

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МАҚАН ЕСБОЛАТОВ АТЫНДАҒЫ АЛМАТЫ АКАДЕМИЯСЫ

*Қазақстан Республикасының ғылым және техникаға еңбек сіңірген қайраткері,
Қазақстан Республикасы ҚЖҒА академигі, заң ғылымдарының докторы, профессор
Елеген Ізтілеуұлы Қайыржановқа арналған*
**ҚОҒАМ МЕН МЕМЛЕКЕТТІ АҚПАРАТТАНДЫРУ ЖӘНЕ ЦИФРЛАНДЫРУ
ЖАҒДАЙЫНДА ҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ**
атты халықаралық ғылыми-тәжірибелік конференциясы
(20 қыркүйек 2024 ж.)

**ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА**
*международная научно-практическая конференция, посвящённая памяти
заслуженного деятеля науки и техники Республики Казахстан, академика КАЕН
Республики Казахстан, доктора юридических наук, профессора
Каиржанова Елегена Изтлеуовича
(20 сентября 2024 г.)*

Алматы
2024

УДК 34:004
ББК 67:32.973
Қ54

Жауапты редактор:

Ж.Р. Дильбарханова Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы бастығының уақытша міндетін атқарушы,
з.ғ.д., профессор, полиция полковнигі

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.)

Қ54 Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл: халықар. ғыл.-тәж. конф. мат-ры (20.09.2024ж.) = Противодействие преступности в условиях цифровизации и информатизации общества и государства: мат. межд. науч.-практ. конф. (20.09.2024г.). – Алматы: ҚР ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2024. – 118 б. қазақша, орысша.

ISBN 978-601-360-139-7

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 Елеген Ізтілеуұлы Қайыржановқа 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 памяти 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.

*Жинақтағы материалдар автордың редакциясымен берілді.
Материалы, публикуемые в сборнике, даны в авторской редакции.*

УДК 34:004
ББК 67:32.973

ISBN 978-601-360-139-7

© Қазақстан Республикасы ІІМ
М. Есболатов атындағы
Алматы академиясы, 2024

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

Өткізу уақыты мен күні	2024 жылғы 20 қыркүйек сағат 09.00-де
Өткізу орны	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы (Өтепов көшесі 29)
Өткізу форматы	Аралас (offline/ сырттай)
Модератор	СЕЙЛХАНОВА Саида Айдарбековна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының бастығы, з.ғ.к., полиция полковнигі

Сөз сөйлеу

Уақыты	Спикер	Баяндама тақырыбы
09.00-09.05	ДИЛЬБАРХАНОВА Жанат Рахимжановна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының м.у.а., з.ғ.д., профессор, полиция полковнигі	Кіріспе сөз
09.05-09.10	БИМОЛДАНОВ Ержан Малайұлы Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары., қауымдастырылған профессор, з.ғ.к., полиция полковнигі	Алғыс сөз
09.10-09.20	СЕЙЛХАНОВА Саида Айдарбековна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының бастығы, з.ғ.к., полиция полковнигі	Модератор
09.20-09.30	КАИРЖАНОВА Солидат Елегеновна Батыс Қазақстан инновациялық-технологиялық университетінің тарих және құқықтану кафедрасының профессоры, з.ғ.д., кіші әділет кеңесшісі	Адам саудасының пайда болуы мен дамуының детерминанттары (себептері мен шарттары)
09.30-09.40	СОРОКУН Николай Сергеевич Ресей Ішкі істер министрлігі Ростов заң институтының қылмыстық құқық және криминология кафедрасының доценті, з.ғ.к., доцент, полиция полковнигі	Ақпараттық және телекоммуникациялық технологиялар саласындағы қылмыстарды жасаудың себептері мен шарттарын анықтау және жою, мұндай әрекеттердің алдын алудың негізі ретінде

09.40-09.50	МЕЛЬНИК Светлана Львовна СмолМУ сот және прокурор қызметін ұйымдастыру кафедрасының меңгерушісі, Халықаралық заң институтының Смоленск филиалының қылмыстық пәндер кафедрасының доценті, з.ғ.к., доцент	Жәберлерді тау проблемалық мәселелері жемқорлық істер туралы
09.50-10.00	РУСТЕМОВА Гаухар Рустембековна Қазақстан Республикасы ІІМ Алматы академиясының М. Есболатов атындағы ғылыми орталықтың ғылыми қызметкері, з.ғ.д., профессор, отставкадағы полиция полковнигі	Денсаулық сақтау туралы заңнамадағы цифрландырудың құқықтық тәуекелдері
10.00-10.10	БАПАНОВ Талғат Абдирович Алматы гуманитарлы-экономикалық университеті Экономика, қызмет көрсету және құқық кафедрасының аға оқытушысы, з.ғ.к.	Кибер алаяқтық; сипаттамасы және әдістері
10.10-10.20	МАРАТ Айгүл Маратқызы Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры	Интернет-алаяқ тұлғасы туралы
10.20-10.30	БАТЫРБАЕВ Адылхан Кошкенович Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры	Қоғам мен мемлекетті ақпа- раттандыру және цифрлан- дыру жағдайында қылмысқа қарсы іс-қимыл
10.30-10.40	КУРМАНОВА Гульнара Сагиндыковна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының доценті	Қылмыс жасаған құқық қорғау орган қызметкерінің тұлғасына құқық- тұрақтылық зерттеуді ақпараттық-аналитикалық қамтамасыз етуді жетілдіру мәселесі туралы
10.40-10.50	ЗУЛЕЕВА Айнагуль Жаңылбекқызы Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының доценті полиция подполковнигі	Сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы оң үрдістер
10.50-11.00	АБАЖАНОВА Асем Зейноллаевна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға оқытушысы полиция подполковнигі	Қазақстан Республикасының ақпараттық қауіпсіздігі: киберқауіптердің түсініктері мен жіктелуі
11.00-11.10	ТАЖЕНОВА Салтанат Ирисмахановна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға	Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында қылмысқа қарсы күрестің халықаралық тәжірибесі

	оқытушысы полиция подполковнигі	
11.10-11.20	БАПАНОВ Мағжан Талғатұлы Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция майоры	Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимылда заңнаманы жетілдіру жолдары
11.20-11.30	АЙТКЕШ Айбек Қанатұлы Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция майоры	Киберқылмыспен күрес саласындағы мемлекетаралық ынтымақтастықты жетілдіру
11.30-11.40	ТУРГУНБАЕВА Альбина Маратовна Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция капитаны	Қазақстан Республикасы киберқылмыс динамикасының ерекшеліктері және оның алдын алу мәселелеріне әсері
11.40-12.00	Пікірталас, қарарды талқылау Қорытындылау, дөңгелек үстелді аяқтау	

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

Дата и время проведения	20 сентября 2024 г. в 09.00 часов
Место проведения	Алматинская Академия МВД Республики Казахстан им. М. Есбулатова (ул. Утепова 29)
Формат проведения	Комбинированный (offline/ заочный)
Модератор	Сейлханова Саида Айдарбековна начальник кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова , к.ю.н., полковник полиции

Выступления

Время	Спикер	Тема доклада
09.00-09.05	ДИЛЬБАРХАНОВА Жанат Рахимжановна Вр.и.о. начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова д.ю.н., профессор, полковник полиции	Вступительное слово
09.05-09.10	БИМОЛДАНОВ Ержан Малаевич Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., ассоциированный профессор, полковник полиции	Приветственное слово
09.10-09.20	СЕЙЛХАНОВА Саида Айдарбековна Начальник кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ю.н., полковник полиции	Модератор
09.20-09.30	КАИРЖАНОВА Солидат Елегеновна Д.ю.н., профессор кафедры Истории и юриспруденции Западно-Казахстанского инновационно-технологического университета младший советник юстиции	Детерминанты (причины и условия) возникновения и развития торговли людьми
09.30-09.40	СОРОКУН Николай Сергеевич Доцент кафедры уголовного права и криминологии Ростовского юридического института МВД России, полковник полиции, к.ю.н., доцент	Выявление и устранение причин и условий совершения преступлений в сфере информационно-телекоммуникационных технологиях, как основа профилактики таких деяний

09.40-09.50	МЕЛЬНИК Светлана Львовна Зав.кафедрой организации судебной и прокурорской деятельности СмолГУ, доцент кафедры уголовно правовых дисциплин Смоленского филиала Международного юридического института, к.ю.н., доцент	Проблемные вопросы признания потерпевшим по коррупционным делам
09.50-10.00	Рустемова Гаухар Рустембековна Научный сотрудник научного центра Алматинской академии МВД Республики Казахстан им. М. Есбулатова, д.ю.н., профессор, полковник полиции в отставке	Правовые риски цифровизации в законодательстве о здравоохранении
10.00-10.10	БАПАНОВ Талгат Абдирович Старший преподаватель кафедры экономики, сервиса и права алматинского гуманитарно-экономического университета, к.ю.н.	Кибермошенничество: характеристика и способы
10.10-10.20	МАРАТ Айгуль Маратовна Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова	О личности интернет-мошенника
10.20-10.30	БАТЫРБАЕВ Адылхан Кошкенович Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова	Противодействие преступности в условиях цифровизации и информатизации общества и государства
10.30-10.40	КУРМАНОВА Гульнора Сагиндыковна Доцент кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова	К вопросу совершенствования информационно-аналитического обеспечения криминологических исследований личности сотрудника правоохранительных органов, совершившего преступление
10.40-10.50	ЗУЛЕЕВА Айнагуль Жанилбековна Доцент кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	Положительные тенденции в сфере противодействия коррупции
10.50-11.00	АБАЖАНОВА Асем Зейноллаевна Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	Информационная безопасность Республики Казахстан: понятия и классификация киберугроз
11.00-11.10	ТАЖЕНОВА Салтанат Ирисмахановна	Международный опыт в противодействие

	Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	преступности в условиях цифровизации и информатизации общества и государства
11.10-11.20	БАПАНОВ Мағжан Талғатұлы Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции	Пути совершенствования законодательства в противодействии уголовным правонарушениям в сфере информатизации и связи
11.20-11.30	АЙТКЕШ Айбек Қанатұлы Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции	Совершенствование межгосударственного сотрудничества в области противодействия киберпреступности
11.30-11.40	ТУРГУНБАЕВА Альбина Маратовна Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции	Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения
11.40-12.00	Дискуссия, обсуждение резолюции Подведение итогов, завершение работы круглого стола	

