Біріншіден, дене күші мен арнаулы құралдар жеке тұлғаларға, қызметкерлерге және қоғамдық тәртіпті қорғау, қоғамдық қауіпсіздікті қамтамасыз ету және қылмыстылыққа қарсы іс-қимыл бойынша қызметтік немесе қоғамдық борышын атқарып жүрген өзге де адамдарға жасалған шабуылды тойтару үшін қолданылады.

«Соттардың бандитизм және қылмыстық құқық бұзушылықтарға қатыса отырып, басқа қылмыстық құқық бұзушылықтар жасағаны үшін жауапкершілік туралы заңнаманы қолдануының кейбір мәселелері туралы» Қазақстан Республикасы Жоғарғы Сотының нормативтік қаулысы 2001 жылғы 21 маусым N 2. [16] Жәбірленушіге күш қолдану не оны дереу қолданамын деп шынайы қауіп туғызу арқылы қылмыстық нәтижеге қол жеткізуге бағытталған әрекетті бандитизм кезінде шабуыл жасау деп түсіну қажет. Осы қылмыс құрамының басқа да міндетті белгілері болған жағдайда, ішінде адамдары жоқ мекемелерге, кәсіпорындарға, ұйымдарға шабуыл жасау және оларға күш қолданбау жағдайларында және шабуыл жасау үрдісі кезінде адамдар зардап шекпей, мүліктің жойылу (кеңсені қопару, пәтерді, автомашиналарды өртеу) фактілерін бандитизм деп қарастыру қажет. Бұл ретте банданың құрамындағы шабуыл жасаушылардың олардың қылмыстық мақсаттарына жетуіне кедергі жасайтын кез келген адамға қарсы күш қолдануға дайын екенін назарда ұстау қажет. Банда мүшелерінің қолындағы қару қолданылмаған жағдайларда да қарулы банданың шабуыл жасауы орын алды деп есептеледі.

Аталған негізде шабуыл жасаудың нақты ұғымы айқындалмағандықтан осы құқықты пайдалануда қиындықтар кездесіп отыр.

Екіншіден, кепілге алынған адамдарды босату, жаппай тәртіпсіздіктердің және қоғамдық тәртіпті топтасып бұзудың (қылмыстық-атқару жүйесі мекемелерінде ұстаудың белгіленген режимін топтасып бұзушылықтарды), сондай-ақ сотталғандар, күдіктілер және айыпталушылар түзеу мекемелерінен және тергеу изоляторларынан қашқан кездегі немесе қашқандарды ұстау кезіндегі құқыққа қарсы әрекеттердің жолын кесу жатады.

«Адамдарды қоғамнан уақытша оқшаулауды қамтамасыз ететін арнаулы мекемелерде, арнаулы үй-жайларда ұстау тәртібі мен шарттары туралы» 1999 жылғы 30 наурыздағы заңға сай [17] күдіктілер және айыпталушыларды ұстау орындарына тергеу изоляторларынан бөлек уақытша ұстау изоляторлары да жатады. Бірақ көрсетілген негізде бұл норма қаралмаған.

Арнайы құралдың түрі, оны қолдану уақытының басталуы мен қарқындылығы орын алған жағдай, құқық бұзушылықтың сипаты және құқық бұзушының жеке басы ескеріле отырып айқындалады.

Ал «Құқық қорғау қызметі туралы» Қазақстан Республикасы заңының 60-бабына сәйкес, айналадағылардың өмірі мен денсаулығына қауіп төндіретін шабуыл, топтасқан шабуыл жасаған не қарулы қарсылық көрсеткен жағдайларды қоспағанда, әйелдерге, мүгедектік белгілері анық білініп тұрған адамдарға және жас балаларға қатысты арнаулы құралдар мен жауынгерлік күрес тәсілдерін қолдануға тыйым салынады.

Бірақ біздің пікірімізше аталған нормаларға толықтырулар мен өзгерістер ендіру керек. Сот тәжірибесі барысында әйелдер тарапынан да көптеген қылмыстық құқық бұзушылықтар жасалып отыр. Сонымен қатар, мүгедектік белгілері анық білініп тұрған адамдарға да арнаулы құралдар мен жауынгерлік күрес тәсілдерін қолдануға тыйым салынады. «Қазақстан

Республикасында мүгедектерді әлеуметтік қорғау туралы» Қазақстан Республикасының 2005 жылғы 13 сәуірдегі N 39 Заңына [18] сәйкес, «мүгедек – тұрмыс-тіршілігінің шектелуіне және оны әлеуметтік қорғау қажеттігіне әкеп соқтыратын, ауруларға, мертігулерге (жаралануға, жарақаттарға, контузияларға), олардың зардаптарына, кемістіктерге байланысты организм функциялары тұрақты бұзылып, денсаулығы нашарлаған адам» болып танылады. Тіршілік ету әрекетінің, оның ішінде еңбек ету қабілетінің шектелу дәрежесіне қарай мүгедектік үш топқа бөлінеді. Тәжірибе барысы көрсетіп отырғандай мүгедектік белгіні бірден анықтауға көп жағдайларда мүмкіншілік бола бермейді. Ал, қолданыстағы заң нормаларында «жас бала» деген мәртебе мүлдем кездеспейді. Қолданыстағы «Қазақстан Республикасындағы баланың құқықтары туралы» Қазақстан Республикасының 2002 жылғы 8 тамыздағы N 345 Заңының 1 бабына сай [19] «бала – он сегіз жасқа (кәмелетке) толмаған адам» болып табылады. Сондықтан аталған норманы да қолданыстағы заңмен сәйкестендіру керек. ІІО қызметкерлері атыс қаруын және өзге де қаруды «Құқық қорғау қызметі туралы» Қазақстан Республикасы заңының 61-бабына бекітілген негіздердер болған кезде қолданады: 1) жеке адамдардың өмірі мен денсаулығына қатер төнген жағдайда оларды қылмыстық қол сұғушылықтан қорғау, сол сияқты кепілге алынғандарды босату; 2) қызметкерлерге және олардың отбасы мүшелеріне, қоғамдық тәртіпті қорғау, қоғамдық қауіпсіздікті қамтамасыз ету және қылмыстылыққа қарсы іс-қимыл жасау жөніндегі қызметтік немесе қоғамдық борышын атқарып жүрген адамдарға жасалған шабуылға тойтарыс беру; 2-1) құқық қорғау органының атыс қаруын және өзге де қаруды, арнайы көлік құралын тартып алу әрекеттерінің жолын кесу; 3) жеке тұлғалардың тұрғын үй-жайларына, құқық қорғау органдары күзететін объектілерге, мемлекеттік ұйымдардың үй-жайларына жасалған шабуылға тойтарыс беру, қызметтік немесе әскери нарядқа жасалған шабуылға тойтарыс беру; 4) қарсылық көрсететін не қылмыс жасау кезінде үстінен түскен, қамаудан қашқан адамдарды (әкімшілік қамақта ұсталатындардан басқа) ұстау, қаруланған адамдарды ұстау; 5) егер көлік жүргізуші қызметкердің заңды талаптарына бағынбаса және жеке адамдардың өмірі мен денсаулығына қатер төндірсе, көлік құралдарына ақау келтіру арқылы оларды тоқтату; 6) адам өміріне немесе денсаулығына іс жүзінде қатер төндірген жағдайларда хайуанаттардың шабуылынан қорғану; 7) қару қолдану ниеті туралы азаматтарға ескерту, дабыл сигналын беру немесе көмекке шақыру үшін; 8) қажетті қорғаныстың және аса қажеттіліктің барлық өзге де жағдайларында қолдануға құқығы бар.

Жалпы атыс қаруы дегеніміз - оқ дәрі немесе өзге де заряд қуатының әсері нәтижесінде ұңғы оқпанынан оқты, снарядты, гранатаны ұшырып шығаратын қару. Өзінің бағытталған мақсаты бойынша қару: 1) жауынгерлік қол атыс қаруы мен суық қару; 2) азаматтық қару; 3) қызметтік қару болып бөлінеді.Қызметтік қаруларды қолданудың негізгі мақсаты – адамның жеке басының қауіпсіздігін қамтамасыз ету мақсатында Қазақстан Республикасының заңнамасына сәйкес қызметтік қаруды сатып алуға (алуға) құқығы бар мемлекеттік саяси қызметшілердің, Қазақстан Республикасы Парламенті депутаттарының, сондай-ақ азаматтардың өмірі мен денсаулығын, меншікті қорғау, қоршаған орта объектілерін және табиғи ресурстарды, бағалы және қауіпті жүктерді, арнаулы хат-хабарды күзету бойынша өздеріне заңнамамен жүктелген және өз жарғыларында (ережелерінде) көзделген міндеттерді жүзеге асыру кезінде қолдану [20, б. 3].

Қажетті қорғаныс және аса қажеттілік жағдайларында немесе қылмыс жасаған адамды ұстаған кезде қызметкер өзінде қажетті арнайы құралдар немесе қару болмаған кезде қолда бар кез келген құралды пайдалануға, сондай-ақ осы Заңда белгіленген негіздер бойынша және тәртіппен жарақтандыруда тұрмаған өзге де қаруды қолдануға құқылы.

Әйелдерге, анық мүгедектік белгілері бар адамдарға, жасы белгілі немесе анық болған кезде кәмелетке толмағандарға қатысты, олар қарулы шабуыл жасаған, қарулы қарсылық көрсеткен, адамдарды кепілге, көлік құралдарын, оның ішінде әуе кемесін басып алған не топтасып шабуыл жасаған жағдайларды қоспағанда, қару қолдануға тыйым салынады.

Атыс қаруын және өзге де қаруды, арнайы құралдарды, дене күшін қолданған кезде қызметкерлер: атыс қаруын және өзге де қаруды, арнайы құралдарды, дене күшін қолдануды кешіктіру азаматтардың, қызметкерлердің өмірі мен денсаулығына тікелей қауіп төндіретін, өзге де ауыр салдарларға әкеп соқтыруы мүмкін болатын немесе қалыптасқан жағдайда мұндай ескерту орынсыз немесе мүмкін емес болып табылатын жағдайларды қоспағанда, атыс қаруын және өзге де қаруды, арнайы құралдарды, дене күшін қолдану ниеті туралы ескертуге, бұл ретте оларды қолдану көзделіп отырған адамдарға өзінің талаптарын орындау үшін жеткілікті уақыт беруге міндетті. Атыс қаруын және өзге де қаруды, арнайы құралдарды және дене күшін бөлімшенің (топтың) құрамында қолданған жағдайда, көрсетілген ескертуді бөлімше (топ) басшысы немесе арнаулы атағы, сыныптық шені, біліктілік сыныбы жоғары қызметкер жасайды.

Жоғарыда көрсетілгендердің негізінде келесідей ұсыныстар жасалынды:

– қызметкерлердің дене күштері, арнаулы құралдары мен атыс қаруын қолдану алгоритімін реттейтін кодекс қабылдау керек;

– Қазақстан Республикасының «Құқық қорғау қызметі туралы» заңына өзгерістер мен толықтырулар ендіру қажет;

– қызметкерлердің дене күштері, арнаулы құралдары мен атыс қаруын қолданылатын тұлғалардың мәртебесін айқындау шарт.

Әдебиет

1. Қазақстан Республикасының Конституциясы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
2. «Құқық қорғау қызметі туралы» Қазақстан Республикасының 2011 жылғы 6 қаңтардағы №380-IV Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
3. «Қазақстан Республикасының арнаулы мемлекеттік органдары туралы» Қазақстан Республикасының 2012 жылғы 13 ақпандағы №552-IV Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
4. «Қазақстан Республикасы Мемлекеттік күзет қызметі туралы» Қазақстан Республикасының 1995 жылғы 3 қазандағы N 2483 Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
5. «Қазақстан Республикасының ұлттық қауіпсіздік органдары туралы» Қазақстан Республикасының 1995 жылғы 21 желтоқсандағы N 2710 Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
6. «Сыртқы барлау туралы» Қазақстан Республикасының 2010 жылғы 22 мамырдағы №277-IV Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
7. «Қазақстан Республикасының ІІМ қарасты Ұлттық ұлан Комитетінің атыс қаруын қолдану тәртібі «Қазақстан Республикасының Ұлттық ұланы туралы» Қазақстан Республикасының Заңы 2015 жылғы 10 қаңтардағы №274-V ҚРЗ // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
8. «Қазақстан Республикасының қорғанысы және Қарулы Күштері туралы Қазақстан Республикасының Заңы» Қазақстан Республикасының 2005 жылғы 7 қаңтардағы N 29 Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
9. «Қазақстан Республикасының кейбір заңнамалық актілеріне Қазақстан Республикасының арнаулы мемлекеттік органдары мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» Қазақстан Республикасының 2012 жылғы 13 ақпандағы №553-IV Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
10. «Қазақстан Республикасындағы кедендік реттеу туралы» Қазақстан Республикасының Кодексі 2017 жылғы 26 желтоқсандағы №123-VI ҚРЗ // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
11. «Қазақстан Республикасының Ұлттық қауіпсіздік комитеті Шекара қызметінің мәселелері» Қазақстан Республикасы Президентінің 1999 жылғы 10 желтоқсандағы N 282 // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.
12. «Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен әскери құралымдарының жалпыәскери жарғыларын бекіту туралы» Қазақстан Республикасы Президентінің

2007 жылғы 5 шілдедегі N 364 Жарлығы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

13.Қазақстан Республикасы Бас прокуратурасының есебі // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

14.«Қазақстан Республикасының ішкі істер органдары туралы» Қазақстан Республикасының Заңы 2014 жылғы 23 сәуірдегі №199-V ҚРЗ // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

15.«Қоғамға қауіпті іс-әрекеттерді тоқтату, оларды жасаған адамдарды ұстау және ішкі істер органдарына жеткізу мақсатында ішкі істер органдарының қызметкерлері қолданатын арнайы және көлік құралдарының тізбесін бекіту туралы» 2001 жылғы 30 қазандағы Қазақстан Республикасы Үкіметінің N 1375 қаулысы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

16.«Соттардың бандитизм және қылмыстық құқық бұзушылықтарға қатыса отырып, басқа қылмыстық құқық бұзушылықтар жасағаны үшін жауапкершілік туралы заңнаманы қолдануының кейбір мәселелері туралы» Қазақстан Республикасы Жоғарғы Сотының нормативтік қаулысы 2001 жылғы 21 маусым N 2 // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

17.«Адамдарды қоғамнан уақытша оқшаулауды қамтамасыз ететін арнаулы мекемелерде, арнаулы үй-жайларда ұстау тәртібі мен шарттары туралы» 1999 жылғы 30 наурыздағы заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

18.«Қазақстан Республикасында мүгедектерді әлеуметтік қорғау туралы» Қазақстан Республикасының 2005 жылғы 13 сәуірдегі N 39 Заңы // Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

19.«Қазақстан Республикасындағы баланың құқықтары туралы» Қазақстан Республикасының 2002 жылғы 8 тамыздағы N 345 Заңы //Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

20.«Жекелеген қару түрлерінің айналымына мемлекеттік бақылау жасау туралы» Қазақстан Республикасының 1998 жылғы 30 желтоқсандағы N 339 Заңы //Айналыс режимі: http://adilet.zan.kz (жүгіну күні: 01.03.2021) – интернет көздері.

СУЛТАНОВ САЛИМЖАН ИСАЕВИЧ
Еуразия технологиялық университеті Құқық мектебінің
қауымдастырылған профессоры, з.ғ.к.

ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫ САРАЛАУДЫҢ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ЖӘНЕ ҚЫЛМЫСТЫҚ-ПРОЦЕСТІК МӘСЕЛЕЛЕРІ

Мемлекет басшысы Қасым-Жомарт Тоқаевтың 2022 жылғы 1 қыркүйекте «Әділетті мемлекет. Бәртұтас ұлт. Берекелі қоғам» атауымен белгілі болған Қазақстан халқына Жолдауында «Қылмыстық және Қылмыстық-процестік кодекстерді мұқият саралап, ондағы қолданылмайтын немесе сот төрелігіне кедергі келтіретін артық-ауыс нәрсенің бәрінен арылу қажет. Тиісті түзетулер енгізілгеннен кейін оларды қайта-қайта өзгерте бермеу қажет» екендігі туралы айтқан болатын [1].

Қылмыстық және Қылмыстық-процестік кодекстерді бірге қарастыру дұрыс шешім деп ойлаймыз. Сондай-ақ. Қылмыстық атқару кодекс те осы кезде де қайта қарауды, ой елегенінен өткізуді талап етеді. Көрсетілген кодекстер, әдетте бір қоғамдық қатынастарды реттейді және бір-бірімен тығыз байланыста. Оны кодекстердегі баптардың мазмұны мен мәтіні де растайды. Аталмыш кодекстерді жеке-дара қарастыру тиімсіз әрі кейін оларды қайтадан қарастыруға әкеледі немесе көптеген негізсіз толықтырулар мен өзгертулер енгізуге тура келеді.

Қылмыстық құқық мемлекеттің құқық жүйесінің ажырамас бір бөлігі болып табылады және өз алдына негізгі құқық саласын білдіреді. Қылмыстық құқық жеке құқық саласы бола тұра, қылмыстық іс жүргізу және қылмыстық-атқару құқықтарымен бірге қылмыстық құқықтар кешеніне кіреді [2, 20]. Сол себепті де, осы құқықтарға тиесілі кодекстерді қарастыру бірге жүзеге асырылуы тиімді.

Осы кезде, жоғарыда көрсетілген кодекстерден бөлек, Әкімшілік құқық бұзушылықтар туралы кодексті де бірге қараған тиімді болар еді. Әсіресе, қылмыстық құқық бұзушылықтар мен әкімшілік құқық бұзушылықтар ара-жігін ашып, бір-бірінен шектеу мәселесінде маңыздылығы ерекше. Құқық бұзушылықтардың сыртқы белгілері ғана емес, сонжай-ақ осы құқық бұзушылықтардың әсер ететін қоғамдық қатынастары да бір болып келеді.

Қылмыстық кодекс [3] пен Қылмыстық-процестік кодекстердің [4] өзара байланысы құқық бұзушылықтарды саралау кезінде айқын көрінеді. Жалпы қылмыстық процесс қылмыстық құқық бұзушылықты саралаудан басталады десек, қателеспейміз. Кез-келген құқық бұзушылық белгілері бар оқиға орын алған кезде, ең алдымен оның құқық бұзушылық екені, одан кейін қандай құқық бұзушылық екені анықталып, қылмыстық құқық бұзушылық болса, онда оның Қазақстан Республикасы Қылмыстық кодексінің Ерекше бөлігіндегі қай баптың қандай бөлігі мен тармағына сай келетіндігі айқындалады. Тек, осыдан кейін барып, сотқа дейінгі тергеп-тексеру басталады және сараланған қылмыстық құқық бұзушылық бойынша, оны тергеу бойынша жұмыстар жүзеге асырылады. Әрине, қылмыстық құқық бұзушылықты саралау осымен шектеліп қалмауы тиіс. Сотқа дейінгі тергеп-тексеру барысында жаңадан мән-жайлар ашылуы мүмкін немесе тергеу барысында жиналған дәлелдемелердің жиынтығы қайта саралауды талап етеді. Әрине, қылмыстық іс бойынша

жиналған дәлелдемелер сараланған қылмыстық құқық бұзушылықтың дұрыс сараланғандығын растауы да мүмкін, бұл кезде қайта саралау талап етілмейді.

Қылмыстық қудалау органдарының лауазымды адамы болып табылатын тергеуші ҚР ҚПК 60-бабына сәйкес қылмыстық құқық бұзушылық жасағанын көрсететін оған қатысты жеткілікті дәлелдер жиналған күдіктінің іс-әрекетін саралауға міндетті екенін көрсеткен. Бұл тергеушінің қалауынан тыс міндет екенін білдіреді, егер адамның іс-әрекеттерінде (әрекет немесе әрекетсіздік) қылмыстық құқық бұзушылық белгілері бар болса, онда тергеуші қылмыстық құқық бұзушылықты ҚР ҚК Ерекше бөлігінде көрсетілген бапқа, сол баптың бөлігі немесе тармағына сәйкестігін анықтап саралауға міндетті. Қылмыстық құқық бұзушылықты саралау адамды күдікті деп танумен тең мағынаны білдіреді. Бұл туралы ҚР ҚПК 64-бабының 1-бөлігі 3-тармағында «өзіне қатысты күдіктінің іс-әрекетін саралау туралы прокурор не сотқа дейінгі тергеп-тексеруді жүзеге асыратын адам прокурормен келісілген қаулы шығарған» адам күдікті болып табылатындығын меңзейді.

Қылмыстық құқық бұзушылықты саралау ҚР ҚПК-нің «Адамды күдікті деп тану және күдіктінің іс-әрекетін саралауды, қылмыстық құқық бұзушылықты саралауды айқындау» деген атаумен берілген 25-тарауында қарастырылады.

Адамды күдікті деп тану үшін де оның іс-әрекетінде қандай қылмыстық құқық бұзушылық белгілері бар екені анықталады және сол қылмыстық құқық бұзушылықты жасады деп күдік келтірілгені күдікті деп тану туралы қаулыда көрсетіледі. Бұл күдікті деп тану үшін оның іс-әрекеттерінде ҚР ҚК Ерекше бөлілігінің нақты бабы, баптың бөлігі немесе бап бөлігінің тармағында көрсетілген қылмыстық құқық бұзушылық құрамының бар екенін анықтауды талап ететінін білдіреді.

ҚР ҚПК 203-бабының 1-бөлігіне сәйкес, адамның қылмыс жасағаны туралы күдікті растайтын оған қатысты жеткілікті дәлелдемелер болған кезде прокурор, Сотқа дейінгі тергеп-тексеруді жүзеге асыратын адам күдіктінің іс-әрекетін саралау туралы уәжді қаулы шығарады.

ҚР ҚПК 204-бабының 1-бөлігінде көрсетілгендей, күдіктінің іс-әрекетін саралау туралы қаулыда:

1) қаулының жасалған уақыты мен орны;

2) қаулыны кімнің шығарғаны;

3) күдіктінің тегі, аты және әкесінің аты (ол болған кезде), туған күні, айы, жылы және туған жері;

4) қылмыстың жасалған уақыты, орны, сондай-ақ ҚР Қылмыстық-процестік кодексінің 113-бабына сәйкес дәлелденуге жататын өзге де мән-жайларды көрсете отырып, осы адам жасады деп күдік келтірілген қылмыстың сипаттамасы;

5) адамға оны жасады деп күдік келтіріліп отырған қылмыс үшін жауаптылықты көздейтін қылмыстық заң, яғни ҚР Қылмыстық кодексінің бабы, бөлігі, тармағы нақты көрсетілуі тиіс.

Қылмыстық құқық бұзушылықты саралау мәселесін шешкен кезде, ҚР ҚПК 189-бабында көрсетілгендей, сотқа дейінгі тергеп-тексерудің қандай нысанда жүргізілетінін де бірге шешу қажет. Бұл кезде сотқа дейінгі тергеп-тексеру анықтау, алдын ала тергеу нысанында және хаттамалық нысанда жүргізілуі мүмкін. Егер, тергеуші сотқа дейінгі тергеп-тексеруді алдын ала тергеу нысанында жүргізу қажет деп тапса, онда оны қай органның тергеулігіне жататынын да анықтауы тиіс. ҚР ҚПК 60-бабына сәйкес, тергеушілер ішкі істер органдарының тергеушісі, ұлттық қауіпсіздік органдарының тергеушісі, сыбайлас жемқорлыққа қарсы қызметтің тергеушісі және экономикалық тергеу қызметінің тергеушісі болып бөлінетінін ескерсек, онда олардың тергейтін қылмыстық істері де заңмен шектелген.

ҚР ҚПК 7-бабы 46-тармағына сәйкес, тергеулік – осы қылмыстық құқық бұзушылықты тергеп-тексеруді қандай да бір қылмыстық қудалау органының құзыретіне жатқызатын, ҚР Қылмыстық-процестік кодесінде белгіленген белгілердің жиынтығы болып табылады.

Тергеулік ҚР ҚПК 187-бабында көрсетілген, соған сәйкес жоғарыда көрсетілген тергеу органдарының тергеушілері сотқа дейінгі тергеп-тексеруді жүзеге асырады. Кейде, әртүрлі

тергеулікке жататын бірнеше қылмыстық құқық бұзушылықтың да белгілері де кездесуі мүмкін, бұл жағдайда тергеулікті прокурор анықтайды. Бұл жөнінде көрсетілген баптың 8-бөлігінде: «түрлі алдын ала тергеу органдарының тергеулігіне жататын қылмыстық істерді бір іс жүргізуге біріктірген кезде тергеулікті прокурор айқындайды» делінген.

Қылмыстық құқық бұзушылықты саралау сырт көзге қарапайым болып көрінгенімен, бұл өте күрделі және салмағы мол жауапты үрдіс. Құқық бұзушылықты саралау кезінде жіберілген қате, сотқа дейінгі тергеп-тексеруді жан-жақты, объективті әрі әділетті жүргізілуі кері әсер ететіні сөзсіз.

Қылмыстық құқық бұзушылықты саралау осы кезге бар дәлелдердің жиынтығында жүзеге асырылады.

Ал, дәлелдемелерді бағалау, ҚР ҚПК 125-бабының 2-бөлігінде көрсетілген және судья, прокурор, тергеуші, анықтаушы дәлелдемелерді ҚР ҚПК 25-бабына сәйкес заң мен арожданды басшылыққа ала отырып, дәлелдемелерді жиынтығымен жан-жақты, толық және объективті қарауға негізделген өздерінің ішкі сенімі бойынша бағалайды.

Осылайша, қылмыстық құқық бұзушылықты саралау мәселесін шешкен тергеуші заңды басшылыққа алады және адамның іс-ірекетінде қылмыстық құқық бұзушылықтың екенін қолда бар дәлелдемелерге сүйене отырып, өзінің ішкі сенімімен оларды бағалап, бір тоқтамға келеді. Соның нәтижесінде күдікті деп тану туралы немесе қылмыстық құқық бұзушылықты саралау туралы шешім қабылдайды және оны қаулыда уәждеп көрсетеді.

Әдебиет

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауы https://www.akorda.kz/kz/memleket-basshysy-kasym-zhomart-tokaevtyn-kazakstan-halkyna-zholdauy-181416

2. Бекмагамбетов А.Б., Ревин В.П., Ревина В.В. Уголовное право Республики Казахстан. Особенная часть. Учебник. 2-ое изд., перераб. и доп./ Под ред. доктора юридических наук., профессора, Заслуженного деятеля науки Российской Федерации Ревина В.П.– М.: Издательский дом Академии Естествознания, 2017. – С. 396.

3. Қазақстан Республикасының Қылмыстық кодексі https://adilet.zan.kz/kaz/docs/K1400000226

4. Қазақстан Республикасының Қылмыстық-процестік кодексі https://adilet.zan.kz/kaz/docs/K1400000231

ИМАНБАЕВ АЗАМАТ ЖАНАТОВИЧ
Сениор-лектор, Казахско-Британского технического университета,
магистр технических наук

ЗИРО ААСО АРАЗ
Сениор-лектор, Казахско-Британского технического университета,
магистр технических наук

СТАНДАРТЫ БЕЗОПАСНОСТИ 5G-СЕТЕЙ

С развертыванием 5G-сетей стандартные группы предприняли усилия по определению механизмов безопасности и лучших практик для этих систем следующего поколения. В данной статье рассматриваются действия 3GPP, GSMA, NIST и других организаций по стандартизации возможностей безопасности 5G. Также анализируются методы, используемые при разработке этих стандартов.

3 GPP опубликовал обширные спецификации безопасности 5G через свою рабочую группу SA3, формируя основные стандарты для полной безопасности 5G от конца к концу:

1. Протокол 5G ASN.1 обеспечивает передовое шифрование с использованием новых алгоритмов 5G, разработанных 3GPP. Формальный анализ подтвердил его свойства безопасности.
2. 5G AKA улучшает аутентификационный протокол 4G, добавляя новые параметры, такие как RES* для подтверждения. Симуляции продемонстрировали его стойкость к общим атакам.
3. Новые идентификаторы абонентов, устройств и сетей 5G были получены из существующих идентификаторов LTE. Их структура и кодирование обеспечивают большую анонимность.
4. Естественные алгоритмы шифрования и целостности 5G были разработаны экспертами по безопасности 3GPP для обеспечения высокой криптографической стойкости при оптимизации производительности.
5. Подробные контексты безопасности и процедуры были определены через итерационное развитие и обзор в рамках рабочих групп 3GPP.
6. GSMA определила свою структуру NESAS для обеспечения безопасности цепочки поставок 5G с использованием информации от операторов и поставщиков:
7. Требования к безопасности процесса поставщика были основаны на установленных стандартах, таких как ISO 27001.
8. Мандаты по шифрованию были разработаны на основе рекомендаций в документах, таких как NIST 800-175B.
9. Требования к контролю доступа и физическому укреплению были разработаны на основе оценки рисков атак на инфраструктуру.
10. Обзоры практик безопасности программного обеспечения с открытым исходным кодом формировали требования к компонентам сторонних поставщиков.
11. NIST разработало свои рекомендации по безопасности 5G, опираясь на предыдущую работу в области безопасности LTE и облака:
12. Ссылочная архитектура 5G интегрировала успешные средства контроля безопасности в развертываниях 4G.

13. Рекомендации по управлению идентификацией и доступом были построены на проверенных протоколах, таких как OAuth 2.0 и SAML 2.0.

14. Рекомендации по безопасности сегментации и виртуализации были получены из принципов безопасности облака NIST.

Анализ проводился путем тщательного изучения последних версий спецификаций и документации 3GPP, GSMA и NIST, связанной со стандартами безопасности 5G. Технические решения, методология разработки и внешние ссылки оценивались для определения основы каждого стандарта.

Комплексные стандарты безопасности 5G, разработанные организациями по стандартизации, следуют основанным научным техническим и методологическим практикам. По мере развития 5G соблюдение этих стандартов, дополнительно усиленных с помощью последовательных, строгих процессов разработки, останется важным для защиты 5G-сетей.

Литература

1. 3GPP TS 33.501 – 5G Security Architecture and Procedures
2. GSMA NESAS – Network Equipment Security Assurance Scheme
3. NIST SP 500-325 – Cybersecurity Reference Architecture for 5G Infrastructure
4. NIST SP 500-302 – 5G Mobile Core Network Architecture

АШИРБЕКОВ МАРАТ ЕРКЕНОВИЧ
Старший помощник Главного транспортного прокурора советник юстиции,
магистр юридических наук

К ВОПРОСАМ НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗЕМЕЛЬНЫХ ПРАВООТНОШЕНИЙ НА ТРАНСПОРТЕ С УЧЕТОМ ВЛИЯНИЯ ПРОЦЕССОВ ЦИФРОВИЗАЦИИ

В статье рассмотрены актуальные вопросы, возникающие при осуществлении прокурорского надзора в сфере землепользования на транспорте в условиях цифровизации и информатизации общества и государства.

На основе правового анализа, эмпирического материала подготовлены предложения по повышению эффективности прокурорского надзора в рассматриваемой сфере, а также по совершенствованию действующего законодательства Республики Казахстан.

Предложены пути решения проблемных вопросов, связанных с рассматриваемой тематикой возникающих в различных отраслях права.

Наступившие в Республике Казахстан в 1991 году экономические и политические катаклизмы необратимо повлекли за собой перезагрузку всех отраслей жизнедеятельности казахстанского общества.

Преобразования земельных правоотношений претерпели значительные изменения, которые привели к замене исключительного государственного владения землей разнообразными формами земельной собственности.

Земля и ее недра стали объектами бурно развивающихся рыночных отношений, по сути, став дорогим и весьма востребованным товаром. На этом фоне все чаще стали фиксироваться различного рода махинации и спекуляции с землей. Назрела необходимость надлежащей защиты со стороны государства имущественных прав добросовестных землепользователей, в том числе посредством усиления норм уголовного права.

На заре независимости Республики Казахстан наиболее распространенным, но в то же время скрытым и внешне особо не проявляющимся правонарушением явился самовольный захват земель. Общественная опасность данного вида правонарушений заключается в нарушении интересов государства, а также других участников земельных отношений.

Последствиями подобных правонарушений выступают концентрация земельного фонда в руках латифундистов, а также его неправомерное изъятие из сельскохозяйственного оборота.

Основная часть. Органами Главной транспортной прокуратуры *(далее – ГТП)* выявлены системные нарушения земельного законодательства в части незаконного предоставления земельных участков в зонах транспорта, а равно последующего возведения (строительства) на них зданий, сооружений и т.д. [1].

В сфере воздушного транспорта:

Так, проверкой проведенной в конце 2022 года установлено следующее:

В соответствии с пунктом 1 статьи 90 Закона «Об использовании воздушного пространства Республики Казахстан и деятельности авиации» *(далее – Закон об ИВП),* [2] к деятельности, которая может представлять угрозу безопасности полетов, относятся

строительство объектов, линий электропередач, других препятствий, расположенных на приаэродромной территории и на местности в пределах воздушных трасс, работы, вследствие которых в воздушном пространстве производятся электромагнитное, световое, акустическое, корпускулярное и иные виды излучения, размещение объектов, приводящих к массовому скоплению птиц или ухудшению полетной видимости, а также любая другая деятельность, не связанная непосредственно с использованием воздушного пространства, но влияющая на безопасность полетов воздушных судов, их оборудования и находящихся на них людей.

Такая деятельность может осуществляться только с разрешения, выдаваемого в соответствии с Правилами выдачи разрешений на осуществление деятельности, которая может представлять угрозу безопасности полетов воздушных судов (утверждены постановлением Правительства от 12.05.2011 №504, далее – Правила №504) [3]. Перед размещением указанных объектов физические и юридические лица должны пройти процедуру согласования с аэропортом (постоянно действующей комиссией, создаваемой на аэродромах решением первого руководителя организации, осуществляющей эксплуатацию аэропорта), специалисты которого выносят соответствующее заключение.

В свою очередь действующей комиссией аэропорта заключение и иные документы, перечень которых установлен Правилами, вместе с заявкой направляются в Комитет гражданской авиации Министерства индустрии и инфраструктурного развития Республики Казахстан.

Заявка на получение разрешения в соответствии с пунктами 17 и 18 Правил №504 рассматривается комиссией, создаваемой Комитетом гражданской авиации, (далее – КГА) после чего только выдается разрешение (на основании положительного заключения указанной комиссии).

Получение разрешения требуется для размещения всех объектов любой высоты на удалении до 4 км от ближайшей точки взлетно – посадочной полосы, истинная (геометрическая) высота которых относительно уровня аэродрома 45 метров и более, и расположенных в пределах 15 км от контрольной точки аэропорта, истинная (геометрическая) высота которых относительно уровня земли 100 м и более, а на приаэродромной территории - 100 м и более относительно уровня аэродрома, линий связи, электропередачи, а также других объектов радио, электромагнитных и световых излучений, которые могут создавать помехи для нормальной работы авиационных радиотехнических средств и светосигнального оборудования, факельных устройств для аварийного сжигания сбрасываемых газов, промышленных и иных предприятий и сооружений, деятельность которых может привести к ухудшению видимости в районах аэродромов (вертодромов); взрывоопасных объектов.

В нарушение установленных требований на приаэродромных территориях 20 аэропортов Республики без получения заключения постоянно действующей комиссии аэропортов и разрешения КГА возведено 70 534 строений различной категории.

К примеру, без согласования с аэропортовой комиссией АО «Международный аэропорт Алматы» и выдачи положительного разрешения уполномоченного органа в приаэродромной территории возведено 9 жилых массивов, состоящих из 15 979 строений с проживанием в них 171 424 человек.

Другим немаловажным фактором, являются санитарно – защитные зоны (далее – СЗЗ).

Обоснованность размеров СЗЗ вдоль стандартных маршрутов полета в зоне взлета и посадки воздушных судов подтверждается расчетами рассеивания выбросов в атмосферу для всех загрязняющих веществ и распространения физических факторов, выполненными по согласованным и утвержденным в установленном порядке методам с учетом вклада действующих, намеченных к строительству или проектируемых предприятий.

Установлено, что на территории СЗЗ 11 аэропортов Республики местными исполнительными органами физическим и юридическим лицам незаконно предоставлено 636 земельных участков (162,52 га).

На этих землях построено 5 населенных пунктов и в настоящее время проживают 2 660 человек.

Между тем, в нарушение п.17 Санитарных правил «Санитарно-эпидемиологические требования по установлению санитарно-защитной зоны производственных объектов» от 20.03.2015 года №237 (далее – Санитарные правила) [4]. в зонах аэропортов «Боралдай», «Акши» (Алматинская область), «Актобе», «Зайсан» (Восточно-Казахстанская область), «Костанай», «Павлодар», с.Урджар и «Орал» такая зона не установлена (СЗЗ устанавливается с целью обеспечения безопасности населения, размер которой обеспечивает уменьшение воздействия загрязнения на атмосферный воздух (химического, биологического, физического) до значений, установленных документами государственной системы санитарно-эпидемиологического нормирования).

Выдача земельных участков и размещение объектов, ухудшающих орнитологическую обстановку в районах ряда аэропортов, создает прямую угрозу безопасности полетов.

Так, в нарушение пункта 7 Правил №504 на расстоянии в пределах 15 километров от аэропортов ряда городов функционируют полигоны по размещению твердо-бытовых отходов (свалка), скотобойни, мясные базары, создающие условия для массового скопления птиц и ухудшения орнитологической обстановки на приаэродромных территориях вышеуказанных аэропортов.

Наряду с этим, в 2022 году органами транспортной прокуратуры проведен анализ соблюдения законности в сфере регулирования вопросов выделения земельных участков вблизи аэропортов.

Результаты анализа показали на наличие системных проблем, связанных с незаконным выделением местными исполнительными органами (далее – МИО, акиматы) земель рядом с аэропортами, создающими реальную угрозу безопасности полетов и подвергающими риску жизнь и здоровье людей.

Несмотря на поручения Правительства, в том числе адресованные во исполнение представления Генеральной прокуратуры, принимаемые акиматами меры по обеспечению безопасности населения и формированию необходимой обстановки для безаварийной эксплуатации объектов транспорта недостаточно эффективны.

Об этом свидетельствует и увеличение авиационных событий, произошедших ввиду столкновения птиц с воздушными судами с 23 (в т.ч. 3 с их повреждением) в 2021 году до 61 (9) за 10 месяцев 2022 года.

Основной причиной этих происшествий является осуществление деятельности, способствующей привлечению и массовому скоплению птиц на приаэродромных территориях.

К примеру, акиматом города Шымкент вопреки запрету, установленному пунктом 4 статьи 90 Закона об ИВП для строительства животноводческих комплексов, скотобоен и т.п. предоставлено 37 земельных участков на расстоянии менее 15 километров от аэропорта.

В городе Кокшетау вблизи от контрольной точки аэродрома АО «Авиакомпания Кокшетау» расположены сельскохозяйственные угодья и животноводческие комплексы, отличающиеся массовым скоплением птиц и негативно влияющие на орнитологическую обстановку вокруг аэропорта.

Подобная ситуация отмечается и на приаэродромных территориях городов Алматы, Актобе, Атырау, Жезказган, Зайсан, Караганда, Петропавловск, Семей, Тараз, Уральск, Урджар и Шымкент, где во время возделывания земель сельскохозяйственного назначения наблюдается скопление птиц.

Расположение вблизи аэропортов полигонов твердо-бытовых отходов и несанкционированных свалок только ухудшают и без того крайне нестабильную ситуацию вокруг рискованной зоны полетов.

Например, в зоне аэропорта города Алматы функционирует свыше 10 таких объектов.

Акиматом города Семей до настоящего времени не приняты меры по переносу общегородской свалки, расположенной на расстоянии 7,2 км от аэропорта Семей. При этом по акту транспортной прокуратуры еще в 2018 году в Генеральный план города внесены изменения и выделено 100 га земли для переноса полигона, а также приобретено оборудование для механической и биологической обработки мусора.

К такому положению дел привело отсутствие алгоритма взаимодействия между местными исполнительными и уполномоченными органами по недопущению возведения без соответствующего согласования объектов на землях транспорта.

В силу требований пункта 5 Правил № 504 для размещения всех объектов на удалении до 4 км от ближайшей точки взлетно – посадочной полосы требуется разрешение Комитета гражданской авиации.

Однако, вопреки этому условию без одобрения КГА в 4-х километровой зоне аэропорта города Шымкент возведено 1 303 объекта.

Данное обстоятельство лишило возможности осуществления посадки воздушных судов в аэропорт с восточной стороны и ограничению взлета для больших самолетов.

Подобные нарушения выявлены во всех регионах страны (за исключением Костанайской области), где без соответствующего согласования возведено более 100 тысяч различных строительных объектов.

Не нашли своего логического разрешения и вопросы установления санитарно – защитных зон.

Установление таких зон согласно требованиям пункта 24 Санитарных правил, утвержденных приказом и.о. Министра здравоохранения от 11 января 2022 года ҚР ДСМ – 2 призвано обеспечить безопасность населения, гарантировать уменьшение воздействия загрязнения на атмосферный воздух (химического, биологического, физического) до значений, установленных гигиеническими нормативами.

Вместе с тем анализом выявлено полное игнорирование собственниками аэропортов городов Актобе и Талдыкорган отмеченных запретов, что свидетельствует о недостатках в деятельности санитарного государственного контроля, поскольку в ходе проведения самостоятельных проверок должностными лицами отмеченных региональных органов вопросы по определению этих зон предметом рассмотрения не являлись.

Следует отметить, что до настоящего времени не разрешены вопросы изъятия в целях государственных нужд 1,5 тыс. участков земли, предназначенных для возведения объектов различного назначения, предоставленных в границах СЗЗ транспортной инфраструктуры городов Алматы, Астана, Атырау, Жезказган, Караганда, Костанай, Кызылорда, Павлодар, Тараз, Туркестан, Уральск и Шымкент с выплатой владельцам компенсаций.

Причиной перечисленных нарушений является несоблюдение акиматами обязанностей по зонированию земель, расположенных на приаэродромной территории.

В соответствии с пунктом 1 статьи 121 Земельного кодекса (далее – Кодекс) [5] в целях обеспечения безопасности населения и создания необходимых условий для эксплуатации промышленных, транспортных и иных объектов устанавливаются зоны, в пределах которых ограничиваются или запрещаются те виды деятельности, которые не совместимы с целями установления зон.

К зонам с особыми условиями пользования землей относятся приаэродромные полосы (подпункт 4) пункта 2 статьи 121 Кодекса).

Своевременная реализация указанных требований позволила бы регулировать целевое назначение земель вблизи аэропортов или ограничить их выдачу.

Необходимо отметить, что наличие градостроительной и прочей разрешительной документации не могло быть бесспорным доказательством правомерного предоставления земельных участков местными исполнительными органами на отмеченных территориях.

Примером трагических последствий такой незаконной выдачи земли и разрешения на строительство в границах СЗЗ аэропорта города Алматы явился случай крушения самолета авиакомпании «Bek Air»

В этой связи вопросы предоставления земельных участков вокруг приаэродромных территорий для обеспечения бесперебойной работы воздушного транспорта, строительства на них промышленных, жилищных и социально – бытовых и других объектов требуют постоянного и качественного контроля со стороны уполномоченных органов с обязательной цифровизацией всего процесса выделения земельных участков.

Учитывая изложенное, в адрес первого заместителя Премьер Министра внесено представление с предложением принятия мер по устранению выявленных нарушений законности, причин и условий, им способствующих, для чего поручить местным органам власти и столицы:

1.1. Совместно с министерствами индустрии и инфраструктурного развития, здравоохранения:

−выработать алгоритм взаимодействия между местными исполнительными и уполномоченными органами по недопущению возведения без соответствующего согласования объектов вблизи аэропортов;

−обеспечить зонирование земель на приаэродромных территориях;

−провести работу по установлению санитарно - защитных зон аэропортов;

1.2. Совместно с Министерством сельского хозяйства:

−рассмотреть вопросы изъятия из неправомерного владения и возврата земельных участков в санитарно - защитные зоны аэропортов;

−запретить размещение (на расстоянии ближе 15 км от контрольной точки аэродрома) мест выброса пищевых отходов, мусорных свалок, строительство звероводческих ферм, скотобоен и других объектов промышленной и бытовой инфраструктуры, способствующих привлечению и массовому скоплению птиц;

−провести исчерпывающие мероприятия по обеспечению надлежащего исполнения требований земельного и транспортного законодательства.

В настоящее время по акту прокурорского надзора уполномоченным государственным органом составлен план мероприятий до 2024 года, исполнение находится на контроле прокуратуры.

Предложения по совершенствованию законодательства:

В настоящее время, порядок установления радиуса приаэродромной территории в разных нормативно - правовых актах прописан не единообразно, что создает дополнительные сложности при их применении.

Так, радиус приаэродромных территорий, определенный Правительством Республики Казахстан (постановление от 23 января 2012 года №156 «Об утверждении норм годности к эксплуатации аэродромов (вертодромов) гражданской авиации»), равен 46 километров от контрольной точки аэродрома [6].

В силу положений (пп.32) ст.1) Закона об ИВП радиус приаэродромной территории *определяется* уполномоченными органами в сферах гражданской и государственной авиации.

В то же время, установление столь большого радиуса для приаэродромных территорий делает затруднительным исполнение многих норм законодательства.

В частности, в соответствии с п.1 ст.90 Закона об ИВП осуществление на *приаэродромной территории* деятельности, которая может представлять угрозу безопасности полетов (в т.ч. строительство объектов, линий электропередач, др.) требует наличие разрешения уполномоченного органа в области гражданской и государственной авиации. Аналогичное требование предусмотрено для воздушных трасс.

Под данное определение подпадает широкий спектр видов хозяйственной деятельности и с учетом большого радиуса этих территорий, вышеуказанное законодательное ограничение может парализовать хозяйственную деятельность городов и их пригородных территорий.

Помимо данного пробела в земельном законодательстве имеются не конкретизированные нормы, создающие условия для разночтений.

Так, в п.1 ст.90 Закона об ИВП определен перечень видов деятельности, для осуществления которых необходимо получение разрешения уполномоченного органа в сфере гражданской авиации в соответствии с Правилами выдачи разрешений на осуществление деятельности (утверждены постановлением Правительства Республики Казахстан от 12.05.2011 г. №504, далее – Правила выдачи разрешений).

Как следует из содержания пп.1) п.5 Правил выдачи разрешений для размещения объектов любой высоты на удалении до 4 км от ближайшей точки взлетно – посадочной полосы, а также объектов, истинная (геометрическая) высота которых относительно уровня аэродрома 45 метров и более, и, расположенных в пределах 15 км от контрольной точки от аэропорта, требуется получение соответствующего разрешения (выдается уполномоченными органами в сферах гражданской и государственной авиации, подтверждающего право юридических и физических лиц на осуществление деятельности, которая может представлять угрозу безопасности полетов воздушных судов).

Вместе с тем, в данном пункте Правил выдачи разрешений имеются не конкретизированные требования, что затрудняет их исполнение.

В частности, предусмотрено требование о необходимости получения разрешения для размещения, дословно: «2) линий связи, электропередачи, а также других объектов радио, электромагнитных и световых излучений, которые могут создавать помехи для нормальной работы авиационных радиотехнических средств и светосигнального оборудования; 3) факельных устройств для аварийного сжигания сбрасываемых газов; 4) промышленных и иных предприятий и сооружений, деятельность которых может привести к ухудшению видимости в районах аэродромов (вертодромов); 5) взрывоопасных объектов».

Из смысла указанной нормы следует, что разрешение требуется на размещение любого из указанного перечня объектов независимо от того, насколько они удалены от объекта воздушного транспорта, что не соответствует существующей на данный момент обстановке по вопросу обеспечения безопасности.

Также, нормы данных правил, устанавливающих ограничения на пользование земельным участком, не основываются на нормах земельного законодательства, что противоречит требованиям статьи 6 Земельного кодекса.

На основании изложенного предлагается инициировать внесение соответствующих дополнений и изменений в действуюшее законодательство, направленных на устранение вышеуказанных пробелов и коллизий, а именно предусмотреть в законодательстве дефиницию «приаэродромных полос», регламентацию в земельном законодательстве терминов «воздушные трассы», «приаэродромные территории», их радиуса, а также упорядочивание неурегулированных норм о порядке получения разрешений на осуществление деятельности, создающей угрозу безопасности полетов.

В сфере трубопроводного транспорта:

Проведенным анализом в сфере трубопроводного транспорта установлено следующее:

По республике проложено 37 магистральных газопроводов и 25 магистральных нефтепроводов соответственно (D – 500 и более мм).

При этом серьезными предпосылками, влияющими на безопасность эксплуатации трубопроводного транспорта выступают многочисленные недвижимые строения в зонах их функционирования.

В правоприменительной практике используются понятия охранных зон и минимальных расстояний магистральных трубопроводов, которые не тождественны между собой и имеют различия в правовом статусе.

Так, в соответствии с п.п.5) п.2 ст.121 Земельного Кодекса Республики Казахстан (далее – Кодекс) охранные зоны относятся к территориям, на которых землепользование

производится с особыми условиями. Среди таких можно отметить магистральные трубопроводы, связующие линии, линии радиосообщений и передачи электрической энергии.

Понятие охранных зон закреплено в п.1 ст.14 Закона Республики Казахстан «О магистральном трубопроводе» (далее – Закон), согласно которому *в целях обеспечения безопасности населения, предотвращения причинения вреда окружающей среде и создания условий для безопасной эксплуатации магистрального трубопровода вдоль его трассы вне зависимости от вида прокладки, а также вокруг объектов магистрального трубопровода устанавливаются охранные зоны, обозначаемые на местности специальными знаками в соответствии с требованиями технического регламента по безопасности магистрального трубопровода.*

Согласно п.4 ст.121 Кодекса границы *охранных зон* и режим использования земель в них определяются органом, принявшим решение о предоставлении земель в собственность или землепользование, в соответствии с нормами и проектно-технической документацией.

Институт «минимальных расстояний» упоминается в законодательстве лишь в п.8 ст. 14 Закона, в п.п. 5.3.9 и 5.3.10 СНиП 3.05-01-2010 «Магистральные трубопроводы» [7], а также в п.18 Правил обеспечения промышленной безопасности при эксплуатации магистральных трубопроводов [8] .

В указанной норме Закона предусмотрено, что «в целях обеспечения безопасности запрещается строительство любых объектов, не относящихся к магистральному трубопроводу, в пределах минимальных расстояний, установленных строительными нормами и правилами».

Значения охранных зон и минимальных расстояний существенно разнятся, где при равных исходных данных (к примеру, газопровод с диаметром сечения 500 мм и рабочим давлением 5,4 МПа), охранные зоны магистрального трубопровода будут равны 50 метрам от его оси, а минимальные расстояния – 150 метрам.

В Кодексе ссылок на минимальные расстояния магистральных трубопроводов не имеется.

Вместе с тем, в соответствии с п.1 ст.6 Кодекса земельное законодательство в Республике Казахстан основывается на Конституции Республики Казахстан и состоит из настоящего Кодекса *и принимаемых в соответствии с ним* нормативных правовых актов Республики Казахстан.

В связи с неурегулированностью в Кодексе статуса минимальных расстояний, остаются не регламентированными вопросы установления их границ на местности.

В результате, минимальные расстояния не установлены на местности и никак не обозначены на картах, а местные исполнительные органы не учитывают их при решении вопросов о выделении земельных участков.

Как следствие, основная масса выявленных в ходе проверки нарушений требований земельного законодательства касаются нарушений минимальных расстояний.

На данный момент установлено 918 объектов (земельных участков, строений и др.), из которых 670 объектов находятся в границах минимальных расстояний, 248 – в пределах охранных зон магистральных трубопроводов.

Кроме того, следует отдельно заострить внимание на вопросах регламентации обязанности собственников магистральных трубопроводов по установлению границ их охранных зон.

Так, согласно п.4 ст.121 Кодекса границы охранных зон и режим использования земель в них определяются органом*, принявшим решение о предоставлении земель в собственность или землепользование,* в соответствии с нормами и проектно – технической документацией, за исключением зон, указанных в подпункте 8) пункта 2 настоящей статьи.

В данной норме не конкретизировано при предоставлении каких земель в собственность (землепользование) исполнительным органом определяются границы охранных зон.

Из смысла данной нормы следует, что охранные зоны магистральных трубопроводов определяются исполнительным органом при предоставлении права собственности (землепользования) на размещение основных объектов магистрального трубопровода (его линейной части, компрессорных, нефтеперекачивающих станций и др.), где сразу в связи с предоставлением указанных земель устанавливаются охранные зоны для этих объектов.

Вместе с тем, согласно сведениям собственников магистральных трубопроводов, свыше 60% магистральных трубопроводов республики введены в эксплуатацию более 30 лет (газопроводов – 74%, нефтепроводов – 47%), то есть до введения в действие Кодекса, впервые закрепившего данное требование.

На землях сельскохозяйственного назначения охранная зона магистрального трубопровода ограничивается условными линиями, проходящими в 25-ти метрах от оси трубопровода с каждой стороны.

В нарушение установленных требований местными исполнительными органами в 12 областях (Туркестанской, Алматинской, Жамбылской, Костанайской, Кызылординской, Павлодарской, Абайской, ВКО,СКО, ЗКО, Жамбылской, Мангистауской) в границах охранных зон магистральных газопроводов и нефтепроводов выделено 543 земельных участка общей площадью 142,027 га.

На этой площади в результате активного возведения различных объектов, в том числе и домостроений, образовались 24 жилых массива, с проживанием 23 611 человек.

Аналогичная ситуация наблюдается и по санитарным зонам.

В соответствии с приложением 4 Санитарных правил, санитарно-защитные зоны для магистральных газопроводов и нефтепроводов диаметром 500 мм, проложенных вблизи городов и других населенных пунктов (коллективные сады и дачные поселки; тепличные комбинаты; отдельные общественные здания с массовым скоплением людей), составляет 150 метров от оси трубопровода, а диаметром 1000 мм – 250 метров.

Вместе с тем, местными исполнительными органами без соблюдения установленных требований по соблюдению санитарных зон предоставлено 1 118 земельных участков (площадью 56 615,33 га), на которых возведены 24 населенных пунктов с проживанием в них 30 736 человек.

При этом, в Кодексе отсутствуют нормы, регламентирующие иной порядок установления охранных зон магистральных трубопроводов, в том числе, предусматривающие случаи, когда субъектам первоначально предоставлено собственническое право или право на землепользование на объект трубопроводного транспорта без установления границ их охранных зон.

С учетом изложенного предлагается инициировать внесение поправок в Земельный Кодекс, предусматривающих регламентацию института минимальных расстояний, а также обязанности собственников магистральных трубопроводов по установлению границ охранных зон и минимальных расстояний, в том числе цифровых во взаимодействии с местными исполнительными органами.

Данный вопрос имеет существенное значение, поскольку содержащийся в п.8 ст. 14 Закона запрет на строительство объектов в пределах минимальных расстояний, не имеет оснований в Кодексе, а применение данной нормы станет для местных исполнительных органов ограничительным условием при решении вопроса о выделении земельных участков с целевым назначением, предусматривающим строительство каких-либо объектов, в том числе ИЖС.

В сфере железнодорожного транспорта:

Из 16 068 км эксплуатационной длины магистральных железнодорожных путей, 3 705 км (или 23%) требуют проведения капитального ремонта, доля изношенности путевого хозяйства составляет 59 %, отдельные его участки и вовсе подлежат к ограничению скоростного режима или полному их закрытию.

Пунктом 4.3.13 СП РК 3.03-116-2014 «Отвод земель для железных дорог» установлены контролируемые зоны железных дорог: за чертой населенных пунктов – на расстоянии 50 метров от полосы предоставления железных дорог в обе стороны; в населенных пунктах – на расстоянии 20 метров от полосы предоставления железных дорог в обе стороны.

Между тем, в контролируемых зонах дислоцируются 4 652 земельных участка (площадью 63 778,5153 га), на которых образовались 5 609 строений,150 жилых массивов с проживающими в них жителями общей численностью 304 063 человек (во всех областях).

В соответствии с п.п.3, 4 ст.114 Кодекса определяются охраняемые территории железнодорожного транспорта *с особыми условиями землепользования*, в пределах которых ограничиваются или запрещаются те виды деятельности, которые не совместимы с целями установления зон, в перечень которых входят:

−защитные лесные полосы,

−земельные участки, необходимые для обеспечения сохранности, прочности и устойчивости сооружений, устройств и других объектов транспорта,

−земельные участки, примыкающие к полосе отвода железнодорожного транспорта, расположенные в селеопасных, оползнеопасных зонах и в местах, подверженных другим опасным воздействиям.

Вместе с тем, в ст.121 Кодекса, в которой более детально конкретизируется порядок использования *территорий о специальными аспектами землепользования*, прописаны не все категории земель, относящиеся к охранным зонам железнодорожного транспорта, что противоречит ст.114 Кодекса.