**«Қоғам мен мемлекетті ақпараттандыру және цифрландыру
жағдайында қылмысқа қарсы іс-қимыл»
атты халықаралық ғылыми-тәжірибелік конференцияның қатысушылар
ТІЗІМІ**

Аты-жөні, тегі	Лауазымы
ДИЛЬБАРХАНОВА Жанат Рахимжановна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының м.у.а., з.ғ.д., профессор, полиция полковнигі
БИМОЛДАНОВ Ержан Малайұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары., қауымдастырылған профессор з.ғ.к., полиция полковнигі
СЕЙЛХАНОВА Саида Айдарбековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы қылмыстық құқық және криминология кафедрасының бастығы, з.ғ.к., полиция полковнигі
КАИРЖАНОВА Солидат Елегеновна	Батыс Қазақстан инновациялық-технологиялық университетінің тарих және құқықтану кафедрасының профессоры, з.ғ.д., кіші әділет кеңесшісі
СОРОКУН Николай Сергеевич	Ресей Ішкі істер министрлігі Ростов заң институтының қылмыстық құқық және криминология кафедрасының доценті, полиция полковнигі, з.ғ.к., доцент
МЕЛЬНИК Светлана Львовна	СмолМУ сот және прокурор қызметін ұйымдастыру кафедрасының меңгерушісі, Халықаралық заң институтының Смоленск филиалының қылмыстық пәндер кафедрасының доценті, з.ғ.к., доцент.
РУСТЕМОВА Гаухар Рустембековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы ғылыми орталықтың ғылыми қызметкері, з.ғ.д., профессор, отставкадағы полиция полковнигі
БАПАНОВ Талғат Абдирович	Алматы гуманитарлы-экономикалық университеті Экономика, қызмет көрсету және құқық кафедрасының аға оқытушысы, з.ғ.к.
МАРАТ Айгүл Маратқызы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры
БАТЫРБАЕВ Адылхан Кошкенович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының профессоры
КУРМАНОВА Гүльнара Сагиндыковна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының доценті
ЗУЛЕЕВА Айнагуль Жаңылбекқызы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының доценті полиция подполковнигі
АБАЖАНОВА Асем Зейноллаевна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға оқытушысы полиция подполковнигі
ТАЖЕНОВА Салтанат Ирисмахановна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға оқытушысы полиция подполковнигі
БАПАНОВ Мағжан Талғатұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция майоры
АЙТКЕШ Айбек Қанатұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция майоры
ТУРГУНБАЕВА Альбина Маратовна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының оқытушысы полиция майоры полиция капитаны

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

ФИО	Должность
ДИЛЬБАРХАНОВА Жанат Рахимжановна	Вр.и.о. начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова д.ю.н., профессор, полковник полиции
БИМОЛДАНОВ Ержан Малаевич	Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., ассоциированный профессор, полковник полиции
СЕЙЛХАНОВА Саида Айдарбековна	Начальник кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ю.н., полковник полиции
КАИРЖАНОВА Солидат Елегеновна	Д.ю.н., профессор кафедры Истории и юриспруденции Западно-Казахстанского инновационно-технологического университета младший советник юстиции
СОРОКУН Николай Сергеевич	Доцент кафедры уголовного права и криминологии Ростовского юридического института МВД России, к.ю.н., доцент, полковник полиции
МЕЛЬНИК Светлана Львовна	Зав.кафедрой организации судебной и прокурорской деятельности СмолГУ, доцент кафедры уголовно прововых дисциплин Смоленского филиала Международного юридического института, к.ю.н., доцент
РУСТЕМОВА Гаухар Рустембековна	Научный сотрудник научного центра Алматинской академии МВД Республики Казахстан им. М. Есбулатова, д.ю.н., профессор, полковник полиции в отставке
БАПАНОВ Талгат Абдирович	Старший преподаватель кафедры экономики, сервиса и права алматинского гуманитарно-экономического университета, к.ю.н.
МАРАТ Айгуль Маратовна	Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова
БАТЫРБАЕВ Адылхан Кошкенович	Профессор кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова
КУРМАНОВА Гульнара Сагиндыковна	Доцент кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова
ЗУЛЕЕВА Айнагуль Жанилбековна	Доцент кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
АБАЖАНОВА Асем Зейноллаевна	Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
ТАЖЕНОВА Салтанат Ирисмахановна	Старший преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
БАПАНОВ Мағжан Талғатұлы	Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции
АЙТКЕШ Айбек Қанатұлы	Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции
ТУРГУНБАЕВА Альбина Маратовна	Преподаватель кафедры уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции



БЕЙСЕНАЛИЕВ

Бауржан Нуралыұлы

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



БИМОЛДАНОВ

Ержан Малаевич

заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., ассоциированный профессор, полковник полиции



КАИРЖАНОВА

Солидат Елегеновна

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

ДЕТЕРМИНАНТЫ (ПРИЧИНЫ И УСЛОВИЯ) ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ТОРГОВЛИ ЛЮДЬМИ

*Библия благословляет торговлю людьми,
этнические и массовые убийства, но поскольку
ее написали дикие, невежественные млекопитающее,
мы вовсе не обязаны ей следовать
Кристофер Хитченс, писатель 1949-2004*

*Торговля и азартные игры, а иногда
и женщины – это была жизнь мужчины
Энтони Берджесс, 1917 – 1993*

Как отметил в своем Послании от 2 сентября 2024 года « Справедливый Казахстан: закон и порядок, экономический рост, общественный Оптимизм» Президент страны Токаев К.К., говоря о безопасности граждан ...В настоящее время разрабатывается проект нового Закона «О профилактике правонарушений». Его реализация потребует консолидации усилий госаппа-

рата и общества. Только в этом случае можно изменить ситуацию, обеспечить верховенство закона и безопасность граждан.

Во всех обществах, в нашем в том числе, существуют запросы на такие базовые категории, как справедливость и безопасность. Полноценное удовлетворение этих основных потребностей является надежным показателем эффективности государства.

Анализируя условия, способствующие такому преступлению, как торговля людьми, Управление ООН подчеркивает сложности взаимодействия социальных, экономических и политических факторов, конфликты и преследования, бедность и политическая нестабильность, отсутствие доступа к образованию рабочим местам, миграция, гендерное неравенство и дискриминация, участвовавшие стихийные бедствия и изменения климата – все это способствует торговле людьми.

Ведь торговля людьми – это эксплуатация человеческого потенциала для получения прибыли. Масштабы торговли людьми растут, так как приносит высокие доходы.

Криминогенные детерминанты, т.е. причины и условия преступности, в том числе отдельных видов и категорий преступлений, – одна из центральных проблем криминологии, имеющая не только теоретическое, но и практическое значение, ибо «нельзя выработать и осуществить необходимые практические мероприятия по устранению определенного социального явления, не зная всех питающих его истоков» [1].

В материалистической науке причинность определяется как объективная, генетическая связь между явлением, при котором одно или несколько явлений (причин) вызывает, определяет, изменяет, или производит другое явление (следствие) [2].

Криминологические мысли о причинности появились в период развития советской криминологии, а многие полезные разработки в этой области относятся к периоду Советской власти. С обретением Республикой Казахстан суверенитета изменился и подход к проблеме причинности. Во-первых, переход плановой экономики на рыночные отношения и изменение видов и характера сегодняшней преступности, а во-вторых, влияние запада и других государств на внутренние процессы в государстве, становится очевидным тот факт, что устоявшиеся теории, касающиеся причин преступности, заметно расширили свои границы. Установление причин преступности имеет не только самостоятельное значение, но и помогает понять причины индивидуального преступного поведения [3].

В криминологии под причинами преступления понимают такие негативные социальные явления, которые порождают и воспроизводят преступность и преступления как свое законное следствие. Под условием явления, в отличие от его причин, понимается комплекс явлений, не могущий самостоятельно породить непосредственно данное явление – следствие. Но, сопутствуя причинам в пространстве, времени и влияя на них, обеспечивают определенное их развитие, необходимое для возникновения следствия [6].

Считается общепринятым разделение явлений и процессов, детерминирующих преступность, на причины и условия, но разграничить их в реальной жизни не просто. Это объясняется тем, что «всякая причина является в определенном отношении условием, а всякое условие в другом отношении может быть причиной».

В связи с этим, зачастую невозможно, описывая систему детерминант, однозначно обозначить то или иное явление в качестве причины либо условия, являющегося главным в причинно-следственной связи возникновения торговли людьми и связанных с ней преступлений. Это в свою очередь вынуждает описывать причинный комплекс в качестве системы факторов, обуславливающих преступность.

Факторы, детерминирующие преступления, так или иначе связанные с торговлей людьми, представляют собой достаточно сложный комплекс: наличие глубоких исторических корней; обострение политической борьбы; острые проблемы социального, межнационального, религиозного и иного характера; кризис экономики; войны, конфликты и прочие экстремальные ситуации, приводящие к дестабилизации существующих государственных систем и к фрустрации на индивидуальном уровне, а также порождающие слои населения, ориентированные, в том числе и профессионально, на насилие; отсутствие внимания к деятельности той или иной груп-

пы; социальная неудовлетворенность личности. К числу дополнительных факторов, способствующих развитию торговли людьми, следует отнести: обострение криминогенной обстановки и снижение правовой культуры населения; общий рост случаев рабства и торговли людьми в мире.

Сложная система факторов причинности торговли людьми объясняется тем, что данный вид преступной активности можно отнести, как указывалось выше, к разряду корыстно-насильственных преступлений. Исходя из этого, можно отметить, что возникновению рабства и торговли людьми (как явлению) способствует многообразие факторов, которые характерны, в том числе и корыстно-насильственным преступлениям.

По своему источнику и характеру действия, факторы могут быть подразделены на объективные и субъективные, а также внешние и внутренние факторы.

По характеру отрицательных тенденций, возникающих в обществе, из факторов, обуславливающих причины и условия торговли людьми, можно выделить: организационно-правовые; социально-экономические; социально-психологические; демографические. Указанные сферы социальной жизни взаимно дополняют друг друга и не могут существовать по отдельности.