Так, в соответствии с пп.2) ст.121 Кодекса к зонам, с особыми условиями пользования землей относятся только селеопасные, оползнеопасные и защитные лесные зоны, примыкающие к полосе отвода железных и автомобильных дорог.

Тем самым, в данную статью не попали такие категории охранных зон железных дорог, как защитные лесные полосы (в ст.121 - «лесные защитные зоны»), земельные участки, необходимые для обеспечения сохранности, прочности и устойчивости сооружений, устройств и других объектов транспорта, а также земельные участки, примыкающие к полосе отвода железнодорожного транспорта, подверженным другим (помимо селеопасных и оползнеопасных зон) опасным воздействиям.

Единого определения «охранных зон железных дорог», предусматривающего конкретные значения, в законодательстве не предусмотрено.

Составляющие собирательного понятия «охранные зоны», прописанные в п.4 ст. 114 Кодекса, не раскрыты в иных законодательных и подзаконных актах.

В частности, не нашли своего отражения в Правилах (по определению размера, режима пользования землями охранных зон и использования земель для нужд железнодорожного транспорта в полосе отвода, утвержденных приказом Министра транспорта и коммуникаций Республики Казахстан от 23 июля 2004 года N 284-I – далее Правила) такие категории охранных зон железных дорог, как защитные лесные полосы (вместо них - «охранные зоны на землях лесного фонда» п.8 Правил), земельные участки, необходимые для обеспечения сохранности, прочности и устойчивости сооружений, устройств и других объектов транспорта, а также земельные участки, примыкающие к полосе отвода железнодорожного транспорта, подверженным опасным воздействиям (в т.ч. это касается селеопасных и оползнеопасных зон).

Тем самым, ввиду отсутствия законодательной конкретизации таких составляющих института охранных зон железных дорог, как защитные лесные полосы, земельные участки, необходимые для обеспечения сохранности, прочности и устойчивости сооружений, устройств и других объектов транспорта, а также земельные участки, примыкающие к полосе отвода железнодорожного транспорта, подверженные опасным воздействиям (в т.ч. риску возникновения селя и оползня), охранные зоны железных дорог не установлены и не определены их границы.

Также в ходе анализа определены нормы подзаконных актов, закрепляющих дополнительные категории специальных зон железнодорожного транспорта, не предусмотренные законодательством.

Пунктом 1 СН РК 3.03-17-2001 «Нормы отвода земель для железных дорог» (далее – СН РК) [9] регламентированы следующие термины:

−*полоса предоставления* – территории передвижения железнодорожного транспорта, в пределах которых располагаются магистральные, станционные и подъездные пути, а также здания и сооружения необходимые для их обслуживания;

−*зона с особыми условиями пользования* – расположенная за границей полосы предоставления полоса местности на которой устанавливается особый режим пользования землей;

−*контролируемая зона* – расположенная за границей полосы предоставления полоса местности, на которой устанавливаются ограничения пользования землей.

В п.15 СН РК предусмотрено, что местными исполнительными органами устанавливаются контролируемые зоны железных дорог, в пределах которых запрещается проектирование и строительство зданий, сооружений, инженерных коммуникаций и других объектов, организация выпаса скота без предварительного согласования с уполномоченными железнодорожными органами:

−за чертой населенных пунктов – на расстоянии 50 метров от полосы предоставления железных дорог в обе стороны;

−в населенных пунктах – на расстоянии 20 метров от полосы предоставления железных дорог в обе стороны.

Вместе с тем, в нарушение требований ст.6 Кодекса данные термины СН РК («полоса представления» и «контролируемая зона») не предусмотрены (отсутствуют ссылки на них) ни в одном нормативно-правовом акте, в т.ч. Кодексе.

Предусмотренное в СН РК определение *зон с особыми условиями пользования* не соответствует аналогичному понятию Кодекса.

Так, в п.14 СН РК указано, что зоны с особыми условиями пользования определяются при необходимости при разработке проекта железной дороги одновременно с определением площадей земель, необходимых предоставлению в постоянное и временное землепользование.

При этом, согласно пп.2) п.2 ст.121 Кодекса зоны с особыми условиями пользования землей конкретно определены и ими являются селеопасные, оползнеопасные и защитные лесные зоны, примыкающие к полосе отвода железных дорог.

В результате вышеуказанных коллизий и пробелов, национальный перевозчик не обременен обязанностью по установлению границ указанных зон, а местные исполнительные органы не учитывают их при решении вопросов о выделении земельных участков.

В сфере автомобильного транспорта:

В соответствии с пунктом 2 статьи 7 Закона «Об автомобильных дорогах» [10] размер полосы отвода проектируемой автомобильной дороги общего пользования устанавливается в зависимости от ее категории согласно нормам отвода земель для автомобильных дорог общего пользования, а именно: для дорог I технической категории – по 35 метров от оси дорог, для дорог II технической категории – по 20 метров, для дорог III технической категории – по 15 метров, для дорог IV технической категории – по 13 метров, для дорог V технической категории – по 12 метров.

Так, в нарушение вышеуказанных требований, на придорожных территориях автодорог местными исполнительными органами в 13 областях и 2 городах республиканского значения (Алматы, Шымкент) предоставлено 782 земельных участка (общая площадь составляет 296,3849 га), в границах которых имеются 1908 строений, 193 населенных пункта и в которых проживают 452 375 человек.

Учитывая изложенное, целесообразно инициировать внесение в действующее законодательство поправок, предусматривающих устранение всех обозначенных пробелов и

коллизий с применением методов цифровизации и информатизации всего процесса выделения земель.

В целях профилактики и недопущения вышеуказанных правонарушений предлагается дополнить Главу 14 «Транспортные уголовные правонарушения» Уголовного Кодекса Республики Казахстан [11] новой уголовно-правовой нормой – статьей 351-1 «Незаконное изменение целевого назначения земель, в пределах санитарно – защитных зон, приаэродромных территорий, земель железнодорожного и автомобильного транспорта, а также в зонах магистральных газо- и нефтепроводов», предусматривающей ответственность за незаконное изменение целевого назначения отдельных категорий земель, а равно незаконное выделение земельных участков на их территории.

Введение предлагаемой уголовно-правовой нормы, на наш взгляд позволит предупредить и минимизировать факты незаконного использования земли.

Литература

1. Материалы проверки органов Главной транспортной прокуратуры законодательства о земельных отношениях;

2. Закон «Об использовании воздушного пространства Республики Казахстан и деятельности авиации»;

3. Постановление Правительства Республики Казахстан от 12.05.2011 №504 «Об утверждении Правил выдачи разрешений на осуществление деятельности, которая может представлять угрозу безопасности полетов воздушных судов»;

4. Санитарные правила «Санитарно-эпидемиологические требования по установлению санитарно-защитной зоны производственных объектов» от 20.03.2015 года №237;

5. Земельный кодекс Республики Казахстан;

6. Постановление Правительства Республики Казахстан от 23 января 2012 года №156 «Об утверждении норм годности к эксплуатации аэродромов (вертодромов) гражданской авиации»;

7. Строительные нормы и Правила Республики Казахстан 3.05-01-2010 «Магистральные трубопроводы»;

8. Приказ Министра по инвестициям и развитию Республики Казахстан от 30.12.2014 г. №354 «Об утверждении Правил обеспечения промышленной безопасности при эксплуатации магистральных трубопроводов».

9. Строительные нормы и Правила Республики Казахстан 3.03-17-2001 «Нормы отвода земель для железных дорог»;

10. Закона Республики Казахстан «Об автомобильных дорогах»;

11. Уголовный Кодекс Республики Казахстан.

МАЙМАКОВ АЙБОЛАТ ТЛЕУБАЕВИЧ
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедра бастығының орынбасары з.ғ.м., полиция полковнигі

ИНТЕРНЕТ АЛАЯҚТЫҚПЕН КҮРЕС – ЗАМАН ТАЛАБЫ

«Кімде кім козбояушылық
жасаса олар бізден емес»
Мұхаммед ғ.с.,

Бөтеннің мүлкін жымқыру не болмаса мүлде танымайтын бейтаныс адамды жалған уәделермен сендіру арқылы алдау және оған шығын келтіріп, өзгеге зардап шектіру алаяқтық болып табылады.

Пайда көру үшін алдау «Малым жанымның садағасы, жаным арымның садағасы» деген халықтың менталитетінің жаһандану заманындағы алаяқтықпен жасаған әрекеті ұлттық құндылықтарымыз бен қарым қасиетіміздің төмендеп жатқанын көрсетеді. Бұл бұрыңғы ашаршылықты көрген халықтың бүгінгі ұрпағының тойымсыздығынан туған дағдарыс кезіндегі өте өзекті тақырып болып отыр. Алдау арбау жағдайға байланысты адамның ситуациядан шығуға бар мүмкіншіліктерін пайдаланудың ақылды және ақылсыз ойлары мен ниеттерінен шығатын әрекеттері сияқты. Алаяқтар азаматтардың ақшаға деген қызығушылығын еш қиындықсыз пайдаланады. Қазақтың «Заманың түлкі болса тазы боп шал» деген мәтел қоғамдағы алаяқтық түлкі бұлаңға тазыдай қырағы, жүйрік, адал болуды меңзеп отыр. Қазақстандағы алаяқтықтың жаңа түрлері көбейді. Алаяқтық схемалар үнемі дамып, азаматтардан жеке ақпарат алудың жаңа әдістері ойлап табылып жатыр. Осы схемалардың бірі – ақшалай өтемақы беруді сылтауратып, пайдаланушылардың жеке деректерін жинау. Бұл схема цифрлық жүйеге көшуден пайда болды, Ел арасында, әлеуметтік желілерде алдау көріністері белсенді түрде тарала бастады. Бейнежазбалардың әрқайсысының ұқсас атаулар арқылы шатасуларға себеп болатын бағытта да жұмыс жүргізуде. Өтірік сөйлеу ауыруды, шын сөйлеу сау екендігіңді білдіреді деген. Сондықтан қоғамның рухани жетіліп отыруы жаһанадану кезеңіндегі кертартпа, адамшылыққа жатпайтын әрекеттер адамның гуманистік синтезіне жетелеуіне кері әсері болары ақиқат.

Қазіргі таңда алаяқтық қылмыстардың пайыздық өлжемі жоғары болып тұр. Арнайы осымен айналысып пайда табуға құштарланған адам ойының азартты кезеңіне ұласып кету қаупі бар. Ол үшін оған қарсы нақты дұрыс пікірлер адам санасына жеткізіліп, зиянды жақтарының ақыры қалай болатынын дәлеледеп көрсету арқылы өмірлік, заңды жазалардың барлығын түсіндіре отырып жеткізу керек. Бұндай жағдайда қай заманда да қателіктер болған кезде жазалық шешімдері шығып отырған. Сол арқылы қандай құқық бұзушылықтар жол берілгенде себептерін таба отырып, оны алмастыратын жақсы қандай бағыттар бар екенін тауып ортаға қоғамға кеңес беру керек,

Ал бүгінгі таңда цифрлық білімнің баршаға ортақ оқытулары терең меңгерілмегендіктен барлық салада қателесулерге жол беріледі. Сондықтан әрбір адам өзіне сақ болып өзіндік білімін арттыру арқылы цифрлық білімнің кеңістігіне жол ашады. Қызығушылық, біреуден

сұрау арқылы жауап алып қоғамның ағысынан қалып қоймау керек. Бұл бүгінгі күннің сын қауіп қатері.

Цифрлық құрылғыларды бұзу арқылы кедергілер туғызып соны жөндеу үшін мәжбүрлеу шаралары арқылы пайда табуды ойлайтындар да болады.

Адам құқықтары мен бостандықтарына Қазақстан Республикасы Конституциясының 18-бабында «Әркімнің жеке өміріне қол сұғылмауына, өзінің және отбасының құпиясы болуына, ар намысы мен абыройлы атының қорғалуына құқығы бар. Әркім өзінің жеке салымдары мен жинаған қаражатының, жазысқан хаттарының, телефон арқылы сөйлескен сөздерінің, почта, телеграф арқылы және басқа да жолдармен алысқан хабарларының құпиялығы сақталуына құқығы бар. (Тексеру заңды ретпен ғана шектеледі). Сондай ақ ӘҚБтК 444-бабында құмар ойындарға қатысу, тарту немесе рұқсат беру жауапкершілігінің 21 жасқа дейінгі тиым бар екені, жазаларының да көрсетілгені анық. Алайда цифрлық жүйенің қолжетімділігі, ондағы жарнамалар жастарды улаумен келеді. Ал бүгінгі таңда шет елдерден келген техникаладың барлығын тиімді екен деп пайдаланамыз. Соның барлығын тексеріп бақылаудан өткізетін мамандар дайындап қадағалап отыру қауіпсіздігіміздің кепілі болатын шаралар қабылдауымыз дұрыс болар. Қазіргі таңда әрбір адамды, оның үйін, қай жерде тұрғанын спутниктік жүйе арқылы тез біле қоямыз. Ол қаншалықты дұрыс. Қол жетімділік жақсы ал кейінгі қауіпсіздік жағы қалай болады соны да ойлауымыз керек. Әрбір үйде қолданылатын техникалардың да залалды жақтары да болып қалуы мүмкін дайындаушы ел оның зиянды жақтарын білуі, ақпараттық мәліметтер алуы, өздерінде пайдаланбауы мүмкін. Алайда шығарылған заттың қаражатын қайтару үшін адам баласы сата береді, бірі біліп, бірі білмей ұсынуы мүмкін. Еліміздің ең қымбат қазынасы адам адамның өмірі болғандықтан мемлекеттің қауіпсіздігін, адамдарын қорғау, оларға титтей де зиян келмеу керектігін ойлауымыз керек.

Интернет сауда арқылы шығындалып жатқан қаншама азамат шағымдануда. Ал оның себептері қылаң бергеннен құқық қорғау органдары жұмыс жасап тоқтатып отыру керек. Адам тұзақтарға түсіп қалмау үшін егжей-тегжейлі толық сенімде болу керек. Адамдардың салықтан қашу арқылы өтемақы алу, төлеу кезінде банкоматтардың жанында тұрып нақты алмастыру жасауы әдетке айналып келеді. Ал сол жерлерде жалған ақшамен немесе телефондарды пайдалану арқылы чекті көрсетіп ақша түспей қалу операцияларын да жасауы мүмкін осылай алданып қалмасына кім кепіл. Соның заңдылығы мен заңсыздығы мен да ашып көрсетіп ақпарат құралдар арқылы халыққа жеткізу керек. Жеке деректерді қорғау қоры биік деңгейде жұмыс істеу керек.

Қазіргі таңда сіздің счетіңізден ақша шығарылғалы жатыр, біз ішкі істер министрлігінен хабарласып тұрмыз, сіздің атыңыздан банктен ақша алғалы тұр сіз келісесіз бе деген сияқты сұраулар қойылады. Алайда қайта хабарласқан жағдайда сол телефондардың барлығы қайтып алмайды. Сондықтан сондай жағдайларда хабар шалған телефондардың барлығын тексеріп тез арада шешімі айтылу керек. Сондай қадағалаулардың болмауы себепті де кез келген қылмыскер оңай құтылып құқықтық жауапкершілікті сезіне алмайды. Бұл әдеп белең алса адамның бойындағы адамгершілік қасиеттің жоғалып қоғамның қасиетсіз қабілеттері пайда болып мемлекеттің құруына бірден бір себепкер болады. Сондықтан қазіргі таңнан алдын-алу шаралары уақыттан кеш қозғалмай әрекет ету керек. Әрбір азамат ұрпағына деген жауапкершілікті арттыру керек. Абайдың әкесі болған, болыс болған, ел деп елдің мүддесін ойлаған, Қазақтың соңғы ханы Кенесарыға көмек қолын созған Құнанбайды анасы ұлын қалай қадағалады. Кәмелетке толмағандар Конвенцияның 1-бабына сәйкес 18 ге толмаған әрбір адам танылса, Қазақстан Республикасы Азаматтық кодексінде, «Неке және отбасы туралы» заңдарында аталып өткен. Осыған орай ата ана тәрбиесі ұрпағын шалыс қадам басудан қадағалауын тоқтатпау керек. Сервистік полицияның да негізгі қағидаттарында қылмыстың себеп салдарын табу арқылы қоғамды дұрыс жолға салу жазалау емес.

Сені Жаратқанды, ата анаңның абыройын ойлап ұятқа қалдырмай әрекет ет. Құжаттарды рәсімдеу туралы ұсыныс, атынан кредитеттер алу т.б. Алаяқтар сайты егер пайдаланушы әрі қарай келісіп, толтырса, онда оның картасынан теңге алынады. Бірақ уәде етілген өтемақы келмейді. Бұл схеманың зияны мынада: Алаяқтар, сайып келгенде, жәбірленушінің жеке шотынан барлық ақшаны ала алады. Алаяқтардың арбауына түсіп қалмау үшін не істеу керек. Бұл схемалар аңқау және тәжірибесіз пайдаланушыларды алдау арбаумен болады. Сондықтан барлық құжатқа қырағылық танытып, ақпаратқа сын көзбен қарау керек. Сіз сондай-ақ кейбір ережелерді сақтауыңыз керек: Сенбеңіз. Тек сауалнамаға немесе сауалнаманы толтыруға, келтірілген зиянды өтеуге және тағы басқаларға оңай ақша табу туралы уәде берулерге мұқият болу керек. Ал егер олар сізден бірдеңе үшін алдын ала төлем жасауыңызды сұраса, онда бұл сөзсіз алаяқтық. Өзіңіз тексеріңіз. Мұндай нәрсені уәде еткен акциялар немесе компаниялар туралы қосымша ақпарат іздеу керек. Барлық толық ақпаратты іздеу жүйелерінен табуға болады. Жеке деректерді енгізбеңіз. Банк картасының нөмірі, телефон нөмірі, жеке деректер – мұның бәрі тексерілмеген сайттарға жіберілмеуі керек. Мұндай ақпараттың шығуы пайдаланушыға айтарлықтай зиян келтіруі мүмкін. Алаяқтықтың ерекшелігі-қылмысты іске асыру тәсілінде, яғни алдау немесе сенімділікті пайдалану жолымен жасалады.

Меншікке заңмен кепілдік берілген. Ешкімді де соттың шешімі болмайынша өз мүлкінен айыруға болмайды.

Бұл ережелер пайдаланушыға алаяқтықтан қорғануға және олардың деректерін сақтауға көмектеседі. Алаяқтардың басқа да сан мың түрлі әдісі жаңарумен жасалып келеді. Солардың біліп жүру үшін атап өтсек:

1. Интернет-дүкен алаяғы. Ол үшін алаяқтар онлайн дүкендерді пайдаланады. Себебі бүгінде көпшілігіміз үйде отырып-ақ өзімізге керекті заттарға тапсырыс беруді әдетке айналдырғанбыз. Бұл бір жағынан тиімді болғанымен, екінші жағынан қауіпті. Себебі алаяқтар сіздің сеніміңізді пайдалана отырып, сан соқтырып кетуі бек мүмкін. Олар алдын ала төлем жасауды сұрайды. Ал ақшаңызды алып алғаннан соң зым-зия жоғалады. Сондай-ақ бастапқыда берілген мекен жайды анықтау мүмкін емес болып қалады. 2. Интернет-қайыршылық. Яғни мұнда қайырымдылық ұйымдары, құрылыс жұмыстарына ақша жинау секілді әдістерімен ұйымдастырылады. Компания болып құрылдық деп, жұмыс істеп тұрады. Салымшылардың сеніміне кіріп, ақшаны жымқырғаннан соң жабылып қалады. Кейіннен жаңадан және жаңа атаумен ашылып қайтадан алаяқтық әрекеттерін жүзеге асырады. Оның ғаламтордағы сайтының ақпары 2 беттен аспайды. Бұл жағдайда күмәнмен қараған жөн. 3. Фишинг. Алаяқтықтың бұл түрі құпия деректерді пайдаланушылардың «логин парольдеріне» қол жеткізу арқылы жүзеге асады. Кез-келген адамның аккаунтын бұзу арқылы оның қаражаттарын алып, құпия болған жеке мәліметтеріне қол жеткізеді. 4. Кликджекинг. Көбіне лүпіл жинап беру, жазылушылар санын арттыру секілді уәделерді беріп, ақшаңызды алғаннан соң оларды табу мүмкін болмай қалады. 5. Биржалардағы интернет-алаяқтық. Мұнда акцияларды арзанға сатып алып, қымбатқа өткізу. Сондай-ақ қызықты акцияларды көрсетіп жарнаманы жақсылап жариялайды да, соңында жасанды болып шығады. Кей жағдайларда адамдардан түрлі сылтаулармен қосымша төлем жасау керектігін алға тартып, ақшаларын алады. 6. Интернеттегі күтпеген ұтыс. Тосын сый секілді сіздің қатысуыңызсыз ұтыс ұттыңыз деп хабарлайды. Ұялы телефонға смс хабарлама немесе поштаңызға жүлде ұтысы туралы ақпар келеді. Оны алу үшін ақша аударуыңызды сұрайды. 7. Интернет-казино. Онлайн-казино ұтып алғысы келетін құмар ойынға жақын адамдарды құрыққа түсіреді. Сенімді сайттар сенімді ұтыстың әдістерін ұсынады, бірақ рулеткадағы математикалық схемалардың ешқандай түрлері әрекет етпейді. 8. Интернеттегі қаржы пирамидалары. Табысты ұлғайту үшін ақша салуды басқа да адамдарға таратуды айтады. Осылайша ақшаңызды қалталарына оңай басып отырады. 9. Танысу сайттарындағы және әлеуметтік желілердегі алаяқтық. Неке алдау- бәрі кез-келген сайтта немесе әлеуметтік желіде хабарландыру бойынша әдеттегі танысудан басталады. Адамның сеніміне 2-3 ай ішінде ие болып, өзінің қаржылық мәселелерін шешуге ақша сұрайды. Бірақ ақшаны алғаннан соң жоғалады. Онымен байланысу мүмкін болмай

қалады. 10. Валюта айырбастаудағы табыс. Пайдаланушыларға валюта айырбастау үшін электрондық айырбастау пункттерін пайдалана отырып, ақша табу ұсынылады. Алаяқтар түрлі төлем жүйелерінде екі шот ашып, екі айырбастау пунктінің көмегімен валютаны өзгертіп, кері айырбастауды сұрайды. Айырбастау орындарының бірі жалған болып шығады. 11. Интернет-кредиттеу саласындағы алаяқтық. Жеке фирмалар мен жеке тұлғалардан алдын ала төлемнен кейін ғана қызмет көрсететін несие рәсімдеу кезінде несие беруге уәде береді. Ал ақша алғаннан кейін жоғалады. Кейде интернет сайттар сізге өтінім қалдыруды, сауалнама толтыруды ұсынады. 12. Жалған крипто-валюта алаяқтары адамдарды ақша аударуға, арзан бағада крипто валюталарды сатып алуға, сол арқылы көп табыс табуға болады деп сендіреді. 13. СМС арқылы алаяқтық. «Несиеде қарызым бар, нөмірмен қателестім, басқаның ақшасы аударылып кетті, кәртішкем блокқа түсіп қалды, туыстарым қайғылы жағдайға душар болды», – деген секілді түрлі хаттарды сізге жолдау арқылы ақшаңызды жымқырады. 14. Фрилансдағы интернет-алаяқтық. Яғни сіздің жеке мәліметтеріңізге қол жеткізіп, сіздің атыңыздан түрлі несиелерді рәсімдейді. Жеке мәліметіңізді пайдалана отырып, әрекет етеді. Сонымен қатар, күнделікті және үйден шықпай-ақ табыс табу секілді түрлі сылтаулармен ақша аудартады. 15. Киберсквоттинг – бұл компаниялардың атаулары мен жаңа тауарлардың брендтері арқылы ақша табу тәсілі тағы басқалар.

Алайда мұның барлығы үшін құқықтық мемлекетіміздің заңдарындағы жауапкершіліктердің, жазаның бар екенін ескертеді.

Қазақстан Республикасы Қылмыстық кодексінің 190-бабы. Алаяқтық. Яғни бөтеннің мүлкін жымқыру немесе алдау, сенімді теріс пайдалану жолымен бөтен мүлікке құқықты иемдену мүлкі тәркіленетіні, еселенген айыппұл арқалайтыны, түзеу жұмыстарына, қоғамдық жұмыстарға тартылатыны, белгілі бір лауазымдарды атқаруы, айналысу құқығынан өмір бойына айырыла отырып бас бостандығынан шектеу, бас бостандығынан айыру сияқты жазалардың бар екенін ескертеді. Ал бүгінгі мақсатымыз алаяқтардың әдістерінен хабардар ете отырып, одан сақтандыру. Алаяқтар үнемі басқа да жолдарын ойластырып, іске асырады. Сақтанғыңыз келсе, әрбір іске сауатты қарап, кеңесіп дұрыс шешім шығаратын адамдық қабілетіңізді ұмытпаңыз.

Өнеге болсын деп өлеңіммен қорытындылаймын.

Ау адамдар жалған айтып, жан сатпа,
Көңіл, нәпсің, жүгірмесін сан-саққа.
Алдау, арбау, ұрлап жеген асыңнан,
Адалдықпен жеткен жақсы мақсатқа.

Әдебиет

1. Қазақстан Республикасының Конституциясы 1995 жыл 30.08.
2. Қазақстан Республикасының қылмыстық кодексі 2014 жыл 3.07.
3. Қазақстан Республикасының әкімшілік құқық бұзушылық туралы кодексі 2014 жыл 5.07
4. Караван жаңалықтары -https://kaz.caravan.kz/zhangalyqtar/
5. https://kaz.nur.kz/nurfin/1876221-internettegi-alaaktyk
6. Абай Құнанбайұлы «Қара сөздер» Алматы «Атамұра 2020 жыл»
7. Әке аманаты А.Маймақов 2014 ж.
8. «Жекелеген қылмыс түрлерін тергеу ерекшеліктері» Елеген Қайыржанов, Ардақ Шакенов Алматы. 2007 жыл.
9. Қазақстан Республикасы Қылмыстық процестік кодексі 2014 жыл. 4 шілде
10. Қазақстан Республикасының азаматтық кодексі 1999 жыл 1 шілде
11. Қазақстан Республикасының неке және отбасы туралы кодексі 2011 жыл 26.12.
12. Баланың құқығы туралы жаднама Ж.Тұрмағамбетова 2002жыл.

БАТЫРБАЕВ АДЫЛХАН КОШКЕНОВИЧ
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры, з.ғ.к., полиция полковнигі

КОМПЬЮТЕРЛІК ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТЫҢ ҰҒЫМЫ ЖӘНЕ МӘНІ

Қазіргі қоғамның әлеуметтік проблемаларының қоғамдық қатынастарға үлкен зиян келтіретін компьютерлік қылмыстың пайда болуы болды. Оның пайда болуы азаматтардың компьютерлік құрылғыларды жеке, өндірістік немесе қызметтік мақсатта қолдануы, компьютерлік бағдарламалау және бағдарламалық қамтамасыз ету мүмкіндіктері, компьютерлік ақпаратты құру, сақтау, өңдеу, беру, қорғау құралдарының жұмыс істеу ерекшеліктері туралы әлсіз түсінікке ие болуының арқасында мүмкін болды, осылайша компьютерлік қылмыскерлердің ықтимал құрбаны болды.

Сондықтан азаматтардың, мемлекеттік мекемелердің, кәсіпорындардың, билік органдарының ақпараттық қауіпсіздігі туралы мәселе компьютерлік ақпаратқа, зиянды компьютерлік бағдарламаларға және басқа да компьютерлік қауіптерге рұқсатсыз қол жеткізуден өзекті болып отыр.

Компьютерлік қылмыстардың дамуы тұралы ғылыми ортада дамуының басталуы 1960 жылдарға келеді деген пікірлер қалыптасқан.

1960 жылдары транзисторлық компьютерлік жүйелердің пайда болуы, олардың мөлшері кішірек және лампалық есептеу машиналарына қарағанда арзан, компьютерлік технологияны кеңінен қолдануға әкелді. Осы ерте кезеңде құқық бұзушылықтар компьютерлік жүйелер мен жинақталған деректердің физикалық зақымдалуынан тұрды.

1970 жылдары компьютерлік жүйелер мен деректерді пайдалану одан да белсенді бола бастады. Кейбір бағалаулар бойынша, онжылдықтың соңында Америка Құрама Штаттарында шамамен 100 000 әмбебеп компьютер жұмыс істеді. Бағаның төмендеуімен компьютерлік технологиялар мемлекеттік секторда және іскерлік ортада, сондай-ақ жұртшылық арасында кеңінен қолданыла бастады. Компьютерлік қылмыстың жаңа түрлері пайда болды. Бұған компьютерлік жүйелерді заңсыз пайдалану, сондай-ақ электрондық деректерді заңсыз манипуляциялау кірді. Қолмен жасалатын операциялардан компьютерлерді пайдалануға көшу нәтижесінде қылмыстың тағы бір жаңа түрі пайда болды-компьютерлерді қолданумен байланысты алаяқтық.

1980 жылдары дербес компьютерлер барған сайын танымал бола бастады.

Компьютерлік жүйелердің таралуының осындай әсерлерінің бірі Бағдарламалық жасақтамаға деген қызығушылықтың артуы болды, бұл бағдарламалық жасақтама қарақшылығы мен патенттік қылмыстардың алғашқы түрлеріне әкелді. Сонымен қатар, бағдарламалық жасақтаманы желілер арқылы тарату мүмкіндігіне ие бола отырып, қылмыскерлер зиянды бағдарламалық жасақтаманы жіберді және компьютерлік вирустар көбірек табылды.

1990 жылдары графикалық интерфейсті (www) енгізу, содан кейін Интернет қолданушыларының қарқынды өсуі жаңа мәселелерге әкелді. Компьютерлік қылмыстар

жалпы жергілікті сипатта болғанымен, интернет электронды қылмыстарды трансұлттық қылмыстарға айналдырды.

XXI ғасырда компьютерлік қылмыста жаңа тенденциялар пайда болды. Жаңа мыңжылдықтың бірінші онжылдығы жалған электрондық хабарламалар жіберу (фишинг) және ботнет шабуылдары, сондай-ақ Интернет арқылы IP протоколы (VoIP) арқылы дауыс беру және «бұлтты компьютинг» сияқты құқық қорғау органдарымен жұмыс істеу қиынырақ технологияларды тарату сияқты қылмыс жасаудың жаңа, өте күрделі әдістерінің белгісімен өтті. Қылмыс жасау әдістері ғана емес, олардың ауқымы да өзгерді. Құқық бұзушылар автоматты түрде шабуыл жасау мүмкіндігіне ие болғандықтан, құқық бұзушылықтар саны артты.

Дегенмен, қазіргі уақытта компьютерлік қылмыс деп нені түсіну керек деген сұраққа ғылыми қоғамдастықта нақты жауап жоқ және осы заңды тұжырымдаманың мазмұны мен мағынасы туралы көптеген пікірталастар әлі де жалғасуда.

Қазіргі уақытта отандық және шетелдік криминология ғылымында қарастырылып отырған тұжырымдаманы анықтауға көптеген тәсілдер бар.

Отандық және шетелдік басылымдар мен бұқаралық ақпарат құралдары «ақпараттық қылмыс», «компьютерлік қылмыс», «киберқылмыс» және «байланыс саласы» сияқты терминдерді жиі қолданады.

Қазақстан Республикасының Қылмыстық кодексінде «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» жеке тарауыға біріктіру өмір қажеттілігінен пайда болған құбылыс [1, 165б].

Ақпараттық және коммуникациялық технологиялар өзінің даму процесінде қоғам өмірінде маңызды орын алады. Олар мемлекеттік органдардың, қаржы-экономикалық институттардың қызметіне кеңінен енгізілуде [2].

«Ақпарат туралы» 2015 жылғы 24 қарашадағы ҚР Заңы ақпаратты осылай айқындайды :бұл мемлекеттік органдардың, жеке және заңды тұлғалардың қызметін автоматтандыруға бағытталған ұйымдастырушылық, әлеуметтік-экономикалық және ғылыми-техникалық процесс [3].

«Байланыс туралы» 2004 жылғы 5 шілдедегі ҚР Заңы байланысты ақпаратты қабылдау, жинау, өңдеу, жинақтау ,беру (тасымалдау), жеткізу, тарату, пошталық және арнайы негіздемелер, пошталық ақша аударымдары ретінде айқындайды [4].

Мысалы, Т. Л. Тропина «компьютерлік қылмыс» ұғымы есептеу техникасы, ғаламдық желілер арқылы жасалған барлық әрекеттерді қамтымайды деп санайды. Киберқылмыс, оның пікірінше, киберкеңістікте компьютерлік жүйелер немесе компьютерлік желілер, сондай-ақ компьютерлік жүйелер немесе желілер шеңберінде және компьютерлік жүйелерге, компьютерлік желілерге немесе компьютерлік деректерге қарсы киберкеңістікке қол жеткізудің өзге де құралдары арқылы жасалатын қылмыстардың жиынтығы [5, 39 б].

Осындай ұстанымды ұстанатын И.Г. Чекунов, ол киберқылмысты қылмыстарда зиянды компьютерлік бағдарлама немесе компьютерлік желіге немесе ұялы байланыс операторына қосылған бағдарламалық-техникалық құрал ретінде әрекет ететін құрал немесе құрал сияқты объективті жақтың белгілерінің міндетті түрде болуын анықтау негізінде анықталатын қылмыстың дербес түрі ретінде қарастырады [6, 7 б].

Кейбір авторлар осы жағымсыз әлеуметтік құбылысты тар және кең мағынада қарастыруға болады деп санайды.

Тар мағынада компьютерлік қылмыс деп белгілі бір уақыт аралығында белгілі бір аумақта адамдар жасаған қылмыстардың жиынтығын түсіну ұсынылады, мұнда қылмыстық қол сұғушылықтың негізгі объектісі компьютерлік ақпараттың, компьютерлік ақпаратты, ақпараттық-коммуникациялық құрылғыларды іздеу, жинау, сақтау, өңдеу, беру, тарату, қорғау саласындағы нақты қоғамдық қатынастар болып табылады. Компьютерлік желілер, ақпараттық-телекоммуникациялық желілер; компьютерлік ақпаратты жасау, сақтау, өңдеу,

беру құралдары қылмыстық қол сұғушылықтың нысанасы ғана емес, сонымен бірге қылмыс жасау құралы және (немесе) қаруы ретінде де пайдаланылады.

Сондықтан компьютерлік қылмыс өзінің «тар мағынасында» «киберқылмыс», «интернет-қылмыс», «компьютерлік ақпарат саласындағы қылмыс», «Ақпараттық технологиялар саласындағы қылмыс» сияқты ұғымдардың көлемі мен мазмұны жағынан кеңірек, өйткені қылмыс құрамының объективті және субъективті белгілері тұрғысынан (қылмыстың объектісі мен нысаны қол сұғушылық; әрекет түрі; қылмыстың тәсілі, құралдары; қылмыстың жалпы және арнайы субъектілері және т.б.) оларды қамтиды.

Өз кезегінде, компьютерлік қылмыс кең мағынада адамдардың компьютерлік және өзге де IT - технологияларды жеке, өзімшіл және өзге де қылмыстық мақсаттарда пайдалануы нәтижесінде пайда болған құқыққа қайшы және теріс әлеуметтік құбылыс болып табылады.

«Компьютерлік қылмыс» ұғымын анықтауға екі жақты көзқарас отандық криминология мен қылмыстық құқық ғылымында жаңа емес, оның жақтастары да, қарсыластары да бар.

Сонымен қатар, екі жақтылық компьютерлік қылмыс ұғымын анықтаудағы заңды тәсіл ретінде (БҰҰ – киберқылмыс терминологиясында) халықаралық деңгейде 2000 жылы БҰҰ-ның қылмыстың алдын алу және құқық бұзушылармен жұмыс жөніндегі оныншы конгресі аясында танылғанын атап өткен жөн, онда қылмыстың екі санаты бар екендігі атап өтілді:

1) тар мағынадағы компьютерлік қылмыстар-мақсаты компьютерлік жүйелер мен олар өңдейтін деректерді қорғауды еңсеру болып табылатын электрондық операциялар жолымен жүзеге асырылатын кез келген құқыққа қайшы әрекет;

2) кең мағынадағы компьютерлік қылмыстар (компьютерлерді пайдалануға байланысты қылмыстар) – компьютерлік жүйені немесе желіні пайдалануға байланысты жасалатын кез келген құқыққа қайшы әрекет, соның ішінде компьютерлік жүйелер немесе желілер арқылы ақпаратты заңсыз сақтау, ұсыну немесе тарату сияқты қылмыстар.

Сондықтан кейбір авторлардың пікірі бойынша «компьютерлік қылмыс» ұғымын анықтаудағы екі жақты көзқарас әлі де қисынды болып көрінеді деп санайды, өйткені бұл қылмыстық құбылыстың барлық күрделілігін, әртүрлілігін, көп деңгейлілігін бағалауға және бар ғылыми көзқарастар арасында белгілі бір тепе-теңдікті табуға мүмкіндік береді.

Жоғарыда айтылғандарды қорытындылай келе келесі тұжырымдарға келуге боладыі. Компьютерлік қылмыс күрделі әлеуметтік және мемлекеттік-құқықтық ұғым ретінде тар және кең мағынада қарастырылуы керек. Компьютерлік қылмыс кең мағынада адамдардың компьютерлік және өзге де IT-технологияларды жеке, өзімшіл және өзге де қылмыстық мақсаттарда пайдалануы нәтижесінде пайда болған құқыққа қайшы және теріс әлеуметтік құбылыс болып табылады.

Өз кезегінде, компьютерлік қылмыс тар мағынада белгілі бір уақыт аралығында белгілі бір аумақта адамдар жасаған қылмыстардың жиынтығы болып табылады, мұнда қылмыстық қол сұғушылықтың негізгі объектісі компьютерлік ақпараттың, компьютерлік ақпаратты іздеу, жинау, сақтау, өңдеу, беру, тарату, қорғау құралдарының, ақпараттық коммуникациялық құрылғылардың қауіпсіз жұмыс істеуі саласындағы нақты қоғамдық қатынастар болып табылады, ал компьютерлік ақпарат, компьютерлік желілер, ақпараттық-телекоммуникациялық желілер; компьютерлік ақпаратты жасау, сақтау, өңдеу, беру құралдары қылмыстық қол сұғушылықтың нысанасы ғана емес, сонымен бірге қылмыс жасау құралы және (немесе) қаруы ретінде де пайдаланылады.

Кейбір авторлардың пікірінше, компьютерлік қылмыс өзінің «тар мағынасында» киберқылмыс, «интернет-қылмыс», «компьютерлік ақпарат саласындағы қылмыс», байланыс саласындағы «ақпараттық технологиялар саласындағы қылмыс» сияқты ұғымдардың көлемі мен мазмұны жағынан құрамның объективті және субъективті белгілері тұрғысынан кеңірек қылмыстар (қылмыстық қол сұғудың объектісі мен нысанасы; іс-әрекет түрі; қылмыстың тәсілі, құралдары, қаруы; қылмыстың жалпы және арнайы субъектілері және т.б.).

Жоғарыда айтылғандардың негізінде компьютерлік қылмыстың мәнін сипаттайтын келесі маңызды белгілерді ажыратуға болады:

Компьютерлік қылмыс қылмыстың басқа түрлерімен тығыз байланысты, өйткені компьютерлік ақпарат саласындағы қылмыстар көбінесе басқа қылмыстық әрекеттерді жасау тәсілі болып табылады (ұрлық, бопсалау, коммерциялық, салықтық немесе банктік құпияны құрайтын ақпаратты заңсыз алу және жария ету; сатқындық, тыңшылық және т.б.).

Әдебиет

1. Ағыбаев А.Н. Қылмыстық құқық: Ерекше бөлік: Оқулық. – Алматы: Жеті жарғы, 2015. – 608бет.

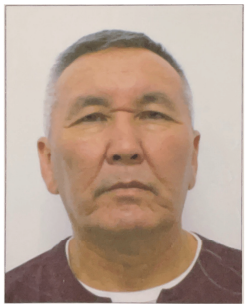
2. Борчашвили И.Ш. Комментарии к Уголовному кодексу Республики Казахстан. Особенная часть. Том 2. – Алматы: Жеті Жарғы, 2021. Т.2. – С. 1152.

3. Закон РК от 24 ноября 2015 г. «Об информации» https://adilet.zan.kz/rus/docs/Z070000217_/compare

4. Закон РК от 5 июля 2004 г. «О связи» https://adilet.zan.kz/rus/docs/Z040000567_

5. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: 12.00.08 : дис. … канд. юрид. наук. Владивосток, 2005. – С. 234.

6. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореферат : 12.00.08 : дис. … канд. юрид. наук. – М, 2013. – С. 223.



САТЫБАЛДИНОВ МАРАТ ТЕМИРГАЛИЕВИЧ
Старший преподаватель Школы права, Евразийский технологический университет

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ДЛЯ ФОТО-ВИДЕО ФИКСАЦИИ МЕСТА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

При осуществлении осмотра места происшествия согласно ст. 219 Уголовно-процессуального кодекса Республики Казахстан [1], (УПК РК) во многих случаях применяется фото-видео фиксация, с целью запечатления вещной обстановки. Для этого руководствуясь криминалистическими рекомендациями, применяем такие съемочные приемы как: ориентирующий, обзорный, узловой и детальный способы фотофиксации места происшествия, позволяющие обеспечить запечатление необходимой картины произошедшего события [2]. Результаты фотофиксации, оформленные в виде фототаблиц с наглядными изображениями произошедшего события, дополняют такое следственное действия как осмотр: места происшествия.

Вместе с фотофиксацией в настоящее время на практике используется и видео-фиксация процесса, происходящего во время осмотра места происшествия. «Различают съемку с одной точки неподвижной камерой – статичный кадр и съемку движущейся камерой – динамичный кадр», сказано в учебнике криминалистики [3, 187].

К примеру, осмотр трупа на месте его обнаружения обычно состоит из двух стадий общего и детального осмотра трупа. Ход и результаты осмотра отражаются в протоколе осмотра места происшествия.

По прибытии на место обнаружения трупа следователь поручает специалисту-судебной медицины установить наличие или отсутствие достоверных признаков смерти: трупных пятен, окоченения, телесных повреждений, не совместимых с жизнью человека, и т. п. При малейшем сомнении в наступлении смерти необходимо принять все возможные в данной ситуации меры для оказания первой помощи пострадавшему, в том числе организовать доставку его в лечебное учреждение. Если специалист из области медицины констатирует смерть, то безотлагательно производится наружный осмотр трупа. Задачей наружного осмотра трупа является выявление и описание в протоколе обстоятельств, которые невосполнимы в последующем, т. е. при судебно-медицинском исследовании трупа в морге.

Процессуальный порядок осмотра трупа регламентируется ст. 222 уголовно-процессуального кодекса Республики Казахстан далее (УПК РК) [2]. В соответствии с ч. 1 этой статьи следователь производит осмотр на месте его обнаружения с обязательным участием судебно-медицинского специалиста, а при невозможности его привлечения участие врача – желательно общего профиля. Как указано в УПК РК в случае необходимости при осмотре могут привлекаться и другие специалисты, к примеру кинолог, специалист-криминалист и др.

Традиционно, фото-видеосъемка события преступления осуществляется с рук, либо со штатива, параллельно поверхности (плоскости), с этой же целью, может быть применена

стереофотосъемка. Стереоскопическая фотография – это метод получения фотоизображений, позволяющих видеть объекты в трех измерениях. Особенно полезным этот метод получения фотоизображения является для фиксации мест дорожно-транспортных происшествий, осмотр которых должен производиться в весьма сжатые сроки [3, 161]. Однако, по различным причинам, на практике данный фотографический прием не получил широкого применения. Поэтому, зачастую на фототаблице, получается двухмерное изображение запечатлевающее событие дорожно-транспортного происшествия, которое не способно охватить взаиморасположение, к примеру, находящиеся друг за другом объекты, так как порой бывает невозможно найти такую точку съемки, которая позволило бы запечатлеть положение этих объектов со стороны, откуда видно необходимое обозрение. К тому же, когда возникает необходимость запечатления события ДТП, на оживленных дорогах крупных городов, на открытой или горной местности, в ограниченном пространстве (в туннелях и под мостами) возникают определенные трудности, связанные с физической невозможностью найти оптимальную точку для осуществления фото-видеосъемки.

При таких случаях, фото или видеосъемка, произведенная с удобного и безопасного места, иногда не может полностью охватить событие в целом, и сопряжено с опасностью для жизни и здоровья лица, осуществляющего данное действие, например при пожарах, при необходимости фото-видеофиксации на крутых склонах гор, под туннелями и при других аналогичных обстоятельствах. Поэтому возникает необходимость в более приемлемом способе запечатления события, поиска и выбора такой точки для съемки, которая позволила бы обеспечить полноценную, быструю и безопасную фиксацию места осмотра. (Не только по делам о ДТП, но о по другим видам правонарушений). В законодательстве, УПК РК в ст. 126 ч. 3 п. 3,4., сказано, что применение научно-технических средств признается допустимым, если они: обеспечивают эффективность по уголовному делу и безопасны.

Разрешение данной проблемы видится в трансформации знаний научно-технического прогресса для целей криминалистики, в частности достижения технической отрасли по использованию беспилотных летающих аппаратов, для фото-видео фиксации места происшествия.

Что такое беспилотные летающие аппараты (БПЛА), или беспилотники? Отвечая на этот вопрос, приведем краткий исторический обзор о возникновении и развитии данного явления. Идея применения управлением машин без людей, принадлежит Николе Тесла, который еще, в 1899 году разработал и продемонстрировал миниатюрное радиоуправляемое судно.

В 1910 году американский военный инженер из Огайо Чарльз Кеттеринг предложил использовать летательные аппараты без человека. По его замыслу управляемое часовым механизмом устройство в заданном месте должно было сбрасывать крылья и падать, как бомба, на врага.

В Великобритании в 1933 году, был разработан первый БПЛА многократного использования Queen Bee, были использованы три отреставрированных биплана Fairy Queen, дистанционно управляемые с судна по радио, сделав Великобританию первой страной, извлёкшей пользу из БПЛА. Эта радиоуправляемая беспилотная мишень под названием DH82A Tiger Moth использовалась на королевском Военно-морском флоте с 1934 по 1943 годы. Армия и ВМФ США с 1940 года использовали БПЛА Radioplane OQ-2 в качестве самолёта-мишени.

В течение Второй мировой войны немецкие учёные вели разработки нескольких радиоуправляемых типов оружия, включая управляемые бомбы Henschel Hs 293 и Fritz X (англ. Fritz X), ракету Enzian (англ. Enzian) и радиоуправляемый самолёт, наполненный взрывчатым веществом. Несмотря на незавершённость проектов, Fritz X и Hs 293 с успехом использовались на Средиземном море против бронированных военных кораблей.

Одним из основных поставщиков БПЛА гражданского назначения для США является компания AeroVironment [3]. Семейство БПЛА включает модели Wasp («Оса»), Raven («Ворон») и Puma («Пума») в весовом диапазоне от 5,5 до 6,5 кг. Все аппараты в полевых

условиях переносятся в рюкзаке, собираются за считаные минуты и запускаются с рук. БПЛА оснащены цветными и инфракрасными камерами высокого разрешения, передающими изображение в режиме реального времени. Управление производится с носимого пульта [4].

Изобретенные для гражданских целей БПЛА классифицированы на «микро» и «мини» типы (назначение, вес, размер, продолжительность и высота полета, система запуска и приземления, наличие систем автопилотирования и навигации, формат фото- и видеосъемки и т.д.)

Как видим прообразы БПЛА были изобретены в конце XIX столетия и пройдя закономерный эволюционный путь, дошли до наших дней и нашли широкое применение во многих отраслях науки и техники.

Область применения БПЛА весьма обширна: от сельского хозяйства и строительства до нефтегазового сектора и общественной безопасности. В частности, БПЛА могут быть использованы:

– службами по чрезвычайным ситуациям (контроль пожарной безопасности и природных стихий);

– в сельском хозяйстве (наблюдение за посевами и контроль агротехнических процессов);

– в лесничестве и рыболовстве (лесоохрана и контроль рыбного промысла);

– в компаниях, занимающихся геодезией (картографирование и земле измерение);

– в географии и геологии;

– в нефтегазовом секторе (мониторинг нефтегазовых объектов);

– в строительстве (инспектирование строек и наблюдение за текущими моментами строительных объектов);

– средствами массовой информации (аэро – фото - и видеосъемка) и др.;

– полицией (патрулирование определенных зон, обеспечение информацией об определенных событиях и т. д.).

– и конечно же в нашем обсуждаемом проекте.

Из зарубежного передового опыта можно констатировать, что полиция Швейцарии в г. Цюрих начала использовать беспилотники для съемки дорожно-транспортных происшествий. «Использование беспилотников для такой цели наиболее оправдано, когда происходит авария крупного масштаба, например, с участием подъемного крана или поезда – раньше в таких случаях не было возможности сфотографировать место происшествия полностью» говорит Матт Мак Фарланд [5].

Особенность фиксации места ДТП, с использованием фото-видеосъемки с БПЛА, в том, что появляется возможность использования новой «точки» опоры для съемки, позволяющей запечатлеть по вертикальному фронту - сверху вниз картину произошедшего события. Этот способ позволяет производить видеозапись с точки, находящейся над местом ДТП и запечатлеть положения транспортных средств и их взаиморасположения, действия и положения участников ДТП, образовавшиеся следы, неподвижные ориентиры, что очень важно для получения объективного ответа, на вопрос о происхождении механизма ДТП.

Перспективность использования летающих беспилотных аппаратов (БПЛА), в том, что предоставляется возможность запечатлеть обстановку места совершения ДТП в плане, то есть получить видео-фотоизображение, на котором наглядно видно расположение и взаиморасположение транспортных средств и других участников ДТП. Необходимо отметить то, что схема места происшествия, прилагаемая к протоколу осмотра места происшествия, будет дополнена наглядной и полноценной фототаблицей. Особенно это важно при проведении осмотра с большим количеством транспортных средств, участвовавших в ДТП на автомагистралях, в туннелях или же в местах пересечений автомагистралей и железнодорожных путей сообщения. К тому же рассматриваемая возможность фото-видео фиксации, будет полезной в труднодоступных горных местах или других загруженных участках дорожной сети. Применяемый при этом прием фотосъемки можно назвать:

«вертикальной фото-видеосъёмкой сверху вниз», либо «фасадной фото-видеосъемкой» или же «фото-видеосъёмкой для получения изображений в плане».

Таким образом, предлагаемый прием фото-видео фиксации с использованием БПЛА представляется перспективным для фиксации произошедшего события при проведении осмотра места происшествия по различным делам, с большим количетвом снимаемых объектов. Так как это позволит получить более полную и объективную информацию о расположении и взаиморасположении, различных следов в «широком» криминалистическом понимании, что необходимо для объективного и полноценного досудебного производства по уголовным делам, согласно раздела 6 Особенной части УПК Республики Казахстан.

Литература

1. Уголовно-процессуальный кодекс Республики Казахстан. – Алматы. ЮРИСТ. 2014. – С. 356.
2. Уголовный Кодекс Республики Казахстан. – Алматы. Юрист 2016 г (с изм. и доп.)
3. Белкин Р.С. Курс криминалистики: Учеб. Пособие для вузов. – 3 изд., дополненное. – М.: ЮНИТИ-ДАНА, Закон и право, 2001. – С. 837.
4. Криминалистика том 1 Под редакцией профессоров Р.С. Белкина, В.П. Лаврова, И.М. Лузгина. Москва 1987. – С. 340.
5. Веб-сайт: http://absrf.ru/ru/uav/1411023279.htm
6. Матт Мак Фарланд Источник suasnews.com

МАРАТ АЙГҮЛ МАРАТҚЫЗЫ
Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстаним. М. Есбулатова, з.ғ.к.

ТРУД ОСУЖДЕННЫХ – КАК МЕРА ПРОФИЛАКТИКИ ПЕНИТЕНЦИАРНЫХ ПРЕСТУПЛЕНИЙ

Анализ причин и условий, способствующих совершению преступлений в пенитенциарных учреждениях, позволяет сделать вывод о том, что они в значительной степени коренятся в недостатках работы администрации по организации процесса исполнения наказания и применения мер исправительного воздействия, поэтому устранение указанных недостатков – одна из наиболее действенных форм предупреждения и профилактики преступлений в местах отбывания наказания. Прежде чем перейти к установлению этих недостатков, необходимо уяснить, что подразумевается под мерами исправительного воздействия.

Любое наказание имеет определенные и конкретные цели. Не является исключением в этом отношении и наказание в виде лишения свободы, одной из основных целей которого является исправление осужденных. Исправление – это устранение человеком отклонений в своем развитии, возвращение его к норме, формирование положительных свойств личности.

В философском осмыслении средство есть все то, что ведет к достижению цели. Общепринято к средствам исправления и воспитания относить режим отбывания наказания, общественно-полезный труд, воспитательное воздействие, поддержание позитивных социальных связей, получение образования и меры общественного воздействия. Все перечисленные средства исправления осужденных тесно взаимосвязаны между собой и составляют определенную систему. Суть состоит в том, что эти средства должны реализоваться в совокупности. Исключение хотя бы одного из них разрушит систему. Каждое из этих средств занимает особое место в исправлении и воспитании осужденных. Средства исправительного воздействия рассчитаны на исправление осужденного и возвращение его в общество законопослушным гражданином.

Одним из основных средств исправления осужденных в уголовно-исполнительной политике Республики Казахстан - является общественно-полезный труд.

Неблагоприятная ситуация в экономике, обвальный спад производства создали бедственное положение в трудоустройстве осужденных. В настоящее время в нашей республике заняты полезным трудом лишь 27% осужденных, незанятость многих из них выступает как криминогенный фактор. Поэтому труд осужденных служит важным средством поддержания порядка, и дисциплины в пенитенциарных учреждениях. Безделье разлагающе действует на многих из них, способствует совершению различных правонарушений, а иногда и преступлений. Отметим тот факт, что если производство пенитенциарного учреждения будет нормально функционировать, то этим самым будут покрываться расходы на питание и иные потребности осужденных. Широкое использование труда способствует снятию

стрессовых ситуаций, отрицательных эмоций осужденных, он отвлекает их от лишних переживаний. Мы думаем, что в этом состоит физиотерапевтическое значение труда. Труд является мощным фактором, оказывающим влияние на формирование личности.

Если обратиться к истории, идея использования труда осужденных как средства исправления зарождалась как в отечественных, так и в зарубежных моделях тюремных систем отбывания наказания. Идея о привлечении заключенных к труду была востребована на том основании, что у преступников отсутствует привычка трудиться и имеется чувство праздности, стремление к достижению успеха в жизни нечестным (преступным) путем. Проводимые исследования труда как средства воздействия на профилактику преступлений в пенитенциарных учреждениях показали, что его реальное воздействие различно. Принудительный, обязательный труд в плане воспитания оказывает отрицательное влияние. Внешняя социальная сторона воспринимается личностью как бессмысленная, а внутренняя - как средство «убить время», изготовить запрещенный правилами предмет, реализовать преступный замысел и т.д. Труд как главное средство занятости и воспитания преступника использовался в первые десятилетия советской власти.

В настоящее время в состав уголовно-исполнительной системы входит около 50-60 промышленных и сельскохозяйственных предприятий, являющихся составной частью государственного сектора экономики Казахстана.

Принципиальным положением было следующее: если заключенный здоров, он должен работать, должен быть занят общественно необходимым производительным трудом. [1, с. 132-134.] Труд в условиях закрытых сообществ всегда представлял определенный интерес.

История развития пенитенциарной системы подтверждает непреходящее значение труда в ресоциализации личности преступника, который способствует профилактике преступлений среди осужденных. По мнению немецкого криминолога Г. Шнайдера: «Труд заключенных следует рассматривать не как наказание или средство исполнения уголовных наказаний, снижения расходов на их содержание, а исключительно как фактор ресоциализации [2, с. 405]. Отметим, что ряд ученых-пенитенциаристов видят в труде кару, а другие отрицают ее наличие. На труд как на дополнительную меру карательного воздействия указывал В.О. Ключевский. Он писал: « Труд – нравственный долг и основа нравственного порядка, но труд труду рознь. Известно, что труд подневольный, крепостной производит далеко не то воздействие на хозяйственный и нравственный быт народа, как труд вольный. Он убивает энергию, ослабляет предприимчивость, развращает нравы и даже портит расу физически» [3, С. 44]. По мнению А.И Зубкова, Л.Г. Крахмальник, А.Л. Ременсон, Н.А. Стручкова, И.В. Шмарова, Ю.М. Ткачевского, элемент кары в труде отсутствует, с чем соглашаемся и мы.