В данной связи важно отметить мнение одного из казахстанских ученых Абдирова Н.М., который, затрагивая проблему причинности, отметил, что вопрос о соотношении объективного и субъективного всегда был предметом споров и дискуссий в криминологической науке, а также она остается одной из острых, дискуссионных проблем [7].

Тем самым мы вплотную приблизились к рассмотрению тех причин и условий, которые способствуют возникновению и совершению преступлений, связанных с торговлей людьми.

В нравственном сознании населения, его отдельных социальных групп и слоев стабилизируется мнение о том, что высокая материальная обеспеченность возможна лишь за счет нарушения установленных норм и требований закона. Сформировались представления о допустимости и даже оправданности прямого нарушения норм закона ради получения материальной выгоды [10].

Кроме демографических факторов, значительную роль играют социально-экономические факторы, детерминирующие торговлю людьми. «Глобализация – доминирующая после окончания «холодной войны» единая общемировая система, возникшая в результате интеграции национальных экономик, основанная на беспрепятственном перемещении капитала, на информационной открытости мира, на быстром технологическом обновлении, на понижении тарифных барьеров и либерализации движения товаров, межнациональных социальных движениях, новых видах транспорта, развития технологий, интернациональном образовании» [11].

Более того, необходимо отметить, что в ряду объективных причин возникновения рабства главную роль играют экономические причины. Человек – это единственное средство производства, которое способно своим трудом создавать материальные блага. Поэтому эксплуатация невольников и торговля ими приносит баснословные прибыли. С другой стороны, распространение рабства и работорговли связано с комплексом социальных явлений [12].

Причины и условия как преступности в целом, так и торговли людьми, социальны по своему происхождению. Так, началом возникновения данного явления можно считать разделение общества на классы и рождение частной собственности.

Однако необходимо осветить мнение А.А. Герцензона, который справедливо отмечал, что далеко не все индивидуальные конкретно-личные обстоятельства совершения преступления, даже взятые в большом числе, в состоянии объяснить причины преступности как социального явления [13].

Одним из негативных факторов преступности выступает такое явление, как безработица, которое обуславливает рост преступности, в том числе и тех видов преступлений, которые связаны с торговлей людьми.

Работа человека является одной из важных детерминант его успешной адаптированности в социальном обществе. В то же время, проблема занятости индивида связана с действием различных криминогенных факторов, возникающих в других сферах жизни.

Человек, имеющий постоянное место работы, при условии, что его удовлетворяет та работа, которую он выполняет, т.е. она соответствует его образовательному, профессиональному, интеллектуальному уровням, условиям труда и оплат, имеет меньше шансов быть порабощенным. Однако необходимо отметить, что это и не исключает абсолютно возможности стать жертвой торговли людьми.

Говоря о причинах и, условиях торговли людьми, действующих в социальной сфере жизнедеятельности человека, необходимо отметить такой фактор как обострение межнациональных отношений, который может способствовать возникновению значительного числа преступлений корыстно-насильственного характера таких, как: торговля людьми, убийства, захват заложников, похищения людей с целью выкупа, разбои и др. [14].

В то же время, экономические факторы имеют для криминологии лишь ограниченную ценность. Поскольку само понятие «бедность» или «нищета» – субъективно. Она определяется уровнем благосостояния и оценкой отдельного человека. То, что один считает бедностью, другой признает достатком, а может даже роскошью.

Определенную негативную роль в культивировании безнравственности играет дифференциация населения по уровню материального обеспечения, глубокий духовный кризис общества, о котором часто информируют средства массовой информации [16].

Далее, при рассмотрении причин и условий возникновения преступлений, связанных с торговлей людьми, важно отметить определенный экономический уровень того или иного государства. Так, сравнительно успешный экономический рост в Казахстане на фоне других государств Центрально-азиатского региона создает условия для развития трафика, то есть – торговли людьми [17].

Таким образом, Республика Казахстан вовлечена в зону действия организованной сети преступных групп, извлекающих прибыль из ведения различного нелегального бизнеса, в том числе и из рассматриваемого нами преступления – торговли людьми.

В то же время необходимо учесть, что Казахстан одновременно позиционируется в трех аспектах: Республика Казахстан как страна происхождения; страна транзита; страна назначения для жертв торговли людьми.

Развитие проблемы торговли людьми в Казахстане обусловлено, как отмечалось выше, причинами социального и экономического характера.

Криминальные структуры для вербовки людей используют такие негативные факторы, как безработица, низкая заработная плата, отсутствие возможности самореализации и др. Так, по словам руководителя организации «Центр женской правовой инициативы «Сана сезім», действующей в городе Шымкенте с мая 2001 года, Хадичи Абишевой, случаев торговли людьми на территории Южно-казахстанской области немало [17].

Более того, в период с 15 марта по 15 августа 2019г., в данную организацию обратились за помощью 505 человек, многие из которых хотели заработать за границей значительные суммы денег [17].

Более высокий уровень экономического развития Казахстана, по сравнению с другими государствами Центральной Азии, с каждым годом привлекает в республику все большее количество людей в поисках работы, что, в свою очередь, расширяет поле деятельности преступных сообществ в сфере вербовки, транспортировки и продажи людей для их последующей эксплуатации [17].

Следовательно, граждане других государств, прежде всего - Кыргызстана, Узбекистана и Таджикистана - становятся жертвами торговли людьми в Республике Казахстан. Например, на табачных плантациях в Казахстане эксплуатируют граждан Кыргызстана и Узбекистана, женщин из вышеперечисленных государств используют в интим – услугах.

Отдельно стоит упомянуть, что в Казахстане существует и внутренняя торговля людьми между сельскими районами и городами. По данным неправительственных организаций по реабилитации жертв торговли людьми «Родник» и «Феникс» данная цифра может достигать нескольких тысяч человек.

Таким образом, нет ничего удивительного, в том, что поиск решения проблемы торговли людьми становится все более актуальным. Кроме того, встала необходимость выработки стратегии противодействия с данным явлением.

Однако анализу основополагающих причин торговли людьми, внимания уделяется недостаточно.

Как уже отмечалось выше, основной причиной рабства и торговли людьми являются сложные социально-экономические условия. О том, что торговля людьми имеет глубокие корни, лежащие в сфере экономических, социальных и культурно-нравственных отношений, говорится почти в каждой работе, посвященной данной теме. В качестве корневых причин обычно указывается бедность, а именно: ограниченность экономических возможностей доступа к эффективной занятости, образованию и другим ресурсам человеческого развития, большие разрывы в уровне развития между странами, кризис семьи, насилие в семье, рост неблагополучных семей, социального сиротства, алкоголизм, и другие факторы. Однако в большинстве работ данные факторы лишь упоминаются, механизмы же их влияния с точки зрения торговли людьми остаются нераскрытыми [18].

В заключении отметим, что социально-экономическая природа торговли людьми в целях эксплуатации связана с распространением бедности, сегрегацией на рынке труда, ограниченностью доступа большого количества населения к эффективной занятости, образованию, социальной защите и другим ресурсам.

Причем экономическая ситуация в большинстве стран выезда мигрантов такова, что значительная часть населения оказывается в маргинальном положении. Соответственно, риск оказаться в ситуации эксплуатации и торговли людьми распространяется на значительные совокупности людей, включая и работающее население. Так, трудовым формам эксплуатации, граничащим с рабством и торговлей людьми, может подвергнуться любой человек, вынужденный трудиться неформально без какой бы то ни было социальной защиты [18].

Бедность и недоступность эффективной занятости как мотивация к необдуманным поступкам, заставляет людей использовать рискованные модели экономического поведения, соглашаясь на эксплуатацию и «рабские» условия труда. Эти процессы глубже, чем может показаться на первый взгляд. Меняются модели экономического поведения людей: становление риска нормой, искажение критериев рационального поведения. Трудное экономическое положение людей уменьшает их личные социальные стандарты и, соответственно, требования к обществу, расширяя границы социальной нормы до неприемлемых с точки зрения прав человека и человеческого развития пределов [18].

В результате всего вышеизложенного, нами было доказано наличие значительного количества факторов, способствующих возникновению и развитию рабства и торговли людьми, их многоуровневость и многоаспектность, следовательно, выявление и установление степени негативного воздействия всех детерминантов на повышение уровня рабства торговли людьми и непримиримая борьба с ними является необходимой предпосылкой для эффективного противодействия исследуемого нами преступления.

Литература

1. Сахаров А.Б. О личности преступника и причинах преступности в СССР [Текст] / А.Б. Сахаров. – М.: Госюриздат, 1961. – С. 279.
2. Философский энциклопедический словарь [Текст]: Сов. энциклопедия / [гл. ред. Л.Ф. Ильичев, П.Н. Федосеев и др.]. – М., 1983. – С. 840.
3. Герцензон А.А. Введение в советскую криминологию [Текст] / А. Герцензон, Н. Кузнецова, С. Остроумов. – М.: Гос.юр.издат., 1965. – С. 227.
4. Каракушев С.И. Преступления, связанные с венерическими заболеваниями и ВИЧ/СПИДом (уголовно-правовые и криминологические проблемы) [Текст]: дис. ... канд. юрид. наук: 12.00.08 / С.И. Каракушев. – Астана, 2000. – С. 193.
5. Кибальник А. Новые преступления против личной свободы [Текст] / А. Кибальник, И. Соломоненко // Российская юстиция. – 2004. – №4. – С. 50-54.

5. Макаров С.Н. Реализация международно-правовых обязательств по борьбе с рабством и работорговлей в уголовном законодательстве России [Текст]: дис. ...канд. юрид. наук: 12.00.08 / С.Н. Макаров. – М. 2004. – С. 208.
6. Каиржанова С.Е. Преступность в сфере банковской деятельности [Текст]: монография / С.Е. Каиржанова. – Алматы, 2006. – С. 214.
7. Абдиров Н.М. Концептуальные проблемы борьбы с наркотизмом в Республике Казахстан [Текст]: дис. ... канд. юрид. наук: 12.00.08 / Н.М. Абдиров. – Алматы, 1999. – С. 178.
8. Еникеев М.И. Юридическая психология [Текст] / М.И. Еникеев. – СПб., 2004. – С. 439.
9. Буряк М.Ю. Торговля людьми и борьба с ней: Криминологические и уголовно-правовые аспекты [Текст]: дис. ... канд. юрид. наук: 12.00.08 / М.Ю. Буряк. – Владивосток, 2005. – С. 246.
10. Еникеев М.И. Юридическая психология [Текст] / М.И. Еникеев. – СПб., 2004. – С. 439.
11. Ерохина Л.Д. Торговля женщинами и детьми в целях сексуальной эксплуатации в социальной и криминологической перспективе [Текст] / Л.Д. Ерохина, М.Ю. Буряк. – М., 2003. – С. 430.
12. Ерджанов Т.К. Международно-правовая борьба с рабством и работорговлей [Текст] / Т.К. Ерджанов // Права человека: международный опыт, проблемы и перспективы: сборник материалов научно-теоретической конференции, посвященной международному дню защиты прав человека. – Алматы: Қазақ университеті, 2005. – С. 23-26.
13. Герцензон А.А. Введение в советскую криминологию [Текст] / А. Герцензон, Н. Кузнецова, С. Остроумов. – М.: Гос.юр.издат., 1965. – С. 227.
14. Ильина Н.В. Особенности причинного комплекса преступности в условиях перехода к рыночной экономики [Текст]: дис. ... канд. юрид. наук: 12.00.08 / Н.В. Ильина. – М., 1998. – С. 214.
15. Каиржанов Е.И. Понятие, структура и виды профилактики преступлений [Текст]: лекция / Е.И. Каиржанов. – Караганда, 1986. – С. 72.
16. Баймагамбетова З.М. Сравнительный анализ сферы торговли несовершеннолетними по уголовному законодательству Казахстана и России [Текст] / З.М. Баймагамбетова // Студент. – 2003. – №3. – С. 257-260.
17. Бакиева М. Казахстан: Экономический рост в стране благоприятствует развитию торговли людьми [Текст] / М. Бакиева // Информ. агентство «Фергана.ру»: <http://www.ferghana.ru/article.php?id=4654>
18. Торговля людьми в Российской Федерации: обзор и анализ текущей ситуации по проблеме // Исслед. провед. Е.В. Тюрюкановой совместно с Фондом «Институт экономики города» для рабочей группы агентств ООН и Международной организации миграции (МОМ) по проблемам торговли людьми. – М., 2006. – С. 128.



СОРОКУН

Николай Сергеевич

доцент кафедры уголовного права и криминологии
Ростовского юридического института МВД России,
к.ю.н., доцент, полковник полиции

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРИЧИН И УСЛОВИЙ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ, КАК ОСНОВА ПРОФИЛАКТИКИ ТАКИХ ДЕЯНИЙ

В настоящее время наблюдается активное преобразование всех сфер жизнедеятельности граждан. Не остается без внимания и область информационных технологий, развитие которых стремительно возрастает. Становится невозможно уследить за всеми событиями в данной сфере. Создание современной техники, различных программ и приложений приводит к тому, что совершается множество преступлений в информационной среде. Данные обстоятельства ведут к неблагоприятным условиям в обществе. Уровень воспитания и нравственности становится низким, в результате чего падает и уровень развития людей. Современные технологии помогают не только развиваться и совершенствоваться, но и терять те качества, которые необходимы любому человеку для хорошей жизни.

Вопрос раскрытия и расследования преступлений, совершаемых с использованием компьютерных технологий, становится очень остро в последнее время. Прежде всего, данный факт обусловлен необходимостью развития и совершенствования существующих методик расследования преступлений. Очевидно, что с развитием информационных технологий возникает необходимость в преобразовании стандартных методик и средств. Однако внимание также стоит уделять и предупреждению преступлений данного вида. В связи, с чем видятся актуальными рассмотрение вопросов, связанных с причинами и условиями совершения компьютерных преступлений, а также изучение характеристики личности преступника и потерпевшего.

В настоящее время наблюдается повсеместное внедрение компьютерных технологий во все сферы жизнедеятельности общества. Основное внимание уделяется внедрению в производственные, экономико-финансовые и общественные отношения. Рассматриваемый процесс компьютеризации способствует развитию и совершенствованию жизни общества, а также приводят к появлению новых категорий преступных деяний. Такие преступления совершаются с использованием компьютерной информации и посредством компьютерных технологий.

По общему правилу данные преступления делятся на три категории: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для электронно-вычислительных машин (далее – ЭВМ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Данные противоправные деяния находят свое отражение в нормах Особенной части Уголовного кодекса Российской Федерации.

Рассматриваемые группы преступлений представляют особый интерес, который, прежде всего, обусловлен характеристикой субъекта совершения компьютерных преступлений. Данный аспект объясняется тем, что обычный гражданин вряд ли способен совершить неправомерный доступ к компьютерной информации или создать вредоносную программу, не обладая специальными знаниями в области информационно-телекоммуникационных систем.

В 2020 году наиболее распространены мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70% всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4%, 237,1 тыс.).

В 2021 году мошенничество в сфере информационно-телекоммуникационных технологий составило 73% всех хищений (249,2 тыс.), совершенных путем обмана или злоупотребления доверием. При этом существенно замедлились темпы их прироста (с 73,4 % в 2020 году до 5,1% в текущем).

За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8% до 25%. Большинство «киберпреступлений» совершается с использованием сети «Интернет» (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.).

Кроме того, по своей природе компьютерные преступления носят латентный характер. Немаловажным элементом выступает также и характер совершения данных преступлений. Все преступные деяния, которые совершаются с помощью использования информационно-телекоммуникационных систем, всегда скрыты от обычных людей и выявление таких преступлений представляет собой особый процесс. Прежде всего, для выявления и последующего раскрытия компьютерного преступления необходимо обладать специальными знаниями в области компьютерных технологий, так как доказательственная база будет формироваться в большей степени путем нестандартных методов.

В связи с указанным ранее фактором следует сказать о том, что профилактика в таком случае должна базироваться на уяснении причин и условий совершения преступления данного вида. На этом вопросе хотелось бы остановиться более подробно.

Анализируя различные источники по данному вопросу, был сделан вывод, что причины совершения преступлений в сфере компьютерной информации можно подразделить на две основные категории. Первая категория характеризуется общими причинами преступности с использованием возможностей информационно-телекоммуникационной системы. В данную категорию могут входить причины различного уровня, которые присущи как компьютерным преступлениям, так и иным видам преступности.

Что касается второй категории, то она характеризуется специфическими причинами компьютерных преступлений. В частности, причины данной группы выражаются в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений, связанных с появлением автоматизированных систем обработки информации. В рамках данной категории выделяют следующие причины компьютерной преступности:

- уязвимость и зависимость компьютерных систем друг от друга;
- несоответствие уровня развития юридических и политических структур уровню развития компьютерных и телекоммуникационных технологий;
- динамичное развитие зависимости современных технологий от компьютерных систем;
- отсутствие должного информирования граждан об уязвимости компьютерных систем;
- существующие на сегодняшний день пробелы уголовного законодательства в части, касающейся регулирования общественных отношений в сфере компьютерной информации, а именно, отсутствие некоторых составов в уголовном законодательстве;
- различия в законодательной базе с точки зрения соответствия отечественного и международного законодательства.

Однако хотелось бы заметить, что данные причины не могут рассматриваться в качестве непосредственных. В юридической литературе отмечается, что основной причиной, подталкивающей лицо на совершение компьютерного преступления, будет являться детерминация преступного поведения.

Что касается условий совершения преступлений в сфере информационно-телекоммуникационных технологий, то стоит обратить внимание на следующие:

- открытый доступ к автоматизированным информационным системам, с помощью которых могут совершаться финансовые операции различного характера;
- отсутствие должного контроля за отдельными категориями сотрудников, что позволяет злоумышленникам использовать электронно-вычислительные машины предприятий в качестве оружия преступления;
- низкий уровень защиты компьютерных систем;
- лёгкий доступ к данным электронно-вычислительной машины, ввиду отсутствия надёжной парольной системы;
- отсутствие во многих организациях специально уполномоченного субъекта, отвечающего за сохранения конфиденциальности отдельных информационных данных;
- отсутствие соглашений сотрудников о неразглашении данных, составляющих конфиденциальную информацию, в том числе пароли и иные ключи доступа к электронно-вычислительным машинам.

Хотелось бы отметить, что большинство условий создаются непосредственно потерпевшими лицами. Основной причиной является неосмотрительность лица. Помимо указанных условий могут отмечаться и иные. Нами были рассмотрены наиболее актуальные условия совершения информационных преступлений.

Рассмотрев причины и условия совершения преступлений в сфере компьютерной информации, вытекает вывод о том, что их круг достаточно обширен. На основании рассмотренных данных хотелось бы перейти к характеристике лиц, способных к совершению преступлений в сфере информационных технологий.

Анализируя практическую деятельность, можно сделать вывод о том, что субъектом совершения преступлений в сфере компьютерной информации в большинстве случаев выступает лицо мужского пола. Возрастная группа данных лиц, как правило, варьируется от 18 до 24 лет. Иными словами, совершают данное преступление лица студенческого возраста или же те, которые его только окончили. Считаем, что именно в таком возрасте на человека можно оказывать некое воздействие, которое будет способствовать формированию у него устойчивого преступного поведения.

Хотелось бы также отметить, что огромная доля компьютерных преступлений носят латентный характер, соответственно, не могут быть выявлены и проанализированы. В связи с этим возникает сложность в точном определении возрастных рамок субъекта совершения преступления, а также отдельных черт, характеризующих его.

Характеризуя личность компьютерного преступника, важно обратить внимание на психологические особенности данных лиц. В этом вопросе стоит рассмотреть отдельные качества личности, указывающие на поведение преступника.

Так, изучаемые лица, как правило, имеют замкнутый характер и не стремятся достичь высокого положения в обществе. В большинстве случаев они действуют индивидуально в связи с такой чертой характера, как скрытность. При общении отдельные лица данной категории конфликтны, не обладают особой эмоциональностью.

Указанные выше факторы свидетельствуют об одиночном характере осуществления деятельности данными субъектами. Однако специалистами в данной области отмечается, что они стремятся принадлежать к определённой социальной группе, откуда и вытекает создание хакерских сообществ.