Представляется интересным зарубежный пенитенциарный опыт по использованию труда как средства исправления. К примеру, в Японии физический труд занимает основное место в исправлении осужденных к лишению свободы и частично восполняет затраты на создание тюрем, заключенным выдается денежное вознаграждение при освобождении. В Югославии существует 42-часовая рабочая неделя осужденных и оплачиваемый отпуск 14 дней. В Швеции трудовая деятельность является одной из составных частей программы по их реабилитации. В Великобритании тюремные учреждения должны предоставлять достаточное количество рабочих мест с целью обеспечения организованной и полезной работой всех работоспособных и других заключенных, желающих работать В Германии заключенные должны работать. В Финляндии законодательно предоставлено право выбора: труд или учеба в рабочее время[4, с.22].

Труд осужденных в нашей Республике переживает тяжелые времена. Предприятия исправительных учреждений вынуждены были свернуть существующие кооперативные связи, поскольку ведомствам невыгодно развивать их по ряду причин. Во-первых, техническое состояние предприятий пенитенциарных учреждений находилось на низком уровне по сравнению с аналогичными предприятиями, работающими в обычных условиях. Во-вторых, осужденный как работник, имеется в виду его статус, работает хуже свободного труженика,

производительность его труда и качество выпускаемой продукции ниже, и в перспективе этот разрыв все больше возрастает. Все это обострило проблему трудовой занятости осужденных. Трудовая занятость осужденных имеет тенденцию к дальнейшему увеличению количества неработающих, не занятых трудом в исправительных учреждениях, что приводит к следующему: невозмещение ущерба, нанесенного преступлением, невыплачивание алиментов, неоказание помощи семьям осужденных, совершение правонарушений и преступлений в учреждениях, исполняющих наказания. Возникла острая необходимость в разработке конкретных программ привлечения осужденных к труду и профессиональному обучению. Расширенное трудоиспользование осужденных приведет к следующему:

– широкое использование контрактной системы и индивидуальной деятельности осужденных будет способствовать ресоциализации осужденных и их позитивной адаптации после освобождения;

– дополнительная прибыль для питания и условий содержания осужденных;

– рациональное использование свободного от отдыха и сна времени.

Препятствием на пути полной занятости осужденных общественно полезным трудом по договорам с предприятиями являются изоляция и такие правовые ограничения, как охрана, надзор. Труд должен подготовить осужденного к жизни после выхода на свободу [2, с. 405).

Воспитывающая и профилактическая роль труда осужденных как средства их ресоциализации обусловлена следующими обстоятельствами:

а) социальным содержанием, поскольку труд осужденных должен быть связан с трудом других людей на свободе, что способствует их ресоциализации. Осужденные своим трудом вносят определенный материальный вклад на свое содержание, выплачивают иски, оказывают помощь семьям и родным. Трудом они искупают свою вину. Участие в труде связывает осужденных с происходящими в стране социальными и экономическими процессами. Все это позитивно перестраивает психологию осужденных и формирует социально значимые мотивы трудовой деятельности. В труде осужденный осознает себя как личность, как полезный член общества, поскольку труд является средством удовлетворения материальных и духовных потребностей осужденных, что влияет на их безопасность;

б) коллективным характером трудового процесса осужденный включается в систему отношений с ближайшим социальным окружением, требующим от него сотрудничества, взаимопомощи, инициативы и здорового соревнования. Это способствует сужению у осужденных эгоистических привычек и черт, формирует навыки поведения в групповой и трудовой деятельности, что необходимо при выходе из пенитенциарного учреждения;

в) развитием у осужденных волевых черт характера, нравственных потребностей и интересов. Формируется уважение к людям труда и результатам труда других людей, что способствует ресоциализации осужденных в местах лишения свободы;

г) производительный труд способствует физическому развитию осужденных и поддержанию их здоровья. Труд способствует переключению энергии осужденных на общественно полезные цели и профилактике нарушений режима отбывания наказания;

д) содержательный труд побуждает осужденных учиться, совершенствовать свое мастерство, рационально использовать свое свободное время, что обеспечивает их правомерное поведение.

В то же время один из недостатков, порождающих условия совершения преступления, связан с организацией трудоиспользования осужденных. Бывают случаи, когда осужденные не работают неделями, нередко отрицательная часть осужденных используется на трудноконтролируемых рабочих местах, что мешает пресекать азартные игры, распитие спиртных напитков, правонарушения, преступления.

Обстоятельством, способствующим совершению преступлений против личности осужденных, является засоренность производственных зон различными предметами-отходами производства, избытками сырья и т.д. Почти третья часть умышленного причинения

вреда здоровью была совершена с использованием штырей, труб, кирпичей, палок и других предметов, подобранных осужденными на производстве.

Материалы служебных заключений свидетельствуют о том, что мастерами, бригадирами иногда назначаются лица, не подходящие к занимаемой должности по своим моральным качествам. При составлении нарядов они злоупотребляют своим служебным положением, принуждают других осужденных выполнять работу за других лиц, допускают рукоприкладство и вымогательство, что в свою очередь порождает конфликтные ситуации, перерастающие в насильственные преступления.

Таким образом, труд осужденных способствует их исправлению и ресоциализации; чем выше трудовая занятость, тем менее опасна криминогенная обстановка в пенитенциарных учреждениях.

Литература

1. Детков М.Г. Содержание пенитенциарной политики Российского государства и ее реализация в системе исполнения уголовного наказания в виде лишения свободы в период 1917-1930 годов. – М., 1992. – С. 132-134.

2. Шнайдер Г. Криминология /Пер. с нем; Под общ. ред. Л.О. Иванова. – М.: Издат. Группа «Прогресс» – «Универс», 1994, – С. 405.

3. Ключевский В.О. Сочинения: В 9 т. Т. 1. Курс русской истории. Ч 1. / Под ред. В.Л. Янина, В.А. Александрова; послесл. и коммент., сост. В.А. Александров, В.Г. Зимина. – М.: Мысль, 1987, – С. 44.

4. И. А. Пушкарева, Л. Н. Одинцова: « Особенности содержания различных категорий осужденных к лишению свободы в зарубежных», – С.22.

АБИЖАНОВ СЫРЫМ МАРАТОВИЧ
Доцент кафедры уголовного права и криминологии, доктор PhD, подполковник полиции

ПРАКТИЧЕСКИЕ МЕТОДЫ ПРЕДУПРЕЖДЕНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Информационная безопасность страны – это «состояние защищенности страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз» [1, с. 359].

Проникновение в жизнедеятельность человека современных информационных технологий – это следствие процесса информатизации всего общества, который предполагает трансформацию индустриального общества в информационное. Информационное общество – это социум с высокоразвитой системой каналов информационного обмена и телекоммуникаций, а также средств и систем защиты, циркулирующей по ним информации [2, с. 20].

Эффективность противодействия киберпреступлениям зависит от таких факторов, как уровень развития правовой среды, технические предпосылки, организационные меры, развитие компетенций и кооперация внутри и вне страны [3, с. 127]. Информационные системы и необходимая информационная инфраструктура позволяют отнести к информационному пространству и киберпространству как продукт функционирования любых информационно-коммуникационных технологий (в том числе сети Интернет) [4, с. 143]

Меры обеспечения кибербезопасности реализуются с целью защиты активов, которые определяются как «нечто важное или ценное, включая пользователей, имущество, информацию, системы и оборудование» [5] таких как, работники организации, цифровые устройства, компьютерное программное обеспечение и данные. Активы восприимчивы, т.е. уязвимы к различным видам ущерба. В частности, активы имеют внутренние (или встроенные) и внешние (или привнесенные) уязвимости. Например, применительно к информационно-коммуникационным технологиям (далее – ИКТ), внутренние уязвимости могут присутствовать в конструкции системы, конфигурациях системы безопасности, аппаратном и программном обеспечении и в других компонентах. Примером может служить программная ошибка. В 2018 году была обнаружена программная ошибка в кошельке криптовалюты Monero, которая позволяла отдельным лицам использовать эту уязвимость для незаконного удвоения сумм перевода криптовалюты. Напротив, внешние уязвимости не присутствуют внутри самих активов, таких как устройства ИКТ. Примером такой уязвимости является пользователь ИКТ. Пользователь может выполнять действия, которые делают устройство восприимчивым к заражению вредоносными программами (например, открывать вложения в электронных письмах от неизвестных отправителей). Встроенные и привнесенные свойства делают активы уязвимыми для угроз, т.е. ко всему, что может вызвать неблагоприятные последствия. Эти угрозы могут причинить непреднамеренный и преднамеренный ущерб. Например, аппаратное обеспечение цифрового устройства может работать со сбоями или

может быть преднамеренно повреждено в результате эксплуатации уязвимостей встроенного программного обеспечения. [6, с. 58].

Материалы и методы

Методологическую основу научной статьи составляют общие научные и индивидуально-научные методы: анализ, синтез, описание, обобщение, нормативно-правовые, формально-правовые, сравнительно-правовые методы, использование данных правовой статистики.

Основная часть

В идеале меры реагирования на риски должны преследовать цель защиты конфиденциальности, целостности и доступности систем, сетей, услуг и данных при одновременном обеспечение удобства использования этих мер. [7, с. 55] Удобство использования цифровых устройств зачастую имеет преимущество перед безопасностью этих устройств и их содержимого. Однако, безопасность и удобство использования не обязательно являются взаимоисключающими. Меры кибербезопасности могут обеспечивать, как безопасность, так и удобство использования.

В.П. Талимончик считает, что наиболее полно интересы государств в борьбе с компьютерными преступлениями могут быть обеспечены вследствие создания системы международного контроля за передачей информации в компьютерных сетях и расследования правонарушений, связанных с использованием глобальных компьютерных сетей и отдельных компьютеров, имеющих трансграничные последствия [8, с. 23].

К мерам кибербезопасности относятся меры, направленные на установление личности пользователя, чтобы предотвратить несанкционированный доступ к системам, услугам и данным. Эти меры аутентификации включают в себя проверку того, «что вы знаете» (например, пароли, парольные фразы и PIN-коды), «что вы имеете» (например, смарт-карты и токены) и «кем вы являетесь» (например, биометрические данные, такие как отпечатки пальцев). Многофакторная аутентификация предполагает использование двух или более таких методов аутентификации для установления личности пользователя.

Еще одним типом мер кибербезопасности является контроль доступа. Средства контроля доступа, которые устанавливают привилегии, определяют санкционированный доступ и предотвращают несанкционированный доступ, включают в себя меры аутентификации и другие меры, предназначенные для защиты имен и паролей для входа в систему, приложения, веб-сайты, социальные сети и другие онлайн-платформы и цифровые устройства [9, с. 285]. В качестве примера можно привести ограничение количества попыток ввода пароля на смартфоне. На смартфонах есть опция, которая позволяет пользователям стирать все данные на устройстве после определенного количества неудачных попыток ввода пароля. Эта функция была создана с тем, чтобы обеспечить пользователям возможность защиты данных на своих устройствах в случае кражи цифрового устройства и/или получения к ним доступа без авторизации пользователя.

Другие примеры средств контроля доступа включают в себя добавление времени ожидания при каждом неверном вводе пароля и/или ограничение количества неудачных попыток ввода пароля, которые могут быть допустимыми в течение дня, и блокирование учетных записей пользователей на некоторое время. Эти средства управления, контролирующие попытки входа в систему, предназначены для защиты от попыток получить несанкционированный доступ к учетным записям пользователей. В частности, такие временные задержки служат для защиты от атак методом «грубой силы»

Атака «грубой силой» – это использование скрипта (компьютерной программы) или робота (рассматривается в модуле 2 Серии модулей по киберпреступности: «Основные виды киберпреступности») для угадывания (методом проб и ошибок) учетных данных пользователя (имени пользователя и/или пароля/кода доступа) для получения дополнительной информации об атаках методом «грубой силы». При атаках «грубой силой» используются, среди прочего, общие пароли или взломанные учетные данные для входа в систему. В 2018 году было

обнаружено, что функцию мастер-пароля, которая позволяла пользователям шифровать пароли, хранящиеся в веб-браузере Mozilla Firefox, можно легко взломать с использованием атаки методом «грубой силы».

Пароли либо генерируются системой, либо создаются пользователем. Пароли, генерируемые системой, т.е. созданные программой, являются трудно угадываемыми и могут выдержать атаки парольных взломщиков (хотя это зависит от длины паролей). Проблема, связанная с паролями, генерируемыми системой, заключается в сложности их запоминания. Это приводит к тому, что пользователи записывают пароль, например, на бумагу или сохраняют его в браузере, приложении или цифровом устройстве. Поэтому пароли, создаваемые пользователем, являются более предпочтительными. Однако, могут быть трудными для запоминания. Системы, приложения и онлайн-платформы зачастую устанавливают сложные правила создания паролей, которым должны следовать пользователи, требуя, чтобы пароли соответствовали минимальной установленной длине и включали комбинации букв верхнего и нижнего регистра, цифр и символов. Таким образом, как и пароли, генерируемые системой, большинство паролей, создаваемых пользователями, являются трудно запоминаемыми.

Пользователям также рекомендуется иметь разные пароли для каждой учетной записи. Цель этой рекомендации заключается в минимизации ущерба, причиняемого пользователям, в случае взлома данных для доступа к одной из их учетных записей. В 2017 году одна исследовательская компания обнаружила в Интернете файл с 1,4 миллиардами имен пользователей и паролей для различных социальных сетей, игр, сайтов трансляции телепередач и фильмов и других сайтов сети Интернет. Если кто-либо из этих лиц повторно использует пароли, такая брешь в системе защиты ставит под угрозу безопасность других учетных записей в Интернете, где используются те же имя пользователя и пароль. Хотя использование разных и сложных паролей для каждой учетной записи может обеспечить определенный уровень безопасности для отдельных пользователей, это в конечном итоге отрицательно влияет на удобство их использования, т.е. на их запоминаемость. Как справедливо отмечают «большое количество ограничений в механизмах аутентификации создают большое количество проблем, связанных с удобством использования»

Вместо паролей предлагается использовать различные схемы аутентификации. Использование альтернативных схем аутентификации, таких как техника биометрической идентификации, сопряжено с неблагоприятными последствиями социального и правового характера и даже последствиями для безопасности [10]. В качестве примеров можно привести смартфоны Apple iPhone со сканерами TouchID, который позволяет пользователям разблокировать свои устройства с помощью отпечатка пальца, и FaceID, позволяющий пользователям разблокировать телефоны путем сканирования своего лица. В Соединенных Штатах сотрудники системы уголовного правосудия не имеют права принуждать пользователей предоставлять свои пароли; такая защита не распространяется на отпечатки пальцев и другие биометрические данные, когда суды постановили, что лица могут быть принуждены к использованию своих отпечатков пальцев для разблокировки.

Пользователи считаются самым слабым звеном в цепи кибербезопасности. Более того, некоторые исследования показали, что инциденты в области кибербезопасности, такие как утечка данных и/или атака на сети, системы, услуги и данные являются результатом человеческой ошибки и неспособности применить меры безопасности. В то время как большое внимание уделяется роли пользователей в инцидентах в области кибербезопасности, меры кибербезопасности, действовавшие в момент наступления инцидента, могут также играть некоторую роль в этом инциденте. Реальность такова, что меры кибербезопасности и ожидания пользователей относительно эффективности этих мер безопасности часто не совпадают.

В публикациях и исследованиях, посвященных взаимодействию человека и компьютера, предлагается, чтобы меры обеспечения безопасности цифровых устройств, систем, программ,

приложений и онлайн-платформ разрабатывались с учетом фактора пользователей, на основе концепции проектируемой безопасности. Такая практика не является общепринятой. Обычной практикой является разработка систем и последующая модификация взаимодействия пользователей с системой для удовлетворения потребностей в обеспечении безопасности.

Ситуационное предупреждение преступности сосредоточено на способах предотвращения преступлений и сокращения возможностей для их совершения. Ситуационное предупреждение преступности считается важной частью Руководства Экономического и Социального Совета ООН по предупреждению преступности (далее – СПП).

Меры СПП могут применяться, применялись ранее и применяются в настоящее время для предупреждения и сокращения киберпреступности. Например, один из методов, стратегии СПП, – увеличение рисков обнаружения и задержания – заключается в «использовании управляющих на местах». Применительно к киберпреступности, управляющими на местах, которые контролируют поведение в обозначенном месте, могут быть поставщики Интернет-услуг или администраторы и модераторы онлайн-платформ. Управляющие на местах используются для борьбы с киберпреступностью в социальных сетях. Например, Facebook увеличил количество модераторов и усилил мониторинг контента, пропагандирующего насилие и жестокость, после того, как Стивен Стивенс (Steven Stephens) убил человека и транслировал это убийство через FacebookLive. Некоторые из этих методов СПП, применяемые для борьбы с киберпреступностью, могут нарушать права человека (например, при блокировании или удалении контента) (для получения дополнительной информации об ограничениях прав человека и некоторых обстоятельствах, в которых пропорциональные ограничения определенных прав могут быть оправданы в соответствии с международным правом в области прав человека.

Хотя концепция СПП применяется к предупреждению преступности в реальном мире, она также может использоваться в качестве меры предотвращения киберпреступности в контексте практики обеспечения кибербезопасности. Применительно к киберпреступности меры СПП направлены на сокращение и/или предотвращение возможностей для совершения правонарушений и подрыв способностей киберпреступников совершать преступления. Технические меры предупреждения киберпреступности представляют собой одну из форм ситуационного предупреждения преступности. Примеры таких технических мер включают в себя программы обнаружения вредоносных программ, брандмауэры, которые предотвращают несанкционированный доступ путем проверки и блокирования трафика, и системы обнаружения вторжений, которые позволяют обнаруживать кибератаки, несанкционированный доступ и несанкционированное использование систем, сетей, данных, услуг и соответствующих ресурсов [11, с. 444].

Меры СПП сосредоточены на возможности материализации угроз кибербезопасности в определенный момент времени. Таким образом, эти меры применяются на основании предположения о том, что угрозы будут материализованы, и поэтому необходимо предпринять соответствующие действия. В то время как меры СПП преимущественно (но не исключительно) направлены на препятствование совершению преступлений, реальность такова, что даже после принятия этих мер преступление, вероятней всего, будет совершено. В связи с существованием такой вероятности реализуются меры, направленные на обнаружение инцидентов в области кибербезопасности, реагирование на них и восстановление после них.

Обнаружение инцидентов представляет собой процесс определения угроз путем активного мониторинга активов и выявления аномальной активности. Сразу после обнаружения угрозы предпринимаются соответствующие действия для нейтрализации угрозы (если эта угроза является активной на момент принятия мер реагирования) и расследования инцидента. После принятия мер реагирования на инцидент первым шагом в процессе восстановления является восстановление доступа и доступности систем, сетей, услуг и данных до состояния, существовавшего до инцидента.

Процесс восстановления также включает в себя элемент планирования, который требует определения, разработки и окончательной реализации мер по усилению устойчивости и обеспечению возможности восстановления систем, сетей, услуг и данных, которые были недоступны, нарушены, повреждены и/или скомпрометированы во время инцидента. Важным элементом обеспечения устойчивости является наличие современного плана непрерывности бизнеса или плана действий по урегулированию чрезвычайных ситуаций с изложением инструкций, которые необходимо соблюдать, и действий, которые необходимо предпринять в случае возникновения инцидента в области кибербезопасности. Проще говоря, этот план включает в себя подробную информацию о способах реагирования на инцидент и восстановления после него. Все лица, участвующие в принятии мер реагирования на инциденты в области кибербезопасности и восстановления после них, должны быть проинформированы о плане действий по урегулированию чрезвычайных ситуаций. При этом необходимо организовать тренинги, включая учения, предназначенные для проверки эффективности и действенности этих планов. Примером учений такого рода являются учения «Кибер-шторм» (Cyber Storm exercises) Министерства внутренней безопасности США с участием представителей национальных публичных и частных организаций, а также организаций из других стран (например, Австралии, Канады, Дании, Финляндии, Франции, Германии, Венгрии, Италии, Японии, Новой Зеландии, Нидерландов, Швеции, Швейцарии и Великобритании), проводимые с целью проверки текущей практики обмена информацией между этими организациями, а также их возможностей обеспечения готовности, защиты и реагирования на инциденты в области кибербезопасности.

Помимо организационных мер, существенную профилактическую роль играют меры технического характера. Технические меры предназначены для защиты от нежелательного воздействия на информационные системы и сети телекоммуникации, «закрытия возможных каналов утечки конфиденциальной информации за счет применения лазерных, радиотехнических и других способов перехвата, а также средств визуального наблюдения и средств связи, других технических приспособлений».

Применение этих методов осуществляется путем использования различных технических разработок, устройств, специального оборудования, программного и аппаратно-программного обеспечения.

Условно технические меры, в зависимости от характера и специфики защищаемого объекта, можно разделить на две основные группы: аппаратные и программные. Аппаратные методы применяются для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для блокирования возможных каналов утечки конфиденциальной информации и имеющихся данных. [12, с. 59]

Правительства, неправительственные организации, образовательные учреждения, предприятия и частные лица широко используют информационно-коммуникационные технологии (ИКТ). Взаимозависимость устройств и систем во всем мире и важность ИКТ для экономической и национальной безопасности стран, а также для национального и мирового развития требуют принятия коллективных и согласованных ответных мер всеми странами мира. Национальные стратегии кибербезопасности принимаются с целью описания способов осуществления защиты, а также мер, которые необходимо предпринять, и организаций, ответственных за надзор за реализацией этих мер. Существуют показатели, которые можно использовать для оценки эффективности этих стратегий. Более того, имеются инструменты и ресурсы, которые позволяют странам оценивать свои силы и средства обеспечения кибербезопасности и помогают им улучшить свое состояние дел в области кибербезопасности.

Меры обеспечения кибербезопасности предназначены для защиты пользователей, имущества, систем, сетей, данных и связанных с ними ресурсов от угроз. Они включают в себя меры по предупреждению и выявлению инцидентов в области кибербезопасности, реагированию на них и восстановлению после них. Прежде чем приступить к разработке и реализации мер кибербезопасности необходимо определить активы и оценить угрозы,

уязвимости и риски. Исследования в области безопасности могут позволить получить ценную информацию для разработки новых и совершенствовании существующих мер кибербезопасности. Зачастую меры кибербезопасности не учитывают фактор пользователей, которые их используют. Пользователи могут либо способствовать усилиям по обеспечению кибербезопасности, либо мешать осуществлению таких усилий. Поэтому эффективные меры и системы кибербезопасности должны разрабатываться с учетом лиц, которые будут их использовать.

Литература

1. Бачило, И.Л. Информационное право: учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под ред. Б.Н. Топорнина. – СПб., 2001. – С. 477.
2. Сеитов, Т.Е. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: учебное пособие / Т.Е. Сеитов. – Алматы: Данекер, 2004. – С. 328.
3. Имангалиев, Н.К. Актуальные проблемы выявления и раскрытия уголовных правонарушений, совершаемых в сети Интернет / Н.К. Имангалиев., Л.А. Темиржанова // Вестник ЕНУ имени Л.Н. Гумилева. Серия Право. – 2022. – №1(138). – С. 124-132.
4. Исатаева Б.Т. Ақпараттық киберкеңістікте жасалатын меншікке қарсы қылмыстық құқық бұзушылықтар/ Б.Т. Исатаева., // Ученые труды Алматинской академии МВД Республики Казахстан имени Макана Есбулатова. – 2022. - №3(72). – С. 145-147.
5. Maras, M.-H. Transnational Security [Electronic resource] / M.-H. Maras. – CRC Press. – 2014. – №1. – pp. 185-193. Access mode: https://www.taylorfrancis.com/books/mono/10.1201/b17551/transnational-security-marie-helen-maras (Access data: 10.11.2022).
6. ENISA / Hardware Threat Landscape and Good Practice Guide. – Version1. – 2017. №1. – 58 p.
7. NIST / Framework for Improving Critical Infrastructure Cybersecurity // National Institute of Standards and Technology. – 2018. – №1.1. – 55 p.
8. Талимончик, В.П. Компьютерные преступления и новые проблемы сотрудничества государств / В.П. Талимончик // Законодательство и экономика. – 2005. – №5. – С. 17-25.
9. Lehtinen, R. Computer Security Basic. / R. Lehtinen, D. Russell, Sr. G.T. Gangemi. – O'Reilly Media. – 2006. – №2. – pp. 283-292.
10. Greenberg, A. Hackers Say they've broken FaceID a week after iPhone X release [Electronic resource] / A. Greenberg. – 2017. – №1. – 44-51. – Access mode: https://www.wired.com/story/hackers-say-broke-face-id-security/ (Access data: 08.11.2022).
11. Maras, M.-H. Computer Forensics: Cybercriminals, Laws, and Evidence / M.-H. Maras // Jones and Bartlett. – 2014. – №1. – pp. 438-447.
12. Рустемова Г.Р. Профилактика уголовных правонарушений в сфере информатизации и связи в Республике Казахстан/ Г.Р. Рустемова // Вестник Могилевского Института МВД. – 2020. - №1. – С. 58-63

ВОЛКОВ БОРИС ВИТАЛЬЕВИЧ
преподаватель кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, подполковник, магистр педагогики

СЕЙІТЖАН ҚАНАТ КӨШЕРБАЙҰЛЫ
старший инженер отдела автоматизации штаба Академии Национальной гвардии Республики Казахстан, старший лейтенант

ЦИФРОВЫЕ ПРЕОБРАЗОВАНИЯ В ОБЛАСТИ ПРОТИВОСТОЯНИЯ КИБЕРУГРОЗАМ И КИБЕРПРЕСТУПНОСТИ

Информационные технологии (ИТ) имеют огромное влияние на современное общество и предоставляют множество возможностей как для благоприятных, так и для негативных целей. Использование ИТ в качестве способа совершения преступлений называется киберпреступностью.

ИТ могут использоваться в качестве средства совершенствования различных видов преступлений. Это связано с тем, что с разработкой технологий созданы новые возможности для злоумышленников. Вот некоторые способы, как информационные технологии могут использоваться для совершения преступлений:

1. Кибермошенничество: Злоумышленники могут использовать технологии для мошенничества в сети. Это может включать в себя создание фальшивых веб-сайтов, фишинговые атаки, мошенничество с кредитными картами и другие виды онлайн-преступлений.

2. Кибершпионаж: государственные и нет следствия, актеры могут использовать технологии для шпионажа и сбора конфиденциальной информации. Это может включать в себя хакерские атаки на компьютерные системы, а также сбор данных через социальные сети и другие онлайн-платформы.

3. Кибератаки на инфраструктуру: Злоумышленники могут атаковать критическую инфраструктуру, такую как энергетические системы, транспортные сети и здравоохранение, с угрозой смертельного ущерба и создать хаос. Эти действия могут привести к серьезным последствиям для общества.

4. Распространение конкурентного программного обеспечения (ПО): вирусы, троянские кони и другие виды конкурентного программного обеспечения могут использоваться для воровства данных, вымогательства денег и нарушения конфиденциальности пользователей.

5. Кибербуллинг и онлайн-нападения: Интернет предоставляет площадку для кибербуллинга, онлайн-гонений и других форм домогательств. Это может нанести серьезный вред психическому и эмоциональному здоровью.

6. Незаконный доступ к информации: Злоумышленники могут обвиняемым получить несанкционированный доступ к конфиденциальной информации, такой как личные данные, финансовые сведения или коммерческие секреты.

Использование ИТ для совершения преступлений, также известных как киберпреступность, стало серьезной проблемой не только в нашем государстве, но в всём мире. Так называемые «Киберпреступники» могут использовать различные технические средства и навыки для достижения своих незаконных целей.

Для борьбы с киберпреступностью правительства, организации и физические лица применяют технические и юридические меры безопасности, чтобы защитить себя и свои данные от опасной угрозы со стороны киберпреступников. Однако киберпреступники постоянно разрабатывают новые методы и тактики, а борьба с киберпреступностью остается сложной и актуальной проблемой в современном мире.

Киберпреступность представляет собой серьезную директиву и требует поддержки со стороны правоохранительных органов, организаций и общества в целом для борьбы с ней и защиты от нее. Создание национальной кибербезопасности и соблюдения правил и законов в Интернет пространстве имеет решающее значение для предотвращения и борьбы с киберпреступностью.

Состояние преступности, связанной с использованием ИТ, постоянно меняется в зависимости от развития технологий, общественных трендов и законодательных мер.

Противодействие преступности, связанной с использованием ИТ, является важным фактором в современном мире, где цифровая среда играет ключевую роль в повседневной жизни. Преступники могут использовать ИТ для совершения различных преступлений, включая кибермошенничество, кибершпионаж, киберзапугивание, распространение конкурентных программ и многие другие виды атак. Вот несколько способов для предотвращения преступности с использованием цифровых технологии:

1. Законодательство и регулирование: Разработка и ужесточение законодательных и нормативных актов, будущей киберпреступности. Это включает в себя определение преступлений и наказаний за них.

2. Специализированные дополнительные органы: создание специализированных подразделений и отделов в дополнительных органах для борьбы с киберпреступностью.

3. Международное сотрудничество: Сотрудничество между государствами и международными организациями для обмена информацией и коалиционными действиями в регионах с трансграничной киберпреступностью.

4. Киберполитика: Разработка национальных стратегий по кибербезопасности и мерам по защите критической информационной индустрии.

5. Судебные процессы и последствия: обеспечение проведения судебных процессов и наблюдение за преступниками, совершившими киберпреступления.

6. Исследования и разработка новых технологий: Исследование и разработка новых методов и технологий для выявления и предотвращения кибератак.

7. Сотрудничество с частным сектором: Совместное участие мировых компаний и организаций в усилении кибербезопасности и обмене информацией о возможных угрозах.

8. Системы видеонаблюдения: видеонаблюдение с использованием камер и датчиков могут помочь в следящем режиме наблюдения за общественными местами, транспортными системами и другими местами. Анализ видеоматериалов с использованием искусственного интеллекта (ИИ) Позволяет автоматически выявлять подозрительное поведение и реагировать на него.

9. Анализ данных и прогнозирование: Системы анализа данных и машинного обучения позволяют включать анализ криминальной статистики, моделей преступности и закономерностей. Это позволяет прогнозировать место и время, что помогает в усилении патрулирования и реагировании на угрозу.

10. Системы управления чрезвычайными ситуациями и связью: цифровые системы для управления чрезвычайными ситуациями и связи позволяют легче координировать действия служб безопасности и коммунальных услуг в случае возникновения ситуаций или явлений в городах и регионах.

11. Мобильные приложения и онлайн-платформы: Разработка мобильных приложений и онлайн-платформ, предоставляющих информацию о безопасности и способах передачи сообщений об авариях, может помочь гражданам быстрее и проще подключаться с внешними гарантиями.

12. Интернет-вещи (IT): Умные устройства, подключенные к Интернету, могут использоваться для защиты Диптихов в разных местах и рабочих местах. Например, датчики движения и камеры могут отправлять уведомления в случае вторжения.

13. Социальные сети и медиа-мониторинг: Мониторинг социальных сетей и онлайн-СМИ может помочь выявить угрозы и предупредить опасные происшествия.

14. Анализ текста и распознавание речи: Технологии анализа текста и речи могут использоваться для автоматических систем связи «Диптих», чтобы выявить подозрительные обращения или угрозы.

15. Биометрическая идентификация: Технологии биометрической идентификации, такие как сканеры отпечатков пальцев и распознавание лиц, используемые для расследования подозрительных личностей и повышения безопасности в ограниченных зонах.

16. Геопространственные данные: Геопространственные системы (ГИС) и GPS-технологии, используемые для анализа и прогнозирования преступности на основе местоположения. Это позволяет лучше использовать ресурсы полиции и создавать более эффективные стандарты.

17. Образование и осведомленность: цифровые средства, такие как веб-сайты и мобильные приложения, могут использоваться для образования общества в области безопасности и методов борьбы с преступностью.

Однако при внедрении цифровых технологий на местах с учетом преступности важно учитывать вопросы конфиденциальности, этичности и защиты данных как физических лиц, так и юридических, чтобы избежать злоупотреблений прав граждан. Также необходимо обеспечить доступность и обучение граждан использованию этих технологий для обеспечения безопасности.

Цифровые технологии помогают принятым законодательным актам и властям различных степеней уровня более эффективно управлять и реагировать на преступность, улучшать общественную безопасность и снижать уровень преступности в городах и регионах республиканского масштаба.

Противодействие киберпреступности требует комплексного заседания, включая нормативно-правовые, технические и образовательные меры, а также сотрудничество не только внутри государства, но всех иностранных сторон международного отношения для создания единой платформы противостояния.

Мера противодействия высокотехнологичным вирусам включает в себя ряд действий и стратегий, направленных на предотвращение и борьбу с такими вирусами.

Кибербезопасность – это непрерывный процесс, требующий постоянных обновлений и адаптации к новым угрозам и технологиям. Для защиты от кибератак существуют различные IT-технологии, включая межсетевые брандмауэры, антивирусное ПО, системы обнаружения вторжений, мониторинг безопасности, аутентификацию с множеством факторов и обучающие средства вычислительной техники. Также особое внимание обучению сотрудников и грамотности в области кибербезопасности, чтобы снизить риски кибератак.

Обучение сотрудников и повышение их грамотности в области кибербезопасности является важнейшим фактором защиты информации и честных интересов от киберугроз. Вот несколько шагов, которые помогут привлечь особое внимание к обучению сотрудников в этой области:

1. Разработка политики безопасности: начать с разработки четкой и понятной политики безопасности в организации. В этой политике должны соблюдаться стандарты и правила обращения с конфиденциальной информацией, паролями, устройствами и сетями.

2. Создание обучающих материалов: Разработайте обучающие материалы, которые будут доступны всем сотрудникам. Это могут быть онлайн-курсы, видеоуроки, информационные брошюры и т. д. д.

3. Организация тренингов и семинаров: Регулярно проводит тренинги и семинары по кибербезопасности для сотрудников. Обучение должно быть интерактивным и практическим, чтобы сотрудники могли применять полученные знания на практике.

4. Тестирование знаний: Проведите тестирование среди руководителей, чтобы оценить их уровень грамотности в области кибербезопасности. Это позволит выделить слабые места и сосредоточить усилия на их устранении.

5. Обновление учебных материалов: Киберугрозы постоянно изменяются, поэтому учебные материалы и программы необходимо регулярно обновлять. Внимательное наблюдение за последними тенденциями и уязвимостями.

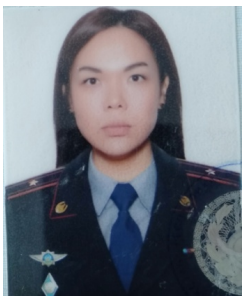
6. Поддержка и мотивация: Поощряйте сотрудников активно участвовать в обучении по кибербезопасности. Это можно сделать через систему наград и признания за активное соблюдение политики безопасности.

7. Создание сознательной культуры безопасности: Старайтесь создать организацию культуры безопасности, в которой каждый сотрудник осознает свою ответственность за защиту информации.

8. Сотрудничество с экспертами: если это возможно, установите партнерские отношения с кибербезопасными организациями.

Литература

1. https://infobezopasnost.ru/blog/
2. https://ru.wikipedia.org
3. https://www.kaspersky.ru/
4. Исследования Остерман. 2018. «Лучшие практики защиты от фишинга, программвымогателей и мошенничества с электронной почтой». https://www.knowbe4.com/hubfs/Best_Practices_for_Protecting_Against_Phishin Ransomwar e_and_Email_Fraud.pdf
5. Livingsecurity. «Погружающий обучающий контент по кибербезопасности для вовлечения сотрудников ... и продолжения их обучения». По состоянию на 11 декабря 2020 г. https://www.livingsecurity.com/products/cybersecurity-training-content.
6. Бойенс Джон М., Селия Полсен, Рама Мурти и Надя Бартол. 2015. «Практика управления рисками для федеральных информационных систем и организаций». NIST SP 800-161. Национальный институт стандартов и технологий. https://doi.org/10.6028/NIST.SP.800-161.
7. Хаас Джереми и Райан Бергквист. «Пять вопросов о сторонних поставщиках и кибербезопасности». SupplyChainBrain. 19 ноября 2019 г. https://www.supplychainbrain.com/blogs/ 1-think-tank/post/30489-the-company-you-keep-fivequestions-to-ask-about-third-party-vendors-and-cybersecurity.
8. Уистик. «Запрос предложений: введение стандартов информационной безопасности и кибербезопасности в запросы предложений». Медиум. 16 января 2019 г. https://blog.whistic.com/rfps-introducing-information-security-cybersecurity-standards-in-rfpsabeddb80ced9
9. Структурные элементы кибербезопасности в энергетическом секторе (Морис Мартин, Тами Рейнольдс, Анудж Сангви, Сэди Кокс и Джеймс Элсворт), Национальная лаборатория по исследованиям в области возобновляемых источников энергии, Март 2021 г.



ҒАЛЫМ АЖАР МАРАТҚЫЗЫ
Старший преподаватель кафедры УПиК Костанайской академии МВД Республики Казахстан им. Ш. Кабылбаева подполковник полиции

ON THE STATE OF DIGITALIZATION OF THE PENAL SYSTEM OF THE REPUBLIC KAZAKHSTAN

President of Kazakhstan Kassym-Jomart Tokayev in his annual address to the people stressed that the republic should become an IT country. Following the rinciple of humanization in Kazakhstan is becoming more and more important every year [1].

The Law of the Republic of Kazakhstan "On Amendments and Additions to

Certain Legislative Acts of the Republic of Kazakhstan on issues of the penal enforcement system" dated January 18, 2012 No. 547,amended and supplemented the Law of the Republic of Kazakhstan "On Internal Affairs Bodies of the Republic of Kazakhstan" dated December 21, 1995.

According to which, the tasks of the internal affairs bodies, in particular, the execution of criminal punishments, ensuring legality, law and order and maintaining the regime of detention of convicts in the bodies and institutions of the penal enforcement system, ensuring the rights and legitimate interests of suspects, accused and convicted persons, as well as citizens in the penal enforcement system of the Republic of Kazakhstan, the organization of correction of convicts are indicated.

Further, it should be pointed out that several laws were adopted in 2011, softened the repressiveness of criminal legislation and influenced the further decline of the "prison population". The greatest role in this was played by the laws "On Amendments and Additions to some legislative acts of the Republic of Kazakhstan on further humanization of criminal legislation and strengthening guarantees of legality in criminal proceedings" dated January 18, 2011, "On Amendments and Additions to Some Legislative acts of the Republic of Kazakhstan on improving law enforcement and further humanization of criminal legislation" dated November 9, 2011 and "On amnesty in connection with the twentieth anniversary of the state independence of the Republic of Kazakhstan" dated December 28, 2011 [2].

During the last decade there have been fundamental changes in the nature and content of the activities of the PES of the Republic of Kazakhstan.

Socio-economic transformations in society stimulated the solution of problems that had been brewing for a long time. Measures were taken to humanize the regime of serving sentences, improve the organizational and staff structure of bodies and institutions of the penal enforcement system, which were accompanied by a deep and

comprehensive revision of the regulatory framework for the activities of bodies and

institutions executing criminal penalties.

In order to implement the instruction of the Head of State dated January 6, 2012 (No. 51-14.20), a new Penal Enforcement Code was adopted in 2014 Of the Republic of Kazakhstan, which entered into force on January 1, 2015 [3].

The new edition of the Penal Enforcement Code marks the completion of the next stage of the implementation of the directions of development of criminal policy

defined by the Concept of Legal Policy of the Republic of Kazakhstan for the period from 2010 to 2020, approved by the Decree of the President of the Republic Kazakhstan dated August 24, 2009 No. 858.

In 2018, a joint order of the Ministry of Internal Affairs, PGO, JM, FM approved Roadmap for the development of the PES for 2019-2023 [4].

On May 29, 2019, on the instructions of the Head of State, instructed at the expanded meeting of the Board of the Ministry of Internal Affairs of the Republic of Kazakhstan dated April 17, 2019, the forum "Open Dialogue - a tool for reforming the penitentiary system" was held. At the forum, along with representatives of state bodies and deputies, representatives of the public took part in the work of the forum, scientific community, lawyers, etc., who are interested in the issues of reforming the criminal justice system, as well as diplomatic missions and organizations.

As a result of the forum, an Interdepartmental Working Group was created a group for a comprehensive analysis of existing problems and their solutions.

For openness and transparency in this work on the departmental website organized the heading "Public discussion on the improvement of the penal system". The section publishes proposals and overview information about the measures taken to amend the legislation. On the basis of proposals requiring by-law regulation, relevant draft orders of the Ministry of Internal Affairs, of which many are already being implemented.

There is a project of the electronic store service for purchases of goods by convicts. Distance learning of convicts in higher educational institutions is being introduced.

Along with this, other areas of development of the activities of the PES are being introduced. For example, digitalization, one of the directions of which is equipping institutions with video surveillance cameras and employees of the PES with video recorders. Further, it is the development of production, the employment

of convicts and their re-socialization in society, as well as the improvement of medical care.

In recent years, the Committee of the Penal Enforcement System has been actively working to modernize the domestic system of execution of sentences, including through the introduction of digital innovations.

For the first time, electronic stores for the purchase of permitted goods, terminals for filing complaints and appeals, as well as electronic tracking devices for convicted probation service began to function in Kazakhstan's colonies.

Convicted persons who systematically violate the conditions of serving their sentences and have several warnings, as well as those convicted of crimes against the sexual integrity of minors, will be subject to electronic supervision. These persons are restricted in a number of rights, firstly, a person under probation control does not have the right to change his permanent place of residence without written notification of the probation service, he also does not have the right to freedom of movement. Secondly, a number of prohibitions are also established: to visit certain places, to stay at the wrong time of day in specific places. To track convicts, a system of electronic monitoring tools is used – the so-called electronic bracelets that transmit a radio signal. These transmitters work via GSM/GPRS channel and allow you to track the movement of a person in real time due to the global positioning system.

The system provides an opportunity for a probation officer to establish full electronic control during his sentence and promptly respond to the facts of violation of the conditions of serving his sentence. They allow you to prevent possible risks of committing a repeat crime.

In addition, tablets with the installation of a special program (on average 95% of the total number of convicts) will be used to monitor positively characterized convicts.

The use of an electronic tracking device is formalized by the decision of the head of the probation service in accordance with the restrictions imposed on the convicted person by the court and the Law.

By the way, if the student violates the regime, a signal is immediately received about it. The probation service inspector immediately contacts the convict. If several such violations are recorded, electronic supervision may be replaced by imprisonment.

In general, we rented 2.5 thousand bracelets for all regions of the republic.Vandal-proof anklet with hypoallergenic strap that does not cause skin irritation. Relative humidity – 100%. You can take water treatments with it.

The next main stage of digitalization is the creation and provision of conditions for electronic appeals of convicts. terminals for electronic appeals and complaints have been installed in institutions of the penal enforcement system.This innovation makes it possible to ensure the principle of legality and transparency of criminal proceedings. Convicted persons can freely file complaints to the supervisory authorities in case of violation of their rights and freedoms, as well as lawlessness against them. In addition to complaints, convicts are given the opportunity to contact state bodies and provide public services through terminals.

Installation of video surveillance systems in places of deprivation of liberty is the most important and urgent issue in the field of digitalization in institutions of the penal system. In addition, employees of the penal enforcement system are equipped with video recorders.

The video monitoring system in institutions allows viewing visible and so-called blind spots in prisons to prevent and suppress violations of the regime of serving sentences, including the commission of offenses in the process of serving a sentence. In some cases, the video monitoring system makes it possible to identify illegal actions of convicts against employees of the penal enforcement system. These video recordings serve as an evidence base for bringing the offender to justice.

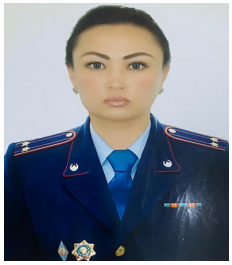
Literature

1. Message to the People of Kazakhstan by the President of the Republic of Kazakhstan, September 2023.

2. Джансараева Р.Е. Вестник КазНУ. Серия юридическая. – Караганда, 2005. - №3(35). – С. 46-49

3. The Penal Enforcement Code, edited by 2014, with changes and additions by 2023.

4. Совместный приказ Генеральной прокуратуры №98 «31»июля 2018 год, МВД №549 от «27»июля 2018 год, МЮ №1245 от «09»августа 2018 год, МЗ №499 от «15» августа 2018 год, МФ №846 от «24»сентября 2018 год «Об утверждении Дорожной карты развития уголовно-исполнительной системы на 113 2019-2023 год» в соответствии с пунктом 5.2 Протокола заседания Правительства Республики Казахстан от 15 мая 2018 года №20



АБАЖАНОВА АСЕМ ЗЕЙНОЛЛАЕВНА
Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., подполковник полиции

УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КРАЖ И МОШЕННИЧЕСТВА, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

В настоящее время, в связи со стремительным развитием цифровизации, Республика Казахстан, как и многие страны мира, также столкнулась с ростом киберпреступности. Каждый год наблюдается увеличение числа таких преступлений, что вызывает общественный резонанс, особенно в отношении мошенничества. Таким образом интернет-мошенничество представляет собой серьезную проблему в современном мире. Разнообразие методов и способов совершения киберпреступлений требует особого внимания и принятия соответствующих мер. Оно может проявляться в различных формах, включая кражу личных данных и фишинг, взлом компьютеров через спам-письма с требованием выкупа, а также незаконное изменение данных.

В Казахстане существует ряд нормативных актов, регулирующих информационное поле и закрепляющих права человека на защиту от посягательств: Конституция Республики Казахстан, Уголовный кодекс Республики Казахстан, Кодексе Республики Казахстан «Об административных правонарушениях», законах Республики Казахстан «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «Об информатизации».

В них были внесены дополнения и изменения в соответствии с разработанной Концепции кибербезопасности («Киберщит Казахстана») от 30 июня 2017 года №407, однако понятие «киберпреступление» отсутствует во всех нормативно правовых актов. Уголовная ответственность за преступления в сфере компьютерных технологий предусмотрена главой 7 «Уголовные правонарушения в сфере информатизации и связи», а также существуют отдельные виды преступлений, которые совершаются с помощью компьютерных технологий, ярким примером является статья 190 – мошенничество, а именно п. 4, ч. 2 статьи 190 «путем обмана или злоупотребления доверием пользователя информационной системы» [1].

Однако, несмотря на наличие данной статьи, она не полностью охватывает все аспекты этого вида преступлений. Кибермошенничество включает в себя широкий спектр преступлений, совершаемых в киберпространстве, таких как фишинг, кибератаки, кража личных данных и другие. Квалификация преступления «кибермошенничество» требует тщательного теоретического анализа для определения его состава и, следовательно, соответствующей правоприменительной практики. В частности, важно учитывать объект и объективную сторону данной конкретной категории преступлений, отражающие их уникальные особенности.

Цифровая безопасность часто оказывается под угрозой в правовой базе, направленной на предотвращение киберпреступлений, что включает в себя технические, организационные и другие факторы, влияющие на действия пользователей сети. Поэтому необходимо усилить контроль за безопасным использованием локальных сетей и беспроводной связи со стороны государственных органов, обеспечить установку обязательных антивирусных программ,

создать прозрачную систему мониторинга протоколов безопасности на официальных сайтах, систематически предлагать расширенные возможности курсы подготовки сотрудников правоохранительных органов по цифровой криминалистике [2].

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание и password – пароль) – вид интернет-мошенничества, цель которого – получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации [3]. Фишинг реализовывают через фиктивные сообщения на электронную почту, мессенджеры и всплывающие уведомления. В большинстве случаев мошенники преследуют финансовый интерес, поэтому маскируются под банковские организации, провайдеров и системы электронных платежей для получения доступа к онлайн-банкингу или кошельку жертвы для вывода денежных средств.

Схема работает таким образом, что лица, получают электронное фишинг-письмо с просьбой перейти на веб-сайт, обновить систему или направить ответ для подтверждения личности. Мошенники действуют достаточно грамотно и убедительно, что практически невозможно отличить поддельное письмо. Как правило преступники создают идентичный веб-сайт на короткое время, где запрашивают конфиденциальную информацию. Например, сайт банка, где нужно ввести свой логин и пароль, номер телефона, данные кредитных карт, PIN-код и код доступа (если таковое имеется) и вот уже ваши данные на руках у злоумышленников, которые вы предоставили сами. Для этого они используют методы социальной инженерии, придумывая различные ситуации, например, угрозы блокировки банковской карты без подтверждения личности, либо сообщают о взломе аккаунта и предоставляют фишинговую ссылку для авторизации.

Фишинг эволюционировал и теперь имеет несколько разновидностей, использующих аналогичные методы: вишинг, смишинг и фарминг. Вишинг (англ. Vishing, от voice – голос +phishing) – одна из разновидностей фишинга, реализуется методами социальной инженерии с помощью телефонного звонка. На телефон атакуемого поступает звонок, и злоумышленник различными способами выуживает все необходимые данные для реализации умысла. Еще одним видом является смишинг (англ. Smishing, от sms – служба коротких сообщений +phishing) реализуется с помощью рассылки через СМС – сообщения с вредоносной ссылкой, зачастую это оповещения о выигрыше какого-либо приза. В текстовом сообщении указывается поздравительный текст и ссылка для получения гарантированного приза. Осведомленность пользователей про фишинговые атаки с каждым разом растет, в связи с этим хакеры создали новый метод – фарминг. Технически фарминг сложнее в реализации, так как посредством кэша DNS-серверов (серверы доменных имен) и вируса программного обеспечения перенаправляют с легитимного веб-сайта на сторонние страницы с поддельными доменами и IP-адресами без ведома пользователя, что также приводит к краже данных. Распознать фарминг труднее, так как замена сайтов происходит незаметно и если не обратить на этот факт внимание, то все имеющиеся данные окажутся в уязвимом положении [4].

Компрометация деловой электронной почты (BEC). Ключевым элементом в совершении данного мошенничества является фишинг/спуфинг. При BEC-атаке злоумышленники получают доступ к корпоративным сетям, далее могут рассылать различные электронные письма сотрудникам от имени компаний, поставщиков, с которыми они сотрудничают и производят оплату зачастую безналичным способом. Здесь могут применяться как методы социальной инженерии, таки технический взлом компьютеров.

Центр жалоб на интернет-преступления (IC3) ФБР сообщает, что мошенничество с BEC было самой дорогой из кибератак в 2020 году: было подано 19369 жалоб и скорректированные убытки в размере около 1,8 миллиарда долларов, а также 71% организаций признали, что они были свидетелями атак с целью компрометации деловой почты [5].

Нигерийские письма или мошенничество «419». Еще один вид цифрового мошенничества, при котором злоумышленники присылают письма о якобы полученном вами наследстве, для которого необходимо всего-то оплатить доставку или что-то еще и для этого

требуются данные карты. Также довольно распространённая схема такого мошенничества – вывоз денежных средств «чиновником» с Нигерии. Злоумышленники, выдавая себя за чиновника предлагают процент от переводимых сумм, которые выплатят после незаконного перевода или переезда чиновника.

Жертвы предоставляют свою конфиденциальную информацию: номера банковских счетов, бланки, которые в последствии используются для вывода средств с их счетов. Несмотря на то что, казалось бы, никто не поведется на «письма счастья» ежегодно убытки достигают миллионы долларов. Особо доверчивых заманивали в Нигерию, где в результате они были заключены в тюрьму, так как Правительство Нигерии не сочувствуют своим жертвам, поскольку жертва буквально вступает в сговор в незаконном переводе, которое противоречит законодательству данного государства. Название такого вида мошенничества исходит из статьи 419 Уголовного кодекса Нигерии о мошенничестве, который конкретно касается людей, обращающихся за помощью в переводе денег, через электронную почту [6].

Также существуют другие виды кибермошенничества, например, проведение псевдолотерей и конкурсов – для такого вида мошенничества, как правило пользователя просят заполнить регистрационную форму для получения данных; инвестиционные схемы, проекты и финансовые пирамиды – быстрые и легкие деньги с красивой рекламой, на которые ведутся множество людей, добровольно переводя деньги на счета злоумышленников, после чего те или пропадают, или блокируют «жертв»; письма в социальных сетях и рассылки – после взлома социальных сетей, всем друзьям пользователя приходит сообщение с просьбой одолжить денег или оплатить лечение кому-то из его близких и номер карты, после чего злоумышленник пропадает, а пользователь возвращает доступ к странице себе; фальшивые интернет-магазины – со времен пандемии множество людей стали заказывать все необходимое в интернете, в связи с чем на ряду с нормальными интернет-магазинами, появились фальшивые, которые сложно отличить. После перевода денег за товар вы окажетесь в черном списке или вас просто будут игнорировать. Тем самым, злоумышленник получит ваши денежные средства от вас добровольно.

В интернет-магазинах всегда нужно смотреть настоящие ли там отзывы, живая ли страничка, а лучше брать только у проверенных или спрашивать о таких у своих знакомых; фальшивые платежные системы – никогда не стоит оплачивать что-то в интернете через свою кредитную карту на непроверенных сайтах и через незнакомые платежные системы. Злоумышленники получают полный доступ к вашей карте, так как вы самостоятельно вводите все данные карты; программы-вымогатели – это один из типов вредоносного ПО, которыми пользуются мошенники для вымогательства денежных средств путем удержания данных или блокировки устройств через электронные письма или USB-накопителя, с целью получения выкупа.

Примерно таким же образом и мотивом осуществляется отказ в обслуживании, для вымогания денежных средств. Данный список пополняется каждый день новыми видами кибермошенничества и все перечислить невозможно, поэтому мы раскрыли самый распространённый вид мошенничества в отношении физических лиц (фишинг), мошенничество, направленное на юридических лиц (компрометация деловой электронной почты) наносит большой финансовый ущерб, а также Нигерийские письма, за которые могут привлечь уголовную ответственность за содействие в совершении преступления.

Говоря о способах, самыми распространенными оказались получение денежных средств за товар или услугу на сайтах, предназначенных для размещения объявлений (8,2 тысячи случаев), благодаря получению конфиденциальной информации, мошенникам удалось оформить 2,7 тысячи микрокредитных займов на людей, вишинг также не остался в стороне и составил 2,3 тысячи случаев, «выгодные» предложения о легком заработке и вложениях составили 1,9 тысяч случаев, фишинг и фальшивые ссылки – 1,3 тысячи случаев [7]. Мошенничество растет пропорционально вместе с количеством пользователей в сети, которые

активно попадаются на уловки злоумышленников. Это также наглядно показывает отсутствие кибергигиены и осведомленности населения.

Чтобы оценить масштабность проблемы цифрового мошенничества, стоит рассмотреть статистические данные. Так, согласно статистике, в Республике Казахстан в 2021 году количество фактов цифрового мошенничества составило 17800, что в 2 раза выше показателей 2019 года. Самыми «атакуемыми» оказались город Нур-Султан, Алматы, Карагандинская, Костанайская и Восточно-Казахстанская области. Только 5% уголовных дел по киберпреступлениям доходит до суда в Казахстане. В Казахстане на 46,3% выросло число инцидентов нарушения информационной безопасности, которые зафиксированы Национальной службой реагирования KZ-CERT. За январь-июнь таких случаев в стране было выявлено более 12,9 тыс. против 8,9 тыс. в первом полугодии 2022 года [8].

Большая часть из них – 8,5 тыс. инцидентов – это распространение компьютерных вирусов, «червей», троянских программ. На втором месте по количеству фактов кибер-нарушений, согласно данным АО «Государственная техническая служба» (ГТС), – выявленные 2,4 тыс. ботнетов. Это такие компьютерные сети, которые используются хакерами для выполнения кибератак и разных вредоносных операций. В шесть раз больше стало фактов несанкционированного доступа и модификации интернет-данных – 258 против 41 в первом полугодии прошлого года.

При этом если сопоставлять статистику кибератак за 2022-й и 2017 годы, то можно увидеть снижение числа выявленных инцидентов на треть: 2022 году таких случаев выявлено 16,7 тыс. против 25,4 тыс. в 2017 году. Статистика ГТС показывает, как сильно изменилась структура таких фактов. Например, в 2017 году одним из самых распространенных видов компьютерных инцидентов были ботнеты, а спустя пять лет их число сократилось в десять раз – с 22,9 тыс. до 2,2 тыс. Зато многократно чаще выявлялись компьютерные вирусы и вредоносное ПО – 10,9 тыс. против 360 в 2017 году.

Интерпретировать эти данные исключительно в количественном аспекте будет некорректно. Слишком много изменений произошло за это время и в развитии цифровизации, и в системе национальной кибербезопасности страны. Появились новые варианты защиты, создана система «Киберщит Казахстана». Те пути, которые использовали преступники пять лет назад, уже давно не работают. Впрочем, взломщики тоже не сидят на месте, постоянно создавая новые схемы проникновения в информационные и финансовые системы. Поэтому само по себе уменьшение количества выявленных киберинцидентов с 2017 по 2022 годы не говорит об эффективности или неэффективности системы защиты или уменьшении активности киберпреступности.

В статистике уголовных дел ни о каких сотнях или тысячах киберпреступлений речи не идет. Количество правонарушений в сфере информационной безопасности, которые расследуются сотрудниками МВД РК, исчисляется лишь десятками. В последнюю пятилетку их число от года к году менялось незначительно. Согласно данным комитета по правовой статистике и спецучётам Генпрокуратуры РК (КПСиСУ), в 2022 году в Едином реестре досудебных расследований (ЕРДР) было зарегистрировано 85 таких правонарушений, а с учетом рассматриваемых дел предыдущих лет – 142. За год количество новых преступлений выросло на 14,9%. В первой половине этого года заведено еще 43 уголовных дела.

Чаще всего дела возбуждались по статье 205 УК РК – неправомерный доступ к информации или информационной системе. И в прошлом, и в этом году почти половина зарегистрированных правонарушений связана именно со взломом. На втором месте по количеству возбужденных дел статья 206 УК РК – неправомерное уничтожение или модификация информации. В 2022 году было зафиксировано 15 таких дел, за первое полугодие этого года – уже 14. Что касается создания и распространения в сети вирусов и других вредоносных программ, то таких правонарушений в системе КПСиСУ зарегистрировано, напротив, немного: за последнее время – по 4-5 в год.

Собрать доказательную базу и довести такие уголовные дела до суда, вероятно, не менее сложно, чем поймать хакера. Большинство из них просто рассыпаются по пути, закрываются из-за недостатка улик или отсутствия подозреваемых. Допустим, из 142 уголовных дел, рассматриваемых органами следствия в прошлом году, до суда дошли только 8. Это всего 5,6%. 40 уголовных дел прекращены по истечению срока давности или в связи с невменяемостью, смертью подозреваемого, отсутствием состава преступления или по другим причинам. Еще 46 правонарушений считались нераскрытыми и были закрыты, по ним тоже истекли все возможные сроки расследования.

В первом полугодии этого года похожая ситуация. Из 106 рассматриваемых уголовных дел в суд направлены только три, или 2,8%. По 20 киберпреступлениям следствие прекращено, 19 закрыты как «висяки» по истечению срока давности. Судя по официальным данным, «улов» хакеров, попавших под внимание следствия, за эти годы был относительно невысок. В прошлом году сумма причиненного такими преступлениями ущерба была равна 58 млн тенге, из них 27,6 млн тенге – это урон государству, а 30,4 млн тенге– физическим лицам. Вернуть украденное удалось только в госбюджет. Стоит упомянуть, что в 2022-м и в первой половине этого года государству нанесен самый большой за последние годы финансовый ущерб от киберпреступлений – по 27,6 млн тенге. Если по итогам прошлого года деньги были возвращены, то в этом году возмещения пока не было.

Важно отметить: мы привели статистику только по уголовным статьям в сфере информационной безопасности и связи [11]. В этом разделе уголовного кодекса таких статей всего девять. Однако многие преступления, связанные с воровством персональных данных, неправомерным доступом к приложениям и личным кабинетам, кражей денег со счетов, нередко квалифицируют по статьям другой категории – преступлений против собственности. К таким, например, относятся интернет-мошенничество, мошенничество с использованием платежных карт и другие. Яркий пример – резонансный судебный процесс над хакерами из транснациональной преступной кибергруппы «Карбанак», взломавшими информационные системы двух казахстанских банков и похитившими около 2 млрд тенге. Решением суда двух преступников осудили на 8 лет тюрьмы.

В свете этих событий, необходимо провести более глубокое изучение и адаптацию законодательства, чтобы оно соответствовало современным вызовам и угрозам, связанным с использованием информационно-коммуникативных систем. Важно разработать более точные и подробные определения и нормы, которые учитывали бы все особенности киберпреступлений и позволяли эффективно пресекать их.

Кроме того, для борьбы с кибермошенничеством необходимо усилить сотрудничество между правоохранительными органами, информационными технологическими компаниями и обществом в целом. Важно проводить информационные кампании и образовательные программы, чтобы повысить осведомленность граждан о возможных угрозах и способах защиты от киберпреступлений. Также следует обратить внимание на международное сотрудничество в области борьбы с киберпреступностью. Ведь киберпреступники действуют глобально, и только совместными усилиями стран можно достичь значимых результатов в этой области. Разработка и подписание международных соглашений и протоколов помогут установить эффективные механизмы сотрудничества и обмена информацией для предотвращения и расследования киберпреступлений.

В целом, борьба с киберпреступностью является важной задачей для Республики Казахстан. Необходимо постоянно обновлять и совершенствовать законодательство, разрабатывать технические средства защиты, повышать осведомленность граждан и укреплять международное сотрудничество, чтобы обеспечить безопасность в киберпространстве и защитить интересы граждан и бизнеса от киберугроз.

Интернет-мошенничество представляет собой серьезную проблему в современном мире. Оно может проявляться в различных формах, включая кражу личных данных и фишинг, взлом компьютеров через спам-письма с требованием выкупа, а также незаконное изменение

данных. Квалификация таких преступлений обычно включает рассмотрение связанных статей, таких как Статья 207 УК РК «Нарушение работы информационной системы или сетей телекоммуникаций» и Статья 208 УК РК «Неправомерное завладение информацией». Вопрос о том, следует ли рассматривать интернет-мошенничество как отдельное преступление, обсуждается уже давно. Исследователи высказывали мнение о необходимости введения отдельной нормы в законодательство.

Например, Т. Тропина считает, что различные манипуляции с компьютерными данными, которые в итоге приводят к незаконному завладению имуществом других лиц, нельзя квалифицировать по статьям 158 «Кража» и 159 «Мошенничество» Уголовного кодекса Российской Федерации. Она также указывает на противоречие с принципом уголовного права «nullum crimen, nulla poena sine lege» – «нет преступления без указания о нем в законе», если применять квалификации по совокупности. Однако простое добавление действий с использованием компьютерных технологий в статью «Мошенничество» не решит проблемы, связанные с квалификацией преступлений, совершаемых с использованием информационных технологий. Это может быть вызвано сложностью определения и классификации таких преступлений, а также постоянным развитием технологий, что требует постоянного обновления законодательства.

Таким образом, необходимо провести дальнейшие исследования и обсуждения, чтобы разработать более точные и эффективные методы борьбы с интернет-мошенничеством. Это может включать создание отдельного состава преступления, учитывающего специфику таких преступлений, а также обновление законодательства с учетом новых технологий и методов совершения преступлений.

Литература

1. Уголовный Кодекс Республики Казахстан – ИПС «Әділет» (Adilet.zan.kz, 2023);
2. Комментарий К Уголовному Кодексу Республики Казахстан (Особенная Часть)' (Zakon.uchet.kz, 2023);
3. «Что Такое «Фишинг» (Encyclopedia.kaspersky.ru, 2022) ;
4. Фишинг, Вишинг, Смишинг, Фарминг – В Чем Разница' (Protectimus.com, 2022);
5. Antipov A, 'Лучшие Методы Предотвращения Атак Компрометации Деловой Электронной Почты (BEC)' (Securitylab.ru, 2022);
6. Welcome To FBI.Gov | Federal Bureau Of Investigation' (Federal Bureau of Investigation, 2022);
7. Названы Распространенные Схемы Кибермошенничества' (Деловой портал Капитал.кз, 2022);
8. Портал inbusiness.kz со ссылкой на Finprom;
9. 'Вдвое Выросло Количество Интернет-Мошенничеств В Казахстане' (profit.kz, 2022).

ЖИЕНГАЛИЕВА АЙГЕРИМ АЛТЫНБЕКОВНА
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға оқытушысы. з.ғ.м., полиция майоры

ІШКІ ІСТЕР ОРГАНДАРЫНДАҒЫ ТАЛДАМАЛЫҚ ЖҰМЫС ЖӘНЕ ОНЫ ЖЕТІЛДІРУ ЖОЛДАРЫ

Ішкі істер органдарының тұрақты және тиімді жұмыс істеуі басқарушылық қызметті жоғары кәсіби деңгейде жүзеге асыру.

Бұл тиісті ұйым қызмет жетістігін қамтамасыз етеді ішкі істер органдары жүйесінің алдында тұрған мақсаттар мен міндеттерді шешеді.

Басқару процесі-бұл басқарма басшысының және аппаратының жұмыс істеуін ретке келтіру жөніндегі іс-қимылдары ұйымға және оның элементтеріне қол жеткізу олардың алдында тұрған мақсаттар жиынтығы. Басқару процесінің бөлігі ретінде екі негізгі шешім қабылданады:

–тактикалық-бағытталған, бірінші кезек, тұрақтылықты, өзара әрекеттестікті сақтау және барлық элементтердің өнімділігі басқару жүйелері;

–стратегиялық-жүйені дамытуға және жетілдіруге бағытталған басқару, оны сапалы аудару және басқа күйге сандық.

Айта кету керек, басқару шешімдері белсенді форма болып табылады басқару процесінде әсер ету. Өз негізінде басқару процесі басқару шешімдерінің үздіксіз тізбегі болып табылады.

Ішкі істер органдарының қылмысқа қарсы күрес саласындағы жұмысының тиімділігі ол, ең алдымен, қалыптасқан жедел жағдайды жан-жақты талдауға және оның негізінде әзірлеуге бағытталған уақтылы басқару шешімдері.

Бұл мақсаттар ақпараттық-аналитикалық жұмыс болып табылады, оның мәні кең көлемді алу және зерттеу болып табылады жан-жақты ақпарат кешені, басқарушылық қабылдау үшін қажет шешімдер.

Қазіргі қоғамда О.В. Галущенко, «ақпараттық аналитика, адамның кез-келген іс-әрекеті сияқты, жеке тұлғаны қоғамда өзін-өзі жүзеге асыруға бағытталған, танымдық сипатта болады және сайып келгенде, оның мақсаты жаңа білім құру болып табылады» деп тұжырымдайды [1, 6-7 б.]. Ішкі істер органдарының ақпараттық-талдамалық қызметін мынадай құрамдас бөлігі:

1)басқару объектісі туралы мәліметтерді өңдеу және сақтау;

2) талдамалық қызмет – зерттелетін басқару объектісінің себептік байланыстарын, тенденциялары мен заңдылықтарын белгілеу жөніндегі ой процесі;

3) ақпараттық қамтамасыз ету-ақпаратты өңдеудің автоматтандырылған жүйелерінің, бағдарламалық-аппараттық кешендердің және бағдарламалық-техникалық құралдардың, сондай-ақ жедел орындау үшін қажетті байланыс және деректерді беру жүйелерінің жиынтығы-ведомствоның қызметтік міндеттері.

Басқару функцияларын іске асыру кезінде ішкі істер органдары басшыларының уақтылы, негізделген және ұтымды басқару шешімдерін әзірлеуді қамтамасыз ету. Сондықтан ақпараттық-аналитикалық жұмыстың төмен деңгейі оңтайлы емес басқару шешімдерін

қабылдауға, жедел-қызметтік қызметтегі қателіктер мен кемшіліктерге әкеледі. Функцияларды ұйымдастыру мен орындаудың негізгі субъектісі.

Аналитикалық жұмыстарға тиісті көңіл бөлінбеді. Қызметтің бұл бағыты аналитикалық жұмыстың негізгі бағыттары мен түрлері бөлігінде ғана көрінді [2], бірақ оны жүргізу тәртібі мен негізгі ережелері қарастырылмаған. Штаб қызметкерлері тиісті дайындықсыз зерттеу жұмыстарын интуитивті түрде жүргізді, жедел жағдайды талдау әдістемесі мен математика мен логика туралы жалпы түсініктерге сүйенді.

Зерттеу қызметін жүзеге асырудағы штабтық бөлімшелердің рөлі сөзсіз, бірақ штабтық бөлімшелер аналитикалық материалдың сапасына және зерттеу процесінің өзіне тікелей әсер ететін басқада ілеспе функцияларды орындайды.

Штаб Қазақстан Республикасы ІІМ аумақтық органының бөлімшелерін көп өлшемді ақпараттық қамтамасыз ету және бағынысты органдар мен ұйымдардың Қазақстан Республикасы ІІМ аумақтық органының ақпараттық-талдау қызметін жүзеге асыру міндеттерін шешу үшін анықтамалық-ақпараттық қорларды қалыптастырады.

Ішкі істер органдарының құқықтық тәртібінің жай-күйіне ақпараттың негізгі көздері қылмыстар, әкімшілік құқық бұзушылықтар, оқиғалар туралы арыздар мен хабарламалар, сондай-ақ оларды тексеру нәтижелері бойынша қабылданған шешімдер болып табылады.

Алынған ақпарат мынадай: құқық бұзушылықты жасау орны, уақыты,тәсілі,ауырлық дәрежесі бойынша; құқық бұзушылық жасаған адамдардың және жәбірленуші болған адамдардың жынысы, жасы, жұмыспен қамтылуы бойынша; келтірілген залал бойынша және т. б. біріктіруші белгілер бойынша өңделеді және топтастырылады. есептеулер зерттелетін құбылыстардың құрылымы мен динамикасын анықтайды.

Ішкі істер органдарының талдамалық қызметі тікелей басқару объектісін талдаумен шектелмеуі керек (ведомство ішілік жұмыс; құқық бұзушылықтар және оларды жасаған адамдар). Ақпараттық-талдамалық қызметтің толықтығын, дұрыстығын және салыстырымдылығын қамтамасыз ететін деректерге әлеуметтік-экономикалық факторлар: халықтың саны мен тығыздығы жатады.

Аналитикалық қызмет кезеңінде зерттелетін құбылыстың (басқару объектісінің) тенденцияларын анықтау жеткіліксіз,жоғарыда аталған факторлардың зерттелетін басқару объектісіне әсерін түсіндіру қажет. Бұл жағдайда біз басқару объектісінің сандық және сапалық сипаттамаларын талдау туралы айтып отырмыз.

Айта кету керек, ресми статистикалық мәліметтер қылмыстың жай-күйі ішкі істер органдары қалыптастыратын және аналитикалық қызмет кезеңінде қолданылатын, көбінесе аумақтық ішкі істер органының қызмет көрсету аумағындағы криминогендік жағдайдың нақты жай-күйін емес, заңды қолдану тәжірибесін көрсетеді.

Осылайша, ішкі істер органдарындағы аналитикалық қызметті қылмыс пен қоғамдық тәртіптің жай-күйі, ішкі істер органдарының алдында тұрған міндеттерді орындау жөніндегі практикалық қызметінің нәтижелері, сондай-ақ осы міндеттер шешілетін жағдайлар туралы ақпаратты зерделеу және бағалау үшін ұйымдастырушылық іс-шаралар мен әдістемелік әдістердің кең спектрін қамтитын тұрақты зерттеу қызметі ретінде анықтауға болады және басқарушылық әсерлердің тиімділігін мақсатты басқаруды және бағалауды қамтамасыз етеді [3].

Ақпараттық-талдау жұмысының негізгі бағыттары:

1) Қызмет көрсетілетін аумақта болып жатқан, криминогендік жағдайға әсер ететін процестер туралы ақпаратты жинақтау, қорыту және бағалау;

2) ішкі істер органының бастығы үшін немесе инстанцияға ақпараттық-талдамалық және анықтамалық материалдарды жіберу үшін дайындау;

3) қылмысқа қарсы күрес, қоғамдық тәртіпті және қоғамдық қауіпсіздікті қамтамасыз ету мәселелері бойынша ақпаратты кешенді талдау;

4) ақпараттық құжаттар мен материалдар шоғырланатын және сақталатын ішкі істер органы бөлімшелерінің мұқтаждары үшін анықтамалық-ақпараттық қорды қалыптастыру.

Жоғарыда айтылғандарға қорытынды жасай отырып, қазіргі уақытта жедел-қызметтік қызметтің тиімділігін бағалау ақпараттық-аналитикалық жұмысты ұйымдастыру мен жүзеге асыру деңгейіне тікелей байланысты екенін атап өткен жөн [4].

Ішкі істер органдарындағы ақпараттық-аналитикалық жұмыстың мақсаты мен субъектілерін анықтауға қатысты теориялық аспектілерді қарастыра отырып, бүгінгі күні ақпараттық-аналитикалық жұмысты практикалық іске асыруда қызметкерлердің қызметіне келесі басым бағыттарды енгізу арқылы жоюға болатын бірқатар кемшіліктер бар екенін атап өткен жөн:

1. Тиісті мамандарды тарта отырып, ішкі істер органдары қызметкерлерінің қызметінде ақпараттық-коммуникативтік технологияларды пайдалану ерекшеліктері бойынша қызметтік даярлық шеңберінде сабақтар өткізу.

2. Ішкі істер органдарының қызметкерлерін талдамалық ізденістің тиімді тәсілдеріне оқытуға бағытталған арнайы оқу-әдістемелік құралдар мен ұсынымдар әзірлеу.

3. Ұйымдастырушылық-техникалық жүйелердің автоматтандырылған деректер банктерін туындайтын криминогендік жағдайларды жан-жақты, толық және объективті зерттеу жүргізу үшін қажетті өзекті ақпаратпен уақтылы толықтыру. Сондай-ақ ішкі істер органдары қызметкерлерінің қызметіне"Интернет"ақпараттық-телекоммуникациялық желісіндегі мәліметтерді пайдалануға мүмкіндік беретін жүйелерді енгізу қажет.

4. Ішкі істер органдарында ақпараттық-талдау жұмыстарын жүзеге асыру процесінде бөлімшелер мен қызметтер арасындағы тиімді ақпараттық өзара іс-қимылды құқықтық реттеу шараларын әзірлеу.

5. Құрылымдық бөлімшелер басшыларының ішкі істер органдарының қызметін ақпараттық қамтамасыз ету жай-күйіне тұрақты және тиімді бақылауды жүзеге асыру.

Әдебиет

1. Рустемова Г.Р., Насырова Э.М. К вопросу о семейно-бытовом насилии// «Бытовое насилие: переосмысление системы противодействия» материалы международной научно-практической конференции (12.09.2022) – Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы, 2022. – С. 115-118.

2. Закон РК от 4.12.2009 №214-IV «О профилактике бытового насилия» (с изм. и доп. по сост. на 01.07.2023) //[Электронный ресурс] – Режим доступа: // https://online.zakon.kz/Document /?doc_id=30525680&pos=64;-51#pos=64;-51 (Дата обращения: 27.08.2023).

3. Гаухман Л.Д. Борьба с насильственными посягательствами. – М. Изд-во: «Юрид. лит.» 1969. – С. 119.

АРЫНОВА АСИЯ НУРЛАНОВНА
Преподаватель кафедры уголовного права и криминологии Карагандинской академии МВД Республики Казахстан имени Б.Бейсенова,
магистр права, подполковник полиции

ТЕКУЩИЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Эволюция научно-технического развития на сегодняшний день коснулось практически всех сфер жизни общества. Возможно, было бы просто предполагать, что изменения, происходящие в данной области, остались необнаруженными криминальными структурами. Дефицит формальных препятствий, наблюдаемых при внедрении современных информационных технологий в практическую деятельность правоохранительных органов и других систем государства, позволяет криминальным структурам в минимальные сроки подстраивать для своих нужд самые новаторские технологии для достижения преступного результата и извлечения сверхприбыли при реализации преступной деятельности, не считаясь с территориальными ограничениями ее реализации [1]. На сегодняшний день проблемы информационных технологий, применяемых и используемых в качестве орудий и средств совершения уголовных правонарушений, находятся на самом высоком уровне.

Серьезные опасения в области применения информационных технологий при совершении преступлений вызывают у руководителей практически всех правоохранительных структур государства, которые задействованы в процессе борьбы, с рассматриваемыми видами преступлений. Так, по данным представителей Следственного Департамента МВД Республики Казахстан, количество преступлений в сфере интернет - мошенничества за два месяца 2022 года увеличилось на 139% в сравнении с аналогичным периодом 2021 года – с 1 685 до 4 027. Резкий рост интернет – мошенничеств полиция связывает с введением ограничительным мер, в результате которых граждане были вынуждены выполнять многие процессы онлайн, в том числе – банковские операции, оформление документов, покупку вещей и продуктов. «К такому стремительному внедрению информационных технологий во все сферы нашей жизни готовыми оказались не все. Частично не готовыми оказались государство, общество и граждане»,

Низкая выявляемость мошенников объясняется тем, что многие люди не обращаются в полицию из-за небольшой суммы ущерба. Осложняет процесс следствия и то, что большинство интернет-преступлений носят трансграничный характер – то есть, жертва может находиться в одном регионе, а мошенник – в другом, иногда и в другой стране. В процесс реализации преступлений с использованием информационно-телекоммуникационных технологий активно включились организованные преступные формирования, сущность деятельности которых имеет высокоорганизованный характер, в том числе террористической и экстремистской направленности, а их уровень определяется транснациональным характером реализации преступной деятельности. Это обусловлено тем, что для повышения эффективности уровня своей преступной деятельности активно используются компьютерно-технические средства и телекоммуникационные. Вся совокупность современных средств и

технологий позволяют не только осуществлять процесс координации деятельностью формирований и их структурных подразделений, функционирующих по всему миру, активно вербовать их членов, но и достаточно быстро и без серьезных проблем и потерь осуществлять финансовые операции в любой точке мира. Кроме этого, технические средства и информационные технологии используются в качестве орудий и средств совершения не только корыстных преступлений, но и более тяжких, таких как терроризм и экстремизм. Приходится констатировать, что такая ситуация в области роста преступлений, связанных с применением современных информационных и телекоммуникационных технологий, в свою очередь, обусловливает рост организованной преступной деятельности, которая активно и повсеместно использует возможности современных информационных и телекоммуникационных технологий.

Самыми распространенными способами совершения преступлений в этой сфере являются покупка несуществующих товаров или услуг по фейковым объявлениям, где обязательным условием является внесение предоплаты до получения товара, вложение денег в различные проекты, игры, ставки, а также перевод денег на другие счета по просьбе лиц, которые представляются во время звонков сотрудниками служб безопасности банков.

Помимо этого, распространенным случаем мошенничества является использование персональных данных граждан для доступа к их банковским счетам. Как правило, жертвы сами вводят свои данные на фишинговых сайтах либо преступники используют утерянные или похищенные документы жертв.

Принимаемые меры и их результат в данной сфере указывает на необходимость реализации комплексного подхода, направленного на противодействие преступлениям, совершаемым с применением современных информационных технологий. Представляется, что в системе реализации мер такого комплексного подхода должны быть задействованы все правоохранительные органы, на уровне активного взаимодействия с учеными и специалистами, активно ведущими исследования в рассматриваемых сферах, а его результаты должны активно внедряться в практическую деятельность правоохранительных органов. Активную работу в разработке и внедрении данного решения и других аналогичных мер должны принять ученые и специалисты в рассматриваемой сфере. В рамках реализации комплексного подхода ими должен осуществляться постоянный мониторинг появления новых и совершенствования уже существующих способов, орудий и средств совершения преступлений, с применением информационных технологий, выявление проблем и недостатков в области правого, научного и практического обеспечения деятельности по раскрытию и расследованию рассматриваемых видов преступлений. Необходимо отметить, что такая деятельность уже ведется достаточно успешно на протяжении длительного времени и, учитывая указанные обстоятельства, учеными и специалистами разрабатываются [2], совершенствуются и внедряются методические и практические рекомендации [3, 4] выявления, раскрытия и расследования преступлений, совершаемых с применением информационных технологий, учитывая характер изменений и активного использования высоких технологий в повседневной жизни общества и преступной среде. В современных условиях развития научно-технического прогресса наиболее приемлемой и необходимой в области противодействия преступлениям, совершаемым с применением информационных телекоммуникационных технологий, особенно организованными преступными формированиями, сегодня была бы активная прогностическая деятельность ученых и специалистов, реализуемая в целях разработки научных положений и создании на их основе практических рекомендаций, по борьбе с преступлениями рассматриваемого характера правоохранительными органами. Такая деятельность в условиях активной разработки и внедрения новых информационных и телекоммуникационных систем и технологий их применения позволила бы сформировать систему активного взаимодействия всех государственных структур, в том числе и с зарубежными заинтересованными учреждениями, на уровне взаимовыгодного сотрудничества. Результаты такой деятельности способствовали

бы снижению уровня преступности в сфере IT-технологий и явилось бы существенным фактором не только выявления и пресечения, но и предупреждения и профилактики рассматриваемых видов преступлений. Особенно необходимой в этой сфере видится такая деятельность в области противодействия преступлений, совершаемых организованными преступными формированиями, в том числе на транснациональном уровне.

Литература

1. Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М., 2001. – С. 234.

2. Лопашенко Н.А. Уголовно-правовая и криминологическая политика государства в области высоких технологий //

3. Информационные технологии и безопасность: Сб. науч. тр. Междунар. конф. Вып. 3. – Киев, 2003. – С. 89-97.

4. Войниканис Е.А., Якушев М.В. Информация. Собственность. Интернет: Традиция и новеллы в современном праве. – М., 2004. – С. 368.

ИСКАКОВ АСЕТ КАБДЫЛХАМИТОВИЧ
Преподаватель цикла специальных дисциплин Учебного центра КУИС
МВД Республики Казахстан, майор юстиции, магистр юридических наук

ЦИФРОВИЗАЦИЯ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ: АНАЛИЗ ЕЁ ВЛИЯНИЯ НА ПРОЦЕССЫ РЕЛИГИОЗНОЙ РАДИКАЛИЗАЦИИ СРЕДИ ОСУЖДЕННЫХ

Понятия, такие как «цифровая экономика», «цифровая эпоха», «электронное правительство» и «онлайн-образование», становятся все более распространенными и являются ключевыми компонентами цифровизации.

Цифровизация – это процесс интеграции цифровых технологий, информационных систем и сетей в различные сферы общества и экономики с целью улучшения эффективности, доступности и качества услуг, а также оптимизации процессов и ресурсов. Этот процесс включает в себя переход от аналоговых методов к цифровым, что позволяет более эффективно обрабатывать, хранить и передавать информацию, а также использовать ее для принятия более обоснованных решений.

Цифровизация охватывает различные сферы, включая экономику, образование, здравоохранение, государственное управление, и даже повседневную жизнь. Она предоставляет новые возможности для автоматизации процессов, сбора и анализа данных, обеспечивая лучшую информированность и улучшение качества жизни.

Однако, вместе с преимуществами, цифровизация также несет ряд вызовов и рисков, таких как угрозы кибербезопасности, проблемы с конфиденциальностью данных, и социальные вопросы, связанные с доступом к цифровым технологиям. Тем не менее, цифровизация остается важным фактором в современном мире, который влияет на общество, экономику и культуру, и требует сбалансированного подхода к управлению ее последствиями и регулированию.

Данное явление имеет две стороны как положительную, так и отрицательную. Помимо очевидных плюсов цифровизации, необходимо обратить внимание и на ее негативные аспекты. Один из главных негативных атрибутов цифровизации связан с киберпреступностью, которая представляет собой угрозу информационной безопасности и, следовательно, наносит урон системе национальной безопасности современных государств.

Экстремистские группировки и организации все чаще используют цифровизацию и современные информационные технологии в своих целях. Цифровизация предоставляет им новые возможности для распространения своей идеологии, рекрутинга новых членов и координации действий. Вот несколько способов, которыми экстремисты могут использовать цифровизацию:

Социальные сети: экстремистские группы активно используют социальные сети для пропаганды и коммуникации. Они могут создавать страницы, сообщества и группы, где распространяют свою идеологию и привлекают новых сторонников.

Веб-сайты и форумы: экстремисты могут создавать собственные веб-сайты и форумы, где публикуют материалы, обсуждают свои взгляды и координируют действия.

Мессенджеры: использование шифрованных мессенджеров позволяет экстремистам общаться безопасно и организовывать свои действия.

Видеоматериалы и стриминг: экстремисты могут создавать видеоматериалы и стримы, чтобы пропагандировать свои идеи и демонстрировать свои действия.

Криптовалюты: использование криптовалют может обеспечивать анонимность и финансирование экстремистских групп.

Это представляет серьезную угрозу для безопасности общества и требует дополнительных мер для борьбы с цифровой радикализацией. Правоохранительные органы должны активно мониторить и реагировать на экстремистскую активность в сети, разрабатывать стратегии по предотвращению радикализации и сотрудничать с провайдерами и платформами для блокировки экстремистского контента.

Мировые экстремисты активно используют инновационные подходы, включая цифровизацию, для распространения своей радикальной идеологии и координации действий. Цифровизация предоставляет им новые и мощные средства для достижения своих целей.

Современные экстремистские группировки, такие как ИГИЛ (Исламское государство Ирака и Леванта), активно вовлекают социальные сети в свою деятельность с целью вербовки новых последователей по всему миру и создания зарубежных ячеек. Они используют социальные сети как мощное средство для распространения своей радикальной идеологии и привлечения новых боевиков. [1].

Современная ситуация с экстремизмом в Казахстане вызывает тревогу, «только в этом году на ранней стадии приготовления сорваны попытки совершить подрыв самодельного взрывного устройства в мавзолее Ходжи Ахмета Ясави в Туркестане, а также вооруженного нападения в местах массового скопления в Астане»[2]

Согласно оценкам экспертов, за последние три года в странах ШОС было зафиксировано не менее 80 серьезных терактов, и идет увеличение, «если в 2022 году было 18 (терактов), в 2023 уже 47. От рук террористов погибло более 400 мирных граждан, порядка 940 человек получили ранения. Для пресечения насильственных действий силовым структурам и правоохранительным органам проведено свыше 300 громких антитеррористических операций. Задержаны 1,6 тысячи террористов и их пособников. Ликвидировано около 60 преступников, оказавших сопротивление властям» [2].

Противодействие транснациональному экстремизму, является одним из ключевых приоритетов в обеспечении безопасности и защите мирового сообщества, «при этом развитие современных информационно-коммуникационных технологий диктует появление новых форм экстремизма, а информационное пространство буквально стирает под его влиянием все границы» [3].

Учитывая, что террористические организации активно используют киберпространство для своих целей и привлечения «одиночек», то пенитенциарные учреждения являются удобной площадкой для онлайн-вербовки радикальных элементов. Это обусловлено несколькими факторами, включая доступность цифровых технологий в закрытом пространстве, социальную изоляцию осужденных и их потенциальную уязвимость перед радикальными идеологиями. Этот феномен требует серьезного исследования и разработки мер для предотвращения онлайн-вербовки радикальных элементов в пенитенциарных условиях.

Цифровизация экстремизма в пенитенциарных учреждениях – это процесс использования современных информационных и коммуникационных технологий экстремистами в тюрьмах и местах лишения свободы для распространения экстремистской идеологии, рекрутинга новых членов и организации действий. Этот процесс представляет собой новое и важное вызов для системы исполнения наказаний и требует адекватных мер и контрметодов.

Учитывая, что с начала текущего года в «…учреждениях страны пресекли 463 попытки доставки запрещенных предметов, 80 граждан привлечены к административной ответственности» [4], по сей день нерешенным вопросом остается проникновение запрещенных предметов, включая мобильные телефоны, алкоголь, наркотические вещества и религиозную литературу в пенитенциарные учреждения.

В результате чего, осужденные могут иметь доступ в интернет, через мобильные телефоны, планшеты, через которые у них появляется неограниченный доступ к запрещенному контенту.

Таким образом цифровизация и радикализация осужденных связанна между собой следующими аспектами:

1) Осужденные и экстремистские организации могут использовать социальные сети для обмена информацией, пропаганды и рекрутинга.

2) Осужденные могут создавать веб-сайты и форумы для обсуждения экстремистских идей и обмена информацией.

3) Использование шифрованных мессенджеров позволяет осужденным общаться с внешним миром и координировать свои действия.

4) Экстремисты могут создавать и распространять образовательные материалы, которые позволяют распространять свою идеологию внутри тюремных стен.

5) Интернет может быть средством для радикализации осужденных и их превращения в потенциальных экстремистов.

Учитывая вышеизложенное, необходимо принять следующие меры:

1) Мониторирование в интернет пространстве запрещенных материалов, а также выявление осужденных, посещающих запрещенные сайты. Блокировка доступа к определенным веб-сайтам и ресурсам, где распространяется экстремистская информация.

2) Проведение образовательных программ среди осужденных для профилактики радикализации и предостережения от экстремизма.

3) Сотрудничество с интернет-провайдерами для выявления и блокировки экстремистского контента.

4) Развитие строгой политики безопасности в тюрьмах для предотвращения незаконного доступа к Интернету и электронным устройствам.

5) Проведение программ по профилактике радикализации и дерадикализации осужденных.

Таким образом, цифровизация экстремизма в пенитенциарных учреждениях требует комплексного подхода и сотрудничества всех уровней власти и общества для эффективной борьбы с этой угрозой.

Однако, цифровизация, как современный феномен, может еще служить фактором в предотвращении радикализации среди осужденных в учреждениях уголовно-исполнительной системы. Рассмотрение влияния цифровизации на динамику радикальных убеждений и поведения осужденных представляет собой актуальную область исследований и разработки стратегий для обеспечения безопасности и реабилитации в контексте цифровой эпохи.

Вопросы связанные с цифровизацией и профилактикой экстремизма требуют дополнительных исследований и анализа со стороны ученых. Эти темы имеют огромное значение с учетом быстрого развития цифровых технологий и их влияния на современное общество. Исследования в этой области могут помочь разработать эффективные стратегии и методы борьбы с цифровой радикализацией и поддержать общественную безопасность.

Литература

1. Террористы осваивают киберпространство и вербуют «одиночек» // https://news.un.org/ru/story/2021/01/1394092

2. Теракты в Мавзолее Ходжи Ахмета Ясави и Астане предотвратил КНБ// https://tengrinews.kz/kazakhstan_news/teraktyi-mavzolee-hodji-ahmeta-yasavi-astane-predotvratil-509836/

3. Телефоны, Wi-Fi-роутеры, спирт. Как заключенным проносят запрещенку в Казахстане // https://tengrinews.kz/kazakhstan_news/telefonyi-wi-fi-routeryi-spirt-zaklyuchennyim-pronosyat-498742/

ҚҰЛАЖАНОВА АЯЖАН НҮСІПЖАНОВНА
Еуразия технологиялық университеті, «Құқық» факультетінің аға оқытушысы,
заң ғылымдарының магистірі

ЛАТЕНТТІК ҚЫЛМЫСТЫЛЫҚТЫҢ КРИМИНОЛОГИЯЛЫҚ СИПАТТАМАСЫ

Қылмыстылық – бұл белгілі бір уақытта белгілі бір территориядағы қылмыс белгілерінен тұратын іс-әрекеттер және осы іс-әрекеттерді жасаған адамдар жиынтығын беретін тарихи ауыспалы әлеуметтік құқықтық жалпылама құбылыс.

Қылмыстылық және қылмыс арақатынасы жөніндегі сұрақтарды зерттеу барысында қылмыстылық қоғамда белгілі бір уақыт арасында жасалған барлық қылмыстардың жай ғана жиынтығы еместігін ескерген жөн. Қылмыстылық күрделі жүйе құрушы қылмыстар мен олардың нысаналарының жиынтығы болып табылады.

Қылмыстылықтың негізгі санды-сапалық сипаттамалары және олардың көрсеткіштеріне тоқтала кетейік.

Қылмыстылықтың жай-күйі – көлемі, деңгейі, динамикасы, құрылымы, территориялық таралымы, латенттілігі секілді қасиеттерімен сипатталатын қылмыстылықтың негізгі жағдайы.

Қылмыстылық көлемі – белгілі бір территорияда белгілі бір уақыттағы қылмыстардың және оларды жасаған адамдардың абсолюттік саны.

Қылмыстылық деңгейі – белгілі бір уақыт аралығында белгілі бір территорияда 100 мың (кейде 10 мың) тұрғын адамға шаққандағы жасалған қылмыстар (оны істеген адамдар) саны. Қылмыстылық деңгейінің көрсеткіштері: қылмыстылықтың жалпы коэффициенті, қылмыстылықтың қылмыстық құқықтық коэффициенті, қылмыстылық белсенділігінң коэффициенті, сотталғандық коэффициенті.

Қылмыстылық динамикасы – қылмыстылықтың, оның ішінде қылмыстылықтың жеке қасиеттерінің уақыт аралығындағы өзгерісі.

Қылмыстылық динамикасының көрсеткіштері – бұл қылмыстылықтың абсолюттік өсуі (кемуі), өсу қарқындылығы, қылмыстылық көлемі мен деңгейінің қосылу қарқындылығы.

Қылмыстылық құрылымы – бұл оның жеке түрлерімен арақатынасын сипаттайтын ішкі құрылысы. Қылмыстылықтың жалпы көлеміндегі қылмыстылықтың жеке түрлерінің үлестік салмағы.

Әдебиеттерге көз жүгіртсек, қылмыстылық түсінігі мен оның негізгі қасиеттерінің сипаттамасы тек кеңестік дәуір криминологиясының ғана зерттеу заты болғанын анықтаймыз.

Латенттік қылмыстылық дегеніміз әр түрлі себептермен құқық қорғау органдарының назарынан тыс қалған қылмыстардың жиынтығы. Ол ол латынша latens сөзінен шыққан , ол жасырын дегенді білдіреді. Мысалға теңізде қалқып жүрген мұздың (айсберг) су бетінде бізге көрініп жүрген бөлігінен су асты көрінбейтін бөлігі әлдейқайда көлемді болады. Криминология дәл осындай Архимед ашқан физикалық заңдылыққа бағынбаса да қылмыстылық мәселесі туралы осы бір заңдылықты мысал ретінде келтіруге болады. Өйткені қылмыстылықтың көрінетін бөлігінен де жасырын бөлігі (латенттік) көлемді болып келеді [1].

Латенттік қылмыстылықтың болуы әралуан келеңсіз салдарларға әкеп соғады: қылмыстылықтың шынайы жай-күйі туралы, оның азаматтар мен қоғамға әкеп соғатын зардаптары туралы қате түсініктің болуы; құқық қорғау органдарының қызметіне қанағаттанбау және т.с.с.

Латенттік қылмыстылық ұғымын анықтау кезінде криминологиялық ғылымның алдына қойылған мақсатқа, сондай-ақ терминологияның ресми логикалық түсінігіндегі бірлігіне сүйену қажет. «Латенттік қылмыстылық» ұғымы «қылмыстылықтың» жалпы ұғымын «латентті» және «латентті емес» деп бөлудің нәтижесі болып табылады. Кез – келген бөлу белгілі бір белгіге сәйкес жүзеге асырылады-бөлу негізі. Әр бөлімде белгілі бір негізді таңдау адамның материалдық әлемнің объектілерін зерттеу барысында қойған мақсаттарына байланысты. Латенттік қылмыстылықтуралы «кең» түсініктің авторлары мұндай негіз жасалған қылмыс үшін адамның қылмыстық сипатындағы жауапкершіліктің сөзсіздігі принципін атайды. Алайда, сонымен бірге, бұл принцип негіздер мәселесін басқа бағытқа – жазалау мақсаттарына бағыттайтыны негізсіз ұмытылады .

«Криминология ғылымының алдында тұрған мақсаттардың бірі-қылмыс пен оны анықтайтын құбылыстардың алдын алу. Осы мақсатты іске асыру профилактикалық сипаттағы қызметті тиісті ақпараттық қамтамасыз ету болған жағдайда ғана мүмкін болады. Криминологиялық тұрғыдан маңызды ақпараттың ресми көзі-қылмыстарды статистикалық есепке алу жүйесі. Ондағы мәліметтер осы жағымсыз құбылыстармен күресуге бағытталған шараларды әзірлеу жағдайында да, осы күресті жүзеге асыруға шақырылған органдар жүйесін ресурстармен қамтамасыз етуді жоспарлау жағдайында да қолданылады. Тек статистикалық есеп жүйесінде көрсетілген қылмыс туралы толық және сенімді ақпараттың болуы криминологияның мақсаттарын тиімді жүзеге асыруға көмектеседі.

Сонымен, қылмысты «жасырын» және «жасырын емес» деп бөлудің негізі ретінде қылмыстардың статистикалық есеп жүйесінде бұл туралы мәліметтердің болмауы немесе болуы танылуы керек. Осыған сәйкес, осы жүйеде көрініс таппаған нақты қылмыстың бір бөлігі ғана жасырын деп саналуы керек .

Жасырын және жасырын емес қылмыс туралы мәліметтерді біріктіру зерттеушіге қылмыстың нақты көрінісін береді. Егер жасырын қылмысты оны «кең» түсіндіруді жақтаушылар қалай ұсынатынын түсінсе, онда жасырын емес және жасырын қылмыс туралы мәліметтерді біріктірген кезде, нақты қылмыс туралы ақпараттың бұрмалануына әкелетін тіркелген әрекеттер мен сол әрекеттердің қосарланған жиынтығы болады. Сонымен қатар, жасырын қылмысты түсіну арқылы ұғымдарды бөлу ережелері бұзылады, яғни бөлудің кем дегенде екі негізі бар – қылмыстарды тіркеу және ашу. Осылайша, криминология ғылымы шеңберіндегі жасырын қылмыстың «кең» түсіндірмесі қолданылмайды»[8].

Бірақ сонымен бірге, қазіргі кезеңде қылмысты кеңейту әрекеттері – қылмыстық әрекеттер мен оларды жасаған, қылмыстарды жүзеге асыратын адамдардың жиынтығы ретінде пайда болғанын ескерген жөн. Криминология бойынша оқулықта айтылғандай, ред. А.И. Долгова, «қылмыс бізге қылмыстық іс-әрекеттің фактілері ретінде ғана емес, ол өзін қылмыс жасаған адамдардарретінде де көрсетеді. Әрекеттер мен іс-әрекеттердің субъектілерін бөлуге болмайды. Қазір қылмыстың статистикалық есебі адамдар мен фактілер бойынша жүргізілуде. Осы себепті, жасырын қылмыс тіркелмеген әрекеттер мен оларды жасаған адамдардың жиынтығы ретінде анықталуы керек. Бірақ бұл ұғымдар көп деңгейлі болғандықтан, фактілер мен адамдардың кідірісін бөлек бөлу, жасырын қылмысты «тар» (әрекеттердің кідірісі) және «кең» (адамдар мен әрекеттердің кідірісі) мағынасында анықтау қажет»[2].

Сондай-ақ, 1993 жылғы «Жасырын қылмыс: таным, саясат, стратегия» халықаралық семинарында қабылданған жасырын қылмыстың анықтамасына сыни баға беруге болады. «Жасырын қылмыс дегеніміз-құқық қорғау органдары тіркемеген немесе мәлімделген әрекеттер немесе қылмыстық соттөрелігі жүйесі тарапынан ешқандай іс-әрекеттер қабылданбаған әрекеттер» [3].

Жасырын қылмыс неғұрлым кең ұғымға енеді – тұтастай алғанда қылмыстылық. Осыған байланысты бұл құбылыстың барлық маңызды белгілері жасырын қылмысқа тән. Жасырын қылмыстың табиғатын толық түсіну үшін жұмыстың осы бөлімінде осы белгілерді қарастыру қажет.

Қылмыстылық түсінігі Қазақстан Республикасында қылмысқа қарсы күрес бағдарламасында бекітілген. Бұл құжат қылмыстылықты «белгілі бір аумақта белгілі бір уақыт ішінде жасалған қылмыстық заңмен тыйым салынған әлеуметтік қауіпті әрекеттердің жиынтығын қамтитын әлеуметтік-құқықтық, салыстырмалы түрде жаппай құбылыс» ретінде анықтайды.

Жоғарыда айтылғандай, әрекеттің әлеуметтік қауіптілігі оны қылмыстық заңның шеңберіне енгізуге негіз болып табылады. Бірақ кез-келген жағдайда криминологиялық тұрғыдан қауіпті әрекет қылмыстық-құқықтық бағалауды ала бермейді. Қылмыс субъектілері болып табылмайтын адамдардың әрекеттері қылмыстық болып саналмайды. Бұл ретте мұндай іс – әрекеттер объективті түрде қоғамға қауіпті болып табылады-құқық қорғау органдарының «ресурстарын» алаңдатады, азаматтардың құқықтарын бұзады, қоғамдық қатынастарға зиян келтіреді, өзінің әлеуметтік негізіне ие болады. Бұл әрекеттердің әлеуметтік қауіпті сипаты криминологиялық тақырыптағы әдебиеттерде бірнеше рет атап өтілді. Сонымен қатар, жасөспірімдердің іс-әрекеттері анағұрлым прецедентті, өйткені олар осы субъектілердің әлеуметтік қауіптілігі туралы айтады және әлеуметтік қауіпті қайталанатын әрекеттерді жасауға негіз болады. Жоғарыда баяндалғандар қылмыста болатын сандық және сапалық өзгерістер туралы неғұрлым нақты түсінікке ие болу үшін және осы жағымсыз құбылысқа профилактикалық әсер ету шараларын әзірлеу мақсатында алынған ақпаратты пайдалану үшін осы іс-әрекеттерді мемлекеттің статистикалық есепке алу жүйесінде тіркеуге негіз береді. Бірақ қылмыс ұғымының ресми сенімділігін сақтау үшін мұндай әрекеттерді заңсыз сипаты жоқ әлеуметтік қауіпті деп атаған жөн» [4].

Сонымен, жасырын және құқық қорғау органдары жасырған жасырын қылмыс құрылымында меншікке қарсы қылмыстар (бопсалау, қарақшылық, тонау, ұрлық, алаяқтық), жеке тұлға қарсы қылмыстар (зорлау, ұрып-соғу, денсаулыққа әртүрлі дәрежеде зиян келтіру) басым. Сарапшылардың бағалауына сәйкес жасырын қылмыс құрылымында едәуір үлес «жәбірленушілерсіз қылмыстарға» бөлінеді, оларға экономика саласындағы қылмыстар мен лауазымдық қылмыстар жатқызылуы мүмкін.

Жоғарыда айтылғандарға сәйкес, жасырын қылмыстылықта ауыр емес әрекеттер басым болады деген тұжырым даулы.

Тіркелмеген қылмыстылыққа ауыр емес қылмыстар да және аса ауыр қылмыстар да жатады.

ҚПКсәйкес, «қылмыстық іс қылмыстық іс қозғалғанға дейін алдын – ала тексеру кезінде анықталған жасалған қылмыс туралы дәлелденген мәліметтер болған жағдайда ғана қозғалуы мүмкін. Бұл тексерудің максималды мерзімі 10 күн-жасалған қылмыс туралы ақпарат түскен сәттен бастап. Дәл осы сәттен бастап қылмыстық іс қозғау үшін себеп болуы керек. Осыдан 10 күн өткен соң, жасалған қылмысты жасырын деп тануға негіз бар» [5].

Сонымен, жасырын қылмыс құрамынан екі негіз болған жағдайда алынып тасталуы мүмкін: мемлекеттің статистикалық есеп жүйесінде тіркелу және адамды осы қылмысты жасағаны үшін қылмыстық жауапкершілікке тартудың ескіру мерзімінің аяқталуы. Бұл мерзімдер ҚР Қылмыстық кодексінің 71-бабында белгіленеді және 1 жылдан 15 жылға дейін көрсетіледі. ҚК-нің 71-бабының осы бөлігінде көрсетілген мерзімдер қылмыстың да, оны жасаған адамның да қоғамдық қауіптілігіне байланысты болғандықтан, бұл қылмыстардың кідірісі ол тіркелген кезден бастап, сондай-ақ аталған адам қайтыс болған кезден бастап алынып тасталуға тиіс.

Жасырын қылмыстың бұл ерекшелігі осы құбылыстың кумулятивті немесе жинақтаушы сипаты туралы мәлімдемені анықтайды. «Уақыт өте келе кішігірім қылмыстар одан жойылып, ауыр қылмыстар жиналады. Кішігірім қылмыстарды ауыр қылмыстармен ауыстыру тек ауыр

қылмыстардың ескіру мерзімі болғандықтан ғана болмайды, сонымен қатар жасырын қылмыстардың ауқымы үнемі шамалы толықтырылып отырады».

Жасырын қылмыстың аймақтық ерекшелігіне ұқсас тәуелділіктерін Батыс криминологтары да анықтады. Мысалы, М. Планк атындағы институттың ғылыми-зерттеу криминологиялық тобының жетекші мамандары жүргізген виктимизацияға шолуларында,«жасырын қылмыс деңгейінің аймақтың урбанизация деңгейіне, полиция күштерінің әр түрлі тығыздығына, қылмыс құрылымындағы айырмашылықтарға, онда тұратын азаматтардың мінез-құлқына, олардың менталитетіне қатысты басқа аймақтық және жергілікті сипаттамаларға тәуелділігін көрсетті»[20].

Жасырын қылмыстың аймақтық ерекшелігін бағалау кезінде, көрсетілген факторлардан басқа, қарастырылып отырған аймақта дамыған қылмыстарды тіркеудің нақты тәжірибесін және онымен байланысты факторларды ескерген жөн.

Тіркелген қылмыс сияқты, жасырын қылмыс – бұл өте жаппай құбылыс, яғни сараптамалық бағалаулар бойынша тіркелген қылмыстан бірнеше есе артық.

Тіркелген қылмыстың сандық және сапалық көрсеткіштерін қолдана отырып, жасырын қылмысты да сипаттауға болады.

Жасырын қылмыстың сапалық көрсеткіштеріне қылмыстың деңгейі мен құрылымы кіруі мүмкін.

Жасырын қылмыстың жай-күйі (сапалық-сандық көрсеткіш) белгілі бір уақыт кезеңінде белгілі бір аумақта жасалған тіркелмеген қылмыстардың жалпы санын білдіреді (кумулятивтік кідірісті ескере отырып). Жасырын қылмыстың құрылымы-бұл тіркелмеген, белгілі бір негізде алынған қылмыстар санының арақатынасы.

Жасырын қылмыстың сандық көрсеткіші, барлық қылмыс сияқты, уақыт өте келе оның өзгеруін көрсететін динамика.

Жоғарыда айтылғандардың негізінде жасырын қылмысты «пайда болу мен дамудың белгілі бір ерекшеліктерімен, әлеуметтік және қылмыстық-құқықтық сипатымен, қоғамдық қауіптілігімен сипатталатын, өзінің сапалық және сандық сипаттамалары, уақытша және кеңістіктік шекаралары бар мемлекеттік статистикалық есепке алу жүйесіне кірмеген қылмыстардың жиынтығында сыртқы көрінетін қылмыстың бөлігі» ретінде анықтау керек.

Жасырын қылмыстың құрылымы мен мазмұнын егжей-тегжейлі қарастыру оның түрлерін зерттеуді қажет етеді.

Әдебиет

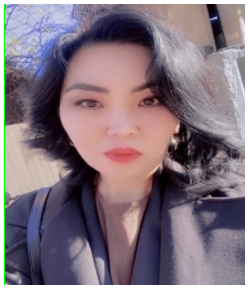
1. Решетников А.Ю. Криминология и предупреждение преступлений: учебное пособие для вузов. – М.: Юрайт, 2021. – С. 83.

2. Карпец И. И. Преступность: иллюзии и реальность. – М., 1992.

3. Джекабаев У.С. О социально-психологических аспектах преступного поведения. Алма-Ата: Наука, 1971.

4. Шелли Дж.Ф. Криминология / Под ред. Дж.Ф. Шелли. СПб. 2003. – С.87

5. Бышевский Ю.В. Латентная преступность и правосознание / Ю.В. Бышевский, А.А. Конев. – Омск, 1986.



ҚҰЛАЖАНОВА АЯЖАН НҮСІПЖАНОВНА
Еуразия технологиялық университеті
Құқық мектебінің аға оқытушысы,
заң ғылымдарының магистры

УСЕНБАЕВА АСЕМГУЛЬ УЗАКБАЕВНА
Еуразия технологиялық университеті
Құқық мектебінің аға оқытушысы,
заң ғылымдарының магистры

ҚҰҚЫҚ ҚОРҒАУ САЛАСЫН ЦИФРЛАНДЫРУ ЖӘНЕ ОНЫҢ АЙҚЫНДЫҒЫН ҚАМТАМАСЫЗ ЕТУ

Қазақстандық қоғамның конституциялық құндылықтарын тиімді және алдын ала қылмыстық-құқықтық қорғауды қамтамасыз ету мақсатында қылмыстық заңнаманы өзектендіруге байланысты жұмысты жалғастыру маңызды болып келеді.

Инновациялық цифрлық технологиялардың қарқынды дамуы жағдайында құқық бұзушылар қылмыстық құқық бұзушылықтар жасаудың жаңа тәсілдерін қолданады, сондай-ақ қоғамдық өмірдің көптеген салалары үшін, оның ішінде кәсіпкерлік қызметтің еркіндігі үшін қосымша қылмыстық қауіптер туындайды, мұны қылмыстық заңнаманы жаңғырту кезінде ескеру қажет.

Азаматтардың конституциялық құқықтары мен бостандықтарын қорғау, қылмыстық қудалауды жүзеге асырудың және соттың сот төрелігін іске асыруының сапасы мәселелері өзекті күйінде қалып отыр.

2023 жылдың 1 қыркүйек күні Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстанның экономикалық бағдары» атты Қазақстан халқына Жолдауында көптеген мәселелерді қамтыды. Жолдауда цифрландыру ісіне және инновацияны енгізу мәселесіне баса мән беру керектігін атап кетті.

Маңызды стратегиялық міндет ретінде – Қазақстанды IT мемлекетке айналдыру, цифрландыру ісінде нақты жетістіктер, электронды үкіметті және финтехті дамыту индексі бойынша әлем көшбасшыларының қатарынан көрініп дамудамыз. Былтырдың өзінде IT саласындағы экспортымыз бес есе өсті. Жыл соңына дейін бұл көрсеткіш 500 миллион долларға жетуі мүмкін.

2026 жылға қарай IT қызметтерінің экспортын бір миллиард долларға жеткізу – Үкіметке жүктелетін жаңа міндет. Шетелдің ірі IT компанияларымен бірлескен кәсіпорындар ашу бұл іске септігін тигізері сөзсіз. Үкімет осы мәселені мұқият зерделеп, нақты ұсыныстар енгізуі керек. Үкімет жасанды интеллектіні дамыту ісіне баса назар аудару қажеттілігі айтылды. Әлемде алдағы бірнеше жылда осы салаға бір триллион доллардан астам инвестиция салынады деген болжам бар. Жасанды интеллект оны дамыта білген елдердің ішкі жалпы өніміне айтарлықтай үлес қосуы мүмкін.

Еліміз есептеу қуаттарын жаһандық тұтынушыларға сататын орынға айнала алады. Сондықтан ірі мәлімет орталықтарын салуға инвестиция тарту үшін түрлі жеңілдіктерді де қамти отырып, барынша қолайлы жағдай жасау керек. Сондай-ақ мәліметті сақтау және өңдеу саласында Қазақстанның мүддесін ілгерілету қажеттігі айтылды.

Цифрландыру ісінде басшылыққа алынатын қағидаттарды заң жүзінде бекіту, Үкіметтен, сарапшылар қауымынан, Парламент депутаттарынан біртұтас салалық құжат әзірлеу мәселесімен айналысу керектігін айтты [1].

Мемлекетте қоғамдық тәртіпті сақтау мәселесінде қылмыстық-атқару жүйесіндегі қайта әлеуметтендірудің маңызы зор. Бүгінгі таңда бұл институт жекелеген жағдайларда заңда белгіленген көмек: медициналық, білім беру, кәсіпті меңгеру, жеңілдіктер мен әлеуметтік төлемдер алу түрлерінің көрсетілмеуіне байланысты проблемалардың болуымен сипатталады [2].

Қоғамның қазіргі заманғы дамуы барабар нормативтік реттеуді талап ететін инновациялық цифрлық технологиялардың күнделікті өмірге жаппай енуімен сипатталады. Жасанды интеллект пен робототехниканы құқықтық реттеу қажеттігі, бірінші кезекте, олардың әрекеттерінен келтірілген зиян үшін жауапкершілікті бөлу мәселесін шешумен, сондай-ақ жасанды интеллектінің көмегімен жасалған туындыларға зияткерлік меншік құқығының тиесілігін анықтау мәселесін шешумен айқындалады.

Қоғамның жеке адамды, қоғамды және мемлекетті қылмыстық қол сұғушылықтардан қорғауға кепілдік беруге қабілетті құқықтық тәртіптің қамтамасыз етілуін объективті қажет етуі және мемлекеттің сыбайлас жемқорлыққа қарсы пәрменді саясаты құқық қорғау органдары қызметкерлерінің әлеуметтік-құқықтық қорғалуын қамтамасыз етудің маңыздылығын айқындайды.