Рассматривая категорию субъектов преступления в сфере компьютерной информации, можно сделать вывод о том, что указанные лица обладают высокой самооценкой. По нашему мнению это связано с тем, что данная сфера деятельности, а именно информационно-телекоммуникационные технологии, требуют высоких знаний для ее осуществления. В связи с чем лица, разбирающиеся в данной области, считают себя на ступень выше от обычных людей, так как обладают высокими знаниями в сфере компьютерных технологий. Указанные факторы позволяют говорить о спонтанном совершении преступлений без должной к тому подготовки.

Изучение поведения субъектов компьютерных преступлений свидетельствует о наличии таких признаков, как:

- установление и поддержание социальных связей с иными лицами, совершающими преступления в сфере компьютерной информации;
- обсуждение способов совершения преступлений в сфере информационно-телекоммуникационных технологий;
- использование словесных оборотов, присущих лицам, разбирающимся в компьютерных технологиях.

В поведении рассматриваемой категории лиц могут выделяться и иные черты.

В рамках исследования данной темы было отмечено также проблематичность получения информации о типичных характеристиках личности компьютерного преступника. Данное обстоятельство обусловлено высокой латентностью данных преступлений и отсутствием должного эмпирического материала, позволяющего изучать данную тему со всех сторон.

Таким образом, подводя итог настоящей статьи, хотелось бы отметить, что компьютерные преступления в настоящее время набирают особую популярность. В большинстве случаев преступления такого рода остаются незамеченными. Данное обстоятельство вытекает из-за отсутствия компетентных специалистов среди сотрудников органов внутренних дел, способных раскрывать и расследовать преступления в сфере информационно-телекоммуникационных технологий.

Одной из причин совершения данной категории преступлений выступает формирование преступного поведения у лиц. Такая причина рассматривается в качестве основной, поскольку именно преступное поведение может подталкивать лицо на совершение преступления.

При рассмотрении особенности личности субъекта преступлений в сфере компьютерных технологий главной характеристикой считается возраст лица, который был отмечен в диапазоне от 18 до 24 лет. Безусловно, данный диапазон не может рассматриваться в качестве основного и единственного, поскольку данные преступления совершаются лицами и в 16 лет, и в 35.

Специфические особенности личности преступника проявляются в его поведенческих чертах. Так, например, компьютерный преступник, как правило, обладает скрытым и замкнутым характером, малообщителен и обладает низким уровнем эмоциональности.

В заключении стоит сказать о том, что криминологическая характеристика компьютерных преступлений будет оставаться актуальным вопросом, поскольку в настоящее время отсутствует достаточная эмпирическая база для изучения данной темы в полном объёме. Указанное обстоятельство вызвано тем, что большинство преступлений в сфере информационно-телекоммуникационных технологий носят латентный характер, ввиду чего не учитываются в общей статистике преступлений.

Литература

1. Аскольская Н.Д. Специфика криминалистической характеристики киберпреступлений // Закон и право. 2019. №8. – С. 89-92.
2. Ахмедханова С.Т., Кахбулаева Э.Х. Криминологическая характеристика преступлений в сфере информационных технологий // Вестник МГОУ. Серия: Юриспруденция. 2018. №4. – С. 16-23.
3. Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. 2018. №1 – С. 31.
4. Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия АлтГУ. 2018. №6 – С. 104.
5. Ханов Т.А., Нуркеев А.Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия АлтГУ. 2017. №6 – С. 98.



МЕЛЬНИК

Светлана Львовна

Зав.кафедрой организации судебной и прокурорской деятельности СмолГУ,
доцент кафедры уголовно правовых дисциплин Смоленского филиала
Международного юридического института, к.ю.н., доцент

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИЗНАНИЯ ПОТЕРПЕВШИМ ПО КОРРУПЦИОННЫМ ДЕЛАМ

Статья посвящена анализу признания лица потерпевшим по коррупционным преступлениям в свете внесения дополнений в Постановление Пленума Верховного Суда РФ от 9 июля 2013 года и судебной практики имеющей противоречивые примеры.

Коррупция, как ржа, разъедает государство изнутри, разрушая не только экономику государства, но и уродуя нравственные устои общества, душу человека. Взятничество, одно из опасных преступлений против службы.

Уголовный кодекс РФ содержит раздел X, преступления против государственной службы и главу 29 содержащую ст. 290-291.2 посвященные этому составу преступления. Причем некоторые статьи, такие как 291.2 появились относительно недавно, в 2016 году благодаря ФЗ от 03.07.2016 года №324 «О внесении изменений в УК и УПК РФ». Этим же законом внесены изменения в ст. 290, 291, 291.1 УК РФ. Помимо указанных, к коррупционным преступлениям относятся такие составы преступлений, как регламентированные ст.ст. 159, 160, 204, 292 и 304 УК РФ.

Конституция РФ, как основной закон страны, в ст. 2 регламентирует признание, соблюдение и защиту прав человека обязанностью государства и его должностных лиц. Часть 1 ст. 19 провозглашает, что все равны перед законом и судом, а ст. 52 – что права потерпевшего от преступления охраняются законом, он имеет право на доступ к правосудию и возмещение причиненного ущерба.

Являясь преступлением с формальным составом, взяточничество не имеет потерпевшего, в обычном его понимании.

Согласно диспозиции ст. 290 УК у данного состава преступления два субъекта – взяткодатель и взяткополучатель, которые подлежат уголовной ответственности по ст.ст. 290 и 291 УК РФ соответственно.

Взяткополучатель это должностное лицо, обладающее организационно-распорядительными и административно-хозяйственными обязанностями, уполномоченное в установленном порядке на совершение юридически значимых действий.

Взяткодатель, это лицо, достигшее возраста 16 лет и передающее взяткополучателю предмет взятки добровольно, либо в результате вымогательства или путем обмана и злоупотреблением доверия со стороны взяткополучателя. В любом случае, это лицо совершает противоправное действие сознательно. Согласно примечанию к ст. 291 УК взяткодатель может освободиться от уголовной ответственности по двум основаниям: во-первых, в результате деятельного раскаяния и оказания активного содействия в расследовании и раскрытии данного преступления, и, во-вторых, если имело место вымогательство взятки или добровольное со-

общение после совершения преступления о даче взятки, посредничестве во взяточничестве либо коммерческом подкупе следственному органу. В этом случае, как разъяснил в своем Постановлении №24 от 9 июля 2013 года Пленум Верховного Суда, (с дополнениями от 24.12.2019 №59), взяткодатель не может быть признан потерпевшим и требовать возмещения ему причиненного материального ущерба, так как в его действиях присутствует состав преступления (п.30 указанного постановления). Правда, о том, какой статус в это случае должен получить взяткодатель, Верховный Суд не пояснил. В п.4 другого постановления Пленума ВС РФ от 29.06.2010 № 17 «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» содержится положение, согласно которому если по поступившему уголовному делу суд установит, что лицо признано потерпевшим без достаточных к тому оснований, предусмотренных ст.42 УПК, он выносит постановление (определение) о том, что такое лицо ошибочно признано потерпевшим, и разъясняет ему право на обжалование принятого судом решения в апелляционном порядке.

В постановление Пленума №24 дано разъяснение, что в том случае, если должностное лицо получило ценности за совершение действий (бездействие), которые в действительности оно не может осуществить ввиду отсутствия служебных полномочий и невозможности использовать свое служебное положение, такие действия при наличии умысла на приобретение ценностей следует квалифицировать как мошенничество, совершенное лицом с использованием своего служебного положения.

Как мошенничество следует квалифицировать действия лица, получившего ценности якобы для передачи должностному лицу или лицу, выполняющему управленческие функции в коммерческой или иной организации, в качестве взятки либо предмета коммерческого подкупа, однако заведомо не намеревавшегося исполнять свое обещание и обратившего эти ценности в свою пользу. Владелец переданных ему ценностей в указанных случаях несет ответственность за покушение на дачу взятки или коммерческий подкуп (п. 24 указанного постановления).

Практике известны примеры, когда исходя из этой позиции Верховного Суда некоторые недобросовестные следователи или гособвинители стали переквалифицировать действия взяткополучателя на мошенничество, ибо оно является менее тяжким преступлением и уголовная ответственность за него соответственно мягче.

Мы согласны с позицией ВС РФ и считаем, что придавать статус потерпевшего взяткодателю в любом случае, как бы не квалифицировались действия взяткополучателя, недопустимо. Однако имеют место случаи, когда суды нарушают его разъяснения.

В соответствии со ст. 42 УПК потерпевший это физическое или юридическое лицо, которым преступлением причинен, физический, имущественный, моральный вред или вред деловой репутации. Данная статья регламентирует обширный перечень прав потерпевшего, включая право знакомиться со всеми материалами уголовного дела по окончании расследования и делать любые выписки из любых материалов или копии документов (п.12 ч.2). Теперь рассмотрим ситуацию, когда взяткодатель становится потерпевшим, знакомится с протоколами следственных действий, затем со всеми материалами уголовного дела и обдумает, возможно, вместе с адвокатом, линию своих показаний в суде, линию обвинения. Конечно, он будет всячески пытаться «обелить» себя и свалить всю вину на взяткополучателя.

Подобной точки зрения придерживаются и некоторые другие ученые. Так, Ф.Ю. Васильев приводит пример приговора Саратовского гарнизонного военного суда (дело №1-3-20/2020), который 22.01.2020 вынес обвинительный приговор, переквалифицировав деяния подсудимого с п. «г» ч. 4 ст. 290 УК на ч. 4 ст. 159 УК и признал взяткодателя потерпевшим [1]. Аналогичные примеры приводят и В.А. Слащев и А.А. Шеляшкова [2]. В научной литературе существует мнение, что в указанной ситуации, при прекращении уголовного преследования в отношении взяткодателя в порядке ст. 28 УПК, логичнее считать его свидетелем по новому уголовному делу.

Свидетель обладает ограниченным кругом прав по сравнению с потерпевшим и поэтому в данном случае, не нарушаются права стороны защиты (взяткополучателя).

Традиционно считается, что мошеннические действия не могут совершаться без наличия потерпевшего, так как мошенник осуществляет свои действия в отношении конкретного лица.