Сот практикасының біркелкілігі мәселесі сот жүйесіне деген сенімді қамтамасыз етудегі түйінді мәселе болып табылады. Соттардың заңдарды біркелкі қолдануы елде бірыңғай әрі тұрақты құқықтық режимді сақтауға, құқықтарды және заңмен қорғалатын мүдделерді тиімді қорғауды қамтамасыз етуге, қабылданатын сот актілерінің сапасын арттыруға мүмкіндік береді.

Сонымен қатар сот практикасының негізсіздігі мен тұрақсыздығы бойынша субъектілердің сот шешімдеріне негізделген сын айтылған өтініштерінің саны бүгінгі таңда азаймай тұр.

Сот арқылы қорғалу құқығы конституциялық құқыққа жатады және оны ешкім, оның ішінде кассациялық іс жүргізуде де шектей алмайды.

Қазақстанның интеграциялық процестерге белсенді қатысуы тұрғысынан халықаралық шарттар жасасу кезінде ұлттық мүдделерді сапалы қорғау сыртқы саяси және сыртқы экономикалық қызметті құқықтық қамтамасыз етудің бірінші кезектегі міндеті болып табылады.

Заңгерлік білім берудің сапасын қалпына келтіру Қазақстанның құқықтық жүйесін орнықты дамытудың қағидатты шарты болып табылады.

Цифрлық технологияларды енгізу мемлекеттік аппараттың жұмысын жеңілдету үшін ғана емес, сонымен қатар, бірінші кезекте, азаматтардың өмір сүруін жақсарту мақсатында жүзеге асырылады. Осы тұрғыдан алғанда, сот жүйесін дамыту бірінші кезектегі мәселе. Сот төрелігіне қол жеткізуді оңайлату және соттарда клиентке бағдарланған тәсілді енгізу жөніндегі шаралар тұрақты негізде қабылдануда.

Сот ғимараттарында 265 фронт-офис жұмыс істейді. Халыққа кедергісіз қызмет көрсетудің қазіргі заманғы стандарттарын ескере отырып, олар ақпараттық орталығы, кіріс кеңсесі мен өзіне-өзі қызмет көрсету аймақтары, медиаторлар мен адвокаттардың жеке кабинеттері, сондай-ақ іс материалдарымен танысуға арналған кабинеттері бар кең залдармен қамтылған.

Сот ісін жүргізуді оңайлату, сот төрелігінің қолжетімділігі мен ашықтығын арттыру, судьялар үшін зерделі көмекшілерді енгізу жөнінде шаралар қабылдануда.

Соттарға қол жеткізудің бірыңғай терезесі – «Сот кабинеті» ақпараттық сервисі 2014 жылдан бастап, оның ішінде ол мобильді нұсқада жұмыс істейді. Пайдаланушылар үйден немесе кеңседен шықпай-ақ, сотқа электрондық форматта жүгіне, мемлекеттік бажды төлей,

сот құжаттарымен таныса, сот отырысының хаттамасын беру туралы өтініш немесе сот отырысының хаттамасына және басқаларына ескерту бере алады.

Жүйеде сотқа дайын талап-арыз автоматты түрде берілетін атқарым енгізілді. Даулардың үш санаты (еңбек, мұрагерлік, некені бұзу, сатып алу-сату шарттары бойынша, жеткізу шарттары бойынша, қарыз шарттары бойынша, жалдау шарттары бойынша) бойынша өтініштердің онлайн-конструкторлары іске асырылды. Сот отырысы басталғанға дейін, азаматтық іс тараптары арасында онлайн-әңгімелесу мүмкіндігі көзделген.

Елдегі барлық сот залдары сот отырысының барысын тіркеуді қамтамасыз ететін заманауи аудио, бейне-жазба жүйелерімен жабдықталған, олар сот процестерінің 96,8%-ы бойынша қолданылды.

Соттарда сот отырыстарының электрондық залдары жасалды. Судьяның және тараптардың әрқайсысының өздерінің автоматтандырылған жұмыс орындары бар. Олар арқылы өтініштер, «цифрланған» дәлелдемелер және басқа да құжаттармен өзара алмасу жүзеге асырылады. Артықшықшылықтары айқын – процестегі кедергілерді азайту, ақпаратты өңдеу жылдамдығын арттыру, процестердің ұзақтығын қысқарту.

Сот ісін жүргізуді цифрландыру шеңберінде «SMART – судьяның көмекшісі» IT-өнімі жасалды. Судьяның қарауын талап етпейтін, даусыз істер бойынша сот актілерінің жобаларын бағдарламаның өзі дайындайды.

Мысалға, жүйе шығуға тыйым салу туралы, шартты түрде мерзімінен бұрын босату туралы, санкция беру және тағы басқалар туралы сот актісінің жобасын тіркейді және дайындайды. Судьяның қатысуы тек құжатты тексеруді және оған электрондық қол қоюды білдіреді.

Сот төрелігіне қолжетімділікті қамтамасыз етумен қатар, барлық мемлекеттік органдардың айқындығы мен ашықтығы қамтамасыз етіледі. Мемлекет басшысының тапсырмасын орындау үшін, орталық атқарушы органдар басшыларының халықпен кездесуінің жаңа форматы енгізілді. Осы өзгерістерге дейін кездесулер жылына бір рет және тек Астанада өткізілді. Енді министрлер өңірлерге тікелей – облыс орталықтарына ғана емес, сонымен қатар аудандарға да баратын болады. Бұл қамтуды кеңейтуге және көптеген мәселелерді «орнында» шешуге мүмкіндік берді (2022 жылы министрлер халықпен 213 кездесу өткізді).

Әкімшілік-рәсімдік-процестік кодексті және «Халық үніне құлақ асатын мемлекет» тұжырымдамасын іске асыру шеңберінде, «e-Otinish» ақпараттық жүйесі өнеркәсіптік пайдалануға енгізілді, ол өтініштерді қарау процесінің айқындығын қамтамасыз етуге және сервистік тәсілді арттыруға бағытталған (бүгінде 25 мыңнан астам әкімшілік органдар мен ведомстволық бағынысты және құрылымдық 26 мың бөлімшеде енгізілген) [3].

Құқық қорғау саласын цифрландыру және оның айқындығын қамтамасыз ету жалғасуда. Бас прокуратураның деректері бойынша 2022 жылы қылмыстық істердің 90,8%-ы (226 030 істің 205 270-і) электрондық форматта тергелді, 8,1 млн. электрондық хаттама мен нұсқама толтырылды, бұл әкімшілік материалдардың жалпы санының 88%-ын құрайды.

Мемлекет басшысының тапсырмасын орындау үшін, полицияның пенитенциарлық мекемелері мен қызметтік үй-жайларында, сондай-ақ құқық қорғау органдарының барлық жедел-тергеу бөлімшелерінде жаппай бейне-бақылау енгізілуде.

Бас прокуратура 2022 жылдың қорытындысы бойынша басқа құқық қорғау органдарымен (СЖҚІА, ҚМА, ІІМ) салыстырып-тексеру жүргізді және 26 386 камерадан 22 215 бейне-камераның нақты жұмыс істейтіні, сондай-ақ бейне-бақылау жүйелерімен қамтылмаған 1 483 «көрінбейтін аймақ» анықталды. Анықталған кемшіліктерді жою бойынша шаралар қабылдануда.

Қаржылық мониторинг агенттігі қаржылық мониторинг субъектілері үшін бірыңғай портал енгізді, ол арқылы күдікті және шекті операциялар туралы хабарламалар жіберу, сондай-ақ КЖҚ/ТҚ саласындағы оқыту материалдарына қолжетімділік қамтамасыз етіледі.

Сыбайлас жемқорлық тәуекелдерін азайту мақсатында, «Экономикалық тергеу қызметі» АЖ-да «қолма-қол ақшаға айналдыру» фирмаларының контрагент-компаниялары басшыларының ғимаратқа кіруі туралы ішкі қауіпсіздік бөлімшелерінің, ҚМА тергеу департаментінің және аумақтық департаменттерінің басшылығын хабардар етудің автоматтандырылған тетігі іске асырылды.

Бизнестің адал субъектілерін қылмыстық қудалау шеңберіне негізсіз тартудан қорғау үшін «Бизнесті қорғау» жобасы іске асырылуда, оның шеңберінде ведомстволық бақылау күшейтілді, мүлікке барлық ауыртпалықтарды, тінту мен алуларды есепке алу цифрландырылды.

Талдамалық IT-құралдарының көмегімен құқыққа қарсы іс-әрекеттің өте жоғары тәуекелдері бар субъектілер ғана көзге түседі.

Заң үстемдігі қағидатын сөзсіз қолдану мақсатында, халықаралық бизнестің азаматтық және коммерциялық дауларын жедел шешу үшін ерекше құқықтық режим шеңберінде жұмыс істейтін "Астана" халықаралық қаржы орталығының Тәуелсіз соты құрылды.

Азаматтардың конституциялық құқықтарын сақтау кепілдіктерін күшейтуге, жазалаудың бұлтартпастығына және сыбайлас жемқорлықтың алдын алуға бағытталған қылмыстық процестің үш буынды моделі енгізілуде.

Пенитенциарлық мекемелерде және полицияның қызметтік үй-жайларында, сондай-ақ құқық қорғау органдарының барлық жедел-тергеу бөлімшелерінде жаппай бейне-байқау енгізілуде.

Күнделікті практикада сотқа дейінгі тергеп-тексерудің, әкімшілік іс жүргізудің, тексеру субъектілері мен объектілерін есепке алудың электрондық жүйелері, сондай-ақ «Qamqor» ақпараттық сервисі қолданылады.

Құқық бұзушылардың лауазымды адамдармен тікелей байланысын болдырмайтын «Сергек» жол жүрісін бейне-бақылау практикасын кеңейту құқық қорғау органдарының қызметіндегі сыбайлас жемқорлық тәуекелдерін төмендету үшін цифрландыруды пайдаланудың жарқын мысалы болып табылады.

Құқық қорғау жүйесіне мемлекеттік қызметте қолданылатын рекрутинг стандарттарын енгізу іріктеудің айқындылығын және тиісінше, кадрлардың сапасы мен «тазалығын» қамтамасыз етуге мүмкіндік береді [4].

Құқық қорғау органдары қызметкерлерінің сыбайлас жемқорлық үшін қылмыстық жауапкершілігін күшейтумен қатар, олардың жалақысын арттыру бойынша шаралар қабылданды, сондай-ақ жекелеген санаттарға тұрғын үйді жалға алу және сатып алу шығындарын өтеу көзделген. Қоғамдық бақылауды кеңейту, мемлекеттік органдардың ашықтығын қамтамасыз ету.

Қазақстанда үкіметтік емес ұйымдардың тұтас қатары әрекет ететін қоғамдық бақылау күшейтілді.

Әдебиет

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстанның экономикалық бағдары» атты Қазақстан халқына Жолдауы 2023 жыл 1 қыркүйек.

2. Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасын бекіту туралы Қазақстан Республикасы Президентінің 2021 жылғы 15 қазандағы №674 Жарлығы.

3. Қазақстан Республикасы Президентінің «Сыбайлас жемқорлыққа қарсы іс-қимыл туралы ұлттық баяндаманы дайындау, Қазақстан Республикасының Президентіне енгізу және оны жариялау қағидаларын бекіту туралы» 2015 жылғы 29 желтоқсандағы №154 Жарлығы.

4. Қазақстан Республикасының сыбайлас жемқорлыққа қарсы саясатының 202-2026 жылдарға арналған тұжырымдамасын бекіту және Қазақстан Республикасы Президентінің кейбір жарлықтарына өзгерістер енгізу туралы Қазақстан Республикасы Президентінің 2022 жылғы 2 ақпандағы №802 Жарлығы.

МУРТАЛИМОВ ШОКАН РАМАЗАНОВИЧ
Преподаватель кафедры вооружения и стрельбы Академии Национальной гвардии Республики Казахстан, подполковник, магистр

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА

Основными проблемами цифровизации в уголовно-исполнительной сфере являются проблемы теории и практики. С одной стороны, появление новых видов преступлений, связанных с использованием информационных технологий, требует разработки новых теоретических подходов к их противодействию. Необходимо разрабатывать стратегии и тактики уголовно-исполнительной деятельности, учитывающие специфику цифровых преступлений. [1]

Одна из проблем теории заключается в том, что понятие «цифровое преступление» еще не четко определено в правовой науке и законодательстве. Определение цифровых преступлений и определение границ их ответственности является сложной задачей, так как технологии развиваются быстрыми темпами, и преступники постоянно находят новые способы совершения противоправных действий.

Также важно отметить практические проблемы преследования и наказания за цифровые преступления. Во-первых, киберпреступники часто оперируют из-за границы, что усложняет их выявление и арест. Модернизация системы правосудия и сотрудничество между государствами становятся необходимостью для эффективной борьбы с такими преступлениями.

Во-вторых, сложностью является доказывание виновности в цифровых преступлениях. Они часто происходят без физического контакта между преступником и жертвой, что усложняет сбор доказательств для возбуждения уголовного дела. Необходимо развивать экспертные знания в области информационной безопасности и цифрового следствия.

Кроме того, цифровизация также предоставляет новые возможности для противодействия преступности. Правоохранительные органы используют технологии видеонаблюдения, системы распознавания лиц и голоса, которые помогают в выявлении и расследовании преступлений. Также появляются системы и алгоритмы для анализа больших данных, которые позволяют выявлять закономерности и предсказывать возможные преступления.

Однако, проблемой является то, что цифровые технологии могут нарушать права граждан на конфиденциальность и личную жизнь. Необходим баланс между использованием технологий для противодействия преступности и защитой гражданских прав. Это требует разработки законодательства, которое устанавливало бы четкие рамки использования технологий правоохранительными органами.

Таким образом, цифровизация и информатизация приводят как к новым возможностям для преступников, так и к новым инструментам для борьбы с преступностью. Однако, противодействие цифровым преступлениям требует разработки новых теоретических подходов и практической работы с использованием новых технологий. Важно разрабатывать

законодательство, которое учитывает быстрый темп технологического развития и обеспечивает защиту прав граждан при борьбе с преступностью в цифровой сфере.

Для решения проблемы противодействия преступности в условиях цифровизации и информатизации общества и государства, следует принять комплексный подход, включающий в себя несколько решений.

1. Развитие законодательства: необходимо разрабатывать и внедрять законы и нормативные акты, которые бы четко определяли понятие «цифровое преступление» и устанавливали ответственность за его совершение. Большую роль должна играть международная координация и сотрудничество, так как киберпреступники могут оперировать из разных стран.

2. Укрепление правоохранительных органов: необходимо обеспечить их современными техническими средствами и обучением сотрудников в области кибербезопасности и цифрового следствия. Также важно развивать сотрудничество между правоохранительными органами, как на национальном, так и на международном уровнях.

3. Образование и просвещение: необходимо проводить информационные кампании и обучающие программы, чтобы повысить информационную грамотность и осведомленность населения о цифровой безопасности. Это поможет людям опознавать потенциальные угрозы и принимать меры предосторожности.

4. Развитие технических средств: необходимо продолжать инвестировать в развитие технологий, которые помогут в обнаружении и предотвращении цифровых преступлений. Это может быть разработка системы раннего предупреждения, специализированных алгоритмов для анализа данных или улучшение систем видеонаблюдения и распознавания лиц.

5. Защита прав граждан: необходимо разрабатывать законодательство, которое будет устанавливать рамки использования технологических средств правоохранительными органами, чтобы не нарушать права граждан на приватность и конфиденциальность. Важно обеспечить баланс между противодействием преступности и защитой гражданских прав.

6. Международное сотрудничество: преступность в цифровой сфере не ограничивается границами одной страны, поэтому важно развивать международное сотрудничество и обмен информацией между правоохранительными органами различных стран. Это позволит эффективно бороться с глобальными киберугрозами и киберпреступностью.

Комплексное решение проблемы противодействия преступности в условиях цифровизации и информатизации общества и государства требует системного подхода и всесторонних мер. Только совместными усилиями государства, правоохранительных органов, образовательных учреждений и общества в целом можно достичь значимого прогресса в борьбе с цифровыми преступлениями и обеспечить безопасность информационного пространства.

Помимо указанных ранее мер, есть несколько дополнительных предложений, которые могут помочь в противодействии преступности в условиях цифровизации и информатизации общества и государства:

7. Сотрудничество с частным сектором: необходимо развивать партнерство и сотрудничество с частными компаниями, особенно в сфере информационных технологий и кибербезопасности. Совместное внедрение новых технологий и обмен информацией может улучшить эффективность борьбы с киберпреступностью.

8. Создание международных стандартов кибербезопасности: необходимо разработать и внедрить международные стандарты и нормативы в области кибербезопасности. Это поможет обеспечить единые требования и подходы к защите информации и противодействию цифровым преступлениям.

9. Развитие кадрового потенциала: важно инвестировать в подготовку кадров в области кибербезопасности и цифрового следствия. Необходимо создавать специализированные образовательные программы, курсы повышения квалификации и центры компетенции,

которые будут готовить профессионалов способных эффективно противодействовать цифровым преступлениям.

10. Активное вовлечение общественности: важно создать механизмы для вовлечения общественности в процесс противодействия цифровой преступности. Это может быть осуществлено через создание специализированных добровольческих групп, проведение образовательных мероприятий и кампаний по повышению осведомленности о цифровой безопасности.

11. Исследования и разработки: государство и научное сообщество должны активно поддерживать исследования и разработки в области кибербезопасности и цифрового следствия. Это поможет в разработке новых технических решений и методов противодействия цифровым преступлениям.

12. Разработка утилит и программного обеспечения для защиты: стимулировать разработку и внедрение программных средств защиты, которые помогут предотвратить цифровые преступления и обнаружить их, если они все же были совершены. Программное обеспечение для обнаружения взломов, защиты персональных данных и предотвращения кибератак должно активно применяться и развиваться.

Комбинированное внедрение данных мер поможет разработать систему, которая будет надежно защищать информацию и обеспечивать безопасность в условиях цифровой среды. Это требует усилий на различных уровнях - от правительственных органов до образовательных учреждений и частных компаний. Только коллективный подход позволит эффективно справиться с угрозами, связанными с цифровой преступностью, и обеспечить безопасность общества и государства.

Литература

1. Гаджиева А.А. Проблемы противодействия коррупции и коррупционной преступности в условиях цифровой и трансформации. Научный журнал: Вестник Алтайской академии экономики и права 2021. - №11 (часть 2). – С. 331-336. (Публикация 09.12.2021 года);

2. Дяблова Ю.Л. Цифровая криминалистика будущее науки или тренд соврменности? Журнал: Известия Тульского Государственного Университета. Экономические и юридические науки. 2021 г. Область наук: Право.

3. Ульянов М.В. Противодействие преступности в сфере информационно-коммуникационных технологий в условиях применения карантинных мер // Национальная безопасность / nota bene. – 2020. – №2. – С. 52-61.

САПАРОВ ЖАНСЕРИК ЖАЙШЫЛЫКОВИЧ

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Ғылыми-зерттеу орталығы, қылмысқа қарсы іс-қимыл және заңнаманы жетілдіру проблемаларын зерттеу бөлімшесінің бастығы, заң ғылымдарының магистрі, полиция подполковнигі

ТМД ЕЛДЕРІ МЕН ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ СТАТИСТИКАЛЫҚ ДЕРЕКТЕРІ ЖӘНЕ АРНАЙЫ ЕСЕПКЕ АЛУ ЖӨНІНДЕГІ ЗАҢНАМАНЫ ТАЛДАУ

Құқықтық жүйенің тиімді жұмыс істеуінің негізгі шарттарының бірі заңнаманың тұрақтылығы болып табылады, оның деңгейін айқындау үшін Қазақстан Республикасының Заңнама және құқықтық ақпарат институты қазақстандық заңнамаға статистикалық талдау жүргізеді.

Адамзат қоғамының дамуы барысында кез-келген мемлекеттің басты міндеттерінің бірі өз азаматтарының құқықтық қауіпсіздігін қамтамасыз ету болды. Өз кезегінде, сенімді статистикалық бақылаусыз азаматтардың құқықтық қауіпсіздігін қамтамасыз ету қиын, кейде мүмкін емес міндет болып табылады. Тәуелсіздік пен қоғамның демократиялануымен қоғамдық процестерді басқару және дұрыс шешімдер қабылдау, соның ішінде алдын-алу және күңгірттікке қарсы тұру үшін сенімді статистикалық ақпарат алу қажеттілігі едәуір өсті. Ресми құқықтық статистика демократиялық қоғамның ақпараттық жүйесінің қажетті элементіне айналды.

Қоғам мен мемлекетті демократияландыру, сондай-ақ қоғамның қазіргі заманғы қажеттіліктеріне сәйкес жүргізілетін құқық қорғау органдарының реформалары құқықтық статистика және арнайы есепке алу жүйесін жетілдіру шеңберінде Қазақстан Республикасы Президентінің 2003 жылғы 28 наурыздағы Жарлығымен уәкілетті мемлекеттік орган болып табылатын Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті (бұдан әрі – Комитет) құрылды құқықтық статистика және арнайы есепке алу саласында [1]. Комитетке құқықтық статистиканы қалыптастыру, арнайы есепке алуды жүргізу және осы салада бақылау мен қадағалауды жүзеге асыру функциялары жүктелді.

Келесі кезең 2003 жылғы желтоқсанда мемлекеттік құқықтық статистиканы жүзеге асырудың және арнайы есепке алуды жүргізудің құқықтық негіздері мен қағидаттарын, Комитеттің өкілеттіктері мен функцияларын айқындаған «мемлекеттік құқықтық статистика және арнайы есепке алу туралы» Қазақстан Республикасының Заңын қабылдау болды. Бұл заңда алғаш рет «мемлекеттік құқықтық статистика», оны «қылмыстық-құқықтық», «азаматтық-құқықтық» және «әкімшілік-құқықтық» статистикаға бөлу, арнайы есепке алудың мақсаты мен түрлері туралы негізгі ұғымдар нормативті түрде бекітілген. Комитет және оның аумақтық бөлімшелері өз құзыреті шегінде құқықтық статистика және арнайы есепке алу саласындағы статистикалық қызметті, оның ішінде – осы саладағы заңдардың қолданылуын қадағалауды жүзеге асырады. Мұндай органның прокуратура жүйесінде болуы құқықтық статистикаға да, прокурорлық қадағалау деңгейіне де әсер етеді, өйткені қадағалау және статистикалық функциялардың өзара әрекеті елдегі қылмыс пен заңдылықтың жай-күйі

туралы объективті көрініс қалыптастыруға ғана емес, сонымен қатар прокурорлық қызметтің барлық салалары бойынша тиімді қадағалауды қамтамасыз етуге мүмкіндік береді.

Елдің бәсекеге қабілеттілігін арттырудың стратегиялық мақсаты қолданыстағы заңнаманы жүйелеу, заңнама салаларын шоғырландыру, оны ескірген және қайталанатын нормалардан босату, құқықтық реттеудегі олқылықтардың орнын толтыру, қолданыстағы құқықтағы ішкі қайшылықтарды жою; заңдардағы анықтамалық нормаларды азайту және тікелей әрекет ететін заңдарды қабылдау практикасын кеңейту және жалпы әлемдік тренд ретінде – заң шығарушы заңдарды цифрландыру және зияткерлендіру бойынша тұрақты шаралар қабылдауды талап етеді.

Заңнамалық немесе өзге де нормативтік құқықтық актілердің тиімділігін арттырудың құқықтық құралдарының бірі құқықтық мониторинг шеңберінде Қазақстан Республикасының Заңнама және құқықтық ақпарат институты жүргізетін статистикалық талдау болуы мүмкін.

Осыған байланысты, жүргізіліп жатқан кешенді ғылыми зерттеулер қолданыстағы заңнаманы жетілдіру жөнінде ғана емес, сонымен қатар анықталған кемшіліктерді жою жөнінде ұсыныстар әзірлеуге, сондай-ақ мемлекеттің дамуының жалпы стратегиясы контекстінде нормативтік құқықтық базаны жаңғыртудың әртүрлі векторлық тәсілдерін талқылауға, оның ішінде нәтижелілік, ашықтық қағидаттарында Мемлекеттік басқарудың сапалы жаңа моделін құру жөнінде диалог алаңын құруға қабілетті азаматтардың құқықтары мен бостандықтарын, қоғам мен мемлекеттің мүдделерін қорғауды қамтамасыз ететін есептілік, қамтамасыз етуге бағытталған.

Жоғарыдағыларды ескере отырып, біз ТМД елдер ішінде олар: Ресей Федерациясы, Қырғызстан Республикасы, Өзбекістан Республикасы, Түркімістан Республикасы және Қазақстан Республикасындағы қолданыстағы «мемлекеттік статистика» туралы Заңы бойынша қысқаша талдау жүргіздік.

Атап айтсақ жоғарыдағы Қазақстан Республасының «мемлекеттік статистика» туралы Заңының 5-ші бабына сйкес мемлекеттік статистика қағидаттары [2], олар:

1) мемлекеттік статистиканың жалпыға бірдей қабылданған халықаралық стандарттармен, сыныптамалармен және әдістермен келісімділігі мен салыстырымдылығы;

2) статистикалық қызметті жүзеге асыру кезіндегі кәсіби тәуелсіздік және дербестік;

3) пайдаланушылардың ресми статистикалық ақпаратқа тең қолжетімділігін қамтамасыз ету;

4) құпиялылық және бастапқы статистикалық деректерді тек статистикалық мақсаттар үшін пайдалану;

5) респонденттердің сапасын, уақтылығын, шығындары мен жүктемесін ескере отырып, ақпарат көздерінің барлық түрлерін пайдалану;

6) ресми статистикалық ақпараттың дұрыстығы, ғылыми негізділігі, уақтылы ұсынылуы және жалпыға қолжетімді болуы;

7) статистикалық ақпараттың, бастапқы статистикалық және әкімшілік деректердің сақталуын және қауіпсіздігін қамтамасыз ету.

Өзбекістан Республикасының 6-бабында [3] және Түркімістан Республикасы 7-бабында [4] ресми статистиканың негізгі принциптері қышқаша нұсқада берілген, олар: тәуелсіздік, айқындық пен ашықтық, дәлдік пен сенімділік, бейтараптық және объективтілік, статистикалық құпиялылық, өзектілігі.

Қырғызстан Рсепубликасының заңнамасы бойынша 5-бап. Ресми статистиканың негізгі принциптері [5], олар:

1) ресми статистиканы өндірушілер статистиканы әзірлеу, өндіру және тарату, оның ішінде пайдаланылатын деректер көздерін, тұжырымдамаларды, анықтамаларды, әдістер мен сыныптамаларды таңдау, сондай-ақ мерзімдер мен мерзімдерді айқындау бойынша өз шешімдерін саяси немесе өзге де сыртқы көздер тарапынан дербес және қандай да бір ықпалсыз және араласусыз қабылдайтынын білдіретін кәсіби тәуелсіздік таратудың барлық түрлерінің мазмұны. Ресми статистиканы өндірушілер өз құзыреті шегінде статистикалық

сұрақтарға және ресми статистиканы дұрыс пайдаланбау фактілеріне көпшілік алдында түсініктеме бере алады;

2) ресми статистика кәсіби стандарттарға сәйкес бейтарап, сенімді және бейтарап түрде әзірленетінін, жүргізілетінін және таратылатынын және саяси мәлімдемелерге немесе пайымдауларға тәуелді болмайтынын білдіретін бейтараптық пен объективтілік. Барлық пайдаланушыларға ресми статистикаға тең және бір уақытта қол жетімділік беріледі;

3) ресми статистика барынша шынайы, дәл және шындыққа сәйкес келетін ақпаратты көрсететінін, сондай-ақ оны өндіру мен таратудың көздерін, әдістері мен рәсімдерін таңдауға қолданылатын ғылыми өлшемдерге сүйенетінін білдіретін дәлдік пен сенімділік;

4) ресми статистиканың халықаралық деңгейде, уақыт бойынша динамикада және өңірлер мен елдер бойынша бөліністе келісілген және салыстырмалы сипатқа ие екендігін білдіретін келісімділік пен салыстырмалылық;

5) ресми статистика анық және түсінікті түрде ұсынылатынын білдіретін айқындық пен ашықтық. Қолданылатын әдістер мен процедуралар пайдаланушылардың назарына ашық түрде жеткізіледі, бұл деректердің дұрыс түсіндірілуін қамтамасыз етеді;

6) ресми статистика өндірушілері жинаған немесе алған және жеке немесе заңды тұлғаларға жататын жеке деректердің қатаң құпиялылығын білдіретін статистикалық құпиялылықты және статистикалық мақсаттарда айрықша пайдалануды, сондай-ақ мұндай деректерді тек статистикалық мақсаттарда пайдалануды көздейді;

7) ресми статистиканың пайдаланушылардың ағымдағы және болашақ қажеттіліктеріне сәйкестік дәрежесін, сондай-ақ азаматтардың жалпыға қолжетімді ақпарат алу құқығын сақтауды көздейтін өзектілігі.

Ресей Федерациясында 4-бап, ресми статистикалық есеп принциптері және мемлекеттік статистика жүйелері деп көрсетілген [6]:

1) толықтығы, дұрыстығы, ғылыми негізділігі, уақтылы ұсынылуы және ресми статистикалық ақпараттың жалпыға қол жетімділігі (ақпаратты қоспағанда, федералды заңдармен шектелген қол жетімділік);

2) ғылыми негізделген ресми статистикалық әдіснаманы қолдану, халықаралық стандарттар мен ресми статистика қағидаттарына сәйкес сондай-ақ, Ресей Федерациясының заңнамасында мұндай ашықтық пен қол жетімділік әдістеме;

3) ресми статистиканы қалыптастыру мақсатында көздерді ұтымды таңдау оның толықтығын, дұрыстығын және уақтылығын қамтамасыз ету үшін ақпарат беру, сондай-ақ респонденттерге жүктемені азайту мақсатында;

4) ресми статистикалық ақпаратты қалыптастыру мүмкіндігін қамтамасыз ету жалпы Ресей Федерациясы, Ресей Федерациясының субъектілері бойынша, муниципалды білім беру;

5) жүзеге асыру кезінде бастапқы статистикалық деректердің құпиялылығын қамтамасыз ету ресми статистикалық есепке алу және оларды қалыптастыру мақсатында пайдалану ресми статистикалық ақпарат;

6) ресми статистикалық есепке алу субъектілерінің іс-әрекеттерінің келісімділігі;

7) ақпараттық технологияларды пайдалану кезінде бірыңғай стандарттарды техникалық-экономикалық және әлеуметтік ақпараттың бүкілресейлік жіктеуіштері мемлекеттік статистика жүйесін оның үйлесімділігі мақсатында құру және пайдалану туралы басқа мемлекеттік ақпараттық жүйелермен қолдану;

8) ресми статистикалық ақпараттың сақталуын және қауіпсіздігін қамтамасыз ету, бастапқы статистикалық деректер мен әкімшілік деректер.

Қарап отырсақ әрине барлығының қағидалары заңға сәйкес, ккей біреулердінде қысқаша нұсқада берілген, кей біреулерінде арине адам санының көптігіне байланысты немесе басқада мәселелерге байланысты толық көлемде жазылған.

Келесі Қазақстан Республикасы заңнамасының 23-бабы статистикалық жіктеуіштер мен регистрлерге тоқталсақ, онда статистикалық бизнес-тіркелім, халықтың статистикалық тіркелімі, ауыл шаруашылығы статистикалық тіркелімі және тұрғын үй қорының

статистикалық тіркелімі болып негізгі төрт тіркелімнен тұрады [2], ал Қырғызстан Республикасы 20-бабында статистикалық регистрлері – ұлттық статистика комитеті статистикалық регистрлерді тек статистикалық мақсаттарда пайдалану үшін құрылып және жүргізе алады, бұл жерде яғни нақты көрсетпеген қай салада екенің көсертпеген [5].

Өзбекістан Республикасының заңнамасында 10-бап. Статистикалық кеңес – деп аталады, ол статистикалық кеңес уәкілетті мемлекеттік орган жанындағы ресми статистиканы дамыту, оның жұмыс істеуі және үйлестіру мәселелері жөніндегі алқалы кеңесші орган болып табылады. Статистикалық кеңестің құрамы мемлекеттік басқару органдарының, ғылыми-зерттеу ұйымдарының, мемлекеттік емес коммерциялық емес ұйымдардың өкілдері, сондай-ақ Статистика жөніндегі ұлттық сарапшылар қатарынан құрылады. Статистикалық кеңестің құрамын Өзбекстан Республикасының Президенті бекітеді. Статистикалық кеңестің жұмыс органы уәкілетті мемлекеттік органның тиісті бөлімшесі болып табылады [3].

Қырғызстан Республикасы заңнамасының 10-бабы, яғни статистика кеңесі, статистика жөніндегі кеңес ресми статистика өндірушілеріне стратегиялық сипаттағы ұсынымдар әзірлеу жөніндегі функцияларды жүзеге асыратын консультативтік кеңесші орган болып табылады [5]. Бұнда да президент кеңес мүшелерін тағайындайды, бірақ Өзбекістан Республикасының заңына қарағанда нақты статистикалық кеңестің принцептері көрсетілген [3].

Түркіместан Республикасы заңнамасының 12-бабында ведомствоаралық кеңес – деп көрсетілген. Оның негізгі функциялары, ол статистикалық қызметті үйлестіру, ведомствоаралық қызметті реттеу үшін, әдістеме және мемлекеттік статистиканы ұйымдастыру, талқылау және органдар өкілдерінің арасынан ведомстволық статистиканы жүргізу жоспарларын келісу. Ол министрліктер мен ведомстволар, ғылыми және өзге де ведомствоаралық кеңес мекемелерден құрылады. Ол кеңесші орган. Ведомствоаралық кеңес туралы ережені Түркіменстан министрлер кабинеті бекітеді [4]. Қарап отырсақ Қырғызстан және Өзбекістан Республикаларында кеңес мүшелерінің құрылуы мен жұмысын президент бекітсе, Түркіменистанда министр кабинеті бекітеді екен. Ал Ресей Федерациясы мен Қазақстан Республикасы заңнамаларында бұндай бап көрсетілмеген.

Құқық теориясы мен практикасына сәйкес заңнамалық актінің сапасы оның мазмұнымен анықталады. Оның сапасының сыртқы көрінісінің белгілерінің бірі заңның тұрақтылығы.

Жүргізілген талдау көрсеткендей, ТМД елдері мен Қазақстан Республикасындағы мемлекеттік статистика туралы Заңдарын салытсру арқылы кейбір өзгерістер бар екенің байқадық. Кей мемлекеттердін заңдарында белгілі бір баптарында толығырақ жазылса, кей баптарында қысқаша нұсқада берілген. Сонымен қатар, айтарлық Түркіместан Республикасы заңнамасының 12-бабында ведомствоаралық кеңес – деп көрсетілген. Оның негізгі функциялары, ол статистикалық қызметті үйлестіру, ведомствоаралық қызметті реттеу үшін, әдістеме және мемлекеттік статистиканы ұйымдастыру, талқылау және органдар өкілдерінің арасынан ведомстволық статистиканы жүргізу жоспарларын келісу. Ол министрліктер мен ведомстволар, ғылыми және өзге де ведомствоаралық кеңес мекемелерден құрылады. Ол кеңесші орган. Ведомствоаралық кеңес туралы ережені Түркіменстан министрлер кабинеті бекітеді [4]. Қарап отырсақ Қырғызстан және Өзбекістан Республикаларында кеңес мүшелерінің құрылуы мен жұмысын Президент бекітсе, Түркіменистанда министр кабинеті бекітеді екен. Ал Ресей Федерациясы мен Қазақстан Республикасы заңнамаларында бұндай бап көрсетілмеген.

Әрине аталған Қазақстан Республикасының «мемлекеттік статистика» туралы заңға өзгерістер мен толықтырулар енгізу сонымен қатар осы сала бойынша заңнаманы жетілдіру жұмыстары жүргізіліп отырады. Ол үшін осы бағытта әлде шешілмеген мәселелер бойынша ғылыми-зерттеу жұмыстары терең жүргізілу керек деп есептейміз.

Әдебиет

1. Қазақстан Республикасы Президентінің 2003 жылғы 28 наурыздағы №1050 Жарлығы инетернет ресурс – https://adilet.zan.kz/kaz/docs/U1100000105 (соңғы қаралым 11.08.2023ж.).

2. «Мемлекеттік статистика» туралы Қазақстан Республикасының 2010 жылғы 19 наурыздағы №257-IV Заңы инетернет ресурс – https://adilet.zan.kz/rus/docs/Z100000257_ (соңғы қаралым 11.08.2023ж.).

3. Өзбекстан Республикасының «ресми статистика» туралы Заңы 2021 жылғы 7 мамырда қабылдады. инетернет ресурс - https://lex.uz/ru/docs/5569612 (соңғы қаралым 11.08.2023ж.).

4. Түркіменстан Республикасының «статистика» туралы Заңы 2012 жылғы 31 наурыздағы №288-IV инетернет ресурс – https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/93953/110083/F1462588494/TKM93953.pdf (соңғы қаралым 11.08.2023ж.).

5. Қырғыз Республикасының «мемлекеттік статистика» туралы Заңы 2007 жылғы 2 ақпан инетернет ресурс - http://www.stat.kg/rus/rule.htm (соңғы қаралым 11.08.2023ж.).

6. «Ресей Федерациясындағы ресми статистикалық есеп және мемлекеттік статистика жүйесі туралы» 2007.11.29 N 282-ФЗ Федералдық заңы инетернет ресурс – https://www.consultant.ru/document/cons_doc_LAW_72844/ (соңғы қаралым 11.08.2023ж.).

7. Қазақстан Республикасының Конституциясы 1995 жылғы 30 тамыз инетернет ресурс – http://adilet.zan.kz/rus/docs/K950001000 (соңғы қаралым 11.08.2023ж.).

8. О государственной правовой статистике и специальных учетах: Закон Республики Казахстан от 22 декабря 2003 года №510 инетернет ресурс http://adilet.zan.kz/rus/docs/Z030000510 (соңғы қаралым 11.08.2023ж.).

ШИДЕМОВ АЗАМАТ ГАРИФУЛЛАЕВИЧ
Старший научный сотрудник Научно-исследовательского центра
Алматинской академии МВД Республики Казахстан, майор полиции

ОСОБЕННОСТИ ВЕДЕНИЯ СТАТИСТИЧЕСКИХ УЧЕТОВ

Правовая статистика представляет собой отрасль статистической науки, изучающую количественные показатели деятельности правоохранительных органов и органов юстиции [1], а также правовые процессы и противоправные действия в обществе. В узком смысле правовая статистика исследует с количественной стороны массовые общественные явления, отражая происходящие в этой сфере процессы в виде количественных закономерностей жизни общества в конкретных условиях места и времени [2].

При правильной организации наблюдения государственный единый статистический учет дает достаточно точные результаты, которые можно считать статистически достоверными. К сожалению, правовая статистика не всегда содержит полную и достоверную информацию. Можно выделить ряд обстоятельств, которые непосредственно влияют на качество статистических данных о преступности, а также на их соответствие реальному положению дел в конкретной области, и, в целом, они представляют собой комплексный и недостаточно изученный результат взаимодействия многих переменных, относительно самостоятельных, но разных по своему значению:

– скрытность преступлений от органов, ведущих борьбу с преступностью (в этом состоит смысл латентной преступности);

– уголовный закон, определяющий составы преступлений и юридически значимые признаки;

– круг преступлений и преступников, подлежащих учету;

– результативность деятельности органов, реализующих государственные меры социального контроля, в первую очередь правоохранительных, непосредственно ведущих борьбу с преступностью.

Исходя из вышесказанного, наиболее актуальным вопросом обеспечения полноты и достоверности криминологических показателей в правовой статистике является определение круга подлежащих учету преступлений и преступников, а также оценка контролирующими органами результативности деятельности правоохранительных органов. Решение данной проблемы определяет научную новизну проведенного исследования: на современном этапе необходимо внедрение единого государственного статистического учета, а именно – Государственной автоматизированной системы правовой статистики, которая будет способствовать наличию более полной и достоверной информации о ее качественных и количественных показателях. В данный момент все статистические данные направляются в Комитет по правовой статистике и специальным учетам при Генеральной прокуратуре Республики Казахстан.

Для начала следует определить, какие криминологические показатели подлежат статистическому учету. Криминологические исследования преступности правовой статистики основываются на данных правовой статистики, а именно – совокупности качественных и количественных показателей, характеризующих уровень преступности, массу совершаемых

преступлений, их причин, а также противодействия, оказываемого преступности со стороны общества. В частности, большинство опубликованных криминологических исследований преступности и отдельных ее видов начинаются с оценки такого признака, как уровень преступности [3; с. 11], при этом, содержание данного показателя характеризует распространенность преступности и определяется общим количеством совершенных преступлений, а также числом лиц, их совершивших на определенной территории за конкретный период времени. Следующий криминологический показатель – масса совершаемых преступлений, или преступное множество. Он отображается при помощи абсолютных (индексы) и относительных (коэффициенты) показателей. Общий индекс зарегистрированных преступлений представляет собой их сумму за определенный период времени (месяц, квартал, год и т.д.).

Наряду с общим индексом употребляется также индекс преступлений, представляющих в конкретный момент времени наиболее актуальную проблему, для оценки определенной ситуации либо в отдельном регионе, либо в их совокупности. Актуальный индекс преступлений в Казахстана, несомненно, должен охватывать такие преступления, как убийство, умышленное причинение тяжкого вреда здоровью, изнасилование, бандитизм, разбой, грабеж, нарушение неприкосновенности жилища, кража, вымогательство, неправомерное завладение автомобилем или иным транспортным средством без цели хищения, терроризм, захват заложника, бандитизм, а также преступления, связанные с незаконным оборотом оружия и наркотиков, при этом данный перечень не является исчерпывающим, находясь в прямой зависимости от криминогенной обстановки в стране. Индекс зарегистрированных преступлений дополняется индексом выявленных лиц, совершивших преступления.

Коэффициент преступного множества показывает соотношение между количеством преступлений либо лиц, совершивших преступление, и численностью населения.

Состав (структура) преступного множества отражает долю в нем различных видов преступного поведения, выделяемых по разным основаниям. Состав преступного множества представляет соотношение видов преступного поведения, различных категорий лиц, совершающих преступления, их характеристики: демографическую (пол, возраст), уголовно-правовую (судимость, опыт отбывания того или иного вида уголовного наказания), социально-экономическую (принадлежность к определенному общественному строю) и иные.

Динамика преступного множества – это изменение его во времени, чаще в иллюстрированной при помощи динамических рядов преступного множества за ряд лет форме. Для характеристики причин воспроизводства преступлений используют различные показатели экономической, социальной и демографической статистики, отражающие обострение противоречий и кризисные явления в соответствующих сферах.

Показателями организации противодействия государства преступности служат затраты на социальную помощь лицам, оказавшимся жертвами преступления, на социальную реабилитацию людей, совершивших преступление, и потенциальных преступников.

В обобщенном виде процесс исследования криминологических показателей состоит из следующих этапов: подготовка наблюдения, проведение массового сбора данных, подготовка данных к автоматизированной обработке, подготовка предложений по совершенствованию статистического наблюдения на основе полученных результатов.

Точностью статистического наблюдения называют степень соответствия действительной величине какого-либо показателя или признака, полученного по материалам наблюдения. Расхождение между результатом наблюдения и истинным значением величины наблюдаемого явления называется ошибкой наблюдения.

По своему характеру ошибки делятся на случайные и систематические; по стадиям возникновения различают: ошибки регистрации; ошибки, возникающие в ходе подготовки данных к машинной обработке; ошибки, появляющиеся в процессе компьютерной обработки.

Отдельно выделяют преднамеренные ошибки, возникающие из-за сознательного искажения данных.

Для минимизации любого рода ошибок в государственном едином статистическом учете нужна четкая и слаженная система контроля за формированием и обработкой в правоохранительных органах документов первичного учета в сфере правовой статистики, а также результативностью их деятельности. Основными видами контроля достоверности и полноты криминологических показателей статистического учета являются синтаксический (означает проверку правильности структуры документа, наличия необходимых и обязательных реквизитов, полноты заполнения строк формуляров в соответствии с установленными правилами), логический (проверяются правильность записи кодов, соответствие их наименованиям и значениям показателей, выполняется проверка необходимых взаимосвязей между показателями, сопоставляются ответы на различные вопросы и выявляются несовместимые сочетания) и арифметический (сравнивают полученные итоги с предварительно подсчитанными контрольными суммами по строкам и по графам) [3].

В целях обеспечения качества и достоверности государственных статистических отчетов, характеризующих деятельность правоохранительных органов, контролирующие органы обязаны вести учет выполненной работы. Исходя из вышесказанного, основной проблемой обеспечения достоверности и полноты криминологических показателей является отсутствие специализированной системы единого статистического учета, необходимой для контроля за формированием и обработкой в правоохранительных органах документов первичного учета в сфере правовой статистики, а также результативностью их деятельности. Однако, первые шаги на пути к созданию такой системы уже сделаны.

Таким образом, введение государственной автоматизированной системы правовой статистики обозначит переход на новый уровень достоверности и полноты данных при формировании государственного единого статистического учета криминологических показателей.

Литература

1. Лунев В. В. «Юридическая статистика», – М. Юристъ. 2007.
2. Воронцова О. Р. Правовая статистика. Теоретическая часть: учебно- методическое пособие / О.Р. Воронцова, О.Б. Садовская. – Кострома: Изд-во Костромского гос. технол. ун-та, 2012. – С. 43.

БАЙТЕЛЕНОВА САМАЛ ГАЛЫМОВНА
Научный сотрудник Центра по исследованию проблем уголовной политики и профилактики преступности Научно-исследовательского института Карагандинской академии МВД Республики Казахстан им. Б.Бейсенова

ОСОБЕННОСТИ ПРОИЗВОДСТВА ЗВУКО-, ВИДЕОЗАПИСИ ПРИ ПРОВЕДЕНИИ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

В условиях всеобщей цифровизации процессов происходит трансформация правоохранительной деятельности, в частности стадии досудебного производства.

Глобальные преобразования не могли обойти стороной и Республику Казахстан. Наше государство уделяет большое внимание внедрению иновационных технологий в работу правоохранительных органов. В системе запущен процесс дебюрократизации, преследующий цели повышения эффективности и оперативности принятия решений, исключения излишней законодательной регламентации деятельности исполнительной власти, сокращения документооборота и отчетности.

Применительно к непосредственной деятельности органов досудебного расследования МВД Республики Казахстан дебюрократизация определяет следующие принципы:

– цифровизация – приоритет всестороннего взаимодействия государственных органов с гражданами, бизнесом и между собой в цифровом формате;

– непрерывное совершенствование – формирование и поддержание организационной культуры государственного аппарата, стимулирующей сокращение бюрократии, системный реинжиниринг и оптимизацию внутренних процедур и процессов [1].

В деятельности органов досудебного расследования МВД Республики Казахстан дебюрократизация через элементы цифровизации позволит оптимизировать все процессы в системе (электронный формат досудебного расследования, применение видео-конференц-связи, проведения дистанционных следственных действий). В этой связи целесообразным является и внедрение видеоформата отдельных следственных действий.

Так, 17 марта 2023 года в часть 3 статьи 199 УПК Республики Казахстан было внесено дополнение: «В случае полного фиксирования хода и результатов следственного действия с помощью средств звуко-, видеозаписи лицо, производящее следственное действие, вправе ограничиться кратким изложением полученных фактических данных и установленных обстоятельств, имеющих значение для дела» [2].

Под видеоформатом следственного действия понимается полное фиксирование хода и результатов следственного действия с помощью средств звуко, видеозаписи, без необходимости подробного описания в бумажном протоколе, где звуко-, видеозапись будет являться основной формой фиксации.

Согласно ст. 199 Уголовно-процессуального кодекса Республики Казахстан обязательным способом фиксации хода и результатов любого следственного действия является его протоколирование, однако по полноте и точности никакое словесное описание не может сравниться с хорошо выполненной звуко-, видеозаписью. Применение звуко-, видеозаписи является одним из самых современных способов фиксации информации и имеет ряд преимуществ.

Применение звуко-, видеозаписи в следственных действиях позволяет:

– повысить качество выполнения функциональных обязанностей лиц, осуществляющих досудебное производство (возможность фиксации звуковой и зрительной информации; возможность фиксации эмоционального состояния запечатленных лиц; возможность останавливать видеозапись на каком – либо кадре для рассмотрения его деталей (стоп–кадр), возможность замедлить движение кадра при просмотре для детального анализа и изучить элементы движения объекта, человека, транспортного средства и т.д.);

– исключить факты фальсификации и превышения должностных полномочий (высокая достоверность информации, предоставленной на видеозаписи);

– сократить сроки досудебного расследования за счет экономии времени, затрачиваемого на составление протокола следственного действия.

К тому же, звуко-, видеозапись следственных действий выступает дополнительной гарантией прав и законных интересов лиц, вовлеченных в уголовное судопроизводство.

При применении видеосъемки должен соблюдаться ряд требований:

1) в ходе следственного действия, звуко-, видеозаписи могут проводиться лицом, ведущим досудебное производство либо с привлечением специалиста, но под контролем и руководством лица, ведущего досудебное производство;

2) все объекты, предметы, вещественные доказательства должны фиксироваться в их первоначальном виде, внешние изменения перед съемкой недопустимы;

3) произведенные звуко-, видеозаписи не подлежат монтажу, ретушированию, удалению некачественных участков съемки и т.п.;

4) все участники следственного действия перед началом производства звуко-, видеозаписи следственного действия должны быть уведомлены об этом (участникам должен быть задан вопрос о наличии замечаний, возражений); об уведомлении участников, о поступивших либо не поступивших замечаниях, возражениях по поводу производства звуко-, видеозаписи должно быть отмечено в протоколе.

При производстве следственных действий с использованием технических средств звуко-, видеозаписи особо важна внимательная и качественная проработка каждой из указанных стадий (т.к. звуко-, видеофиксация следственного действия производится единовременно, непрерывно, без возможности внесения корректировок, поправок).

Звуко-, видеофиксация следственного действия осуществляется с момента его начала и до момента окончания.

В случае применения технических средств звуко-, видеофиксации следственного действия, привлечение понятых не обязательно (за исключением случаев, предусмотренных частью 6 статьи 197 УПК Республики Казахстан).

При подготовке к следственному действию осуществляется проверка исправности и техническая подготовка научно-технических средств (как правило, цифровая видеокамера или иная звуко- видеозаписывающая техника), с помощью которых будет осуществляться звуко-, видеофиксация хода и результатов следственного действия.

Требуется обеспечить наличие необходимого количества заряженных батарей электропитания для видеокамеры, объективов, микрофонных насадок и других необходимых компонентов (с учетом обстановки и условий использования).

Непосредственно перед началом следственного действия все его участники уведомляются о производстве звуко-, видеофиксации следственного действия. При этом участникам следственного действия задается вопрос о наличии замечаний, возражений по данному поводу. О факте данного уведомления участников, поступивших или не поступивших замечаниях, возражениях в кратком протоколе делается соответствующая запись, удостоверяемая подписью каждого участника следственного действия.

Во всех следственных действиях с применением звуко-, видеозаписи вводная часть начинается с фиксации изображения участников следственного действия. Лицо, осуществляющее досудебное расследование, изображается первым, сообщает, какое

проводится следственное действие и по какому делу; затем он просит представиться остальных участников следственного действия и указывает их процессуальный статус. Далее вышеуказанное лицо, находясь в кадре, называет время и место проведения следственного действия и сообщает, кем производится видеосъемка. Если возникают сомнения, владеет ли участник следственного действия языком, на котором ведется производство по делу, выясняется, на каком языке он желает его проведение. В необходимых случаях он обеспечивается бесплатно переводчиком.

Лицо, ведущее досудебное расследование разъясняет участникам следственного действия их права и обязанности, предусмотренные настоящим УПК Республики Казахстан, о чем делается отметка в кратком протоколе.

На этом вводная часть заканчивается, и начинается основная часть, непосредственно само следственное действие

В основной части отражается звуко и видео фиксация хода и результатов следственного действия.

Видеосъемку желательно не прерывать, но это не всегда возможно, например, в случаях, когда необходимо заменить аккумулятор или неблагоприятные погодные условия т.п. В данной ситуации лицо, ведущее досудебное расследование должен сообщить участникам следственного действия о приостановлении, его продолжительности и причинах остановки звуко-, видеозаписи. Причина перерыва фиксируется в кратком протоколе.

Звуко-, видеозапись заканчивается заявлением лица, осуществляющим досудебное расследование об окончании съемки.

В заключительной части, звуко-, видеосъемка останавливается. Участникам следственного действия предоставляется возможность ознакомления, то есть пересмотра записанных следственных действий. В случаях, если у участников имеются дополнения к звуко-, видеозаписи, то они отражаются в кратком протоколе.

Видеозаписи следственных действий будут приобщаться к материалам уголовного дела.

При ведении расследования в бумажном формате, видеозапись будет перезаписываться на DVD-диск или флеш-карту.

При ведении расследования в электронном формате, в случае, наличия технической возможности, видеозаписи будут загружаться в модуль «Е-УД».

Ход и результаты следственного действия с применением звуко-, видеозаписи отражаются в кратком протоколе, который составляется лицом, производящим следственное действие, с соблюдением требований статьи 199 УПК Республики Казахстан.

Данный формат позволит значительно оптимизировать сроки расследования, уголовно-процессуальные процедуры, позволит исключить бюрократическую волокиту, расширит значимость принципа доступности к отправлению правосудия, обеспечит прозрачность в рамках расследования уголовных дел, минимизирует коррупционные риски, а также обеспечит необходимый уровень защищенности должностных лиц, защиту прав и законных интересов участников досудебного расследования.

Литература

1. О мерах по дебюрократизации деятельности государственного аппарата Электронный ресурс – [Режим доступа]: https://adilet.zan.kz/rus/docs/ U2200000872

2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V (с изменениями и дополнениями по состоянию на 24.07.2023 г.) Электронный ресурс – [Режим доступа]: https://adilet.zan.kz

БАПАНОВА ТОГЖАН ТАЛГАТКЫЗЫ
Преподаватель специальных дисциплин ЮКА г. Алматы доктор философии (PhD)

НЕПРАВОМЕРНЫЙ ДОСТУП К ИНФОРМАЦИИ, В ИНФОРМАЦИОННУЮ СИСТЕМУ ИЛИ СЕТЬ ТЕЛЕКОММУНИКАЦИЙ: ОСОБЕННОСТИ КВАЛИФИКАЦИИ

Современное развитие Республики Казахстан сопровождается становлением информационного общества. Высокие технологии повсеместно вошли в человеческую деятельность и постоянно совершенствуется и становится доступным широким слоям общества, появились новые услуги и возможности их реализации, вместе с этим появились и новые виды уголовных правонарушений. Один из них неправомерный доступ к информации, в информационную систему или информационно- коммуникационную сеть, указанный в статье 205 УК РК.

Данная статья гласит:

1. Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере до трехсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот сорока часов, либо арестом на срок до семидесяти пяти суток, с лишением право занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние совершенное в отношении национальных информационных ресурсов или национальной информационный системы, – наказывается штрафом в размере до пятисот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до трехсот часов, либо арестом на срок до девяноста суток, с лишением право занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением право занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового [1].

Информационные и коммуникационные технологии в процессе своего развития широко внедряются в деятельность государственных органов, финансово-экономических институтов. Все большие объемы информации, денежных средств, производственных процессов переносятся в электронную форму. Одновременно с этим становятся актуальными вопросы защиты информационных ресурсов, информационных систем и инфраструктуры связи от

противоправных посягательств, предупреждения использования возможностей этих технологий в преступных целях.

Общественная опасность рассматриваемых в настоящей главе уголовных правонарушений заключается, прежде всего, в том, что они нарушают право и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере.

Информационная безопасность характеризуется как состояние защищенности прав и интересов человека, общества и государства в информационной сфере и отнесена Законом Республики Казахстан от 6 января 2012 г. «О национальной безопасности Республики Казахстан» к одному из видов национальной безопасности [2]. Общественная опасность комментируемого уголовного правонарушения (ч. ч. 1 и 2 – проступки, ч. 3 – преступление) заключается в нарушении право на конфиденциальность информации, ущемлении законных интересов собственников информационных систем и информационно – коммуникационных сетей.

Объектом уголовного правонарушения являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и информационно-коммуникационных сетей.

Предметом данного уголовного правонарушения выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе национальная информационная система; информационно – коммуникационная сеть; национальные электронные информационные ресурсы.

Под информацией следует понимать информацию, хранимую в электронном виде на электронном носителе, представляющую с собой такую последовательность состояний элементов электронной вычислительной техники или иных электронных средств обработки, хранения и передачи информации, которая несет определенные сведения, сообщения, данные. Информация может быть предоставлена в виде цифр, текста, изображения , аудио-, видео-, программного кода или их комбинации. Набор символов, не имеющих смысла и не предназначенных для чего-либо, к информации не относится. К охраняемой законом информации относятся государственные секреты, личная, семейная, служебная, коммерческая, банковская, налоговая, адвокатская, врачебная и иные охраняемые законом тайны, другие конфиденциальные сведения.