В этой связи представляет интерес практика военной юстиции, которая в ситуации коррупционного мошенничества, пошла следующим путем, в обвинительном заключении по уголовному делу, в котором взяткополучатель признан мошенником, они используют следующую формулировку: «Сведений о потерпевшем нет, так как в соответствии с положениями ст. 168 и ст. 169 ГК РФ действия гражданина, направленные на дачу взятки, то есть нарушающие требования закона, совершенные с целью, противной основам правопорядка, не дают ему оснований к возникновению права требования возмещения имущественного ущерба». Такая позиция обосновывается тем, что потерпевший, передавая деньги, пытался решить свои вопросы незаконным путем [3].

Иного мнения придерживается Ф.Н. Багаутдинов, полагающий, что применение разъяснений Верховного Суда правоприменители восприняли неоднозначно, ибо государственные обвинители в суде полагают, что не было бы мошеннических действий взяткополучателя, вероятно, не было бы и преступления. Поэтому они не ходатайствуют в суде об изменении статуса взяткодателя, а суды исходят из позиции гособвинителя. Считаем данную позицию неубедительной.

Поэтому, предлагаем закрепить в ст. 42 УПК РФ положение о том, что по делам о коррупционном мошенничестве, взяткодатель не может быть признан потерпевшим, несмотря на сумму ущерба, причиненного ему преступлением.

Литература

1. Васильев Ф.Ю. Возможность признания потерпевшим лица, преследовавшего незаконный интерес в деле// Уголовный процесс. 2022. №9. URL: [https:// e.ugpr.ru/985670](https://e.ugpr.ru/985670) [Электронный ресурс].
2. Слащев В.А., Шеляшкова А.А. Признание взяткодателя потерпевшим. Ошибочная практика и процессуальное решение//уголовный процесс. 2020. №12. URL: <https://e.ugpr.ru/853548> [Электронный ресурс], (дата обращения 14.09.2022г).
3. Багаутдинов Ф.Н. Может ли коррупционное мошенничество быть без потерпевшего // Уголовный процесс. 2021. № 8. URL: <https://e.ugpr.ru/907909> [Электронный ресурс].



РУСТЕМОВА

Гаухар Рустембековна

научный сотрудник научного центра Алматинской академии МВД Республики Казахстан
им. М. Есбулатова, д.ю.н., профессор, полковник полиции в отставке

ПРАВОВЫЕ РИСКИ ЦИФРОВИЗАЦИИ В ЗАКОНОДАТЕЛЬСТВЕ О ЗДРАВООХРАНЕНИИ

Повсеместное внедрение в практику здравоохранения ИТ (информационных технологий) существенно поменяли взаимоотношения врач-пациент (больной), включая лечебную и профилактическую медицину и реабилитации здоровья человека. О ключевых направлениях развития цифровой медицины мы описали выше. Отметим только, что цифровизация – «ведущий тренд современного здравоохранения в мире и стране, это вызывает необходимость в создании социально-экономических и технологических условий для оказания удалённой медицинской помощи и диагностического контроля».

Самые перспективные направления инвестиций в медицине до 2030г. – это «клеточная (таргетная) медицина, прогнозирующая адресную фармакотерапию; банки собственных стволовых клеток пациентов (больных) для будущих возможных пересадок органов и тканей (трансплантации); круглосуточный беспроводной контроль за состоянием здоровья хронических больных и др.; геронтология, использование крионики; лекарства и технологии, замедляющие процесс старения на клеточном уровне; телемедицина /ИТ-медицина, предполагающая биопринтинг, робототехника, автоматизация процессов терапии, безопасность хранения данных о пациенте (больном), 4П-медицина. В частности, персонализированная медицина, которая предполагает медицинские манипуляции, созданные под генетический паспорт конкретного человека, архив генов».

Особое внимание уделяется сейчас 4-П медицине, которая предполагает индивидуальный подход к каждому пациенту (больному). Это направление хорошо развивается в России благодаря многим научным открытиям российских учёных в сфере биоинформатики, генетики, биоинженерии и др. Первичные структуры ДНК позволяют анализировать транскриптомные данные конкретного пациента (больного). Но в таких случаях есть риск относительно надёжности хранения данной информации, последствий её разглашения и ответственности за это. В будущем наблюдаем переход «от реактивной модели к проактивной предиктивной и превентивной» (Гребенщикова, 2015).

Т.е., нам представляется, что больше следует уделять внимание геномным и биохимическим исследованиям, от здорового образа жизни, чистого воздуха и чистой воды повсюду к профилактической (превентивной) медицине, от них строить новое профилактическое здравоохранение.

Однако в последние годы поднята дискуссия среди биоэтиков и медиков по поводу расширения ответственности пациента (больного) за своё здоровье и её переносом с общественно-го здравоохранения и его социальных институтов на конкретного индивида. Но риск оказывать давление на пациентов со стороны медработников остаётся, он примет новые формы, т.к. якобы под лозунгом защиты интересов и здоровья пациентов окажутся интересы представителей фарминдустрии и страховых компаний.

Многие авторы отмечают два направления здравоохранения – использование ИИ и телемедицину. При этом риски присутствуют и в применении традиционных методов лечения, а не только при цифровой медицине. Поэтому следует для внедрения обозначенных технологий модернизировать законодательство о здравоохранении, гражданское, трудовое, административное и уголовное законодательство для определения статуса ИИ, его сущности и содержания, чего нет в действующем КЗСЗ РК.

В литературе выделено четыре блока пробелов в законодательстве о здравоохранении, они присутствуют и в нашем КЗСЗ. Первый блок – общие проблемы, как противоречия между публичным и частным интересом в здравоохранении в условиях современных глобальных вызовов. Второй блок – развитие медицинских технологий и новых принципов биоэтики, несоответствие правового регулирования и нарастания дегуманизации медицины в целом. Основные правовые риски для врача при применении медицинских технологий: защита генома, вопросы генной инженерии, право на эксперимент и на доступность новых лекарств, противоречия этики и права, права детей «из пробирки» и проблема «лишних эмбрионов».

Третий блок – обеспечение публичного контроля за быстро прогрессирующими технологиями. Перспективы будущей и индивидуальной медицины, правовые риски недоступности новой медицины и дороговизны новых технологий – часть проблем, беспокоящих правовое общество и общественность. Ещё более опасна цифровизация здравоохранения, создание больших данных медицинской информации – как индивидуальной, так и общественной (национальной, региональной и малых групп населения), использование ИИ и роботов, потеря врачебным сообществом «профессиональности» и переход к ИИ, что может стать неуправляемым процессом.

Последний, четвёртый блок – проблемы медицинского сообщества: его корпоративная закрытость как основа ухода от ответственности, латентную ятрогенную преступность среди медицинских работников и декриминализацию врачебной деятельности.

Для всех граждан страны сейчас наступило время ответственного отношения к своему здоровью (ч.1 ст.135 КЗСЗ). Наряду с медицинскими методами государству необходимо обеспечить социально-экономическую безопасность населения, продвигать ЗОЖ (здоровый образ жизни), создать условия и стимулы для приверженности граждан к здоровому питанию, отказу от вредных привычек, занятию спортом всех возрастных категорий.

В науке и на практике отмечается тотальный охват цифровизацией всех сфер общественной жизни – социальную, политическую, экономическую, культурную. Возможен риск постепенного вытеснения государства ИИ, переводом государственных функций в цифровой формат.

«Опыт Китая показал те крайности и риски, которые делают возможным «цифровой тоталитаризм», когда каждый человек, каждое юридическое лицо и предприятие в государстве круглосуточно находятся под тотальным наблюдением и гиперконтролем. С точки зрения глобальной безопасности тотальная цифровизация одновременно и благо и риск... риск – поскольку искусственный интеллект пока не может заменить аналитическую, прогностическую и логическую работу человеческого мозга, когда постоянно нужно предвидеть и просчитывать вероятность новых угроз и вызовов с возможностью превентивного и оперативного реагирования».

Сбор данных не исключают их утечку, сфера медицины лидирует в этом вопросе. Все медицинские данные являются особой категорией персональных данных, их обработка допускается в случаях, прямо установленных законом (ч.4 ст.60): «Передача персональных медицинских данных в Национальный электронный паспорт здоровья и электронные информационные ресурсы уполномоченного органа осуществляется без согласия физического лица, а также

субъектом здравоохранения, только в случаях, указанных в: пункте 1 ст.137 настоящего Кодекса; Законе РК «О персональных данных и их защите».

Пункт 1 ст.137 КЗСЗ гласит:

«Оказание медицинской помощи без согласия пациента допускается в отношении лиц: находящихся в шоковом, коматозном состоянии, не позволяющем выразить свою волю;».

Сейчас важный вопрос стоит о защите персональных данных именно в здравоохранении, т.к. это риск здоровью и жизни человека. К сожалению, по данным некоторых исследований. Здравоохранение находится в лидерах по утечке персональных данных. Думается, это связано с недостатком кадров в отрасли, недостаточной подготовкой их. Введение новых специальностей, дополнительного образования в медвузах и колледжах устранил постепенно этот пробел.

Другая проблема, которая должна была быть гарантией на полную защиту пациента (больного) – это обезличивание персональных данных. Но и это не панацея и не исключает вероятность утечки МИ (медицинской информации). Любые ИС (информационные системы), МИС (медицинские информационные системы) должны исходить из интересов пациентов (больных) и учитывать потребность ими в современных технологиях медицины. Поэтапное внедрение цифровых технологий в здравоохранении наблюдаем в связи с внедрением электронных медкарт, создания МИС, отдельных регистров, расширения в областные и районные центры телемедицинских сервисов, появления специальных устройств, отслеживающих состояние здоровья человека (фитнес браслеты, помпы для определения уровня сахара в крови).

Цифровая медицина предполагает врачу быть больше вовлечёнными в процесс лечения, приёма больных, проведения консультаций путём использования программ, использующие технологии ИИ, для минимизации рисков ошибки и неправильной диагностики. ИИ при этом остаётся лишь помощником врачу, т.к. окончательное решение по каждому диагнозу больного принимает **врач**. А для принятия решения самим ИИ, независимо от врача, не быть просто «*second opinion*», необходимо решения правовых проблем регулирования деятельности ИИ.

К числу рисков цифровой трансформации отрасли отнесены: недостаточная цифровая компетенция граждан (особенно пожилых); отсутствие у населения доверия к существующим медицинским сервисам; двойной бумажный и электронный) документооборот до сих пор; увеличение нагрузки на медработников при введении электронной документации (медкарты, больничные листы, протоколы операций и т.д.); низкие пока темпы перехода от бумажного к электронному документообороту; существующие различия в уровне готовности медучреждений, регионов; различие в финансовом обеспечении в центре и на местах; внесение корректив в силу чрезвычайных обстоятельств (COVID-19, другие заразные болезни).