Согласно нормативного постановления Конституционного совета РК от 20 августа 2009 г., к охраняемой законом тайне следует относить сведения, не являющиеся общедоступными на равных условиях для неограниченного круга лиц, изначально неизвестные третьим лицам [3].

Конституционное право каждого на тайну подразумевает, что только само лицо, которому принадлежит эта тайна, может распоряжаться ею по своему усмотрению, в том числе передавать эти сведения третьим лицам.

Каждый имеет право отнести любые неизвестные третьим лицам сведения к конфиденциальным, если законом прямо не указывается , что эти сведения являются общедоступными либо могут быть преданы огласке или изъяты а предусмотренном законом порядке.

Согласно Закону Республики Казахстан от 15 марта 1999 г. «О государственных секретах» к государственным секретам относятся сведения, составляющие государственную и служебную тайны [4].

Государственная тайна - это сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.

Служебная тайна – это сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести

ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

Электронными носителями называются любые виды материальных носителей, которые позволяют записывать, хранить и воспроизводить информацию в форматах данных, предназначенных для обработки средствами вычислительной техники. Формат данных может быть цифровым, как правило, бинарным и аналоговым. К электронным носителям следует относить не только постоянные запоминающие устройства – к примеру магнитные и оптические диски магнитные и полупроводниковые карты, но и оперативные запоминающие устройства – к примеру, оперативная память компьютера или иного электронного устройства. Информация, как правило, хранится на электронных носителях виде файлов.

Информация, хранимая в электронном виде в информационных системах, называется электронным информационным ресурсом, или иначе – информационный базой данных. Для электронных информационных ресурсов характерен значительный объем и структурированность данных, их определенное функциональное предназначение.

Информация, хранимая в электронном виде в информационных системах, функционирующих в открытой информационно-коммуникационной сети, относится к Интернет-ресурсом.

Информационная система представляет собой систему, предназначенную для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса.

Согласно статье 15 Законом Республики Казахстан от 11 января 2007 года «Об информатизации» по критериям права собственности и категории доступа информационные системы подразделяются на государственные и негосударственное, общедоступное и ограниченного доступа [5].

Государственными являются информационные системы, создаваемые или приобретаемые за счет бюджетных средств либо полученные ими иным предусмотренными законом способом (дарение, конфискация и другие).

Общедоступными являются информационные системы, содержащие электронные информационные ресурсы, которые предоставляются или распространяются их собственником или владельцем без указания условий их использования, а также электронные информационные ресурсы, доступ к которым является свободным и не зависит от формы их предоставления и способа распространения. Общедоступное информационные системы не являются предметом рассматриваемого уголовного правонарушения.

Все государственные электронные информационные ресурсы являются общедоступными, за исключением отнесенных к государственным секретам и конфиденциальных информационных ресурсов. К категории конфиденциальных электронных информационных ресурсов относятся электронные информационные ресурсы, содержащие персональные данные или охраняемую законом тайну.

К информационным системам ограниченного доступа относятся информационные системы, содержащие электронные информационные ресурсы, доступ к которым ограничен законом Республики Казахстан или их собственником или владельцем в случаях, установленных законодательством Республики Казахстан.

Следовательно, к информационным системам, выступающим предметом рассматриваемого уголовного правонарушения, следует относить:

1. Информационные системы, содержащие государственные электронные информационные ресурсы, отнесенные к государственным секретам;

2. Информационные системы, содержащие конфиденциальные электронные информационные ресурсы, в том числе содержащие персональное данные, охраняемую законом тайну;

3. Иные информационные системы, доступ к которым ограничен их собственником или владельцем.

Информационно-коммуникационная сеть представляет собой совокупность технических и аппаратно-программных средств обеспечения взаимодействия между информационными системами или между их составляющими, а также передачи информационных ресурсов.

Объективная сторона рассматриваемого уголовного правонарушения выражается в неправомерным доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть, в результате которого существенно нарушаются права и законные интересы граждан или организаций либо охраняемые законом интересы общества или государства.

Неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, выражается в получении возможности непосредственного завладения этой информацией и может быть осуществлен как с преодолением мер защиты, установленных собственником (владельцем) электронного носителя, так и без такового.

Неправомерный доступ к информационно-коммуникационной сети выражается в получении возможности непосредственного взаимодействия с входящими в нее информационными системами и их составляющими и также осуществляется, как правило, с преодолением мер защиты.

Доступ осуществляется только программно-техническими средствами.

Выделяются три вида мер защиты: правовые, организационные и технические (программно-технические).

Технические (программно-технические) меры защиты информации, хранящейся на электронном носителе, электронных информационных ресурсов и информационных систем от несанкционированного доступа состоят в установлении технических (программно-технических) средств, реализующих функции контроля доступа (в том числе регистрации фактов доступа, блокирования несанкционированного доступа), шифрования информации.

Преодоление технических или программно-технических мер защиты следует рассматривать как действия непосредственно направленное на совершение данного уголовного правонарушения и также осуществляется только программно-техническими средствами.

Правовые меры защиты выражаются в договорных обязательствах между собственником (владельцем) электронных информационных ресурсов и их пользователями устанавливающих условия доступа и использования этими ресурсами.

Организационные меры защиты могут выражаться в разграничении прав доступа к информации по кругу лиц и характеру информации.

Преодоление правовых и организационных мер защиты следует рассматривать как создание условий для совершения неправомерного доступа.

Ознакомление с охраняемой законом информацией содержащейся на электронном носителе, в момент получения неправомерного доступа к ней либо в любой другой момент для квалификации данного уголовного правонарушения значения не имеет. Виновный может не знакомиться с полученными сведениями, а передать их третьим лицам.

Неправомерный доступ к информационной системе и информационно-коммуникационной сети может осуществляться непосредственно через компьютер (сервер), на котором функционирует информационная система, или компьютер (рабочую станцию), ранее подключенный к информационно-коммуникационный сети.

Неправомерный доступ без преодоления защиты может быть осуществляться через компьютер, на котором открыть доступ (сеанс) лицом, имеющим право на это (администратор, пользователь системы и сети).

Неправомерный доступ может осуществляться удаленно, в том числе через Интернет. Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий.

Вредные последствия выражаются в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общество или

государства, под которым, с учетом положений п. 14) ст. 3 УК РК, раскрывающих понятие существенного вреда, следует понимать, в частности:

−нарушение конституционных прав и свобод человека и гражданина, прав и законных интересов организаций, охраняемых законом интересов общества и государства;

−причинение значительного ущерба (то есть ущерба на сумму, в сто раз превышающую месячный расчетный показатель);

−нарушение нормальной работы организаций или государственных органов.

Между неправомерным доступом и наступившими общественно опасными последствиями должно быть установлена причинная связь.

С субъективной стороны рассматриваемое уголовное правонарушение может быть совершено только умышленно (прямой и косвенный умысел): виновный сознает, что он совершает неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно- коммуникационную сеть, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления.

По отношению к причинению существенного вреда в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства возможен косвенный умысел, когда виновное лицо сознательно допускает эти последствия либо относится к их наступлению безразлично.

Мотивы и цели данного уголовного правонарушения разнообразны и на квалификацию не влияют, но они должны учитываться при индивидуализации наказания. В большинстве случаев это корыстный мотив.

В случае совершения незаконного доступа к охраняемой законом информации, хранящейся на электронном носителе, с целью незаконного собирания сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, деяние образует совокупность и квалифицируется по ст. 205 УК РК и соответствующей части ст. 147 УК РК.

В случае совершения незаконного доступа в информационную систему или информационно- коммуникационную сеть с целью незаконного собирания сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия или незаконного нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений физических лиц, деяние квалифицируется по ч, 3 соответственно ст. 147 или ст. 148 УК РК. Дополнительный квалификации по ст. 205 УК РК не требуется.

В случае совершения незаконного доступа к охраняемой законом информации, хранящейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть с целью незаконного собирания, составляющих государственные секреты, деяние образует совокупность и квалифицируется по ст. 205 и соответствующей части ст. 185 УК РК. Не требуется дополнительный квалификации по ст.205 УК в случаях совершения деяния, предусмотренного ст.223 УК РК (Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну).

Субъектом уголовного правонарушения является физическое вменяемое лицо, достигшее 16-летнего возраста.

В ч.2 ст. 205 УК РК установлена ответственность за неправомерный доступ к национальному электронному информационному ресурсу или национальной информационной системе.

Национальными признаются информационные системы, состоящие из государственных электронных информационных ресурсов, имеющих важное стратегическое значение для экономики и безопасности государства.

В ч. 3 ст. 205 УК Республики Казахстан предусмотрен особо квалифицирующий признак – тяжкие последствия.

С учетом положений п. 4) ст. 3 УК РК к тяжким последствиям необходимо относить, в частности: самоубийство потерпевшего (потерпевшей) или его (ее) близкого (близких);

причинение крупного или особо крупного ущерба. Эти последствия должны находиться в причинной связи я умышленным неправомерным доступом.

Законодатель в ч. 3 ст. 205 УК РК специально указал, что тяжкие последствия должны наступить по неосторожности. Следовательно, по отношению к причинению тяжких последствий возможна только неосторожная форма вины, в виде преступной самонадеянности или преступной небрежности. Совершая умышленный неправомерный доступ, лицо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их наступления. При этом в соответствии со ст. 22 УК РК в целом преступление, предусмотренное ч. 3 ст. 205 УК РК, признается совершенным умышленно.

Подводя итоги, мы можем сказать, что деяния, предусмотренные ч.ч. 1 и 2 ст. 205 УК РК, относятся к уголовным проступкам, деяние, предусмотренное ч. 3 ст. 205 УК РК, относится к преступлениям небольшой тяжести.

Литература

1. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.) [Электронный ресурс] // URL: https://online.zakon.kz/Document/?doc_id=31575252&pos=228;-116#pos=228;-116

2. Закон Республики Казахстан от 06 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» [Электронный ресурс] // URL: https://adilet.zan.kz/rus/docs/Z1200000527

3. Постановление Конституционного совета Республики Казахстан от 20 августа 2009 г. [Электронный ресурс] // URL: https://adilet.zan.kz/rus/docs/S090000005_

4. Закон Республики Казахстан от 15 марта 1999 г. «О государственных секретах» [Электронный ресурс] // URL: https://adilet.zan.kz/rus/docs/Z990000349_

5. Закон Республики Казахстан от 11 января 2007 года «Об информатизации» [Электронный ресурс] // URL: https://online.zakon.kz/Document/?doc_id=30085759

БАПАНОВ МАҒЖАН ТАЛҒАТҰЛЫ
Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции, м.ю.н.

ПУТИ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА В ПРОТИВОДЕЙСТВИИ УГОЛОВНЫМ ПРАВОНАРУШЕНИЯМ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Исследование, эффективное предупреждение и раскрытие уголовных правонарушений, совершаемых с использованием высоких технологий невозможно без изучения их детальной криминологической характеристики.

Под криминологической характеристикой понимается описание свойств, закономерностей, факторов и последствий преступности (отдельного ее рода или вида), а также свойств личности преступника. Говоря об уголовных правонарушениях, совершаемых с использованием высоких технологий, следует изучить личность жертвы и ее виктимологическую характеристику.

Исследование свойств и признаков преступности с использованием высоких технологий достаточно сложно по целому ряду причин. Первой и основной из них является отсутствие в науке единого, устоявшегося терминологического аппарата для данной группы противоправных деяний. Поскольку в настоящее время в УК Республики Казахстан отдельно закреплена только группа уголовных правонарушений в сфере информатизации и связи, официальная статистика располагает только данными анализа этих деяний. Однако, если трактовать явление преступности с использованием высоких технологий как любое противоправное деяние, совершенное с помощью компьютерного устройства, необходимо исследовать значительный круг уголовных правонарушений, как попадающих так и не попадающих под признаки норм, главы 7 УК РК.

«Преступления в сфере компьютерной информации», тогда как деяния, совершаемые с использованием компьютерных технологий, но учтенные по иным статьям, не рассматриваются. Таким образом, криминологи вынуждены для изучения компьютерной преступности, оперировать только данными об уголовных правонарушениях в сфере информатизации и связи, либо использовать неофициальные данные и результаты собственных исследований.

Еще одной причиной является достаточно высокий уровень латентности преступности в целом, в том числе и с использованием компьютерных технологий. Как отмечает В.В. Лунеев, «уровень латентной преступности сегодня составляет 70-80% от реальной преступности «… к судебной уголовной ответственности привлекается только около 5% лиц, реально (а не зарегистрировано) совершивших преступления» [1, с.7]. В статистических данных не отражается большая часть совершенных с использованием компьютерных технологий преступлений. В.Г. Степанов-Егиянц определяет латентность таких преступлений на уровне 85-99%, М.В. Старичков называет уровень латентности порядка 99,7-99,8% [2, с.74-112]. Причинами этого являются как отсутствие должной реакции со стороны потерпевших при совершении в отношении них противоправного деяния, так и скрытый характер многих преступлений с использованием компьютерных технологий. Например, злоумышленник

может скопировать файл с информацией, содержащей охраняемую законом тайну, не оставив следов вмешательства. Таким образом, преступление фактически останется незамеченным.

Кроме того, большинство компьютерных преступлений, совершаются путем выполнения нескольких деяний-эпизодов со сходным составом. Например, преступник взламывает сеть банка и списывает со счетов многих вкладчиков небольшие суммы денег, а официальная статистика в данном случае будет учитывать совершение только одного противоправного деяния.

С учетом практики расследования и появления новых видов уголовных правонарушений в Уголовный кодекс Республики Казахстан была введена глава 7 «Уголовные правонарушения в сфере информатизации и связи», которая содержит 9 составов, в отличие от ранее действовавшего Уголовного кодекса Республики Казахстан (ст.ст.227 и 227-1 УК РК).

Наиболее распространенными видами уголовных правонарушений являются оскорбление, клевета в социальных сетях, незаконный доступ к информации путем распространения вредоносных программ, распространение контрафактных произведений, хищения с использованием информационных технологий.

Так как процесс научной разработки криминалистической характеристики есть частный пример отражения объективных закономерностей преступной деятельности, процесс включения в криминалистическую характеристику того или иного элемента должен быть объективно необходим, закономерен, в связи с чем, обосновывается необходимость включения в криминалистическую характеристику уголовных правонарушений в сфере мобильных телекоммуникаций тех элементов, которые закономерно участвуют в процессе отражения при совершении любого уголовного правонарушения, в частности это признаки, характеризующие способ совершения уголовного правонарушения, типичные последствия его применения, личность предполагаемого преступника, мотивы и цели уголовного правонарушения, место, время и обстановку совершения уголовного правонарушения.

По результатам анализа статичных и статистических связей между элементами криминалистической характеристики делается вывод, что их обоснование возможно на основе системы методов, разработанных и заимствованных криминалистикой приемов и способов, адаптированных к задачам, выполняемым криминалистической характеристикой и направленных на создание научной организации деятельности по дополнению, уточнению и использованию данных включаемых в криминалистическую характеристику.

Все это предопределяет необходимость комплексного и детального изучения вопросов, связанных с регулированием уголовной ответственности за уголовные правонарушения в сфере информатизации и связи.

Мы отмечаем, что отечественная криминологическая наука значительно запаздывает в формировании основных признаков криминологической характеристики уголовных правонарушений в сфере информации и связи. Такое положение не может быть признано нормальным и требует теоретического осмысления.

Формулируя основные составляющие криминологической характеристики уголовных правонарушений в сфере информации и связи, автор опирается на апробированную теоретическую модель, включающую 1) криминологические значимые признаки уголовного правонарушений, 2) данные, раскрывающие криминологическую ситуацию, 3) признаки, определяющие специфику деятельности по предупреждению уголовных правонарушений. К первой группе относятся свойства личности преступника, мотивы и цель уголовного правонарушения, свойства личности потерпевшего. Ко второй – статистика уголовных правонарушений, сведения о социальных условиях уголовных правонарушений. К третьей – причины уголовных правонарушений, последствия уголовных правонарушений, механизм уголовных правонарушений, обстоятельства, способствующие уголовным правонарушениям.

Сфера уголовных правонарушений расширяется по мере развития техники электронной обработки данных, ибо компьютеры все чаще встраиваются в различные виды технической продукции. Соответственно, автор выделяет общий тренд киберпреступности – она

становится в меньшей мере преступностью, связанной с аппаратно-техническими носителями, и в большей мере – с информационными технологиями. Так, в настоящее время термин «компьютерная преступность» (CIBER CRIME) стал включать пост-компьютерную преступность или мультимедийную преступность.

Предлагая криминологическую характеристику киберпреступности, необходимо обратить внимание на содержании способов совершения изучаемых уголовных правонарушений, отмечая, что в отечественной и зарубежной криминологической науке не существует сколько-нибудь определенных понятий в вопросах характеристики способов совершения киберпреступлений, их конкретных названий и классификации. Эта проблема настолько нова для науки, что находится пока лишь в стадии осмысления и теоретических разработок. На основе анализа результатов конкретных уголовных дел по уголовным правонарушениям, совершенным с использованием средств различной техники, а также изучения специальной литературы приходим к выводу, что в качестве основного классифицирующего признака выступает метод использования преступником тех или иных технологических действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями. Соответственно, в зависимости от способа совершения уголовного правонарушения можно сгруппировать следующим образом: изъятие информации; перехват информации; несанкционированный доступ к средствам компьютерной техники; манипуляция данными и управляющими командами; комплексные методы.

В качестве самостоятельной криминологической характеристики уголовного правонарушения определяем ситуацию его совершения, понимая под ней (в криминологическом смысле) систему различного рода взаимодействующих между собой до и в момент совершения уголовного правонарушения объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные, бытовые или иные условия окружающей среды. Ситуация совершения уголовных правонарушений в сфере информатизации и связи характеризуется рядом существенных факторов. Прежде всего, следует указать, что эти уголовные правонарушения совершаются в области профессиональной деятельности. Преступники, как правило, владеют не только специальными навыками в сфере управления ЭВМ и ее устройствами, но и специальными знаниями в области обработки информации в информационных системах в целом, а также необходимыми специальными познаниями в соответствующих финансовых, банковских и подробных информационных технологиях. Все эти уголовные правонарушения всегда связаны с нарушением установленного порядка профессиональной деятельности, о котором лицам становится известно в ходе профессиональной подготовки, и, следовательно, вопросы умысла при оценке этих действий могут решаться почти однозначно.

Следующей криминологической характеристикой уголовных правонарушений является личность преступника, который совершает уголовные правонарушения в сфере информатизации и связи. В специальной юридической литературе по компьютерным уголовным правонарушениям относительно недавно появились термины: «ХАКЕР» – это специалист по компьютерным системам и сетям; «КРЭКЕР» – это хакер, основная цель которого взломать программное обеспечение; «ФРИКЕР» – специалист по незаконному и нестандартному использованию телефонии, которая в настоящее время представляет компьютерную сеть. Возникли соответствующие названия «ХАКИНГ», «КРЭКИНГ», «ФРИКИНГ» – это совокупность специального программного обеспечения и оборудования, требуемого для работы такого рода специалиста.

Важной криминологической характеристикой уголовных правонарушений является мотив совершения уголовного правонарушения. В качестве наиболее распространенных мотивов компьютерных уголовных правонарушений, как показало изучение уголовных дел, являются любопытство или развлечение, авантюризм, попытка добиться расположения кого-либо к себе, поиски признания, самовыражение, месть, вандализм, личная или финансовая

выгода, деньги. В настоящий момент основными мотивами уголовных правонарушений стали получение материальной выгоды.

Зарегистрированная преступность является основным статистическим показателем уголовной статистики, но надо иметь в виду и не учитываемую официальной отчетностью часть преступности. За пределами остается так называемая латентная (скрытая) преступность, определяемая как совокупность уголовных правонарушений, оставшихся не зарегистрированными правоохранительными органами. Она зависит от специфики отдельных уголовных правонарушений, совершаемых в большинстве случаев в условиях не очевидности. Компьютерные уголовные правонарушения относятся к категории максимально латентных, из-за технической сложности их раскрытия.

На современном этапе развития мировой цивилизации отмечается переход от индустриального общества к обществу информационному. Информация становится значимым видом общественных ресурсов, требующим, как и любая другая ценность, принятия соответствующих мер безопасности от неправомерных действий. Этот процесс актуализирует проблему обеспечения информационной безопасности как одной из составляющих национальной безопасности Республики Казахстан. Основными средствами обеспечения информационной безопасности выступают юридические меры, составной частью которых являются уголовно-правовые меры, направленные на ограничение доступности криминальным посягательствам на информационные общественные отношения. Признание социальной ценности информации как основной вектор развития общественных отношений определяет необходимость криминологического анализа проблемы и принятия адекватных мер по реализации информационной безопасности.

Важнейшей проблемой в обеспечении информационной безопасности является проблема защиты информации от неправомерного доступа. Наличие данной проблемы заключается в том, что защите от неправомерного доступа подлежит наиболее ценная охраняемая законом информация, а также в том, что неправомерный доступ к охраняемой законом информации влечет, как правило, значительные общественно опасные последствия, в частности, нарушение ее конфиденциальности, целостности и доступности.

Вместе с тем, современные меры защиты информации от неправомерного доступа основаны на приоритетности защиты информации, находящейся на определенных носителях (компьютерной информации), что, в силу несоответствия данного подхода положениям информационного законодательства, влечет отсутствие четкой системы защиты информации от неправомерного доступа. Данные обстоятельства выступают причиной необходимости разработки криминологических мер защиты в сфере информационных отношений, одной из составляющих которой должен выступить неправомерный доступ к охраняемой законом информации. При этом степень защиты информации должна определяться ее содержанием, а не свойствами носителя.

Все это требует детальной разработки элементов нового общего состава уголовных правонарушений, заключающегося в неправомерном доступе к охраняемой законом информации.

По мнению В.П. Числина «уголовно-правовые меры обеспечения информационной безопасности, в силу наибольшей строгости уголовной ответственности по сравнению с другими видами ответственности, могут быть направлены на защиту от неправомерного доступа не всякой информации, а только информации, охраняемой законом» [3, с. 38-49]. Следовательно, возникает проблема отграничения данного вида информации от иного массива информационных ресурсов, не попадающих в сферу уголовно-правового регулирования.

Неоднозначное представление допускает слишком широкое толкование понятия охраняемой законом информации и включающей туда всю документированную информацию. Основываясь на нормах информационного законодательства, определены критерии отнесения информации к категории охраняемой законом.

Основным криминологическим понятием является понятие детерминации, которая отражает одну из существенных особенностей бытия – всеобщую связь, взаимозависимость и взаимообусловленность предметов, явлений и процессов. По мнению Л.А. Сударевой, «важнейшими детерминантами в сфере компьютерной преступности следует считать: 1) объективные причины и условия, связанные с общим низким культурным и экономическим уровнем развития общества; 2) социально-психологические факторы, которые оказывают воздействие на лиц, совершающих компьютерные преступления: низкий социальный статус; низкая заработная плата; высокий профессиональный уровень» [4, с. 11].

В связи с вышеизложенным, хотим отметить, что необходимо провести систематизацию уголовных правонарушений в сфере информатизации и связи, характерных для Республики Казахстан, уголовные правонарушения по цели их совершения предлагается подразделять на следующие группы:

1) неправомерный доступ в компьютерную сеть Интернет под чужими учетными именами и паролями;

2) использование телефонов-«двойников» мобильной связи;

3) несанкционированный доступ к компьютерной информации для ее:

4) а) копирования; б) модификации; в) уничтожения или блокирования;

5) модификация фискальной памяти электронных контрольно-кассовых машин;

6) хищение денежных средств и материальных ценностей путем неправомерного доступа к компьютерной информации;

7) уничтожение, блокирование или модификация информации, связанные с трудовыми конфликтами;

8) преодоление программно-технических средств защиты программ для ЭВМ с целью их копирования и использования контрафактных экземпляров;

9) распространение вредоносных программ для ЭВМ.

В заключении, можно сказать, что создать абсолютно стойкую систему защиты невозможно, как невозможно создать универсальную систему взлома. Поэтому при использовании системы защиты необходимо четко представлять диапазон ее применимости и ее способность противостоять воздействию злоумышленников разной квалификации и оснащенности. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. Необходимость всестороннего исследования обозначенных проблем диктуется как потребностью следственной практики, так и задачами дальнейшего совершенствования как уголовно-правовой, так и криминалистической теории, усиления их влияния на результативность борьбы с компьютерной преступностью.

Литература

1. Лунеев В.В. Проблемы науки о борьбе с преступностью // Преступление, наказание, исправление, 2008. №2. – С. 7-11.

2. Сафонов О.М. Уголовно - правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: диссертация ... кандидата юридических наук. – Москва, 2015. – С. 222.

3. Числин В.П. Уголовно-правовые меры защиты информации от неправомерного доступа : Дис. ... канд. юрид. наук. – Москва, 2004. – С. 134.

4. Сударева Л.А. Правовое и информационное обеспечение деятельности органов внутренних дел по предупреждению компьютерных преступлений : диссертация ... кандидата юридических наук. – Москва, 2008. – С. 250.

АЙТКЕШ АЙБЕК КАНАТУЛЫ
Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н, м.э.н., капитан полиции

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ПРОБЛЕМЫ ИХ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ

Глобальная цифровизация – это формирование единого информационного пространства, повсеместное внедрение цифровых технологий в разные сферы жизни общества: промышленность, экономику, образование, культуру, медицину, обслуживание и прочее. Благодаря научно- техническому прорыву компьютеры, мобильные телефоны, Интернет, цифровая отправка данных, сообщений, общение в социальных сетях – неотъемлемая часть нашей повседневной жизни. Цифровизация экономики является глобальной тенденцией, которой следуют все страны, нацеленные на развитие конкурентоспособной экономики и улучшение качества жизни. И Казахстан не исключение. Учитывая глобальную цифровизацию бизнеса, это объективно обусловливает и существенный рост количества совершаемых преступлений с использованием цифровых технологий.

В настоящее время экономические преступления, совершаемые с использованием компьютерных или телекоммуникационных технологий, целесообразно выделять в самостоятельную категорию. Это, в частности, хищение безналичных денежных средств, противоправные деяния в отношениикриптовалют, преступления против интеллектуальной собственности и незаконное распространение аудиовизуальных произведений в сети Интернет, незаконная передача информационных ресурсов компаний и персональных данных третьим лицам, использование вредоносных компьютерных программ, преступные деяния в финансово-кредитной сфере и т.п.

Уголовное законодательство разделяет преступления в сфере компьютерной информации и иные деяния, в которых под угрозу ставится информационная безопасность. Однако детализация составов преступлений, учитывая что информация является не только целью преступных посягательств,но и средством их совершения, страдает неспособностью охватить все возможные противоправные деяния и их последствия.

Рассмотрим особенности преступлений с применением компьютерных технологий, а также сложности правоприменительной практики по киберпреступлениям.

Цифровое пространство, в котором совершаются преступления, существенно затрудняет идентификацию правонарушителя, его изобличение и уголовное преследование. Сложность обнаружения действий компьютерного преступника и его возможности совершать преступления в виртуальной реальности, не имеющей государственных границ, дополнительно увеличивает и степень общественной опасности таких правонарушений. Проблему также вызывает и определение места совершения противоправного деяния с использованием компьютерных технологий. Действующее уголовное законодательство не закрепляет в правовых нормах место совершения компьютерного преступления. Кроме того, использование специальных технических средств позволяют участникам киберпреступлений

эффективно осуществлять совместные действия и при этом снижать риск обнаружения из-за отсутствия личного контакта.

Высокая степень вариативности способов для совершения экономическихпреступлений в цифровой среде обусловлена постоянным развитием и совершенствованием информационных технологий и созданием новейшей компьютерной техники. Применение технических новинок позволяет преступникам придумывать новые способы совершения противоправных деяний, на которые правоохранительные органы могут адекватно реагировать при условии надлежащего технического и правового обеспечения своей деятельности.

Основной проблемой правоприменительной практики по экономическим преступлениям с использованием компьютерных и информационных технологий является несовершенство действующего уголовного законодательства, которое не в полной мере содержит достаточную нормативно-правовую базу для реализации ответственности запреступления подобного рода. Распространенность киберпреступлений, а такжединамичность развития технических средств их исполнения приводит ксущественным различиям в установлении понятийного аппарата и разночтениям при толковании норм уголовного закона. В современном законодательстве отсутствует нормативное закрепление таких понятий, как «преступление, совершаемое с использованием компьютерныхтехнологий», «компьютерные технологии», «использование компьютерных технологий», «киберпреступления», а также отсутствует единая точка зрения на указанные определения, что вызывает ряд вопросов, связанных с квалификацией соответствующих деяний. Понятие «преступления, совершаемые с использованием информационных технологий» весьма широко, в той или иной степени включает большую часть предусмотренных УК составов преступлений. Проблема уголовно-правовых рисков с использованием информационных технологий является в значительной степени более масштабной.

Отметим также, что законодатель в части совершенствования уголовно-правовых норм зачастую опаздывает от развития инновационных технологий и технических средств совершения преступлений. Уголовно -правовые нормы, основной задачей которых является противодействие преступлениям в информационной сфере, страдают пробельностью и не способны охватить все возможные общественно-опасные киберугрозы и их последствия. Помимо вредоносного программного обеспечения, ответственность за создание, использование и распространение которого предусмотрена уголовным законодательством, преступники могут применять компьютерные программы иного рода, предназначенные, например, для дешифрования информации, подбора паролей и кодов доступа, программы-копировщики, а также различные цифровые устройства для сканирования портов и другие. В условиях запрета на применение аналогии закона в уголовно-правовых отношениях, следует поддержать мнение ученых-юристов о криминализации действий по незаконному изготовлению, сбыту и приобретению специального программного обеспечения, предназначенного для нарушения систем защиты цифровой информации. Это поможет снять существенную часть разногласий с квалификацией соответствующих противоправных деяний. В практике достаточно распространено, так как все больше людей пользуются компьютерами, что становится облегчающим фактором для похищения любой информации.

Развитие коммуникационных технологий и их внедрение в экономику обострило проблемы защиты персональных данных, коммерческой, корпоративной и банковской тайны, что представляет собой информацию конфиденциального характера. Например, имеющая специальный правовой режим, инсайдерская информация. Тем не менее, информация, находящаяся в свободном доступе, тоже может представлять интерес для преступных организаций. Сведения, полученные с сайта службы судебных приставов об исполнительных производствах или из единого государственного реестра юридических лиц, могут быть использованы для организации рейдерских захватов и несут в себе риски информационной

безопасности. Эти вопросы также требуют совершенствования уголовного и уголовно-процессуального законодательства.

Активное развитие электронных финансовых технологий привело к появлению такого финансового инструмента как криптовалюта. Правоохранительная система столкнулась с ее широкимиспользованием в криминальной сфере.

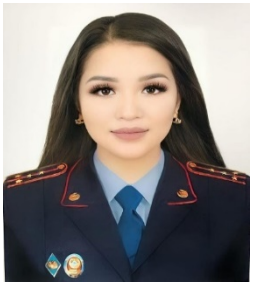
Кибертерроризм во всем мире оценивается как один из наиболее опасных видов преступности, что вызывает острую необходимость развития компетенции правоохранительных органов в обеспечении информационной безопасности. Глобальное цифровое пространство уже стало полемвесьма жесткого геополитического соперничества. В прошлом году только количество наиболее опасных атак на информационные ресурсы, выросло почти в три с половиной раза». Президент также подчеркнул, что «В этих условиях нужна долгосрочная выверенная стратегия действий по защите национальных интересов в цифровой сфере, опирающаяся на самые передовые технологии». Помимо развития технологий, как инструмента информационной безопасности, с целью формирования предложений по решению рассматриваемых проблем правоприменительной практики по преступлениям с использованием информационных технологий, на мой взгляд, необходимо учесть опыт стран, преуспевших в противодействии незаконному использованию цифровых технологий в экономике. Согласно данным The Boston Consulting Group, тройку лидеров с наиболее развитой цифровой экономикой составляют Великобритания (12,4% ВВП), Южная Корея (8%) и Китай (6,9%). С целью адаптации права в условиях развития цифровых технологий, принятие международных конвенций в области компьютерных преступлений должно проводиться с оговоркой на статьи, противоречащие национальному законодательству. Например, Конвенцию о компьютерных преступлениях ETS №185 (Будапешт, 23 ноября 2001 года) на сегодняшний день ратифицировали 53 страны и подписали еще 4, включая все страны ЕС, а также США, Японию, Австралию и Израиль. В настоящее время это единственный глобальный документ международного уровня, который регулирует действия стран-участников по борьбе с киберпреступностью. Казахстан в настоящий момент указанную Конвенцию не подписала, но предложила свой проект конвенции «О сотрудничестве в сфере противодействия информационной преступности». Одной из особенностей данного проекта является отсутствие возможностей вмешательства спецслужб одних стран в сети других - в нем есть отдельная статья о защите суверенитета. Данный проект был предложен для рассмотрения на заседании Генеральной Ассамблеи ООН 30 июля 2019 года. Другим предложением было создание в рамках Генеральной Ассамблеи постоянного форума для обсуждения на основе комплексного и сбалансированного подхода всехаспектов международного сотрудничества в борьбе с киберпреступностью, которое будет направлено на поиск политического решения и достижение консенсуса с учетом насущных потребностей государств в этой области, а также на содействие обмену передовым опытом в этой области. Это позволит, на мой взгляд, предложить мировому сообществу выработку мер по противодействию глобальным киберугрозам и оказать помощь в гармонизации национальных законов в отношении определения основныхкиберпреступлений.

Отсутствие специальных знаний в области современных компьютерных технологий у сотрудников правоохранительных органов также не позволяет надлежащим образом квалифицировать и расследовать преступления в сфере цифровой экономики. С целью подготовки специалистов по борьбе с компьютерными преступлениями необходимо расширить сотрудничество в сфере образования с органами досудебного расследования в части научной и экспертно-аналитической деятельности. В качестве требования к сотрудникам правоохранительных органов предусмотреть наличие IT-образования и знаний судебной практики в области киберпреступности. Первые шаги в этом направлении уже предприняты в Алматинской академии МВД Республики Казахстан имени М. Есбулатова в центре по борьбе киберпреступностью где проходят повышение квалификации сотрудники ОВД со всей Республики Казахстан.

Подводя итоги, хочется отметить, что цифровизация экономики помимо очевидных положительных последствий сопряжена с ростом числа уголовно- правовых рисков, не находящих в полной мере отражения в уголовном законодательстве, что требует пересмотра уголовно-правовой политики и совершенствования уголовного и уголовно-процессуального законодательства.

Литература

1. Уголовное право Республики Казахстан 2020 года Рахметов С.М.
2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V (с изменениями и дополнениями по состоянию на 07.03.2023 г.)
3. Алауханов Е.О.// Проявления коррупции в экономике Казахстана//Предупреждение преступности №2 (2)2008 г. – С. 38-43
4. Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в новой реальности – время действий» (01.09.2020 года) // https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana (02.11.2020)
5. Сведения Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан // https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat (21.02.2021)
6. Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е.Эминова. – 3-е изд., перераб. И доп. – М.: Юристъ, 2004. – С. 734.
7. Криминология: учебник / под ред. Проф. Малкова В.Д. – М.: ЗАО Юстицинформ, 2004. – С. 528.
8. Нукенов М.О. Коррупционные преступления. Криминоглогический и уголовно-правовой анализ: Дисс. канд. юрид. наук. – Алматы, 1999. – С. 189.
9. Абдрахманов С.З. Признаки субъекта коррупционных преступлений: учебное пособие. – Караганда, 2004. – С. 84.
10. Нукенов М.О. Проблемы борьбы с коррупционной преступностью (уголовно-правовые, криминологические и криминалистические аспекты): автореф. д.ю.н.: 12.00.08, – Алматы, 2005. – С. 53.
11. Тургумбаев Е.З. Уголовная ответственность за превышение власти или должностных полномочий. – Алматы: Экономикс, 2004. – С. 228.
12. Мельник Н.И. Криминологические и уголовно-правовые проблемы противодействия коррупции: автореф. д.ю.н.: 12.00.08, – Киев, 2002. – С. 33.
13. Уголовный кодекс Республики Казахстан от 03 июля 2014 года №226 - V ЗРК // http://www. zakon. kz. (20.03.2021)
14. Уголовное право Республики Казахстан. Общая часть: Курс лекций / Под общ. ред. И.Ш. Борчашвили. – Алматы: Жеті жарғы, 2016. – С. 632.



ТУРГУНБАЕВА АЛЬБИНА МАРАТОВНА
Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции

УГОЛОВНАЯ ПОЛИТИКА РЕСПУБЛИКИ КАЗАХСТАН В СФЕРЕ ИНФОРМАТИЗАЦИИ: ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

В настоящей статье исследованы проблемы уголовной политики в сфере обеспечения информационной безопасности, развития уголовного законодательства в этой сфере.

Цель настоящей статьи – исследовать проблемы уголовной политики в сфере информатизации или обеспечения информационной безопасности и теоретических основ противодействия компьютерной преступности. В рамках исследования уточняется понятийный аппарат и теоретические основы уголовной политики в сфере обеспечения информационной безопасности и противодействия компьютерной преступности, изучено состояние, структура динамики компьютерной преступности в современном Казахстане, криминогенных факторов, генерирующих их развитие.

Проблема уголовной политики в сфере информационной безопасности есть комплексная, системная социально-политическая и правовая проблема современного Казахстана, обусловленная общими и специальными экономическими, политическими, духовными, методологическими, юридическими, уголовно-правовыми, криминологическими и иными факторами. Она охватывает и смежные нормы уголовно-процессуального, уголовно-исполнительного и иных отраслей законодательства, обеспечивающих правовое регулирование такой разнородной сферы общественной жизни, как борьба с преступностью в сфере информатизации. Многочисленные исследования не привели пока к выработке достаточно точного и полного представления о феномене соответствующей государственной политики в сфере информатизации. При этом вопросы уголовной политики остаются неизученными. Последнее определяет новизну настоящего исследования. Предлагаемое исследование содержит научно обоснованные положения и выводы о теоретических основах профилактики преступлений в сфере информатизации и это определяет его научную значимость. Кроме того, обозначены основные проблемы по теме и обозначены основные направления их решения, что обуславливает его практическую значимость.

Методологическую основу исследования составляют научные положения уголовного права и криминологии о сущности преступления и преступности, их влиянии на состояние государственной и общественной безопасности. В ходе исследования современные концепции определения сущности преступления и преступности, выводы получены посредством качественного и количественного анализа социально-правовых, уголовно-правовых явлений и процессов.

Проведенный авторами правовой анализ позволяет представить рекомендации определению новых перспективных направлений уголовной политики Казахстана в сфере информационной безопасности и противодействия компьютерной преступности.

Предполагаемые исследования могут внести реальный вклад в решение и преодоление международного аспекта имеющегося в сфере обеспечения информационной безопасности кризисного состояния. Преступления в сфере информационных технологий-особая сфера, поскольку сложившаяся система телекоммуникаций не имеет границ. Преступление может быть задумано в одной стране, пройти по коммуникациям трех-четырех других стран и совершиться в пятой. Эта обстоятельство предполагает необходимость налаживания взаимодействия с другими государствами.

Сложившийся за последние годы эмпирический опыт противодействия преступности в сфере информатизации характеризуется превентивными средствами и нуждается в научном обобщении и интерпретации. Его научное

осмысление приобретает особую актуальность с принятием нового Уголовного кодекса РК, поскольку в настоящее время практика предупреждения преступности в сфере информатизации складывается во многом стихийно, без единой руководящей идеи, нередко представляет собой импульсивные реакции на вызовы преступной среды и обострение криминальной ситуации.

В этой связи возникает необходимость своевременного глубокого теоретического изучения новых правовых явлений в сфере уголовной политики, каковыми и являются компьютерная преступность и информационная безопасность. Актуальность исследования обусловлена, в первую очередь, ростом компьютерных преступлений. За последние десять лет сети Интернет превратились в виртуальную площадку, в пространство, где люди имеют возможность выражать идеи, заниматься общественной деятельностью и пр. На сегодняшний день сети Интернет играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем любую интересующую нас информацию. Конечно, понятно, что все эти действия зависят от информационных технологий. В связи с этим многие пользователи Интернета подвергаются атакам со стороны киберпреступников. По материалам сайта www.crime.vl.ru. котики, проституция и насильственная преступность, безусловно, останутся, но большинство преступников из иных сфер переориентируются в компьютерную.

На сегодняшний день отсутствует научно обоснованная целостная концепция уголовной политики в сфере обеспечения информационной безопасности, поскольку научные исследования практически не проводились. Многие вопросы требуют изучения, поэтому необходимо разработать научно обоснованный терминологический аппарат. До сих пор не раскрыто полностью, что относится к сфере информационных технологий в казахстанском законодательстве, хотя этим термином правоохранительные органы оперируют. К примеру, часто используется термин «преступления в сфере информационных технологий». Само понятие информации вызывает много споров и наиболее распространенными определениями являются те, которые содержатся в словарях [1]. При этом нет единого и достаточно точного представления о понятии, предмете и структуре этого феномена и в научной литературе. Многочисленные исследования понятия «уголовная политика» не привели пока к выработке достаточно точного и полного представления о феномене соответствующей государственной политики в сфере информатизации. Само понятие уголовной политики является предметом научных исследований и вызывает дискуссии [2-4]. Деятельность государства в сфере борьбы с преступностью (целиком либо в той или иной ее части) принято именовать уголовной политикой [3]. Однако, несмотря на многочисленные исследования, до сих пор отсутствует единство мнений в вопросе о содержании этого понятия, его значении и соотношении с иными родственными, так называемыми смежными понятиями. Требуют изучения и вопросы определения направлений установления социального контроля над соответствующими видами преступности в сфере информатизации с помощью правовых и организационно-тактических средств.

Объектом исследования выступили общественные отношения, складывающиеся между субъектами по вопросам противодействия компьютерной преступности и их отражение в уголовно-правовой теории и правоприменительной практике. Предметом исследования стало состояние, структура и проблем противодействия компьютерной преступности и вопросы совершенствования уголовного законодательства.

Целью исследования является изучение со стояния, структуры, динамики компьютерной преступности в современном Казахстане, анализ криминогенных факторов, генерирующих развитие компьютерной преступности в современном Казахстане. Методологическую основу исследования составили положения общенаучного диалектического метода познания социальных явлений. В процессе исследования использовались классические методы исследования, в том числе методы сравнительного, правового, системного и институционального анализов.

Область применения – деятельность законодательных органов по совершенствованию нормативных актов, деятельность правоохранительных органов по совершенствованию мер противодействия компьютерной преступности, учебный процесс, сфера юридической науки.

Высокая общественная опасность преступлений, совершаемых в сфере компьютерной информации, большое количество потерпевших, установленный и более значительный скрываемый материальный ущерб делают борьбу с этим негативным явление актуальной, как и то, что преступность в сфере компьютерной информации все шире используется в контексте организованной преступной деятельности и, особенно, деятельности террористических организаций, которые все активнее начинают использовать в своей противозаконной деятельности новейшие информационные технологии и компьютерную технику. Террористические акты в США 11 сентября 2001 года, которые сегодня называют «цифровым Перл-Харбором», и другие терракты, имевшие место в последние годы, ярчайшее тому подтверждение [5].

Вышеуказанные проблемы подверглись изучению в рамках проекта. В первую очередь исследовано состояние компьютерной преступности в Республике Казахстан. При этом установлено, что Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные еще совсем недавно мировому сообществу виды общественно опасных посягательств. По статистике, за последние десять лет отмечается постоянный рост количества пользователей Интернетом в Казахстане, в частности, отмечается, по данным TNS Web Index, что интернет – единственный растущий медиаканал в Казахстане, охват которого почти в 2 раза превышает охват прессы. В июле 2015 года количество интернет-пользователей в РК достигло 3,47 млн. То есть 71% населения страны в возрасте от 12 до 54 лет заходят в сеть минимум не реже одного раза в месяц. В 2016 году этот показатель по прогнозам специалистов может достигнуть 4,5 млн. человек [3].В ходе сбора и анализа литературы нами были использованы не только работы разных специалистов, статистические данные, опубликованные в интернет-источниках, но и научные труды известных отечественных и зарубежных ученых, в которых отмечается, что если ранее считалось, что компьютерная преступность–явление, присущее только развитым компьютеризированным зарубежным странам, и по причине слабой компьютеризации, т.е. недостаточного внедрения в производственные и общественные отношения информационных технологий, у нас отсутствует. Именно это обстоятельство и привело отсутствию сколько-нибудь серьезных научных исследований вообще. Вместе с тем особенно теперь известная проблематика стала предметом широкого научного диспута и не только в кругах отечественной правовой науки [6; 7].

Определенное внимание уделено современному состоянию компьютерной преступности в нашей стране. В результате исследования сформулированы выводы, основной из которых сводится к тому, что по мнению большинства специалистов, в настоящее время мощный прогресс технологии привел к изменению структуры и качества компьютерных преступлений

и, соответственно, картины компьютерной преступности. Это само по себе заслуживает интенсивного научного внимания, в том числе и со стороны криминологов. Преступность в сфере компьютерной информации, и особенно в Интернете, имеет тенденцию к значительному росту в части статей УК РК, предусматривающих неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ для ЭВМ. Отмечается, что состояние современной компьютерной преступности во многом определяется тенденцией переноса центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей и, прежде всего, Интернета, в котором в результате развивается нелегальный рынок [8].

Преступления в сфере компьютерной информации чаще всего стали совершаться организованно (группой компьютерных преступников), а также все шире используются в контексте организованной преступной деятельности и, прежде всего, в сфере экономической деятельности. С повышением уровня компьютеризации общества может усилиться киберактивность террористов. В связи с этим рекомендуется определять преступления в сфере компьютерной информации (компьютерные преступления) как предусмотренный уголовным законом противоправный, виновный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, а также нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда, подлежащим уголовно-правовой охране [9].

Сегодня все осложняется еще, главным образом тем, что и изучение, и расследование данного вида преступления требует обязательных знаний в области информационных технологий. И в науке, и на практике ощущается острая нехватка юристов, обладающих глубокими знаниями в этой сфере. Это само по себе представляет собой серьезную проблему, над решением которой нужно работать системно, постоянно с учетом постоянного развития информационных технологий.

Кроме того, в настоящее время недостаточно изучены личность участника и причины преступлений в сфере компьютерной информации, а также меры противодействия такому виду преступности. В этой связи эти вопросы были изучены в рамках проекта. В итоге сделан вывод, что компьютерный преступник (хакер) – это, как правило, мужчина в возрасте от 18 до 24 лет (отмечается тенденция снижения возраста); с высоким уровнем образования, часто технического. Компьютерный преступник проявляет склонность к совершению компьютерных преступлений на продолжающейся основе, хотя статистически это сложно выявить, можно даже сказать, что не выявляется. Вместе с тем единой характеристики личности участника преступности в сфере компьютерной информации быть не может, что связан с их типологическим многообразием [10]. В связи с этим проведена типологизация компьютерных преступников по особенностям мотивации преступного поведения и степени устойчивости антиобщественной направленности, по уровню подготовленности и преступной специализации. Одной из характерных особенностей лиц, совершающих киберпреступления, является устойчивое стремление к паразитическому образу жизни, отсутствие какой-либо профессии, постоянного места работы, определенного места проживания. Составление обобщенного криминологического портрета личности компьютерного преступника в ходе исследования проведен на основе материалов судебной и следственной практики, а также изучения зарубежного опыта обеспечения информационной безопасности [11; 12].

В ходе исследования структуры и динамики компьютерной преступности в Республике Казахстан выяснилось, что структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии компьютерных преступлений как преступлений специфических не существует. Анализ криминогенных факторов, генерирующих развитие компьютерной преступности в современном Казахстане, показал, что значительное место в продуцировании компьютерной преступности также занимает виктимность обладателей компьютерной информации вследствие слабой

организации охраны компьютерной информации и того, что ЭВМ характеризуется технической уязвимостью, в этой связи приоритет борьбы с компьютерной преступностью должен быть отдан мерам профилактического свойства. Под факторами в ходе исследования понимаются детерминанты, которые определяющим образом влияют на развитие известного рода преступности. Исследование показало, что факторы преступности в сфере компьютерной информации заложены в социально-экономической, социально-политической и социально-психологической сферах. В связи с уменьшающейся стоимостью и возрастающей миниатюризацией электронных компонентов сегодня возможным сделали самые современные технические средства стали доступными для широких слоев населения. Вместе с тем эта в целом положительная тенденция несет в себе и негативный потенциал, о чем свидетельствуют рост их статистической выявляемости, который по всем подсчетам будет усиливаться по мере увеличения концентрации вычислительных ресурсов, их территориальной распределенности, одновременного доступа к ресурсам многих пользователей [11]. Поэтому действенные меры борьбы с преступностью в сфере компьютерной информации, как представляется, состоят в преодолении ограниченности национального законодательства в русле формирования единой правовой базы, направленной против компьютерной преступности, а также в русле усиления гражданской, административной и уголовной ответственности. Основная рекомендация сводится к определению в качестве основного направления борьбы с преступностью в сфере компьютерной информации становление и развитие правового фундамента в сфере Интернета путем принятия Закона «О правовом регулировании использования сети Интернет». И поскольку абсолютной защиты компьютерной информации не существует, значительное место в предупреждении компьютерной информации должно принадлежать мерам технического и организационного характера. Важнейшее место в борьбе с преступлениями в сфере компьютерной информации должно отводиться политико-организационным, организационно-административным и организационно-администраторским мерам. Однако все меры предупреждения компьютерных преступлений будут эффективными только тогда, когда они будут использоваться все вместе, т.е. комплексно.

Литература

1. Сабитов Д. Информационная безопасность Казахстана: защита данных и смыслов. – Астана, 2015. – С. 68.

2. Назаров Р.И. Роль информации об этнической принадлежности в борьбе с дискриминацией: опыт государств.

3. Этнологический мониторинг переписи населения / под ред. В.В. Степанова. – М.: ИЭА РАН, 2011. – С. 552.

4. Турлаев А.В., Шәкірова А.Б. Правовое обеспечение информационной безопасности в Республике Казахстан // Вестник КарГУ, 2013 // https://articlekz.com/article/6210 4 Ernst & Young. (n.d.). Global Information Security Survey. Retrieved 12 3, 2012, from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

5. Gary McGraw, S. M. (2012, September). BSIMM. Retrieved from http://bsimm.com/download/

6. Gerber, M., & Solms, R. v. (2008). Information security requirements – Interpreting the legalaspects. Computers & Security, 124-135.

7. Höne, K., & Eloff, J. (2002). Information security policy – what do international information security standards say. Computers & Security, 402-409.

8. Polkinghorne, D. E. (2005). Language and Meaning: Data Collection in Qualitative Research. Journal of Counseling Psychology, 52 (2), 37–145.

9. Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 23-29 .

ВОЕВОДКИН ДЕНИС ВИКТОРОВИЧ
Докторант Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан, советник юстиции

К ВОПРОСУ О СУДЕБНОЙ ЭКСПЕРТИЗЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Развитие информационных технологий на современном этапе и цифровизация жизни общества оказало огромное влияние на большинство сфер его жизнедеятельности, включая сферу правоприменения и работу правоохранительных органов. Новые технологии предоставили возможности для улучшения криминалистических методов и средств, но также породили новые способы совершения преступлений, что сделало сбор, анализ и использование доказательств более сложными задачами. Одним из эффектов информационного общества стало появление нового объекта криминалистического исследования – электронных документов. В настоящее время в уголовных и гражданских делах всё чаще используются электронные доказательства. Более того, уже внедрено и активно практикуется расследование уголовных дел в электронном формате посредством модуля электронное уголовное дело (е-УД).

Однако, как показал анализ судебной практики, а также действующего законодательства правоохранительные органы недостаточно подготовлены к адекватной оценке таких доказательств и их эффективному использованию ввиду отсутствия надлежащих инструментов и правового регулирования. Поэтому одной из важнейших задач современной криминалистики является разработка эффективных методов исследования электронных документов.

В соответствии с п. 12 ст. 1 Закона Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи» (далее – Закон) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи [1]. Как видно из представленного определения, законодателем устанавливается два важных элемента, при удовлетворении которым документ может считаться электронным – это электронно-цифровая форма и электронная цифровая подпись.

При этом, в указанном законе дается понятие лишь электронной цифровой подписи, под которой понимается «набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания» (п. 16 ст. 1 Закона), тогда как определения электронно-цифровой формы не имеется.

Кроме того, в п. 7 ст. 1 Закона приведено определение электронной копии документа – документ, полностью воспроизводящий вид и информацию (данные) подлинного документа в электронно-цифровой форме.

В отличие от обычных документов, чьи характеристики и пространственные границы мы привыкли видеть, электронные документы обладают совершенно другой природой. Информация, которая составляет суть электронного документа, имеет особые виртуальные границы, которые определены понятием «файл». В научной литературе файл описывается как

«специально структурированная совокупность взаимосвязанных блоков цифровой информации, представленной в виде двоичного кода, распознаваемая операционной системой как единое целое и хранящаяся в долговременной памяти устройства» [2, с. 63].

Для того чтобы выделить конкретный электронный документ среди множества других, необходимо наделить его особыми характеристиками, которые позволят однозначно идентифицировать его в будущем.

Если криминалистическая характеристика документа включает в себя его свойства, а именно размер, форму, материал изготовления, средства защиты, виды печатей, подписи, резолюции, регистрационные реквизиты и тому подобное, то для характеристики электронных документов используют их специфические свойства, а именно полное имя файла, его размер, хэш-функцию, дату создания и изменения, характеристику электронного носителя и т.д.

В соответствии с п. 43 Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях (утвержденных Постановление Правительства Республики Казахстан от 31 октября 2018 года №703) электронный документ состоит из двух частей: содержательной и реквизитной [3].

Содержательная часть электронного документа состоит из одного или нескольких файлов, использующих разные форматы, включая:

−графические форматы, такие как PDF, PDF/A-1, TIFF, JPEG, JPG.

−текстовые форматы, такие как RTF и DOCX.

−табличные форматы, такие как XLS и XLSX.

−форматы для презентаций, такие как PPT и PPTX.

−архивированные форматы, такие как RAR и ZIP.

Содержательная часть электронного документа имеет такие реквизиты, как:

1) официальное наименование организации отправителя;

2) справочные данные об организации (юридический адрес, телефон, факс, электронный адрес организации (при наличии));

3) наименование вида документа;

4) ссылку на регистрационный номер и дату входящего документа;

5) место составления или издания документа;

6) адресат;

7) гриф утверждения документа (при наличии);

8) заголовок к тексту (при наличии);

9) текст документа;

10) отметку об исполнителе (фамилия и телефон исполнителя) (в органах национальной безопасности Республики Казахстан указываются инициалы и телефон исполнителя);

11) электронную цифровую подпись.

Реквизитная часть электронного документа формируется посредством составления электронной регистрационной контрольной карточки, в которой используются следующие реквизиты:

1) наименование вида документа;

2) регистрационный номер документа;

3) индекс номенклатуры дел;

4) название и версия программного обеспечения, при помощи которого создан документ;

5) электронная цифровая подпись;

6) характер вопроса;

7) количество листов основного документа и приложений;

8) наименование государственного органа-адресата (в Комитете национальной безопасности Республики Казахстан наименования подразделений указываются в соответствии с кодами, за исключением территориальных органов);

9) наименование должности адресата (при наличии);

10) фамилия адресата (при наличии);

11) фамилия исполнителя (в органах национальной безопасности Республики Казахстан указываются инициалы исполнителя);

12) номер телефона исполнителя;

13) отметка о контроле;

14) отметка об исполнении документа и направлении его в дело;

15) отметка о наличии или отсутствии подлинника бумажного документа, бумажной копии электронного документа.

Задачи криминалистической классификации документов зависимы от разработки криминалистических свойств всех видов современных документов, некоторые виды которых (например, криптовалюта) фактически существуют вне поля не только методик исследований, но и научных разработок.

Следует отметить, что не все документы, которые используются в уголовных или административных производствах, считаются объектами криминалистических исследований. Документы, которые считаются доказательствами только благодаря информации, имеющей значение для установления определенных фактов (они часто заменяются в деле копиями), не является предметом криминалистического документоведения.

В связи с этим, представляется актуальным выделение из многообразия компьютерной информации электронных документов как одного из основных источников судебных доказательств при расследовании преступлений, совершаемых с использованием компьютерной техники.

Электронные документы могут выступать как средства совершения преступлений в сфере компьютерной информации, а также других преступлений с использованием компьютерной техники, быть объектами преступного посягательства или информационными «следами», возникающими при подготовке к преступлению и совершении преступных действий.