Россияне также пришли к выводу о принятии Медицинского кодекса РФ как отдельного кодифицированного акта, регулирующего отношения в сфере охраны здоровья. Такое решение должно сократить подзаконное нормативное правовое регулирование, уменьшить использование бланкетного способа правового регулирования.

Пришло время обратиться именно к пациентоориентированной (каждому индивидуально, в зависимости от заболевания, состояния здоровья и других параметров, что берут во внимание медики), а не нынешней клиенто-ориентированной медицине (как в основном сейчас), которая будет соответствовать принципам гуманизма. Поэтому считаем важным при создании и разработке пациенториентированных МИС тесное взаимодействие с профессиональным сообществом. «Пациентоориентированная медицина заключается именно в фокусировке на потребностях больного. Разумеется, это потребует смены приоритетов и перенастройки всех МИС с соблюдением принципов персонифицированной медицины. Причём, анализ лечебного процесса информирует о реализации этих ИТ, раскрывает роли, действия и другие важные данные, такие, как передача информации и требования к осведомленности о ситуации».

Взросла необходимость выработки нравственных ориентиров использования ИИ в сфере здравоохранения, определить границы его применения. При этом использование телемедицины нельзя назвать в полной мере использованием ИИ. Как правильно отмечено специалистами, обеспечение приватности МИ при оказании медицинской помощи является также риском. При оказании медпомощи (неотложной, скорой) при распространении опасных или массовых забо-

леваний (как COVID-19) корректируется режим охраны МИ (медицинская тайна, персональные данные и др.). Использование ИИ при оказании медпомощи (при предложении им новых решений диагностики и лечения), использовании телемедицины и другое, проблема медицинских ошибок (медицинский инцидент) не исчезает, а актуализируется. Они могут возникать при сбоях в ИКТ, внешнего вредоносного вмешательства с целью внесения заведомо недостоверных данных, недостаточной квалификацией медперсонала, ошибок технического плана при соединении цифровых и биологических технологий.

В стране пока не развита разработка стандартов для медицинских изделий и устройств, производимых в Казахстане, либо завозимых в страну, и правовое сопровождение их. Следует обратить внимание на это профильному министерству и юристам. В научных публикациях по теме исследования указаны риски обеспечения информационной безопасности и защиты информации личного характера людей. Помимо хакерских атак, незаконно распространять информацию может и сам медперсонал.

В литературе справедливо отмечены следующие направления цифрового здравоохранения и цифровой медицины, требующих полноценного правового регулирования: «...выделяют следующие проблемы правового регулирования:

- проблемы, связанные с корректным определением юридической ответственности за деяния, совершенные с использованием технологий искусственного интеллекта ...;
- проблемы, связанные с адаптацией вновь создаваемых норм права, направленных на регулирование отношений в этой сфере, в общем массиве существующего законодательства...;
- проблемы обеспечения конфиденциальности персональных сведений и личной информации в условиях сбора и хранения большого массива персональной информации в электронных и автоматизированных базах данных (институт врачебной тайны);
- проблемы стандартизации технологий ИИ в медицине;
- проблемы лицензирования медицинских изделий с использованием технологий ИИ;
- финансово-правовые проблемы оказания медицинских услуг в цифровом формате.

Развитие правового регулирования ИИ в области здравоохранения следует вести по следующим основным направлениям:

- в зависимости от выполняемых работ, оказываемых услуг в системе цифрового здравоохранения и от изготавливаемой высокотехнологичной продукции для медицины (медицинские изделия) и фармакологии;
- в зависимости от задействования в цифровом здравоохранении слабого или сильного ИИ;
- в зависимости от рисков и регулирования требований кибербезопасности, информационной безопасности, безопасности использования киберфизических систем...».

Следующим правовым риском в здравоохранении является отсутствие до сих пор детально отработанной системы юридической ответственности при использовании цифровых технологий (ЦТ) в рассматриваемой области. Определение правовых рисков в области цифровизации здравоохранения необходимо для выявления приоритетных направлений её. Сюда можно отнести создание цифрового профиля пациента (больного); защиту личных данных их; медицинскую диагностику (ежегодные или по графику проводимые скрининги населения по возрастным группам); мониторинг тех, кто страдает хроническими заболеваниями; разработка различных вакцин; медицинская статистика; телемедицина; логистика; фармакология; контроль за медперсоналом; медицинское образование всех уровней.

Как видим, степень использования ИИ по этим направлениям различна. Угроза безопасности отдельного пациента (больного), медработника, медицинских организаций (предприятий, учреждений) и отрасли в целом, как угроза цифровизации здравоохранения, должны быть максимально защищены правом и интегрированы в систему обеспечения национальной безопасности, наряду с другими видами безопасности (ст.4 ЗРК «О национальной безопасности»). Перечисленные правовые риски далеко не исчерпывающие и могут либо пополняться либо утрачивать свою актуальность в процессе цифровизации здравоохранения.

В настоящее время, например, используют две технологии ИИ – экспертные системы и нейронные сети (НС). Первые уже неактуальны. А НС активизировались благодаря своим способностям учиться. Выделяют следующие виды ИИ:

«Узкий ИИ (narrow AI) – для решения определённой задачи.

1.Общий ИИ (general AI, AGI) – решение любых задач, с которыми справится человек.

2. Superintelligence – опережать человека по сложности решаемых задач».

Наиболее применяемые «узкие» ИИ, НС созданы на базе биологических нейронных сетей. Следует всё же сделать шаг для открытия медкарт в поликлиниках и больницах, т.к. многие пациенты (больные) противятся этому, думая. Что из данные личного характера могут использоваться во вред или стать достоянием многих. Поэтому это одно из узких мест ИИ в медицине.

ИИ используется в раннем распознавании онкобольных, что даёт хороший положительный эффект в лечении и продлении жизни больного. IBM Watsonfor

Onkology – суперкомпьютер, выдаёт максимально точный ответ на правильно заданный вопрос. Успешно используется в США, Индии и др. странах.

По просьбе ВОЗ международная группа экспертов подготовила доклад «Этика и управление искусственным интеллектом в интересах здоровья», в котором показаны некоторые риски и приводятся рекомендации по их избежанию. Отмечено ими, что мы столкнулись «с превалированием частных коммерческих интересов под этикой и здоровьем пациентов, риском монополизации и использовании ИИ в целях наблюдения и социального контроля, проблем с ответственностью, нарушением этики при сборе медицинских данных, искажении AI bias. AI bias может быть необъективным. Искажения человеческого сознания, а их установлено более 180 когнитивных искажений, могут ненамеренно передаваться ИИ от его создателей. Например, в США ИИ отдавал предпочтение людям с белым цветом кожи, т.к. обучался алгоритм на базе (информации о предыдущих расходах населения на здравоохранение). Белокожих было больше, их доходы выше доходов людей с другим цветом кожи. Искажение нашего общества отразилось на результатах ИИ.

Вопросы правового регулирования ИИ в медицине, разграничения ответственности при его эксплуатации на практике требуют законодательного регулирования. Однако правовое регулирование встречает серьёзные препятствия.

Следует выходить из «серой» зоны, чтобы не оказаться в «чёрной», т.е. вне закона. Прогресс не остановить, а потребность в повседневном, широком применении ИИ в медицине остаётся, основанные на ИИ услуги всё чаще становятся востребованными населением и МО (медицинскими организациями), будут и дальше оказываться.

Для продвижения ИТ в медицине предлагается ряд мер организационного и технического плана, а также подчёркивается необходимость национальных государств инициировать законодательство «о медицинском ИИ, регулирующих неясные на сегодня вопросы (например, вопрос о приватности информации о состоянии здоровья, вопрос открытия для ИИ-систем историй ответственности в различных ситуациях, возникающих при использовании ИИ в диагностике и лечении)».

Прорабатывается законодательно решить вопросы о том, что, если оказана некачественная медицинская помощь с использованием телевидения в случае сбоя системы на платформе-онлайн, целесообразно разработать норму о привлечении к ответственности самого оператора. Сейчас только договорные отношения защищают интересы МУО (медицинских учреждений и организаций). Сами же стандарты телемедицинских услуг не разработаны, видимо, только приступили к их разработке. Риск остаётся всегда, т.к. каждый человеческий организм по-разному реагирует на манипуляции онлайн (страх, испуг, недоверие и т.п. и т.д.).

Российский эксперт Киселёва А.Ю. считает, что комплексность предложенного метода предполагает «основывать решение проблемы ответственности на детальном определении ролей, прав и обязанностей каждого из ... субъектов (а также пациента) на всех стадиях производства, введении в оборот и использование МИ с ИИ. Это включает в себя и доработку детальных процедур клинических испытаний МИ с ИИ; проработку процедуры приёма МИ ме-

медицинской организации; инструкции для медработников, а также детализацию ролей и процедур по мониторингу безопасности МИ. Это позволит не только создать основу для соответствующей доработки институтов ответственности, но и улучшить контроль за качеством и безопасностью МИ с ИИ, тем самым увеличив доверие пациентов (больных), медицинских работников и общества к таким новейшим технологиям».

Как видим, работы в этих направлениях предстоит немало, немаловажен опыт передовых стран, где законодательство о здравоохранении ушло вперёд, в некоторых случаях даже опережая развития цифровой медицины.

Необходимость в разработке стандартов оказания медпомощи с использованием ИИ, телемедицины, роботов остается, нужны кадры, обученные в странах, где таковые имеются, финансирование должное, ведь здоровье нации и народа есть залог самой национальной безопасности.