Так, перевод значительной части документооборота в электронный формат породил угрозу подделки официальных документов в электронной форме. 5 сентября 2023 года Национальный удостоверяющий центр Республики Казахстан предупредил всех казахстанцев о выявлении фишингового интернет-ресурса, при открытии которого под видом обновления для NCALayer (приложение для подписания данных на государственных порталах Республики Казахстан) загружается и запускается вредоносная программа [4]. Интернет-ресурсы пестрят объявлениями о клонировании сайтов, создании зеркальных копий, вследствие чего не исключена возможность подделки официальных документов в электронном формате.

Как показывает судебно-следственная практика, в правоприменительной деятельности складывается ситуация о безусловном доверии к электронным видам документов, достоверность их, зачастую, не подвергается сомнению.

Между тем, склонны полагать, что без прохождения цифровой судебной экспертизы электронный документ не может быть использован в качестве доказательства, поскольку действительность электронного документа не может быть гарантирована.

Следует отметить, что законодательно закреплен лишь один способ проверки подлинности электронного документа, изложенный в Правилах проверки подлинности электронной цифровой подписи [5].

При этом, данными правилами не регламентируется порядок действий в случае выявления факта поддельности электронной цифровой подписи. В пункте 9 указанных правил констатируется лишь, что при выявлении несоответствия электронной-цифровой подписи (определен отрицательный результат проверки ЭЦП) после проведения процедуры проверки подлинности, электронный документ не признается равнозначным документу, подписанному собственноручной подписью.

На наш взгляд, указанное требует дополнения в части необходимости направления такого документа в правоохранительные органы для решения вопроса о регистрации в Едином реестре досудебных расследований по факту подделки официального документа.

В то же время, в случае регистрации такого факта в ЕРДР по признакам уголовного правонарушения, предусмотренного ст. 385 Уголовного кодекса Республики Казахстан, дальнейшее производство по делу потребует проведения экспертизы.

Однако, в Правилах организации и производства судебных экспертиз и исследований в органах судебной экспертизы (утверждены приказом Министра юстиции Республики Казахстан от 27 апреля 2017 года № 484, далее - Правила) [6] такого вида экспертизы, как цифровая экспертиза, либо экспертиза электронно-цифровой подписи, не предусмотрено.

Указанными правилами регламентируется судебно-техническая экспертиза документов, предметом которой является установление фактических данных, содержащихся в свойствах материалов письма и в признаках реквизитов документов, обстоятельствах их изготовления, о способах внесения изменений в них, а также о предметах и материалах, которые использовались для изготовления документов либо внесения в них изменений. То есть объектами такой экспертизы является непосредственно овеществленный документ, как носитель определенной информации.

С учетом этого, предлагается дополнить указанные Правила введением спецификации для судебной экспертизы, которая будет включать приблизительный перечень вопросов, направленных на установление следующих аспектов:

−подлинности электронно-цифровой подписи и ее принадлежности владельцу сертификата ключа подписи.

−наличия каких-либо искажений в сертификате ключа подписи, которые могут подвергнуть сомнению законность его использования.

−действительности (или актуальности) сертификата ключа подписи на момент подписания документа.

−подлинности сертификата, выданного специализированной организацией, которая занимается выдачей сертификатов ключей электронно-цифровой подписи.

−статуса сертификата ключа подписи, а именно, не был ли он приостановлен или аннулирован.

−наличия несанкционированных изменений в документе, заверенном электронно-цифровой подписью.

−совпадения результатов хеширования на момент подписания и в момент проверки подлинности документа.

−типа используемой электронно-цифровой подписи при заверении документа.

−полномочий конкретного лица на использование данной электронно-цифровой подписи.

Важно подчеркнуть, что для проведения указанного вида экспертизы в экспертной организации должны предоставляться корневые сертификаты электронно-цифровой подписи, выданные соответствующей организацией, спорные электронные документы, подлинность которых вызывает сомнения, а также ключ проверки электронно-цифровой подписи. Для этого необходимо обеспечить их выемку в ходе проведения следственных действий на первоначальном этапе.

Отдельного исследования требует такой вид электронного документа, как криптовалюта. В Казахстане принят Закон «О цифровых активах в Республике Казахстан», введенный в действие с 1 апреля 2023, который фактически легализует как объект юриспруденции – криптовалюту, так и правоотношения, возникшие вместе с появлением в общественной жизни электронного документа нового типа. Термин «криптовалюта» в данном законе отождествляется с термином «цифровой актив». Из понятия цифрового актива следует, что он является имуществом (п. 4 ст. 1). Вместе с тем, на наш взгляд, можно приблизить его к электронным документам (наряду, к примеру, с ценными бумагами, относящимися к

документам), которые имеют определенные характеристики и требуют отдельных исследований их криминалистических признаков. Криптовалюта как предмет преступного посягательства имеет присущие лишь ей признаки, обусловленные использованием технологии блокчейн при функционировании (если рассматривать самую распространенную криптовалюту Bitcoin). Описание криптовалюты имеет важное криминалистическое значение, поскольку предусматривает специфический порядок обнаружения, фиксации, осмотра и даже последующего анализа имеющейся информации («электронных следов»), влияет на установление фактов, в частности использование криптовалют конкретными пользователями и их идентификация.

Еще одним значимым аспектом при рассмотрении экспертизы электронных документов является вопрос о том, можно ли квалифицировать электронный документ как определенный вид доказательства. Из статей 118 и 120 УПК РК следует, что электронные документы признаются вещественными доказательствами, из статьи 100 ГПК РК – письменными доказательствами.

В доктрине нет единой точки зрения относительно классификации электронных документов как определенного вида доказательств. Согласно некоторым ученым, электронные документы могут быть рассмотрены как письменные доказательства, поскольку информация в них отражает человеческие мысли (понятия, суждения и так далее) относительно реальных событий [7, с. 106]. В то же время некоторые исследователи предлагают отнести электронные документы к вещественным доказательствам, так как они сами по себе не поддаются человеческому восприятию и служат средством для установления фактов, имеющих значение в деле [8, с. 145]. Важно отметить, что информация, хранящаяся в памяти компьютера, может быть воспроизведена, что придает ей свойства письменных доказательств [9, с. 29].

Поэтому, на наш взгляд, можно сказать, что электронный документ как вид доказательства обладает смешанными характеристиками, поскольку в отличие от приведенных видов доказательств, электронные документы не существуют в конкретной материальной форме; они представлены в виде файлов различных форматов, и доступ к этой информации осуществляется через специальное программное обеспечение.

С учетом того, что с 2018 года уголовное судопроизводство осуществляется в электронном формате [10], видится необходимым, наряду с понятием «электронное уголовное дело», предусмотреть понятие «электронное доказательство».

Практика использования электронных доказательств подтверждает их актуальность и неотложную необходимость дальнейшего законодательного регулирования в контексте их применения в уголовном судопроизводстве. Установление единообразного, ясного и логичного порядка проведения процессуальных мероприятий с этими доказательствами становится ключевым критерием для их признания допустимыми. Однако важно отметить, что достоверность и признание электронных доказательств полностью зависят от их проверяемости в соответствии с законом.

Проблема использования электронного документа как источника доказательств в уголовном судопроизводстве сейчас все больше актуализируется и, несомненно, требует дальнейших углубленных исследований как с позиции теории судебного доказывания, так и с позиции криминалистики.

Таким образом, склонны полагать, что современные реалии повсеместной цифровизации общества диктуют необходимость внедрения в практику судебно-экспертной деятельности нового вида экспертиз, предусматривающих возможность установления подлинности электронных документов, в т.ч. криптовалют, для обеспечения гарантии их действительности и достоверности, а также внесение изменений и дополнений в действующее законодательство в части определения понятия «электронно-цифровая форма», «электронное доказательство» и разъяснения действий уполномоченных государственных органов при выявлении поддельных электронных документов.

Литература

1. Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z030000370_. Дата обращения: 11.09.2023 г.

2. Арутюнов А.С., Фаниев П.А. «Понятие файлов и метаданных, необходимость их исследования для решения криминалистических задач». Вестник Краснодарского университета МВД России. 2022. №4 (58). – С. 63-66.

3. Постановление Правительства Республики Казахстан от 31 октября 2018 года №703 «Об утверждении Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/P1800000703. Дата обращения: 11.09.2023 г.

4. Новости от 05.09.2023 г. [Электронный ресурс]. URL: https://pki.gov.kz/news/. Дата обращения: 11.09.2023 г.

5. Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/V1500012864. Дата обращения: 11.09.2023 г.

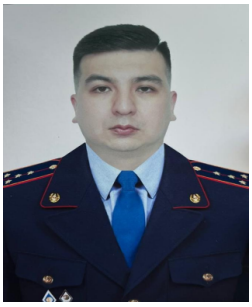
6. Приказ Министра юстиции Республики Казахстан от 27 апреля 2017 года №484 «Об утверждении Правил организации и производства судебных экспертиз и исследований в органах судебной экспертизы». [Электронный ресурс]. URL:https://adilet.zan.kz/rus/docs/V1700015180. Дата обращения: 11.09.2023 г.

7. Вершинин А.П. Электронный документ: правовая форма и доказательство в суде. – М., 2000. – С. 247.

8. Медведев И.Г. Письменные доказательства в частном праве России и Франции. СПб., 2004. – С. 407.

9. Горелов М.В. Современные источники информации как доказательства в гражданском процессе //Информационное право. 2005. №3. – С. 27-29.

10. Приказ Генерального прокурора Республики Казахстан от 3 января 2018 года №2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате». [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/V1800016268. Дата обращения: 11.09.2023 г.



АБИКЕНОВ АБДУЛЛА НУРХАТУЛЫ
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі факультетінің 2-курс докторанты полиция капитаны, з.ғ.м.

ЦИФРОВИЗАЦИЯНЫҢ ҚАЗІРГІ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ ЗАҢДЫЛЫҒЫНА ӘСЕРІ

Қазіргі таңда ақпарат пен технологияның дамуына байланысты, оған қойылатын талаптар да күшейтілуде. Цифровизация әр салада қарқынды дамтып келеді. Тіптен қылмыс әлемін де цифровизация қамтып отыр.

Цифровизация дегеніміз – цифрлық технологияларды кез – келген жерге енгізу; сандық құрылғылардың көмегімен деректерді байланыстыру, жазу және берудің цифрлық тәсіліне көшу немесе көшу [1].

Кейінгі уақытта цифрландыру мәселесі үзіліссіз және жан-жақты талқылануда. Осы цифровизация мәселесімен айналып жатқандар саясаткерлер, экономистер, әлеуметтанушылар, философтар және әрине, заңгерлер. Тіптен цифрландыру мәдениет пен өнер өкілдерінің де назарын тыс қалып жатқан жоқ.

Цифрландыруға деген көзқарас полярлы. Кейбіреулер цифрландыру дамудың жаңа деңгейіне секіру деп болжайды. Жалпы өркендеу дәуірінде адамның ұзақ өмір сүруі, ғарышты белсенді игеру және т.б. цифрлық оптимистер биология мен технологияны біріктіре отырып, «адамды жеңуге» эволюцияның келесі кезеңіне өтуге шақырады [2].

Ал пессимистер керісінше цифрландыруды сезімсіз және жансыз әлем дейді. Суперкомпьютерлер құлдыққа алған қоғам деп санайды және егер адамзат өзінің дамуының жаңа кезеңіне өтсе, онда өркениеттік мағынада ол соңғы болады деп болжайды [3].

Цифрлық дәуір философиясы бізге технологияның дамуын қабылдауға мүмкіндік беруі керек, бірақ оған айналмауы керек [4].

Ал заң ғылымы цифровизацияға қатысты өз міндеттерін алдыға қояды. Цифрландырудың оң және теріс тенденцияларын талдай отырып, қылмыстық доктрина бүгінгі күннің проблемаларын шешуді ұсынып қана қоймай, болашақты түсінуге тырысады.

Эрнест Хемингуэйдің әйгілі шығармасынан үзіндісіне тоқталар болсақ, онда қылмыстық құқықты цифрландыру екі кезеңде жүзеге асырылады. Бірінші кезең қылмыстық заңның тиісті терминологиямен біртіндеп қанықтырылуымен, қорғалатын қоғамдық қатынастарға қол сұғудың жаңа (виртуалды) тәсілдерін ескере отырып, жауапкершілікті саралаумен, «цифрлық нысандарға» қол сұғушылық үшін жауапкершілік туралы жаңа нормалардың пайда болуымен байланысты. Екінші кезең белгілі бір сәттен бастап жеке және ұжымдық санада физикалық және виртуалды бөлу іс жүзінде мүмкін емес және негізінен мағынасыз болатындығымен сипатталады. Мұның өзі шындықты осындай біртұтас қабылдау құқықтық реттеу деңгейінде көрініс табуы үшін негіз болады, мұнда қылмыстық-құқықтық қорғау механизмі виртуалды және нақты (физикалық) әлемдегі оқиғаларға бірдей қолданылады.

Қазіргі кезеңде қылмыстық заң қылмысты цифрландыруға жауап бере алмайды. Қылмыс жасау кезіндегі ақпараттық-коммуникациялық технологияларды қолдану бір орында тұрмайды, заманына сай өзгеріске ұшырап отырады. Сонымен қатар мұндай қол сұғушылықтарды ашу және тергеу өте қиын. Бұл қылмыстың цифрлық трансформациясының осы жағымсыз жақтарын ескере отырып, қылмыстық заңды цифровизацияға бағытталған «қайта құру» қажеттілігі туралы қорытынды жасауға мүмкіндік береді. Қылмыстық заң

бойынша отандық әдебиеттерде қылмыстық заңды «цифрландыру» бойынша бірнеше нақты ұсыныстарды кездестіруге болады. Мұндай бастамалардың кейбіреулері нақты әлеуметтік – құқықтық және криминологиялық негіздерге ие, ал басқалары қылмыстық – құқықтық қорғау механизмінің практикалық мәселелерін шешуге бағытталғаннан гөрі конъюнктуралық болып табылады [5].

Алайда, қылмыстық заңды құрудың абстрактілі әдісі көптеген жағдайларда қылмысты цифрландыру құбылысын қамтуға мүмкіндік беретінін ұмытпауымыз керек. Қылмыстың киберлігі айқын көрінеді: «киберугон», «кибертерроризм», «кибербуллинг» және т.б. қылмыстарда.

Ақпараттық-коммуникациялық технологияларды пайдалана отырып жасалатын қылмыстар үшін қылмыстық жауаптылықты саралау жөніндегі заң жобалау жұмысын жүзеге асыру кезінде қылмыстық заң нормаларының формальды-логикалық айқындылығын қамтамасыз ету мақсатында мынадай ережелерді басшылыққа алу қажет:

Біріншіден, қылмыстық заң нормаларын қоғамның ақпараттандыру жағдайына бейімдеу, дәстүрлі қылмыстық-құқықтық реттеулер «цифрлық егіздерін» құрумен байланысты болмауы керек. Бәрібір де отандық қылмыстық заңнаманы цифрландыруға сай жаңғыртсақ та, оның ережелерінің шамадан тыс қайталануына әкеп соғатыны сөзсіз. Бұл бір-бірімен тек құқықтағы виртуалды және нақты айырмашылықты анықтау проблемасының түйіскен жерінде бәсекелес нормалардың едәуір санының болуымен көрінеді.

Қылмыстық – құқықтық тетікті ақпараттық – коммуникациялық технологияларды пайдалана отырып жасалатын қылмыстарға қарсы іс – қимылға бейімдеудің маңызды бағыты қылмыстық құқықты дәстүрлі – цифрлық емес-қабылдауды еңсеру болып табылады.

Екіншіден, нормалардың мазмұнына тиісті түзетулер енгізу отандық қылмыстық заңнаманың компьютерленген қылмыстың көріністеріне бейімделу қабілеті төмендеу. Қылмыстық құқық норманы түсіндіру жүйелік семантикалық алшақтықта бола отырып, Заңның мағынасынан асып кеткен жағдайларда ғана негізделген болып табылады, бұл заңның ұқсастығын көрсетеді. Қазақстан Республикасының 4- бабына сәйкес: Қылмыстық құқық бұзушылықтар жасау, яғни осы Кодексте көзделген қылмыс не қылмыстық теріс қылық құрамының барлық белгілері бар іс-әрекеттер қылмыстық жауаптылықтың бірден-бір негізі болып табылады. Дәл сол бір қылмыстық құқық бұзушылық үшін ешкімді де қылмыстық жауаптылыққа қайталап тартуға болмайды. Қылмыстық заңды ұқсастығы бойынша қолдануға жол берілмейді [6].

Үшіншіден, қылмыс жасаудың жаңа (ақпараттық) тәсілінің пайда болуы оның дәстүрліден гөрі қауіпті екенін алдын-ала көрсетпейді және көбінесе әлеуметтік бақылаудың қоғамның дамуы мен қылмыстың өзгеруінен артта қалу проблемасын көрсетеді.

Сонымен төртіншіден, ақпараттық- коммуникациялық технологияларды қолдануды қылмыстың біліктілік белгісі ретінде танылып, жалпы алғанда қылмыстық жауапкершілікті саралаудың ғылымда негізделген критерийлеріне сәйкес келуі керек. Бұл ретте ақпараттық – коммуникациялық технологияларды пайдалануды қылмыстың саралаушы белгісі деп тану қажеттілігі халықаралық құқық нормаларында белгіленген болуы шарт. Сондай-ақ ақпараттық-коммуникациялық технологияларды пайдалану қылмыс жасау кезінде айтарлықтай таралуға ие болды және азаматтардың құқықтары мен заңды мүдделерінің, қоғам мен мемлекеттің заңмен қорғалатын мүдделерінің қорғалу жағдайына айтарлықтай әсер етті.

Қазіргі уақытқа дейін ақпараттық - коммуникациялық технологияларды қолдану арқылы жасалған қылмыстар дәстүрлі қылмысқа қарағанда кең таралған. Бірақ бұл жаппай жасалатын қылмыс емес екендігін атап өткен жөн. Бұл XXI ғасырдың жаңа цифрлық әлеміне бейімделу мақсатында қылмыстық заңның жаңғыртылуын болашақта нені байқайтынымызды түсіндіретін өте маңызды жағдай. Бұл кезең комбинаторлық технологиялық өзгерістер адамның өмірін одан әрі тереңірек өзгертетін кезде, шарықтаушегіне жеткен кезде аяқталады және біз нақты және виртуалды өмірімізді ажыратуымыз қажет.

Қылмыстық заңның фрагменттелген цифрландырылуы біз әлі де нақты және виртуалды өмір сүру формаларын бөлетін жағдайлар үшін ғана жарамды. Қылмыс жасаудың цифрлық тәсілі де уақыт келе физикалық әдіс сияқты дәстүрлі құбылысқа айналады, ал кейбір аспектілерде ол соңғысын толығымен алмастыра алады. Мысалы, несие-қаржы секторын

цифрландырудың қазіргі тенденцияларын ескере отырып, болашақта азаматтардың ақша қаражаттарына қол сұғу қағаз ақша айналымынан шығу себебінен іс жүзінде мүмкін болмайды деп болжау қисынды. Нәтижесінде қылмыс жасаудың ақпараттық (цифрлық) тәсілі туралы қылмыстық заңдағы арнайы нұсқаулар өзінің семантикалық жүктемесін шамалы болса да жоғалтады. Адамның биологиялық миын эмуляциялау технологиясының пайда болуы адам туралы ұғым енді оның биологиялық қабығымен байланысты болмаған кезде өмірдің мүлдем жаңа формасының мүмкіндігін білдіреді. Виртуалды өмір нақты физикалық әлемдегі сияқты қылмыстық - құқықтық қорғауды қажет ететіні түсінікті, өйткені біз мұнда тек компьютерлік кодпен ғана емес, адаммен де айналысамыз. Нәтижесінде біз жәбірленушінің қылмыс тұжырымдамасын қайта қарап, дәстүрлі қылмыстық-құқықтық тыйымдардың (кісі өлтіру, адам ұрлау, адам саудасы, жала жабу және т.б.) «цифрлық тұлғаға» қарсы барлық қол сұғушылықтарға қолданылуын кеңейтуіміз керек. Адамның қайтыс болу сәтінің өзі тек биологиялық анықтамасын жоғалтады. Қазіргі уақытта біз компьютерлік ақпараттың қарапайым жойылуы деп атайтын қосымша мазмұнға ие болдық.

Байланысты проблема ол – биологиялық емес шығу тегі бар адам санасының ұқсастығы бар субъектілерді қорғау. Әрине, мұндай «ақылды машиналарды» қылмыстық-құқықтық қорғау моделі туралы мәселе бүкіл адамзаттың (әмбебап халықаралық ұйымдар тұлғасында) олардың табиғаты мен мәртебесіне қатысты ұстанымын білдіруге байланысты. Мұндай субъектілер адамға тең деп таныла ма жоқ па соны анықтайтын, яғни интеллектуалды өмірдің жаңа биологиялық емес түрі немесе тұтастай алғанда олардың жағдайын салыстыруға болады. Мысалы, біз қылмыстық-құқықтық қорғауды қоғамдық моральды қорғау аясында жүзеге асыратын жануарлармен болжау өте қиын. Адамның интеллектуалдық және эмоционалдық қасиеттерінің көбею деңгейіне байланысты мұндай киберфизикалық жүйелер құқықтық өрісте сараланатын – адамға тең, яғни қоғамдық қатынастардың толыққанды қатысушылары, құқықтың жаңа субъектілері ретінде және жасанды интеллекттің функциялары (қабілеттері) шектеулі автоматтандырылған жүйелер ретінде анықталатын аралас сценарий болуы мүмкін жоғары технологиялық құрылғылар, заттар.

«Цифрлық тұлғаның» пайда болуы, біздің ойымызша, XX ғасырдағы индустриалды қоғамның дәстүрлі қылмыстық құқығынан XXI ғасырдағы цифрлық әлемнің қылмыстық құқығына көшумен аяқтайды. Біріншіден, бұл жасанды интеллект пен «цифрлық тұлға» қылмыстық-құқықтық қорғау саласын түбегейлі өзгертетіндігімен түсіндіріледі.

Жаңа буындар үшін қылмыстық құқығына көшу қылмыстың негізгі белгісі – әлеуметтік қауіпті әрекет туралы біздің идеяларымыздың өзгеруімен байланысты болады. «Цифрлық тұлғаның» пайда болуымен ол өзінің адамға бағытталған физикалық интерпретациясын жоғалтады. «Сандық тұлға» жасаған компьютерлік ақпаратпен кез-келген манипуляцияға қатысты әрекет туралы айтуға болады. Физикалық және виртуалды әлем мүшелеріне әсер етуі мүмкін бұл «әрекет» қылмыс субъектісінің әлеуметтік қауіпті мінез-құлқының жаңа цифрлық түріне айналады. Ұқсас түрлендіру процесі орын, жағдай, құрал және қылмыс жасау құралы сияқты объективті белгілерге қатысты жүзеге асырылады.

«Қылмыстық құқықтың» цифровизацияға көшудің негізгі индикаторы қылмыстың субъектісі мен субъективті жағы туралы дәстүрлі идеяның өзгеруі. Отандық заң ғылымында бұл мәселе жалпы түрде айтылып жатыр.

Цифровизация арқылы қылмыстық құқыққа қол сұғылғанда келтірілген зиян үшін меншік иесі немесе әзірлеуші жауап беруі керек. Мұнда күрделі технологиялық жүйемен өзара әрекеттесу кезінде теріс мінез-құлқы (белсенді немесе пассивті) салдардың пайда болуының тікелей себебі болған субъектіге қатысты жауапкершілікті іске асырудың дәстүрлі моделі іске қосылады. Сонымен бірге «цифрлық тұлға» және жасанды интеллект (оның кез-келген түрінде) ол адамның интеллектуалды ерік-жігерінің тәуелсіз тасымалдаушылары. Яғни құқықтың толыққанды субъектілері болатыны сөзсіз. Бұл оларды қылмыстық жауапкершілік субъектілері де мойындауы керек дегенді білдіреді. Осылайша, цифровизация арқасында қылмыс субъектісі туралы қылмыстық құқық теориясы дамуы түбегейлі жаңа кезеңге өтеді. Олай болса қылмыс субъектісі тек жеке және (немесе) заңды тұлға ғана емес, сонымен қатар жеке тұлғаның сандық түрдегі клоны, сондай-ақ жасанды интеллектке ие адамның биологиялық емес субстраты танылады.

Субъект туралы түсініктердің кеңеюі кінә, қылмыстың себебі мен мақсаты сияқты санаттарды қайта қарау мәселесін табиғи түрде қарау тудырады. Кінәнің психологиялық теориясы тек гомосапиенстің физикалық өкілдері үшін қолайлы болып қалады. Жасанды интеллект пен өмірін цифрлық түрде жалғастырған жеке тұлғалар үшін оны тек заңдық фантастиканың бір түрін қолданған кезде ғана қолдануға болады. Егер біз мұндай субъектілерде «хабардар болуға, болжауға және қалауға» мүмкіндік беретін психика бар деп ойлаған болсақ. Алайда, жоғарыда көрсетілгендей бұл мәселе ең алдымен цифрлық әлемде өмірін жалғастырған адамдарға қатысты қойылуы және шешілуі керек.

Әрине, қазіргі жағдайда қылмыстық құқықтың екінші өмірге келуі (палингенез) проблемасын маңызды емес немесе тіпті алыс деп санауға болады. Алайда, бұл тәсілде объективті дамып келе жатқан процестерге негізсіз немқұрайлылық бар. Технологияның түбегейлі өзгеруі біздің көз алдымызда. Кешегі жеке ғалымдардың фантастикалық жобалары бүгінде инновациялық компаниялар жұмысының нақты тақырыбына айналуда, ал ертең жеке адамның өмірі мүмкін болмайтын қарапайым құбылыс. Бұл дербес компьютерлерде және интернетте болады, сонымен қатар цифрлық ойнату және адамның ақыл-ойын басқару технологияларында да болуы мүмкін.

Болашақтың қандай болатынын нақты болжау мүмкін емес. Қылмыстық заң жалпы адамзаттық құндылықтарға сүйене отырып, ең өткір әлеуметтік қақтығыстарды (олар қандай өлшемде пайда болса да – нақты немесе виртуалды) шешу құралының рөлін сақтайды. Технология біздің күнделікті өмірімізге әлдеқайда тереңірек және берік тоқылатыны анық. Гипер байланысқан әлемде қылмыстық-құқықтық тәуекелдер бірнеше есе артады.

Отандық қылмыстық құқықты «цифрландыру» саланың субстанциялық белгілерінің жойылуына әкелмеуі аса маңызды болып табылады. Біздің ойымызша, қылмыстық – құқықтық тетікті ақпараттық – коммуникациялық технологияларды пайдалана отырып жасалатын қылмыстарға қарсы іс-қимылға бейімдеудің маңызды бағыты «дәстүрлі», «цифрлық емес», қылмыстық құқықты қабылдауды еңсеру болып табылады. Бұл өте күрделі және көп қырлы мәселе, ол тек білім беру мекемелерінде кадрлар даярлауға және құқық қорғау органдарының қазіргі қызметкерлерінің біліктілігін арттыруға ғана қатысты емес.

Әдебиет

1. Википедия. Электронный адрес. https://ru.wiktionary.org/wiki

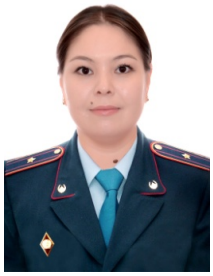
2. Курцвейл Р. Эволюция разума или бесконечные возможности человеческого мозга, основанные на распознавании образов / Рэй Курцвейл. – М.: Эксмо, 2019. – С. 352.

3. Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии. / пер. с англ. С. Филина. – М.: Манн, Иванов и Фербер, 2016. – С. 496.

4. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. №9. С. 5-16.

5. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. – М.: Юрлитинформ, 2018. – С. 312.

6. Қазақстан Республикасының Қылмыстық құқық бұзушылық Кодексі https://adilet.zan.kz/kaz/docs/K1400000226



АМАНОВА ДИАНА ТУРАНОВНА
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі факультетінің 2 курс докторанты полиция майоры,
ұлттық қауіпсіздік және әскери істер магистрі

КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫ ЦИФРЛЫҚ ОРТАДАҒЫ ҚЫЛМЫСТЫҚ ӘРЕКЕТКЕ ТАРТУ: МӘСЕЛЕЛЕР ЖӘНЕ ҚАРСЫ ТҰРУ ЖОЛДАРЫ

Дүниежүзілік желі интернет – бұл бүкіл әлем бойынша көптеген компьютерлерді біріктіретін және ақпараттық ресурстарға қол жеткізуге мүмкіндік беретін ғаламдық желі.

Кез келген адам үшін ақпараттық жаһандық өріс мемлекеттік және құқық қорғау органдарының, бұқаралық ақпарат құралдарының және жеке тұлғаның еркіндігін көрсету кеңістігіне айналғаны сөзсіз. Бірақ қазіргі қоғамның шындығына келсек, онда интернет кеңістігінің деградацияға айналып бара жатқандығы орын алады. Ол тез өзгеретін, сөз бостандығы аумағынан тыңшылық ойындарға ауысқан алаңға айналып жатыр [1].

Бүгінгі таңда интернет, өкінішке орай, адамға белсенді әсер ететін, үлкен көлемдегі деректерді қамтитын үлкен шатастырғыш веб құрал болып табылады. Дүниежүзілік желінің медаль екі жағы секілді оң және теріс жақтары бар. Әлеуметтік желілер немесе қосымшалар арқылы алынатын кез-келген ақпарат автоматты түрде біздің санамызға енеді. Оң көзқараспен қарағанда, егер сіз ақылға қонымды ақпарат алсаңыз интернет біз үшін орасан зор пайда әкеледі деп сенуге болады. Сонымен, дүниежүзілік желі ақыл-ой интеллектісін арттыруға, білімді жетілдіруге мүмкіндік береді. Көптеген адамдар интернеттің көмегімен шет тілдерін үйренеді, түрлі тренингтер, курстар өтеді, шет елдердің мәдениетін, дәстүрлерін, экономикасын және т.б. танысады.

Екінші жағынан, біз ақпараттық кеңістіктің біздің қоғамымызға жағымсыз әсер ететіндігін де байқаймыз. Өйткені адамның ақыл-ойы жағымсыз ақпаратты тез қабылдайды.

Осылайша, біз байқағанымыздай дүниежүзілік желі жыл өткен сайын ойын-сауық сипатындағы әлеуметтік ақпараттық қосымшаларды белсенді түрде дамытуда. Өкініштісі, бүкіл қоғам интернетке қол жеткізе алады, бірақ жас критерийлері, сондай-ақ психологиялық және моральдық белгілер бойынша қарапайым шектеулер бар. Оның ішінде әсіресе кәмелетке толмағандарға теріс әсер етеді.

Әлеуметтік желі бұл шексіз мөлшерде есірткі және психотроптық заттарды, соның ішінде синтетикалық, терабайттарды ашық сатуды, балалар порнографиясын жүзеге асыруды, сондай-ақ қылмыстық кірістердің миллиардтаған ағындарын, экстремистік және террористік бағытты насихаттауды және т.б. жүзеге асыруға болатын аумақ. Географиялық шекаралардың ашықтығы немесе толық болмауы, желі объектілерінің ұлттық тиесілігін анықтаудағы қиындықтар, оның ресурстарына анонимді қол жеткізуді жүзеге асыру секілді факторлардың барлығы қоғамдық және жеке қауіпсіздік жүйелерін осал етеді [2].

Интернет желісінде жасөспірімдер арасында көбінесе зорлық – зомбылық, суицидті насихаттау, дәстүрлі емес жыныстық қатынастар туралы ақпаратқа кеңінен тарап жатады. Көбінесе балалар өздерін қорлайды, мазақ етеді. Оны ғылыми тілде кибербуллинг деп атайды. Қазіргі уақытта жастар көше жүрмейді, ал байланыс болса ол виртуалды кеңістікте, әртүрлі интернет қауымдастықтар арқылы өтеді деп айтуға болады. Интернеттегі жағымсыз жолдар, мысалы ретінде «вписки» және «флэттер», яғни әлеуметтік желілерде құрылған аттас топтар арқылы бейтаныс адамдар ұйымдастыратын кештер қаптар жатыр [3].

Мақсаты ақпараттық ортаға зиян келтіру немесе оны құқыққа қайшы пайдалану болып табылатын жеке адамдардың немесе адамдар тобының іс - әрекеттерінің нәтижесінде интернет желісінде қылмыс жасау және интернет қылмыстың өркендеуі мүмкіндігі пайда болады. Интернет қылмыс – бұл интернет желісі арқылы жасалған заңсыз, әлеуметтік қауіпті әрекеттер [4]. Интернет желісіндегі немесе осы желіні пайдаланатын қылмыстар ақпараттық технологиялар саласындағы қылмыстарға жатады: зиянды вирустардың таралуы, парольдерді бұзу, несие карталарының нөмірлерін және басқа да банктік деректемелерді ұрлау, сондай-ақ интернет арқылы заңсыз ақпаратты (жала жабу, порнографиялық сипаттағы материалдар, ұлтаралық және дінаралық араздықты тудыратын материалдар және т. б.) тарату [5].

Кәмелетке толмағандардың интернет кеңістігіндегі жағдайы туралы мәселе өзекті болып отыр. Өкінішке орай, жасөспірімдер қылмыстың «құрбандары» ретінде ғана емес, сонымен бірге ықтимал қылмыскерлер ретінде де әрекет етуде.

Интернеттегі жасөспірімдермен жасалатын қылмыстар негізінен тауарларға, жұмыстарға, қызметтерге ақы төлеу, электронды әмияндардың баланстарын, онлайн ойындардағы шоттарды толтыру, дүкендерде, фаст-фуд мейрамханаларында басқа адамдардың банктік карталарымен жасалған төлемдер болып табылады. Көбінесе жастар әлеуметтік желілердегі аккаунттарды бұзады, құпия ақпаратты иемденеді, азаматтардың жеке өміріне араласады.

Ақпараттық технологиялардың дамуы жас ұрпақтың құқықтық санасына, қоғаммен өзара әрекеттесу кезіндегі мінез-құлқына әсер етеді.

Интернетке шектеусіз қол жеткізе отырып, жасөспірімдер онда орналастырылған тыйым салынған мазмұндағы ақпараттарды пайдалана алады. Олар өз кезегінде жасөспірімдер қылмысының деңгейінің жоғарылауына әкеп соқтырады. Себебі, жасөспірімдерді қылмыстық әрекетке тартуға ықпал ететін аккаунттар, топтар мен қауымдастықтар бар. Бұндай жағдайда қылмыстық әрекеттің негізгі түрлерін қарастырған жөн: жезөкшелік, балалар порнографиясы, есірткінің заңсыз айналымы, өзін-өзі өлтіру (суицид). Жасөспірімді қылмыстық әрекетке тарту өте оңай. Өйткені бұл жас буын біреудің ықпалына тез еретінін ескеру керек. Бұл өз кезегінде ауыр жағымсыз салдарға әкеліп соғады.

Ғалымдар О. Дамаскин, В. Красинский өскелең ұрпақты қылмысқа тартуға ықпал ететін келесі себептерді атап өткен: «балалардың жекелеген санаттарының сапалы білім алуға қол жеткізуіндегі сараңдылық, балалардың этикалық, азаматтық-патриоттық, мәдени дамуының төмен деңгейі жасөспірімдер ортасында этносаралық және конфессияаралық шиеленістің, ксенофобияның, кемсітушілік мінез-құлыққа, құрдастарының қорлауына («қорқыту») және басқа да әлеуметтік құбылыстарға әкеледі» [6].

Негізінен, интернет желісінде жасөспірімдерді жаппай кісі өлтіру, сатанизм, нашақорлық сияқты тақырыптар, сондай-ақ кез-келген рәсімдер, әртүрлі культтер және т.б. туралы ақпарат қоры бар қауымдастықтар қызықтырады. Өздерін осындай топтарға жатқыза отырып, жасөспірімдер қоғамға наразылық білдіреді. Желілік байланыста көрсетілген мұндай наразылыққа ақпараттық технологияларды қолдану арқылы әрекет ететін қылмыскерлердің реакциясы түседі. Келіп түскен ақпаратты дұрыс қабылдауға және талдауға қабілетсіз жасөспірімдер теріс әрекетке ұшырайды және сәйкесінше қылмыс жасайды. Бұл жағдайда оларға қоғам және өзіне өзі де зиян тигізуі мүмкін. Құқық қорғау органдары жасөспірімдер қылмысының деңгейін арттыруға ықпал ететін ақпараттың интернетте таралуына белсенді түрде қарсы тұрса да, экстремистер өздеріне қызығушылық танытқан аудиторияны едәуір кеңейте отырып, өздерінің ықпалын жас ұрпаққа арттыра алады.

Мұндай құбылыс қалай болып жатқанын А. Осипенко мен В.Соловьев өз жұмыстарында атап өтті: «желіде модераторлар күнделікті қарым-қатынас контекстінде шебер орналастырған нұсқаулар, ұсыныстар, шақырулар ұжымдық түрде келісілген және қоғамның көп бөлігі қолдайды деген елес тудыратын форумдар ұйымдастырылады. Сонымен қатар, соңғы уақытта киберкеңістіктегі құқық қорғау қызметінің күшеюіне байланысты экстремистік бағыттағы материалдар оның «көлеңкелі» сегменттеріне жаппай ауыстырылды, олар жаңа қатысушыларды алдын ала текеріп, «адал» болған соң ғана қол жеткізуге болады».

Интернет желісіндегі коммуникацияның өзіндік ерекшелігі бар. Ол қарым-қатынас ашық (әңгімелесушілер бір-бірін түсінеді) және анонимді (әңгімелесушінің аты-жөні мен басқа да

ақпаратар көрсетілмейді) болуы мүмкін. Көбінесе қылмыскерлер жасөспірімдермен жасырын түрде сөйлескенді жөн көреді. Мұны өздерін қорғау және жасөспірімді қызықтыру үшін жасайды, олар өздерінің бейнесін жасөспірімдердің қиялындағыдай қалыптастырады. Жасөспірімдермен байланысу үшін ақпараттық технологияларды қолданатын қылмыскерлер әртүрлі ниеттерге, әртүрлі терминологиялық қорға ие. Осылайша жаңа сөздер мен сөз тіркестері пайда болды:

– Кибербулинг (интернет-қудалау) – интернет желісіндегі қорқытулармен, жаман ниет білдіруші тарапынан жағымсыз сөздермен сипатталатын, әңгімелесушіні арандатуға, оны агрессивті реакцияға итермелеуге бағытталған іс-әрекеттер;

– Интернет желісіндегі аутинг – жасөспірім туралы теріс ақрпараттармен хабардар етіп жариялауға бағытталған іс-әрекеттер;

- Кибersталкинг – жасөспіріммен онымен жыныстық қатынасқа түсу мақсатында жеке кездесуді ұйымдастыруға бағытталған интернет желісіндегі ересектердің әрекеттері;

- Фрейпинг – шабуылдаушының жасөспірімнің есептік жазбасын, оның білімінсіз басқару мүмкіндігін алуы және т. б. [8].

Интернет арқылы қылмыскерлердің теріс әсеріне ұшыраған жасөспірімдердің әрекеттері туралы айта отырып, біз суицид сияқты әрекетке тоқталуды жөн көріп отырмыз. Жасөспірімдерде өз-өзіне қол жұмсауға деген ұмтылыстың пайда болуына желіде адам өмірінің құнсыздануы, оның мағынасыздығы туралы ақпаратты таратуға ықпал етуде. Мұндай типтегі қауымдастықтардың өзіндік символикасы, жаргондары, суицидтің құралдары мен тәсілдерінің арнайы бейнелері бар. Бұған қоса, мертігуге немесе өлімге әкелуі мүмкін әрекеттер немесе хобби туралы ақпаратты қамтитын қауымдастықтар да бар.

Сонымен қатар, интернетте жасөспірімдер қиялдаған бейнелер де жиі кездеседі, олардың адамдарға немесе жануарларға зиян келтіретіндігі айдан анық. Осындай әрекеттермен жастар өздерінің агрессиясын өздері үшін тұруға мүмкіндігі жоқ адамдарға жібереді.

Мысал ретінде «Dog hunters» деп аталатын қозғалыстың бір түрін қарастырған жөн, Оның мәні иттерді азаптау, ұру немесе өлтіру болып табылады. Жақында мұндай бағыт белгілі болды, оның идеологиясы жасөспірімдер арасында қоғамға жат әрекеттерді жасауға, атап айтқанда, адамның ар-намысы мен қадір-қасиетін қорлауға, бопсалауға бағытталған топтарды құруды көздейді [7].

Жасөспірімдердің жыныстық қол сұғылмаушылығына байланысты қылмыстар құқық қорғау органдарының ықпалына ие болды. Интернет кеңістігінде педофилдер назардан тыс қалған жоқ. Олар өмірлік қиын жағдайға тап болған және сырттан қолдауды қажет ететін жасөспірімдерді іздеуде. Жағдайды пайдаланып, олар қылмыскерлерге сеніп, кейіннен жыныстық сипаттағы әрекеттерді жасайды. Мұндай өзара әрекеттесудің мысалы ретінде: жасөспірімнен интимдік фотосуреттер сұрау, жыныстық тақырыптар бойынша қарым-қатынас жасау, жасөспірімдерге порнографиялық материалды немесе өздерінің ұятсыз фото және бейнематериалдарын жіберу. Сондай-ақ есірткі қылмысын және оған жасөспірімдерді тартуды да назардан тыс қалдыруға болмайды. Жасөспірімдер тыйым салынған заттарды сынап көруге немесе оларды тасымалдау кезінде қолма-қол ақша алуға қызығушылық танытады.

Жастар есірткі бизнесі туралы және онымен байланысты барлық нәрселер туралы: есірткіні дұрыс сақтау, тасымалдау және қолдану туралы ақпаратты қамтитын әртүрлі интернет қауымдастықтардан біледі. Осылайша, ақпараттық технологияларды жасөспірімдер кеңінен қолданады және әрқашан жағымды жағынан емес екендігі өте өкінішті. Көптеген теріс қауымдастықтар, топтар мен аккаунттар бар. Олардың негізгі міндеті жас ұрпақты қылмыстық әрекетке тарту.

Ақпараттық технологиялардың дамуымен қатар киберқылмыс та дамып келеді. Қоғамға наразылық білдіру мақсатында жасөспірімдерді қосатын жаңа қозғалыстар мен бағыттарды пайда болауда. Құқық қорғау органдары өз кезегінде, осы мәселені шешумен айналысып жатыр. Интернет арқылы қылмыскерлерді қадағалап, кейіннен оларды жауапқа тартады.

Алайда, ол анонимді әрекет ететіндіктен, кінәліні табу әрдайым мүмкін емес. Жасөспірімдердің қылмыстық қауымдастықтарға кіруіне жол бермеу үшін, біздің ойымызша, жасөспірімдердің әлеуметтік желілердегі қызметіне ата-аналық бақылауды күшейту керек.

Олардың тәрбиесіне көбірек көңіл бөлу керек, жанжал туындаған кезде бала әлеуметтік желілерден мәселенің шешімін іздемеуі үшін психологқа жүгіну керек.

Құқық қорғау органдары өз кезегінде қоғамға қылмыстық ықпал ету көзін уақтылы анықтап және оны жою мақсатында ақпараттық технологияларды жетік меңгерулері керек.

Сонымен, қорытындылайық, сандық ортада кәмелетке толмағандардың қылмысы көбейіп келеді. Бұл мәселенің көптеген аспектілері бар, соның ішінде:

1. Кибербуллинг: кәмелетке толмағандар интернетті және әлеуметтік медианы құрдастарын қорлау, қорқыту және бопсалау үшін пайдалана алады. Бұдан зардап шегушілер ауыр психологиялық проблемаларына әкелуі мүмкін.

2. Киберқылмыстар: кәмелетке толмағандар интернетті жеке басы тұралы мәліметтерді ұрлау, шоттарды бұзу және басқа да қылмыстар жасау үшін пайдалана алады.

3. Интернетке тәуелділік: кәмелетке толмағандар интернетте тым көп уақыт өткізуі мүмкін. Бұл денсаулыққа кері әсерін тигізіп, әлеуметтік бейімделуге әкелуі мүмкін.

4. Заңсыз мазмұн: кәмелетке толмағандар интернетте порнография немесе зорлық-зомбылық сияқты заңсыз әрекеттерге тап болуы мүмкін.

5. Ойындарға тәуелділік: кейбір ойындар тәуелділікті тудыруы мүмкін және кәмелетке толмағандарды оқу мен әлеуметтік өмірден алшақтатуы мүмкін.

Қорытындылай келе, әртүрлі ақпараттық-телекоммуникациялық технологиялардың дамуы, олардың барлық топтарға кеңінен қол жетімділігі қажетті ақпаратты іздеуде және әртүрлі маңызды жұмыстарды орындауда ыңғайлылық пен игіліктерге ғана емес, сонымен қатар кәмелетке толмағандардың қалыптаспаған жеке басына үлкен қауіп төндіреді деген қорытындыға келеміз. Біріншіден, бұл мұндай қылмыстардың алдын алу және құқық бұзушыларды жазалау бойынша құқықтық шараларды жетілдіруді талап етеді. Сондай-ақ, кәмелетке толмағандардың психикалық және физикалық денсаулығын сақтау үшін бірінші кезектегі жауапкершілік олардың ата-аналары мен заңды өкілдеріне жүктелетіндігін қабылдаған жөн. Өйткені дәл осы адамдар балалар мен жасөспірімдер үшін ең жақын адамдар. Сондықтан, жоғарыда аталған проблемалармен күресу үшін ата – аналардың, мектептердің, үкіметтік ұйымдардың және интернет компаниялардың бірлескен жұмысы қажет. Балаларды интернеттегі қауіпсіздікке үйретететін олардың желідегі белсенділігін бақылайтын , бір сөзбен айтқанда олардың дамуы үшін қауіпсіз орта құру қажет

Әдебиет

1. Cyber security risks for minors: a taxonomy and a software architecture / A. Tsirtsis et al. // Semantic and Social Media Adaptation and Personalization (SMAP) 2016: 11th International Workshop on, Thessaloniki, Greece, Oct. 20-21, 2016. - IEEE, 2016. - P. 93-99.

2. The Global Risks Report 2018 // World Economic Forum //URL:// http://www.iccwbo.ru/news/2018_WEF_GRR18_Report.pdf

3. «Дети онлайн: подростковая преступность в интернете растет» //https://www.bsatu.by/sites/default/files/images/u581/prestupnost_v_internete.pdf

4. Гузеева О.С. Действие УК РФ в отношении интернет-преступлений // Закон России: опыт, анализ, практика. 2013. №10.

5. Преступления в сети интернет: общая информация. URL://https:// www.rukazakona.ru

6. Дамаскин О.В., Красинский В.В. Криминологическая характеристика механизма вовлечения несовершеннолетних в противоправную деятельность // Государство и право. 2020. №8. – С. 41-54.

КУРМАНГАЛИЕВА ЛАУРА ЖУМАБЕКОВНА
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі факультетінің 2-курс докторанты, полиция капитаны, з.ғ.м.

КӨЛІК ҚҰРАЛДАРЫН БАСҚАРАТЫН АДАМДАРДЫҢ ЖОЛ ЖҮРІСІ НЕМЕСЕ КӨЛІК ҚҰРАЛДАРЫН ПАЙДАЛАНУ ҚАҒИДАЛАРЫН БҰЗУ ҚЫЛМЫСЫНЫҢ АЛДЫН АЛУДА ЦИФРОВИЗАЦИЯНЫҢ МАҢЫЗЫ

Кейінгі жылдары елімізде кез-келген сала секілді жол-көлік инфраструктурасы да цифровизацияға бет бұрып келеді. Бұл дегеніміз, технология мен цифрлық жаңалықтар неғұрлым жол қауіпсіздігін арттырған сайын, соғұрлым жол-көлік оқиғасының санын азайтуға септігін тигізеді деген сөз. Мысалға алар болсақ, бейне бақылау камералары мен автокөліктердің нөмірлерін анықтау жүйесі жол жүру ережесін бұзғандарды қадағалап, жол – көлік оқиғаларының алдын алуда көмегін тигізіп жатыр. Дегенмен, цифровизация инвестиция мен қаражатты қажет етеді. Бұл мәселені шетелдік инвесторларды тарту арқылы шешуге болады деп ойлаймын.

Жол қозғалысы саласындағы цифровизация қазіргі ақпараттық технологияларды пайдалану арқылы транспорт инфрақұрылымының тиімділігі мен қауіпсіздігін жақсартуға бағыт береді. Цифрлық технологиялар мен технологиялық жүйелер тұтастай алғанда объектілер мен процестерді тиімді басқару мақсатында электронды түрде ақпарат ағындарын жинауға, өңдеуге, сақтауға, беруге және тасымалдауға арналған құралдар мен жүйелерді білдіреді. Қазір тіптен автомобиль жолдарының жағдайы мен параметрлері және оларды жайластыру туралы ақпараттар базасының бар екендігін естен шығармағанымыз жөн. Осы ақпараттар базасында кеңістіктік географиялық координаталар, тікбұрышты координаттар жүйесіне түрлендіру арқылы мобильді лазерлік сканерлеу технологиялары; белгілі бір дискреттілігі бар жоғары ажыратымдылықтағы панорамалық фотосуреттер және басқа да өлшеу құралдары қамтылған. Алынған ақпарат автомобиль жолдарының ортофотокарталарын (мысалы, қозғалысты ұйымдастыру шараларын әзірлеу кезінде міндетті болады), сондай-ақ көлік инфрақұрылымы объектілерінің үш өлшемді модельдерін және жол төсемдерінің құрылымы мен жай-күйін визуализациялауға мүмкіндік береді. Сонымен қатар олардың ағымдағы жағдайын талдау және кемшіліктерді жою шараларын әзірлеуге де септігін тигізеді. Шамамен 15 жыл бұрын «цифрлық егіздер» жобалық құжаттаманы әзірлеу кезінде ол тек үлгі түрінде ғана болса, бүгінгі таңда технологиялар көлік инфрақұрылымының объектісінің осал тұстарын анықтауға, объектідегі қауіпті жағдайларды болжауға және жедел алдын алуға мүмкіндік береді.[1] Дегенмен, бұл технологиялар біздің Қазақстанда емес, басқа дамыған елдерде оң нәтижесін көрсетуде.

Жолдарда көліктердің жылдамдығын, транспорт ағындарының арасында бағдарлауда жүрген автокөліктерді (муляж), іздеуде жүрген жалған мемлекеттік нөмірмен жүрген және жүргізуші күәлігінен айырылып заңсыз автокөліктерді басқарғандарды анықтайтын интеллектуалды бейнебақылау жүйелерінің рөлін бағаламау мүмкін емес. Сондай-ақ көлік құралдарын негізсіз тоқтату, тұраққа қою және тұраққа қоюдың белгіленген ережелерін бұзу; салмақтық бақылауды бұзу; қарсы қозғалыс жолағына шығу; жол қиылыстарынан, өткелдерден және жаяу жүргіншілер өткелдерінен бағдаршамның тыйым салу сигналына өту;

ақылы автомобиль жолына тиісті төлем енгізбей кіру секілді функцияларды іске қоссақ артық болмас.

Тәжірибе көрсеткендей полицияның барлық күштері мен активтерін тәулік бойы үйлестіретін және басқаратын, қылмыстар мен құқық бұзушылықтар, оқиғалардың барлық сигналдарына жедел назар аударатын Жедел басқару орталықтарын дамыту қажеттілігіне көз жеткізіп отырмыз.

Бейнебақылау камераларының көмегімен жыл сайын 2,5 мыңға жуық қылмыстық және 400 мыңнан астам әкімшілік құқық бұзушылық анықталады.

Өткен жылдың соңында Алматы полицейлері пилоттық режимде «Sergek Qorgau» мобильді қосымшасын сынай бастады. Бүгінгі таңда бұл қосымша Шымкент және Алматы полиция департаменттерінің патрульдерінің жұмысында қолданылады. «Sergek Qorgau» – полиция қызметкерлерінің жұмысына арналған мобильді қосымша. Қосымша патрульдік полицейлердің планшеттеріне орнатылады және қалалардың жолдарындағы «Сергек» аппараттық-бағдарламалық кешендерімен біріктірілген . Сондай-ақ «Sergek Qorgau» құқық бұзушыларды, жалған нөмірлерді, жүргізуші куәлігінен айырылған адамдардың автомобильдерін, іздеуде жүрген машиналарды анықтайды. Бірақ қосымшаның негізгі функцияларының бірі-ықтимал қауіпті жүргізушілерді анықтау. Сондай-ақ мамандандырылған алгоритмдердің көмегімен жолдарда авариялық жағдай туғызатын жүргізушілерді анықтайды. Мұндай көліктер туралы ақпарат операторға да беріледі. Қолданба олардың орналасқан жерін берілген радиуста көрсетеді. Полицей мұндай көлікті тоқтатып, ықтимал ЖКО жасалғанға дейін алдын алу шараларын қолдана алады. Естеріңізге сала кетейін, «Сергек» қазіргі уақытта Астана, Өскемен, Алматы, Атырау және Шымкент қалаларында жұмыс істейді. [2] Автоматты бекіту құралдарының жұмыс принципі оған әсер ететін көптеген факторларды ескеретін көп деңгейлі жүйе болып табылады, ал модельдердің әртүрлілігі оларды қолданудың әртүрлі техникалық ерекшеліктеріне әкеледі. [3] Қазіргі таңда полицияның жалған мемлекеттік нөмірлерді пайдаланатын, көліктерге арнайы белгі беру құрылғыларын орнатқан көлік жүргізушілерін, сондай-ақ көлік құралдарын мас күйінде басқарған адамдарды жауапкершілікке тарту бойынша мақсатты жұмыстары жалғасуда.

Статистикаға сүйенсек, Қазақстанда жыл сайын орта есеппен 16 мың жол-көлік оқиғасы (ЖКО) орын алады, онда орта есеппен 2 мың адам қаза табады, 18 мың адам әртүрлі дәрежедегі жарақаттар алады.

ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу комитетінің деректері бойынша, елде 2022 жылдың қаңтар-қыркүйегінде ғана 10,2 мың апат орын алып, 15 мыңнан астам адам зардап шекті. 2021 жылдың ұқсас кезеңімен салыстырғанда ЖКО санының өсуі 8,9%-құрады. Бұл ретте 1,7 мың адам қаза тапты (21%-ға ұлғайды),оның ішінде 181 кәмелетке толмаған бала, 457 әйел және1 258 ер адам.

ЖКО зардап шеккендер арасындағы кәмелетке толмағандардың үлесі 19,9% (3007) құрайды. Олар негізінен автокөлік құралдарының соқтығысуынан зардап шекті. Сондай-ақ, 542 қоғамдық көліктің қатысуымен 532 ЖКО орын алып, 70 адам қаза тауып, 783 адам жараланды. Салыстыру үшін: Польшада бұл көрсеткіш 5,9 адамды, Германияда – 3,1, Швецияда – 1,9 адамды құрады.

Деректерді талдау көрсеткендей, ЖКО-ның 86,6%-дан астамы жүргізушілердің кінәсінен (8 886, 2021 жылы – 7 726) орын алады, оның 363-і (414) алкогольдік немесе есірткілік мас күйінде болған. Жол апатынан зардап шеккендердің ішінде ең көбісі 30-39 жас аралығындағы адамдар – 2 947, сондай-ақ 21-29 жас аралығындағы жастар – 2 953. Негізінен ЖКО кінәлі тұлғалар 30-39 жас аралығындағы адамдар – 2 616, сондай – ақ 21-29 жас аралығындағы жастар - 2 395. 60 және одан жоғары жастағы қарттар – 670 адам.

Жол апаттарының басым бөлігі немесе 7 471 (6 375) елді мекендерде жасалды, 1 918 (1 702) халықаралық, республикалық маңызы бар трассаларда, 869 (870) облыстық, аудандық маңызы бар жолдарда тіркелді. Жол – көлік оқиғаларының ең көп саны дүйсенбіде

– 1 567, сенбіде – 1 538 және сейсенбіде – 1 493, сондай-ақ күндіз – 6 253, түнде – 1 157 және кешкі уақытта – 1 662 болды.

Жол-көлік оқиғаларының көпшілігі құрғақ жолда – 7 864, дымқыл жолда – 674, қарда – 309, мұзда – 115. Бұрынғыдай Алматы қаласының жолдарында апаттардың ең көп саны – 2 620 жағдай, ал өлім-жітімнің ең жоғары көрсеткіші Алматы облысында белгіленді, онда 327 адам қаза тапты, елордада 495 ЖКО тіркелді. Ең аз ЖКО Солтүстік Қазақстан облысы – 221 және Шымкент қаласы – 217 жолдарында тіркелген.Статиститка көрсеткендей, біздегі қолданыстағы «Sergek Qorgau» - цифрлық мобильді қосымшасын әлі де болса жетілдіріп, басқа да заманауи жол-көлік қылмыстарына төтеп бере алатындай цифрлық құрылғыларды ойлап-табуымызға тура келеді[4].

Қазақстан Республикасының жол қозғалысы қауіпсіздігінің жағдайы маңызды әлеуметтік-экономикалық және құқықтық мәселе болып табылады. Жолдардағы апат деңгейі, оның абсолютті көрсеткіштерінің біршама төмендеуіне қарамастан, айтарлықтай жоғары болып қала береді. Осыған орай Қазақстандағы сарапшылардың пікірінше, еліміздегі жағдайды өзгерту үшін жол қауіпсіздігін арттыру бойынша түбегейлі шаралар қабылдануы қажет. Атап айтқанда, Қазақстанда vision Zero бағдарламасын қабылдау және енгізу ұсынылып отыр. Оған мынадай шаралар кешені кіреді: ерекше авариялық учаскелердегі жылдамдық режимін төмендету, көшелердің дизайны мен геометриясын өзгерту, қауіпсіздік аралдарын салу, қоғамдық көлік жүргізушілерін даярлау тәсілдерін өзгерту, трафикті тыныштандыру жөніндегі іс-шаралар және тағы басқалар. «Азия даму банкінің» зерттеуіне сәйкес Қазақстанда ЖКО-дан жинақталған залал бір адам қайтыс болған жағдайда 113 млн.теңгені және жарақат алған кезде 16 млн. теңгені құрайды. Vision Zero – бұл жолдағы нөлдік өлімге қол жеткізу тұжырымдамасы. Vision Zero бағдарламасы алғаш рет Швецияда 1997 жылы жасалған және содан бері үнемі жетілдіріліп келеді. Швециядағы ЖКО салдарынан өлім – жітім 1997 жылғы 100 мың тұрғынға шаққанда 7 адамнан 2001 жылы 1,9 адамға дейін қысқарды. Бүгінгі таңда бағдарлама Лондон, Вашингтон, Торонто, Чикаго және басқалары сияқты әлемнің көптеген озық қалаларында жұмыс істейді. Бағдарламаның негізгі қағидасы ол өлімге алып келетін жол-көлік оқиғаларына жол бермеу [5].

Цифрландыру көлік құралдарын басқаратын адамдардың жол жүрісі немесе көлік құралдарын пайдалану қағидаларын бұзу қылмыстарын алдын алуда маңызды рөл атқарады:

1. Жол қозғалысын бақылау: бейнебақылау камералары мен басқа да бақылау құралдарының көмегімен жол қозғалысын бақылауға және құқық бұзушылықтарға тез жауап беруге болады. Себебі радарлар мен сканерлер автокөліктердің жылдамдығын өлшеп, жылдамдықты асырған кезде іске автоматты түрде қосылады. Сондай-ақ бағдаршамның қызыл түсінен өтіп кету, бағдаршам жанғанда тоқтау сызығынан асып кеткен кезде бекітетін, сонымен қатар автокөліктің мемлекеттік нөмірін қарап отыратын фото, видео фиксация жасайтын құрылғалар арқылы жүзеге асырылады.

2. Құқық бұзушылықтарды автоматты түрде тіркеу: құқық бұзушылықтарды автоматты түрде тіркеу жүйелері арқылы бұзушылар туралы деректерді жинауға және жол қозғалысы ережелерін бұзғаны үшін жауапкершілікті белгілеуге мүмкіндік береді. Ол дегеніміз жол жүру ережесін бұзу фактілерін қарап отыратын құрылғылар бағдаршамда, жол жиектерінде, жаяу жүргіншілер жүретін жердің алдында т.с.с. орналасуы мүмкін. Ол құрылғыда камера, қозғалыс датчигі, программалық қамтамасыз ету, мәліметтер базасы болады. Осы ата аталған құрылғылар іске қосылғанда автокөлік иесіне айыппұл келіп жатады.

3. Деректерді талдау: цифрлық технологиялар апат туралы деректерді талдауға және оқиғалардың себептерін анықтауға мүмкіндік береді, бұл болашақта осындай жағдайлардың алдын алуға мүмкіндік береді. Бұл өте тиімді талдау. Неге десеңіз, бұл ақпарат қорында жол-көлік қылмысы, оның ішінде апат көп жасалатын жердің себептерін анықтауға болады: құқық бұзушыдықтың түрін, оның уақыты, жол-көлік апатын жасаған автокөліктің маркасы. Осы аталған деректер қоры жиналған соң, жол қозғалысын ережесін бұзудың түрлері, орындары және уақыты бойынша жиілігі мен таралуын; құқық бұзушылықтар мен апаттар арасындағы

байланыс; жол кептелісі, ауа райы жағдайлары және т.б. сияқты факторлардың бұзушылықтар санына әсері; әртүрлі аудандардың немесе қалалардағы жол-көлік оқиғасын салыстыру секілді анализдер жасауға болады.

Анализ жүргізілгеннен кейін жол-көлік оқиғасының санын азайтуға және жол қозғалысы қауіпсіздігін жақсартуға бағытталған шараларды әзірлеуге болады.

4. Жүргізушілерді жол мәдениетіне оқыту: цифрлық технологияларды пайдалану жүргізушілерді жоғары деңгейде оқытуға және олардың жол қауіпсіздігін арттыруға мүмкіндік береді. Электрондық курстар мен тренажерлар арқылы жүргізушілерге жол ережелерін үйретуге және олардың жүргізу дағдыларын жақсартуға болады.

5. Хабардар болуды арттыру: цифрлық технологиялар, оның ішінде видеороликтер халықты жол қозғалысы ережелері мен бұзушылықтардың салдары туралы хабардар етуге мүмкіндік береді, бұл хабардар болуды арттырады және ЖКО санын азайтады.

6. Көлік мониторингі: GPS технологиялары арқылы көлікті бақылау жүйелері көлік құралдарының қозғалысын бақылауға және нақты уақыт режимінде жол қозғалысы ережелерін бұзу туралы білуге мүмкіндік береді. Оны іске асыратын мемлекеттік органдар, автокөлік ұйымдары, қоғамдық ұйымдар.

7. Бейнебақылау: жолдарда бақылау камераларын орнату жол қозғалысы ережелерін бұзушылықтарды тіркеуге және ЖКО кінәлілерін анықтауға көмектеседі.

8. Деректерді талдау: ЖКО туралы деректерді жинау және талдау жолдардың ең қауіпті учаскелерін анықтауға және оларды жақсарту бойынша шаралар қабылдауға көмектеседі. Цифрлық технологиялардың арқасында ЖКО-ның жиі кездесетін түрлерін анықтауға және олардың алдын алу бойынша бағдарламалар мен іс-шараларды әзірлеуге болады.

9. Электрондық деректер базасы: жүргізушілер мен көлік құралдары туралы электрондық деректер базасын құру ЖКО кінәлілерін тез және дәл анықтауға және оларды жазалау бойынша шаралар қабылдауға мүмкіндік береді.

Жоғарыда аталған барлық шаралар апатқа байланысты қылмыстардың алдын алуға және жол қауіпсіздігін жақсартуға көмектеседі.

Әдебиет

1. D. Enin, Ph.D., Director of the Institute of Applied Transport Research LLC, Associate Professor of MADI..

2. https//egemen.kz>article>31052 басты бет

3. Керимов М.А. Модель системы автоматизированной // Развитие теории и практики грузовых автомобильных перевозок, фотовидеофиксации правонарушений [Текст] // М.А. Куримов, Р.Н. Сафиуллин, А.В. Марусин транспортной логистики 02-03 декабря 2015 года к юбилею ФГБОУ ВПО «СибАДИ» Международная научно-практическая конференция. 16.11.2015 г.

4. Қазақстан Республикасының Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің көрсеткіші.

5. Программа по повышению безопасности дорожного движения в Казахстане [Электронный ресурс]. – Режим доступа:https://rus.azattyq-ruhy.kz/society/45639-programmu-popovysheniiu-bezopasnosti-dorozhnogo dvizheniia-v-kazakhstane-predstavili-v-amanat– Загл. с экрана.

САРБАСОВ АЛИХАН ЕРЖАНОВИЧ
Докторант 1 курса послевузовского факультета Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции, магистр права

РАЗВИТИЕ УГОЛОВНОГО ПРАВА В УСЛОВИЯХ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Одно из определений понятия права гласит, что «право – это относительно равный и справедливый масштаб (мера) свободы, диктуемый развитием цивилизации» [1, С. 115], развитие цивилизации и научно-технического прогресса – одни из главных факторов изменений и в праве.

Так, например, уголовно-правовая охрана права частной собственности в том виде, в каком мы его знаем, оформилась в Новое время благодаря состоявшейся первой промышленной революции в XIX в. (создание паровых двигателей и резкое увеличение производительности труда). Затем состоялась вторая промышленная революция, заключавшаяся в тотальной электрификации общества в XX веке. Вследствие, чего такой предмет преступления, как электричество, просто бы не появился. Третья революция ознаменовалась автоматизацией промышленности и внедрением роботизированных производств в середине XX века, как следствие, в уголовном праве криминализируются деяния, связанные, например, с хищением программного обеспечения. Глава, посвященная компьютерным преступлениям, также появляется в уголовных кодексах большинства стран вследствие этого явления.

В настоящее время человеческая цивилизация шагнула в так называемую четвертую промышленную революции, которая подразумевает внедрение вычислительных процессов в повседневную жизнь общества. Речь идет как о ставших уже вполне привычными системах, например учета данных (электронные базы данных, цифровые документы и т. п.), так и о совершенно новых вещах, таких как, в частности, искусственный интеллект, квантовые вычисления, распределенные реестры, автономная роботизация, виртуальная и дополненная реальность и т. п.

Современная криминологическая наука до сих пор не выработала теорий, которые бы однозначно могли заранее предугадать совершение преступления конкретным лицом. Прогнозный анализ – сложный процесс, в котором используются большие объемы данных для прогнозирования и формулирования потенциальных результатов. В сфере уголовного права эта работа в основном принадлежит органам внутренних дел, практикующим и другим специалистам, которые должны приобретать опыт в течение многих лет.

С помощью ИИ объемы информации о праве и правовом приоритете, социальной информации и СМИ могут использоваться для выработки решений, выявления преступных организаций, а также прогнозирования и выявления людей, подвергающихся риску от преступных посягательств.

ИИ также способен анализировать большие объёмы информации, имеющей уголовно-правовое значение, для прогнозирования возможно преступного рецидива. Существующие

автоматизированные поисковые системы содержат огромные массивы информации, анализ которой потенциально может предсказать риск повторного совершения преступления.

Искусственный интеллект может найти свое применение в различных направлениях деятельности правоохранительных органов от методик ведения допроса до выявления заранее запланированных мест проведения несанкционированных акций.

Чем выше технологический уровень государства и общества, чем глубже информационно-коммуникационные технологии проникли во все сферы жизни общества, тем более уязвимыми они становятся для организованной преступности и террористов. Каждая высокая технология имеет тройное применение: гражданское, военное и криминальное. В связи с этим любая промышленная революция не только открывает новые возможности для общества и государства, но и наделяет преступников не существовавшими ранее способами и инструментами для совершения преступлений, порождает новые угрозы объектам уголовно-правовой охраны.

Киберугрозы затрагивают все общество в целом, и их невозможно ликвидировать полностью в связи с тем, что цифровые технологии успешно работают в силу своей открытости, а это сопряжено с риском. Однако уголовному праву под силу выявить эти угрозы и разработать уголовно-правовой механизм по их минимизации. Очевидно, что уголовное право будет вынуждено приспосабливаться к меняющемуся обществу. Проблема в том, что подобных посягательств в последние несколько лет становится все больше, при этом уголовное право не всегда успевает адекватно отвечать новым вызовам. Разумеется, юридическое научное сообщество уже всерьез начинает задумываться о происходящих изменениях, особенно в тех сферах, которые требуют уголовно-правового регулирования. Так, например, на повестку дня выносятся вопросы приспосабливания отдельных уголовно-процессуальных механизмов к развивающимся бурными темпами распределенным реестрам, в частности к технологии блокчейна [2].

Соотнося цифровые технологии и право в целом, чаще всего ученые-юристы касаются тем их практического применения в рамках контроля и регулирования (камеры видеонаблюдения, использование систем определения местоположения, цифровая подпись и т. п.) либо вопросов ограничения или вовсе запрета использования (персональные данные, криптовалюты, цензура в интернете и т. п.).

Думается, что отмеченное является лишь частью глобального вопроса о неизбежной трансформации фундаментальных основ уголовного права в условиях цифровизации и информатизации общества.

В частности, постоянно возрастающая вычислительная мощность компьютеров в обозримом будущем приведет, в том числе, к тому, что существующие сегодня средства шифрования и защиты данных в сети Интернет и цифровых базах данных окажутся неэффективными, если не будут изобретены совершенно иные механизмы их защиты. Мощности компьютеров будет хватать для расшифровки практически любой зашифрованной информации. Наступление такого момента все чаще связывают с появлением в будущем квантовых компьютеров.

Следствием этого станет эпоха практически полностью прозрачных персональных данных в виртуальном пространстве, которые сегодня активно туда загружаются (например, через сервис «egov» в Казахстане).

Традиционные права граждан на тайну личной переписки, неприкосновенность частной жизни станет крайне сложно обеспечивать и охранять. В какой-то момент эти права окончательно станут фикцией в цифровой среде и потребуют пересмотра с точки зрения в первую очередь уголовно-правовых основ. Одновременно с этим могут появиться ранее немыслимые объекты и предметы уголовно-правовой защиты. Пример тому – персональные данные граждан. Другой пример реализуется в настоящее время в Китае. Там уже введена в действие «система социального кредита», или «система социального рейтинга». Не исключено, что со временем подобная система, развившись в Китае, станет

транснациональной. Вполне возможно введение новых непосредственных объектов уголовно-правовой охраны, например, в связи с незаконным использованием подобных рейтингов или манипулированием ими. Следующий пример – это правовой статус искусственного интеллекта. В частности, может ли искусственный интеллект являться субъектом преступления? В случае положительного ответа какое уголовное наказание и как применить по отношению к нему? Другая сторона этого же вопроса заключается в уголовно-правовой охране авторских прав. В настоящий момент с использованием искусственного интеллекта пишутся рассказы, сочиняется музыка, создаются видеоклипы. Способен ли искусственный интеллект присвоить авторство или иметь собственные авторские права? В данной области до сих пор существует правовой пробел, который неизбежно придется устранять. Нельзя не согласиться с точкой зрения зарубежных коллег, что цифровые технологии уже сегодня тонко, но очень эффективно влияют на значимые общественные отношения. Речь идет об осмысленном и управляемом влиянии социальных сетей на новостную и политическую повестку конкретных людей, при котором объективная картина мира подменяется искусственно формируемой. С учетом того, что такая манипуляция может прямо воздействовать на результаты выборов, общественное мнение, рынок ценных бумаг и многое другое, такие правоотношения также должны подлежать уголовно-правовой охране.

В свете озвученных проблем нельзя обойти стороной и так называемый криминологический тупик. Фрагментарность, разрозненность, постоянные терминологические споры рискуют превратить криминологическое знание из науки в астрологию. Развитие цифровых технологий ставят перед этой наукой новые вызовы, решить которые в состоянии только совершенно новые подходы. В таком ключе необходим качественный переход к вычислительной криминологии, где большие данные становятся одним из ключевых объектов криминологического изучения [3]. Переход на новый уровень создаст серьезный инструмент для своевременного выявления зарождающихся проблем, точного прогнозирования и, в конечном счете, для пересмотра уголовно-правовых подходов с учетом новой реальности.

Вышеперечисленные обстоятельства дают основание полагать, что в обозримом будущем радикальная трансформация существующих базовых уголовно-правовых положений в условиях четвертой промышленной революции становится неизбежной. Безусловно, цифровые технологии в уголовном праве необходимо развивать в целях его устойчивого развития, закрепления уровня безопасности общества и адекватного отражения качественных характеристик преступности в уголовно-правовых инструментах. Однако, если мы констатируем данный факт, то непременно возникает вопрос о целях и средствах данного процесса и методах его реализации. Иначе говоря, переводя вопрос из метафизической реальности в чисто практическую плоскость, строить ответ необходимо будет совсем иначе: а именно как это будет происходить и в чем сущность такой цифровизации уголовного права? В рамках поставленного вопроса идея цифровизации уголовного права состоит в необходимости нормализации содержательного элемента уголовно-правовой материи. На деле же все это сводится к ряду предположений, которые в сущностном (практическом преломлении) плане включают в себя ряд аспектов:

а) предварительный сбор и оценку криминологической информации о состоянии киберпреступности и использование существующих цифровых технологий обработки больших данных;

б) «оцифровка» данных по уголовным делам, материалам об административных правонарушениях, материалах об отказе в возбуждении уголовного дела и т.д. с целью направления их в единую информационную базу данных о киберпреступности;

в) цифровизация информации правового характера, массива данных в уголовно-правовой сфере, создание интернет-баз уголовного права;

г) проведение цифрового анализа текста действующего уголовного закона с помощью разработанных программ искусственного интеллекта на предмет выявления и устранения в нем несоответствий, логических ошибок и т.п.;

д) алгоритмизация существующей системы правил квалификации преступлений и разработка цифровой теоретической модели квалификации противоправных деяний правоприменительными органами, а также пошаговых действий работников органов прокуратуры, суда, следствия;

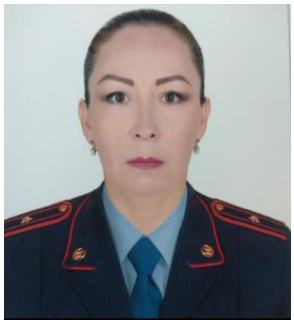
Таким образом, цифровизация уголовного права – это, по сути дела, приведение уголовного закона в формат, обеспечивающий возможность его машинной обработки. С этой точки зрения, она должна будет повысить качество уголовно-правовых институтов, обеспечить исчислимость целей уголовного права, а также повысить эффективность уголовно-правового воздействия на лиц, совершивших преступление.

Литература

1. Абдуллаев М.И. Теория государства и права / М.И. Абдуллаев. – М.; СПб., 2003. – С. 396.

2. Власова С.В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности / С.В. Власова // Библиотека криминалиста. Научный журнал. – 2018. – №1. – С. 9-18.

3. Шеслер А. Мошенничество: проблемы реализации законодательных новелл / А. Шеслер // Уголовное право. – 2013. – № 2. – С. 70-71.



КУБАНОВА НУРГУЛЬ БАЙТОКОВНА
докторант Алматинской академии МВД Республики Казахстан им. М. Есбулатова
майор полиции

КОЙШИБАЕВ ЕРКЕБУЛАН УЛАНОВИЧ
старший оперуполномоченный по особо важным делам отдела по борьбе с киберпреступлениями управления криминальной полиции ДП г. Алматы,
подполковник полиции

ЮРИДИЧЕСКИЕ АСПЕКТЫ БОРЬБЫ С КИБЕРАТАКАМИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ

Цифровизация общества приводит к росту киберпреступности, включая кибератаки. В современном информационном обществе, где все большее количество аспектов нашей жизни зависит от цифровых технологий и сетей, кибербезопасность становится вопросом первостепенной важности. С ростом числа кибератак, угроз и инцидентов, необходимость эффективного противодействия становится неотъемлемой частью стратегии безопасности государств и организаций.

Одним из важных аспектов противодействия кибератакам являются уголовно-правовые меры. Уголовное право должно обеспечить справедливость и наказание за совершение киберпреступлений, а также создать эффективный механизм контроля и санкций для предотвращения таких преступлений в будущем.

Цель данной работы заключается в анализе уголовно-правовых аспектов противодействия кибератакам и разработке рекомендаций по их совершенствованию. Для достижения этой цели рассматриваются основные нормативно-правовые акты, регулирующие кибербезопасность в Республике Казахстан.

«По мере роста киберпреступности важно совершенствовать систему кибербезопасности. В этой связи Президент Республики Казахстан Касым-Жомарт Токаев в своем послании дал ряд поручений. В частности, проведена работа по трансформации программы «Цифровой Казахстан» в концепцию развития сферы информационно-коммуникационных технологий и цифровой сферы. Для его реализации разработан национальный проект «Цифровой образ жизни (DigitEL)» [1].

Так, в июне 2017 года была утверждена государственная концепция кибербезопасности «Киберщит». Документ основан на текущей ситуации в сфере информатизации государственных органов, автоматизации оказываемых государственных услуг, потенциале развития цифровой экономики и технологической модернизации производственных процессов в промышленности, расширении сферы оказания информационно-коммуникационных услуг. Концепция определила основные направления государственной политики в области защиты электронных информационных ресурсов, информационных систем и телекоммуникационных сетей, обеспечения безопасности информационно-

коммуникационных технологий. Он должен, прежде всего, усовершенствовать и наладить систему кибербезопасности Казахстана [2].

По поручению Главы государства Республики Казахстан разработана новая Концепция развития цифровой экосистемы на 2023 – 2027 годы («Киберщит – 2»).

В МЦРИАП объяснили, что из-за изменений ландшафта киберугроз нужно более комплексно подходить к информационной безопасности (ИБ), строить диалог с бизнес-сообществом. Помимо этого, планируется разработать единую техническую политику в сфере ИКТ, в рамках которой предприятия и организации можно будет определять по уровням безопасности. Также будет рассмотрена возможность создания резервного Национального координационного центра информационной безопасности, «Киберполигона» по подготовке специалистов [3].

В соответствии с государственными планами Республики Казахстан, 28 марта 2023 года была утверждена Концепция цифровой трансформации, развития информационных технологий и кибербезопасности на период 2023-2029 годов. Эта Концепция представляет собой другие цели и задачи, а также включает в себя отдельное направление, направленное на усиление кибербезопасности.

В Концепции также включены специальные меры, направленные на укрепление кибербезопасности на национальном уровне. В части развития кибербезопасности освещаются такие вопросы, как реформирование нормативного регулирования, в том числе повышение уровня политики и поддержка отечественного рынка информационных технологий. В рамках данной Концепции, ориентированной на направление «Кибербезопасность», заложены четыре ключевых целевых показателя, направленных на достижение более высокого уровня кибербезопасности в стране [4].

В последние годы различные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение в Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан «Об административных правонарушениях», законах Республики Казахстан «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V ЗРК.

В Уголовном кодексе Республики Казахстан (УК РК) в 1997 году появилась лишь одна статья 227, предусматривающая ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ. С начала 2014 года в Республике Казахстан действует новая редакция Уголовного кодекса, которая включает отдельную главу, посвященную преступлениям в сфере информатизации и связи: Глава 7. Уголовные правонарушения в сфере информатизации и связи. В этой главе содержится следующие статьи, связанные с нарушениями в отношении электронных информационных ресурсов, систем и сетей телекоммуникаций: Статья 205. Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть; Статья 206. Неправомерные уничтожение или модификация информации; Статья 207. Нарушение работы информационной системы или информационно-коммуникационной сети; Статья 208. Неправомерное завладение информацией; Статья 209. Принуждение к передаче информации; Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов; Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа; Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели; Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства [4]. В настоящее время ведутся работы по совершенствованию

уголовного и уголовно-процессуального законодательства для эффективного противодействия киберпреступности.

Защита общества от кибератак возможна только на основе взаимодействия основных направлений противодействия виду преступления: технического и правового. Техническое направление состоит из аппаратно-программных средств противодействия преступности, правовое направление – нормативное регулирование отношений в данной сфере.

Безопасность информационных технологий - проблема, вызывающая озабоченность не только одной страны, но и человечества в целом. Потому что в настоящее время киберпреступность выходит на мировой уровень. Борьба с такими глобальными преступлениями будет результативной только при совместной деятельности правоохранительных органов всех стран.

В связи с быстрым развитием информационных технологий и технических средств статичные механизмы защиты от сетевых угроз часто оказываются неэффективными. Обеспечить эффективную защиту информации позволяют динамические методы, способные оперативно выявлять и устранять угрозы. Работа динамических технологий строится на оценки уровня подозрительности действий в сети со стороны определенной службы или процесса.

Алгоритм действия по устранению атак направлен на идентификацию подозрительных объектов. После этого система реагирует необходимым образом на деятельность таких объектов, которая может быть нацелена на ресурсы сети или компьютерного оборудования.

Рекомендации по совершенствованию мер по противодействию кибератакам:

1. Обучение персонала. Один из наиболее распространенных способов получения киберпреступниками доступа к данным – через ваших сотрудников. Они будут отправлять мошеннические электронные письма, выдавая себя за кого-то из вашей организации, и будут запрашивать либо личные данные, либо доступ к определенным файлам. Ссылки часто кажутся неподготовленному глазу законными, и легко попасть в ловушку. Вот почему осведомленность сотрудников имеет жизненно важное значение.

2. Поддержка программного обеспечение и системы в полном актуальном состоянии. Часто кибератаки происходят из-за того, что системы или программное обеспечение не полностью обновлены, оставляя слабые места. Таким образом, киберпреступники используют эти слабые места, чтобы получить доступ к сети. Как только они появляются, часто бывает слишком поздно принимать превентивные меры.

3. Обеспечение защиты конечных точек. Мобильные устройства, планшеты и ноутбуки, подключенные к корпоративным сетям, предоставляют пути доступа к угрозам безопасности. Эти пути должны быть защищены с помощью специального программного обеспечения для защиты конечных точек.

4. Установка брандмауэра. Существует так много различных типов изощренных утечек данных, и каждый день появляются новые. Размещение сети за брандмауэром - один из наиболее эффективных способов защититься от любой кибератаки. Система брандмауэра заблокирует любые атаки методом перебора, осуществляемые в сети или системах, прежде чем они смогут нанести какой-либо ущерб.

5. Создание резервных копий данных. В случае кибератаки мы должны создать резервную копию своих данных, чтобы избежать серьезных простоев, потери данных и серьезных финансовых потерь.

6. Контроль доступа к системам. Контроль над тем, кто может получить доступ к сети, действительно очень важен. Кто-то может просто зайти в офис или на предприятие и подключить USB-ключ, содержащий зараженные файлы, к одному из компьютеров, что позволит ему получить доступ ко всей сети или заразить ее.

7. Безопасность Wi-Fi. Любое устройство может быть заражено при подключении к сети, если это зараженное устройство затем подключится к вашей бизнес-сети, вся ваша система подвергается серьезному риску. Защита сетей Wi-Fi и их скрытие - одна из самых безопасных

вещей, которые мы можем сделать для своих систем. С каждым днем беспроводные технологии развиваются все больше и больше, появляются тысячи устройств, которые могут подключиться к сети и скомпрометировать нас.

10. Не допускать использования простых паролей. Использование одного и того же пароля для всего может быть опасным. Как только хакер узнает пароль, у него теперь будет доступ ко всему в системе и к любому приложению, которым мы пользуемся. Установка разных паролей для каждого используемого приложения является реальным преимуществом для безопасности, а частая их смена позволит поддерживать высокий уровень защиты от внешних и внутренних угроз. Очень важно контролировать, кто имеет доступ к нашим компьютерам. Установка системы безопасности по периметру – очень хороший способ остановить киберпреступность, а также взломы.

Для борьбы с киберпреступностью государство предпринимает различные меры, однако, чтобы эта борьба была действительно эффективной, не стоит забывать, что соблюдение элементарных правил безопасности при работе в Интернете – дело пользователя.

Литература

1. Каковы риски кибербезопасности?
2. URL: https://egemen.kz/article/288630-kiberqauipsizdiktinh-qauqary-qanday
3. Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)».
4. Казахстан накроет новым киберщитом.
5. URL:https://www.gov.kz/memleket/entities/infsecurity/press/news/details/409913?lang=ru
6. Сайт Комитета по информационной безопасности МЦРиАП РК.
7. URL:https://www.gov.kz/memleket/entities/infsecurity/press/article/details/95401?lang=ru
8. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V (с изменениями и дополнениями по состоянию на 20.05.2023 г.)

ЖИЛХАЙДАРОВА БАЯН АБЛАЕВНА
магистрант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, юрист 2-го класса

ИССЛЕДОВАНИЕ ВЫЗОВОВ И ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В ДОСУДЕБНОМ РАССЛЕДОВАНИИ

Проблемы и перспективы использования цифровых доказательств в досудебном производстве являются важными аспектами в контексте цифровых трансформаций в правоприменительной сфере.

Президент страны в своем ежегодном Послании отметил о необходимости обеспечить верховенство права и качество отправления правосудия [1]. Для реализации этой цели, правоохранительные органы планомерно внедряют электронное судопроизводство. Так, 21 декабря 2017 г. Законом РК в УПК введена ст. 42-1 «Формат уголовного судопроизводства», согласно которой уголовное судопроизводство в республике ведётся в бумажном и (или) электронном форматах [2]. Таким образом, электронный формат расследования был официально закреплён в уголовно-процессуальном законодательстве.

В ходе реализации проекта возникали сложности по 3 направлениям работы по внедрению Е-формата расследования: 1) техническое обеспечение органов уголовного преследования и пропускная способность каналов связи; 2) недоработки самой платформы; 3) подготовка сотрудников следственных подразделений к расследованию дел в электронном формате, влияющая на его качество. С момента начала реализации проекта по цифровизации уголовного процесса проверки технического обеспечения органов и обучение проводились совместно с региональными управлениями КПС и СУ [3].

Несмотря на сложность нового формата расследования, правоохранительные органы приняли его положительные возможности [4]. Дальнейшее совершенствование процесса нами видится в повсеместном использовании цифровых доказательств в досудебном производстве.

Основные проблемы использования цифровых доказательств, заключаются в следующем:

1. Аутентичность и целостность данных: один из основных вопросов при использовании цифровых доказательств – это обеспечение их аутентичности и целостности. Существует риск подделки или искажения цифровых данных, и правоохранительные органы должны принимать меры для защиты от этого.

2. Проблемы конфиденциальности: сбор и использование цифровых доказательств может вмешиваться в частную жизнь граждан и нарушать их права на конфиденциальность. Необходимо соблюдать законы и нормы, чтобы обеспечить баланс между преследованием преступлений и защитой частной жизни.

3. Техническая экспертиза: правоохранительным органам может потребоваться техническая экспертиза для анализа и интерпретации цифровых доказательств. Это может потребовать дополнительных ресурсов и специализированных навыков.

4. Сроки хранения данных: в зависимости от юрисдикции, цифровые данные могут иметь определенные сроки хранения, и их удаление или изменение может вызвать проблемы при следственных действиях.

Для решения проблем, связанных с использованием цифровых доказательств в досудебном производстве, необходимо предпринимать ряд мер и разработать соответствующие стратегии. Вот некоторые шаги, которые можно предпринять:

1) Обучение и подготовка персонала: обучение сотрудников правоохранительных органов и юристов в области цифровых технологий и цифровой форензики позволит им более компетентно работать с цифровыми доказательствами.

2) Установление стандартов и правил: разработка и внедрение стандартов и правил сбора, анализа и хранения цифровых доказательств может помочь обеспечить их целостность и аутентичность.

3) Соблюдение законодательства о конфиденциальности: необходимо соблюдать законы и нормы о конфиденциальности данных и обеспечить соблюдение прав граждан при сборе и использовании цифровых доказательств.

4) Инвестиции в техническую экспертизу: правоохранительные органы могут инвестировать в оборудование и обучение специалистов по цифровой форензике, чтобы обеспечить адекватную экспертизу цифровых доказательств.

5) Разработка цифровых стратегий: государственные органы могут разрабатывать цифровые стратегии для улучшения сбора, анализа и обмена информацией между разными службами.

6) Сотрудничество с частным сектором: сотрудничество с технологическими компаниями и частными экспертами по цифровой безопасности может помочь в разработке современных методов обнаружения и анализа цифровых доказательств.

7) Общественное сознание и образование: образовательные кампании для граждан о правилах использования цифровых технологий и их последствиях могут способствовать снижению рисков в сфере цифровой безопасности.

8) Международное сотрудничество: в рамках международного сотрудничества можно разрабатывать стандарты и процедуры для обмена цифровыми доказательствами в масштабах мирового сообщества.

Решение проблем, связанных с цифровыми доказательствами, требует комплексного подхода, который включает в себя образование, техническую экспертизу, правовую поддержку и сотрудничество всех заинтересованных сторон.

Принятие указанных выше мер, откроет перспективы для использования цифровых доказательств, которые видятся в следующем:

– Улучшенная эффективность: цифровые доказательства могут быть легче обнаружены, анализированы и переданы между органами правопорядка, что способствует более эффективным расследованиям.

– Большая точность: с использованием технологий, таких как цифровая форензика и распознавание лиц, возможно повышение точности и надежности доказательств.

– Сокращение бюрократии: цифровые системы могут сократить бумажную работу и упростить процессы сбора и обработки информации.

– Глобальный доступ к данным: современные технологии позволяют обмениваться информацией и доказательствами между различными странами и юрисдикциями, что может быть полезным в расследованиях международных преступлений.

Важно учесть, что цифровые доказательства должны использоваться с соблюдением законодательства и правил судопроизводства, чтобы гарантировать справедливость и соблюдение прав граждан. Это также означает, что правоохранительные органы и суды должны развивать компетенции и навыки в области цифровых технологий и форензики.

По мнению О. Макаровой, дальнейшая модернизация досудебного производства в рассматриваемом аспекте должна происходить путём перехода на обязательное фиксирование

с использованием средств аудиовидеозаписи и иных технических средств всех процессуальных действий, проводимых следователями (дознавателями) [5].

Таким образом, решение проблем, связанных с использованием цифровых доказательств в досудебном производстве, требует комплексного и многогранного подхода. Необходимо обеспечивать баланс между соблюдением законодательства о конфиденциальности данных и эффективным использованием цифровых технологий для борьбы с преступностью. Это включает в себя обучение и подготовку персонала, разработку стандартов и правил для сбора и анализа цифровых доказательств, инвестиции в техническую экспертизу и сотрудничество с частным сектором. Международное сотрудничество и образовательные кампании также играют важную роль в обеспечении безопасности и справедливости при использовании цифровых доказательств.

Литература

1. Послание главы государства К.К. Токаева народу Казахстана «Справедливое государство. Единая нация. Благополучное общество» 2023 год.

2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V (с изменениями и дополнениями по состоянию на 02.01.2021 г.). [Электронный ресурс]. – Режим обращения: http://adilet.zan.kz/ – Дата обращения: 15 июля 2023.

3. Оракбаев А.Б. Проблемы и перспективы принятия прокурором ключевых решений в рамках электронного уголовного дела (на основе опыта Республики Казахстан) // Законность. 2023. №3 (1061). – С. 14-17.

4. Алькенев Р.Б. О пилотной апробации процедуры согласования процессуальных решений с прокурорами в электронном формате // Сайт электронного журнала «Заңжәнезаман». Вып. 5, – С. 18-20. https://zan-zaman.kz/wp-content/uploads/2020/11/zan-zaman-2020-05.pdf

5. Макарова О.В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела. – Журнал российского права, 2019, №1, – С. 159-168.

САБАНОВА АННА СЕРГЕЕВНА
Магистрант Алматинской академии МВД Республики Казахстан им. М. Есбулатова,
лейтенант полиции

ДЕФОРМАЦИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ

На современном этапе развития наступает стадия Четвертой промышленной революции, концепцией выдвинутой Клаусом Швабом, характерной активным внедрением в промышленность новейших технологий, перехода от физической реальности к цифровой во всех сферах деятельности, включая правоохранительную. Результаты такой тенденции оказали развитие не только в работе сотрудников, но также и открытием новых путей для сокрытия преступлений. Несмотря на улучшение положения в борьбе с бюрократизацией и обеспечения надежности сохранения информации, обратной стороной цифровизации стоит сложность раскрытия личности преступников и нахождение самих преступлений, которые становятся более латентными в цифровом пространстве [1].

DarkNet (от англ. Темная сеть) как один из продуктов цифровизации стал платформой для преступных деяний. Первоначально DarkNet разрабатывался для скрытия уязвимых лиц, политических беженцев и т.п., как части программы защиты свидетелей. DarkNet – термин, относящийся к некоторой группе определенных вебсайтов, которые существуют в зашифрованном сетевом пространстве. Почти все сайты скрывают персональные данные с помощью инструментов шифрования Tor. Эта сеть способна прятать идентификационные данные и сетевую деятельность пользователя. Их нельзя обнаружить традиционными поисковыми механизмами и на них невозможно попасть, используя традиционные браузеры [2]. Сейчас DarkNet также активно используется в торговле людьми, продаже органов, наркотиков и множества других преступлений, популярность которого оправдана тем, что доступ к темной сети ограничен и сложен для опознания личности. Проблема торговли людьми находится под особым наблюдением государства и правоохранительных органов по всему миру. Торговцы людьми используют DarkNet для продажи, распространения, (несуществующие рекламные агенства), способа коммуникации. Так покупатель и продавец могут находится в разных частях мира, сохраняя свою анонимность, тем самым гарантируя безопасность даже при поимке одного из участников.

Появилась и новые формы проституции без физического присутствия «заказчиков» – это вебкам моделинг – сфера бизнеса, построенная на общении веб-модели и наблюдателя в онлайн-видео-чате. Общение обычно происходит на платной основе, что является основным заработком модели и студии. Опасностью представляется вовлечение несовершеннолетних, которые подвергаются сексуальному насилию через видео связь. В Центральной Азии по количеству жертв вебкам модели лидерами являются города Бишкек, Республика Кыргызстан и Алматы, Республика Казахстан. Мужчины чаще попадают в трудовое рабство, особенно эмигрировавших из других стран, работодатель отнимает документы жертв, тем самым оставляя их без возможности идентификации для возвращения в свою страну. Существуют также другие формы торговли людьми трансформирующимся с помощью технологий,

глобализации, открытой доступности информации. Зачастую за преступлениями такого масштаба стоят организованные группировки имея транснациональный характер захватывая множество жертв. Организованная преступность в киберпространстве делится на три вида: киберзависимые, кибервнедряемые и киберпомогаемые [2]. Первый вид не может существовать без компьютеров, Интернета и других девайсов полностью опираясь на технологии. Второй, еще называют гибридным видом, являясь результатом слиянии традиционных преступлений и цифровизации, к таковым относится торговля людьми, интернет-мошенничество. Deepfake одно из ответвлений таких преступлений совершаемых с помощью искусственного интеллекта имитируя голос и внешность человека в финансовых махинациях. И третий вид осуществляется по схожей схеме со вторым, преступные организации передают товар, деньги и общаются между собой через закрытые каналы связи как DarkNet.

Цифровизация изменила и традиционное определение организованной преступности, отличаясь самой структурой. Так преступные группировки делят на:

1) Виртуальные группировки основанные на взаимном доверии в незаконных действиях, которые тоже подразделяются на «рои» – сообщества людей без лидера в основном ведомых одной политической, идеологической идеей, чаще всего это «хакеры» противодействующие политической системе. «хабы» имеют более четкую управленческую систему, состоящими из инструкторов и исполнителей;

2) Второй вид сочетают онлайновые и офлайновые преступления и получившие название «гибриды». Они подразделяются на: «кластерные гибриды», где организация вращается вокруг небольшой группы лиц, которые сосредоточены на преступной деятельности или конкретных методах и плавно переключаются между онлайн и офлайн преступлениями; «расширенные гибриды», которые гораздо менее централизованы, поскольку состоят из множества сообщников и подгрупп, не имеющих четкой иерархической структуры;

3) 3 тип группы, которые действуют преимущественно в офлайне, но используют онлайновые технологии для облегчения своей деятельности. Они подразделяются на: «иерархии», или традиционные организованные преступные группы; «совокупные группы», которые плохо организованы, быстротечны и не имеют четко определенной цели (McGuire 2012) [3].

Специалисты по технологиям и даже практики часто имеют приоритет над криминологами, что означает, что исследования и вмешательства в области технологий и безопасности часто включают «много» технологий, но «очень мало» криминологической и социальной теории и способности рассматривать этические вопросы. Аналогичным образом, криминологи, изучающие цифровое измерение организованной преступности и противодействие цифровой организованной преступности, вряд ли смогут достичь значимых результатов без намерения взаимодействовать с другими дисциплинами.

Организованная преступность – это форма преступности, которая в силу своих уникальных характеристик особенно чувствительна к цифровизации в связи чем, стоит высокая востребованность компетентных сотрудников в направлении информационных технологий, создания отдельного подразделения специализирующегося в киберпреступлениях, совмещая как и знания криминологии, так и навыки в эксплуатации новейших технологий.

Литература

1. Towards digital organized crime and digital sociology of organized crime 2022. Andrea Di Nicola
2. Мэтт Иган. 2017. На темной стороне интернета: Что такое Dark Web и Deep Web?
3. 3.Дамаскин О.В. Актуальные криминологические аспекты противодействия преступности в современном цифровом обществе: проблемы и перспективы // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. 2021.Т.16.№1. – С. 70-93.

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференциясының қарары

Конференция жұмысына көрнекті мемлекет қайраткерлері, құқық саласындағы белгілі қазақстандық және шетелдік ғалымдар, сондай-ақ жұртшылық өкілдері қатысты. Қатысушылардың жоғары мәртебесі конференция тақырыбының және оның шеңберінде қаралатын мәселелердің өзектілігін растайды. Үлкен ғылыми қызығушылық тудырған баяндамалар:

1. Қазақстан Республикасы Орталық сайлау комиссиясының төрағасы, заң ғылымдарының докторы, профессор Н.М. Әбдіровтің «Цифрландыру және электрондық дауыс беру: перспективалар мен тәуекелдер».

2. Қазақстан Республикасы Ішкі істер министрінің цифрландыру және байланыс жөніндегі орынбасары С.С. Сәрсеновтың «ІІО қызметіндегі цифрлық трансформацияны іске асырудың тиімділігін бағалау ерекшеліктері».

3. Қазақстан Республикасының цифрлық даму, инновациялар және аэроғарыш өнеркәсібі вице-министрі А.Н. Тұрысовтың «Мемлекеттік органдардың қызметінде цифрлық технологияларды қолдану».

4. Миколас Ромерис Университеті Құқықтық технологиялар орталығы (LegalTech) заң факультетінің профессоры, Вильнюс (Литва), әлеуметтік ғылымдар докторы, АТ-құқық PhD. Доктор Маиус Лауринайтистің (Литва Республикасы) «Экономиканы цифрландыру: алғышарттар, тенденциялар, перспективалары».

5. Портсмут университеті қылмыстық сот төрелігін зерттеу институтының профессоры, MA MBA FHEA PhD докторы, Лея Фокстың (Ұлыбритания) «Цифрландыруды зерттеу – жаһандық трендтер мен оны оқытудың үрдістерін бақылауы».

Қазақстан Республикасы ІІМ Мақан Есболатов атындағы Алматы академиясында (2023 жылғы 22 қыркүйек) әр елдің ғалымдарын, сарапшылары мен құқық қорғау органдарының өкілдерін жинаған «Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында қылмысқа қарсы іс-қимыл» конференциясы цифрлық қылмыстың маңызды аспектілерін және оның алдын алу мен жолын кесу бойынша тиімді шараларды әзірлеуді қарастырды.

Конференция келесі негізгі тұжырымдар мен ұсыныстарды ескерді:

Цифрлық қылмыс жеке азаматтардың да, жалпы қоғамның да қауіпсіздігіне үлкен қауіп төндіреді. Ол кибералаяқтық, кибертыңшылық, кибертерроризм және сол сияқты шабуылдардың әртүрлі түрлерін қамтиды.

Конференцияға қатысушылар соңында цифрлық қылмыс деңгейі үнемі өсіп келеді және оның алдын алу және күресу үшін әлемдік деңгейдегі күш-жігерді күшейту маңызды деген қорытындыға келді.

Жасанды интеллект және кванттық есептеу сияқты технологиялардың дамуы киберқылмыскерлер үшін жаңа мүмкіндіктер туғызады, сол себепті ақпарат пен киберқауіпсіздікті қорғаудың жаңа әдістері мен технологияларын әзірлеу қажет.

Конференция цифрлық қылмысқа қарсы күресте халықаралық ынтымақтастықтың маңыздылығын көрсетеді. Сондықтан елдер киберқауіпсіздік стандарттары мен шараларын бірлесіп әзірлеп, енгізуі керек.

Цифрлық қылмыстың қауіптілігі туралы білім беру және хабардарлықты арттыру, онымен күресудің маңызды құрамдас бөлігі болып табылады. Қоғам, кәсіпорындар мен ұйымдар үшін білім беру бағдарламаларын және киберқауіпсіздік науқандарын күшейту қажет.

Конференция құқық қорғау органдарының цифрлық қылмысқа қарсы күрестегі рөлін нығайтуға шақырады және тергеу әдістерін жетілдіру және басқа органдармен ынтымақтастық бойынша ұсыныстар береді.

Конференция сонымен қатар цифрлық қылмысқа қарсы іс-қимылды күшейту мақсатында басқа елдер мен ұйымдар арасында ақпарат алмасуға және үздік тәжірибелерді беруге жәрдемдесуге дайын екендігін білдіреді.

Қорытындылай келе, «Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында қылмысқа қарсы іс-қимыл» конференциясы цифрлық қылмыстың қауіп-қатерінің ауырлығын атап көрсетеді және оны болдырмау, алдын алу бойынша тиімді шараларды әзірлеп, енгізу үшін барлық мүдделі тараптарды бірлескен күш-жігерге шақырады.

Резолюция международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»

В работе конференции приняли участие видные государственные деятели, известные казахстанские и зарубежные ученые в области права, а также представители общественности. Высокий статус участников подтверждает актуальность темы конференции и рассматриваемых в ее рамках вопросов. Большой научный интерес вызвали доклады:

1. «Цифровизация и электронное голосование: перспективы и риски» Председателя Центральной избирательной комиссии Республики Казахстан, доктор юридических наук, профессора Н.М. Абдирова.

2. «Особенности оценки эффективности реализации цифровой трансформации в деятельности ОВД» Заместителя Министра внутренних дел Республики Казахстан по цифровизации и связи С.С. Сарсенова.

3. «Применение цифровых технологий в деятельности государственных органов» Вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан А.Н. Турысова.

4. «Цифровизация экономики: предпоссылки, тенденции, преспективы» профессора юридического факультета Центра правовых технологий (LegalTech) Университета Миколаса Ромериса, Вильнюс (Литва), доктора социальных наук, ИТ-права, PhD. Доктора Мариус Лауринайтис (Литовская Республика)

5. «Исследования цифровизации – мониторинг глобальных трендов и тенденции к обучению» профессора института исследований уголовного правосудия Университета Портсмута, доктор PhD, MA MBA FHEA Лея Фокс (Великобритания) и др.

Конференция «Противодействие преступности в условиях цифровизации и информатизации общества и государства» проведенная в Алматинской академии МВД Республики Казахстан имени Макана Есбулатова (22 сентября 2023 года), собравшая ученых, экспертов и представителей правоохранительных органов из различных стран, рассмотрела важные аспекты цифровой преступности и разработки эффективных мер по ее предотвращению и пресечению.

Конференция приняла во внимание следующие ключевые выводы и рекомендации:

Цифровая преступность представляет собой серьезную угрозу для безопасности как отдельных граждан, так и общества в целом. Она включает в себя различные формы атак, такие как кибермошенничество, кибершпионаж, кибертерроризм и др.

Уровень цифровой преступности постоянно растет, и участники конференции пришли к выводу, что важно активизировать усилия на мировом уровне для предотвращения и борьбы с этой угрозой.

Развитие технологий, таких как искусственный интеллект и квантовые вычисления, создает новые возможности для киберпреступников, и необходимо разработать новые методы и технологии для защиты информации и кибербезопасности.

Конференция подчеркивает важность международного сотрудничества в борьбе с цифровой преступностью. Страны должны совместно разрабатывать и внедрять стандарты и меры по кибербезопасности.

Образование и повышение осведомленности об опасностях цифровой преступности являются важными составляющими борьбы с ней. Необходимо усилить образовательные программы и кампании по кибербезопасности для общества, предприятий и организаций.

Конференция призывает к укреплению роли правоохранительных органов в борьбе с цифровой преступностью и предоставляет рекомендации по усовершенствованию методов расследования и сотрудничества с другими органами.

Конференция также выражает готовность содействовать обмену информацией и передаче лучших практик между странами и организациями в целях усиления противодействия цифровой преступности.

В заключение, конференция «Противодействие преступности в условиях цифровизации и информатизации общества и государства» подчеркивает серьезность угрозы, которую представляет цифровая преступность, и призывает к совместным усилиям всех заинтересованных сторон для разработки и внедрения эффективных мер по ее пресечению и предотвращению.

Фотогалерея

АКАДЕМИЯСЫ

Almaty Police
Academy

NAMED AFTER
академия
Казахстан
сбулатова
Almaty acad
Republic
ed after

Мазмұны

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференциясының бағдарламасы
Программа международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства» 3

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» халықаралық ғылыми-тәжірибелік конференцияға қатысушылар тізімі
Список участников международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства» 11

АБДИРОВ Н.М.
Цифровизация и электронное голосование: перспективы и риски.....22

САРСЕНОВ С.С.
Особенности оценки эффективности реализации цифровой трансформации в деятельности ОВД 29

САЙТБЕКОВ А.М.
Особенности развития криминологической науки в Республике Казахстан в эпоху глобальной цифровизации 31

КАНАТБЕК А.
Основные модели развития стратегического управления в информационном пространстве.....35

BIMOLDANOV Y.M.
On the grounds of criminal liability for the creation, use or distribution of malicious computer programs and software products 38

ШЕСТАКОВ Д.А.
«Оцифровка» уголовного права в свете безопасности 41

ДОКТОР М.Л.
Цифровизация экономики: предпоссылки, тенденции, преспективы.....45

ЛЕЯ Ф.
Исследования цифровизации – мониторинг глобальных трендов и тенденции к обучению.....48

РУСТЕМОВА Г.Р.
О цифровизации здравоохранения в Республике Казахстан.....51

ЧУКМАИТОВ Д.С.
Использование цифровых и биометрических технологий в совершенствовании надзора и контроля за осужденными……54

АКИМЖАНОВ Т.К.
Поиск новых путей противодействия преступности в Республике Казахстан в условиях цифровизации и информатизации общества и государства 56

БЕЙСЕНАЛИЕВ Б.Н., СЕРАЛИЕВА А.М., КАИРЖАНОВА С.Е.
Киберпреступность: понятие, виды и предупреждение 63

КЕГЕМБАЕВА Ж.А., САҒЫНБЕКОВА Г.М.
Отбасылық-тұрмыстық саладағы зорлық-зомбылықты алдын алудың кейбір мәселелері 69

ОСМАНОВА Г.Ж., БИЖАНОВА А.Р.
Бас бостандығынан айыру түріндегі жазаның әлеуметтік салдары 72

КЫЗДАРБЕКОВА Б.Ж.
Использование искусственного интеллекта в преступных целях:
постановка проблемы и предпосылки введения уголовной ответственности 77

РОЗЕНКО С.В.
Уголовное право, наказание и искусственный интеллект: проблемы взаимодействия 83

ШАЯХМЕТОВА Ж.Б.
Сравнительно-правовой аспект уголовной защиты цифровой личности 87

САДЫРОВ А.К.
Современные способы борьбы с преступностью 90

АЛТАЙБАЕВ С.Қ.
Бас бостандығынан айыру жазасы – адамды қоғамнан оқшаулаудың бір түрі 93

БИЯТОВ Т.К.
Особенности уголовной ответственности несовершеннолетних граждан Республики Казахстан 97

НАСЫРОВА Э.М., ЛИМ В.В.
Использование информационных систем в деятельности органов внутренних дел
Республики Казахстан 103

СЕРАЛИЕВА А.М., БАЙМАГАМБЕТОВА З.М.
Отбасындағы тұрмыстық зорлық-зорлықтың ұғымдары мен формалары 109

ПАРСИЕВ С.С., МУСАЕВ А.И.
Обеспечение общественной безопасности в условиях цифровизации и информатизаций
общества и государства 113

ҚАРАТАЕВ Т.Ж.
Қазақстан Республикасы ІІО қызметкерлерінің дене күштері, арнаулы құралдары мен атыс
қаруын қолдану проблемалары 115

СУЛТАНОВ С.И.
Қылмыстық құқық бұзушылықтарды саралаудың қылмыстық-құқықтық және
қылмыстық-процестік мәселелері 121

ИМАНБАЕВ А.Ж., ЗИРО А.А.
Стандарты безопасности 5g-сетей 124

АШИРБЕКОВ М.Е.
К вопросам надзорной деятельности в сфере земельных правоотношений на транспорте
с учетом влияния процессов цифровизации 126

МАЙМАКОВ А.Т.
Интернет алаяқтықпен күрес – заман талабы 137

БАТЫРБАЕВ А.К.
Компьютерлік қылмыстық құқық бұзушылықтың ұғымы және мәні 141

САТЫБАЛДИНОВ М.Т.
Перспективы использования современных беспилотных летательных аппаратов для фото-видео фиксации места совершения преступления 145

МАРАТ А.М.
Труд осужденных – как мера профилактики пенитенциарных преступлений 149

АБИЖАНОВ С.М.
Практические методы предупреждения уголовных правонарушений в сфере информатизации и связи 153

ВОЛКОВ Б.В., СЕЙІТЖАН Қ.К.
Цифровые преобразования в области противостояния киберугрозам и киберпреступности 159

ҒАЛЫМ А.М.
On the state of digitalization of the penal system of the Republic Kazakhstan 163

АБАЖАНОВА А.З.
Уголовно-правовая и криминологическая характеристика краж и мошенничества, совершаемых посредством сети интернет 166

ЖИЕНГАЛИЕВА А.А.
Ішкі істер органдарындағы талдамалық жұмыс және оны жетілдіру жолдары 172

АРЫНОВА А.Н.
Текущие проблемы противодействия преступлениям, совершаемым с применением информационных технологий 175

ИСКАКОВ А.К.
Цифровизация в уголовно-исполнительной системе: анализ её влияния на процессы религиозной радикализации среди осужденных 178

ҚҰЛАЖАНОВА А.Н.
Латенттік қылмыстылықтың криминологиялық сипаттамасы 181
ҚҰЛАЖАНОВА А.Н., УСЕНБАЕВА А.У.
Құқық қорғау саласын цифрландыру және оның айқындығын қамтамасыз ету 185

МУРТАЛИМОВ Ш.Р.
Противодействие преступности в условиях цифровизации и информатизации общества и государства 189

САПАРОВ Ж.Ж.
ТМД елдері мен Қазақстан Республикасының статистикалық деректері және арнайы есепке алу жөніндегі заңнаманы талдау 192

ШИДЕМОВ А.Г.
Особенности ведения статистических учетов 197

БАЙТЕЛЕНОВА С.Г.
Особенности производства звуко-, видеозаписи при проведении следственных действий 200

БАПАНОВА Т.Т.
Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций: особенности квалификации 203

БАПАНОВ М.Т.
Пути совершенствования законодательства в противодействии уголовным правонарушениям в сфере информатизации и связи.....209

АЙТКЕШ А.К.
Экономические преступления в условиях цифровизации и проблемы их уголовно-правовой оценки.....214

ТУРГУНБАЕВА А.М.
Уголовная политика республики казахстан в сфере информатизации: вопросы противодействия компьютерной преступности.....218

ВОЕВОДКИН Д.В.
К вопросу о судебной экспертизе электронных документов.....223

АБИКЕНОВ А.Н.
Цифровизацияның қазіргі қылмыстық құқық заңдылығына әсері.....229

АМАНОВА Д.Т.
Кәмелетке толмағандарды цифрлық ортадағы қылмыстық әрекетке тарту: мәселелер және қарсы тұру жолдары.....233

КУРМАНГАЛИЕВА Л.Ж.
Көлік құралдарын басқаратын адамдардың жол жүрісі немесе көлік құралдарын пайдалану қағидаларын бұзу қылмысының алдын алуда цифровизацияның маңызы.....237

САРБАСОВ А.Е.
Развитие уголовного права в условиях современных цифровых технологий.....241

КУБАНОВА Н.Б., КОЙШИБАЕВ Е.У.
Юридические аспекты борьбы с кибератаками в уголовном законодательстве.....245

ЖИЛХАЙДАРОВА Б.А.
Исследование вызовов и возможностей применения электронных доказательств в досудебном расследовании.....249

САБАНОВА А.С.
Деформация организованной преступности в эпоху цифровизации.....252

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференциясының қарары.....254

Резолюция международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства».....255

Фотогалерея.....256

Беттеу:
К.Н. Саратекова

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу
және редакциялық-баспа жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 10 қараша 2023 ж. жіберілді.
Пішімі 60х84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 20,1.
Таралымы 100.