Литература

1. Русанова Н.Е. История и проблемы цифрового здравоохранения в России //Население и экономика. – 2018. – Том 2. №2. – С. 6.
2. Черновицкая Ю.В. Цифровые технологии в медицине: специфика ответственности при их использовании // Научный результат. Социальные и гуманитарные исследования. 2020. – Т.6, №4. – С. 91
3. Крупным планом. Юрист СПбГУ Игорь Акулин – об этико-правовых проблемах цифровизации медицины // <https://spbu.ru/news-events/krupnym-planom/jurist-spbu-igor-akulin-ob-etiko-pravovykh-problemakh-cifrovizacii-10> марта
4. Тимченко А.В. Риски и угрозы тотальной цифровизации: возможности и потенциал управляемости // Российский журнал правовых исследований. 2022.Т.9. №1. – С. 99-106. DOI: <https://doi.org/10.17816/RILS.99747/>
5. Кодекс о здоровье.../adilet.zan.kz/rus/docs/K2000000360//z1214
6. Макарейко Н.В. Правовые риски цифровизации оказания медицинской помощи //Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2022. №1(57). С.69 // <https://doi.org/1036511/2078-5356-2022-1-67-74>
7. Лапина М.А. Организационно-правовые и финансовые аспекты цифровизации и внедрения технологий искусственного интеллекта в области здравоохранения // Финансы: теория и практика. – 2022. –№ 26(3). – С.169-185. / doi: 10.26794/2587-5671-2022-26-3-169-185
8. Закон Республики Казахстан «О национальной безопасности» от 6 января 2012г. №527-IV // Adilet.zan.kz/docs/Z1200000527 /дата обращения: 12.07.2023: 22.37.
9. Искусственный интеллект в медицине. 03.04.2017г. // <https://22century.ru/popular-science-publications/artificial-intelligence-in-medicine>
10. Искусственный интеллект в медицине. Перспективы и риски. 14.05.2022//<https://ALLATRAVESTI.com/> ISkusstvennii – intellect -v- Medicine-PERSPEKTIVIJ-1-Riski /
11. Киселёва А.Ю. Применение искусственного интеллекта в здравоохранении: аспекты медицинского права // – М.: Национальный институт медицинского права. Медицинское право: теория и практика. 2020. №2(12). – С. 29-30.



БАПАНОВ

Талғат Абдирович

Алматы гуманитарлы-экономикалық университеті экономика,
қызмет көрсету және құқық кафедрасының аға оқытушысы, з.ғ.к.

КИБЕР АЛАЯҚТЫҚ: СИПАТТАМАСЫ ЖӘНЕ ӘДІСТЕРІ

XXI ғ. – бұл адамдардың, ұйымдардың, мемлекеттің барлық дерлік өмір салаларына енген және қамтылған ақпараттық технологиялар ғасыры. Шынында да, бүгін біз өз өмірімізді компьютерсіз, смартфонсыз және гаджеттердің басқа түрлерінсіз елестете алмаймыз. Қылмыстық, қылмыстық сала да ерекшелік болған жоқ, бұл компьютерлік және басқа да ақпараттық технологияларды өздерінің қылмыстық мақсаттары үшін жиі қолданатын алаяқтар. Алаяқтық схемалар үнемі өзгеріп отырады, өйткені адамдардың бір-бірімен қарым-қатынас жасау тәсілдері өзгереді. Алаяқтық айтарлықтай дамыды, ең маңызды екі фактор жаһандық коммуникацияның өсуі және технология мен деректерді пайдалану саласындағы үлкен жетістіктер болды.

Алаяқтық – бұл экономикалық салада жасалған қылмыстардың ең көп таралған түрі. Бұл қылмыс тек ұрлаудың ғана емес, жалпы қылмыстың да күрделі түрлерінің бірі болып табылады. Бұл күрделі қылмыстық құқықтық құрамда, қылмыстық әрекетті жүзеге асырудың жақсы ойластырылған жоспары мен жоспарында, сондай-ақ оны жасау тәсілдерінде көрінеді. Көбінесе бұл алаяқтықты ұрлықтың жеке түріне бөлуге мүмкіндік беретін әдістер. Алаяқтық тәсілдеріне алдауды қолдану, яғни ықтимал жәбірленушіні, жәбірленушіні оған жалған ақпарат беру арқылы нақты оқиғаға қатысты адастыруды енгізу, сондай-ақ жәбірленушіге, яғни алданған жәбірленушіге мүлікті немесе оған құқықты өз еркімен берумен сипатталатын сенімді теріс пайдалану жатады. соңғысының ниеттерінің заңдылығы мен заңдылығына сенімді бола отырып, алаяққа. Демек, алаяқтардың қызметінің айрықша ерекшелігі-олардың тарапынан жәбірленушіге қарсы қорқыту, зорлық-зомбылық, қару-жарақ қолданбауы, қылмыстық ниет тек алдау немесе сенімге қиянат жасау арқылы жүзеге асырылады. Осыған сүйене отырып, қылмыстың бұл түрін, дәлірек айтқанда, алаяқтардың бұл түрін адамгершілік сияқты белгі арқылы сипаттауға болады, өйткені алаяқтар қылмысты жәбірленушіге қатысты зорлық-зомбылықты, психикалық әсерді және басқа да қатыгез әдістерді қолданбай, өздерінің тапқырлығы, айлакерлігі және жақсы қастандығы арқылы ғана жасайды.

Айта кету керек, соңғы кездері Интернет желісін пайдалану арқылы киберкеңістікте жасалған қылмыс түрі айтарлықтай өсті. Бұл желі, бір жағынан, шексіз көлемде әртүрлі қажетті ақпаратты алу және оны бөлісу құралы, екінші жағынан, алаяқтардың құрбаны болу қаупін тудырады, өйткені бұл жағдайда соңғысын есептеу іс жүзінде мүмкін емес міндетке айналады. Ақпараттық технологияларды қолдана отырып алаяқтық жасау тәсілдеріне тоқталайық.

Қазіргі әлемде цифрландыру процесі жүріп жатыр, экономиканың өзгеруіне әкелетін технологиялық прогресс қарқын алуда. Бұл өзгерістер әртүрлі өнімдердің ақпараттық көлемінің ұлғаюына, электронды тасымалдаушылар алатын алаңның аздығына, шаруашылық байланыстардың виртуалды сипатына, Интернет желісі арқылы тауарлар мен қызметтердің

қозғалысына, цифрлық валюталардың пайда болуына және қолма-қол ақшасыз айналымға қатысты. Шынында да, қолма-қол ақшасыз есеп айырысу, банктік төлем карталары әр адамның күнделікті өміріне белсенді түрде енгізілуде.

Жоғарыда айтылғандай, ақпараттық технологиялардың дамуымен бірге алаяқтық әрекеттерді жасау тәсілдері де дамуда. Банк карталарының иелері көбінесе зиянкестердің құрбаны болады. Банк карталарын алаяқтықтың ең танымал түрлерін қарастырыңыз. Сонымен, кейбір ғалымдар алаяқтықтың осы түрлеріне скимминг, шимминг, фишинг, кардинг, Ливан циклі, иіскеу, әлеуметтік инженерия жатады. Басқа ғалымдар скимминг, фишинг, вишинг, трапинг сияқты алдау тәсілдерін бөліп көрсетеді. Тағы біреулері банктік карталарды пайдаланып алаяқтық жасау тәсілдеріне фишинг, фишинг, фишинг, фарминг, скимминг, трапинг, шимминг, иіскеу, Ливан циклі жатады.

Көріп отырғанымыздай, мұндай алаяқтық мүлдем басқа жолдармен болуы мүмкін, біз тек ең кең таралғанына қысқаша сипаттама береміз. Скимминг – банк карталарынан ақша алушабуылдаушыларға картадан оның иесінің жеке деректерін және шот нөмірін оқуға мүмкіндік беретін арнайы сканерлеу құрылғысын пайдалана отырып алаяқтық жасау тәсілі, ол болашақта жалған банк картасын жасау үшін пайдаланылатын болады. Трапинг – бұл скиммингтің бір түрі, онда банк картасындағы деректер оқылмайды, тек банк картасын банкоматта ұстауға мүмкіндік беретін құрылғы қолданылады. Бұл жағдайда алаяқтар ұрлықты карта иесі банкте пайда болған проблемамен айналысатын уақытта жүзеге асырады. Вишинг пен смишинг бір-біріне ұқсас және бұл жағдайда ұрлық жалған сайттар арқылы жүзеге асырылатындығында көрінеді, екінші жағдайда мұндай жалған сайтқа сілтеме SMS арқылы жіберіледі. Вишинг – телефон қоңырауларын қолданатын алаяқтық, оның барысында жәбірленушіге қолда бар ақшаны есептен шығару мақсатында картаны бұзу әрекеті туралы хабарланады. Осыдан кейін алаяқтар белгілі бір, алдын-ала дайындалған, белгіленген нөмірге қоңырау шалуды сұрайды, содан кейін қоңырау шалу арқылы, мысалы, картадан пароль туралы хабарлау қажет болады. Ливан циклі – алаяқтық түрі, онда алаяқ банкоматта картаны ұстайтын арнайы құрылғыны алдын ала салып, жәбірленушінің артында кезекке тұрады. Карточка иесі ПИН-кодты енгізіп жатқанда, алаяқ артта тұрып, оны есіне алады. Потенциалды жәбірленуші қажетті операцияны жүзеге асыра алмай, картаны шығарып алғаннан кейін, ол көмек алу үшін банкке жүгінеді. Осы уақытта алаяқ осы сәтті пайдаланып, банк картасын шығарып, одан қажетті соманы алып тастайды. Снифферинг – бұл, әдетте, қорғалмаған wi-Fi желілері арқылы адам көп жиналатын жерлерде жеке деректерді ұстап қалудан көрінетін алаяқтық әдісі. Мұндай адамдар көп жиналатын орындар ретінде алаяқтар вокзалдарды, кафелерді және басқа орындарды таңдайды. Көріп отырғанымыздай, банктік карталарды пайдалану арқылы алаяқтықтың көптеген әдістері бар, өйткені алаяқтар технологиялық прогреске оңай және тез бейімделіп, ұрлықтың жаңа және жаңа түрлерін ойлап табады.

Іс жүзінде Интернет желісінде жасалған алаяқтық бірдей қызығушылық тудырады. Айқын артықшылықтардан басқа, осы дүниежүзілік желінің дамуы жаһандық қауіп-қатерлерге, соның ішінде мемлекеттің экономикалық қауіпсіздігіне нұқсан келтіреді. Сонымен, қажетті ақпаратқа жедел қол жетімділік, кедергісіз қашықтықтан байланыс, әртүрлі ақша аударымдарын онлайн режимінде жүзеге асыру мүмкіндігі және тауарлар мен қызметтерге ақы төлеу Интернет желісінің сөзсіз артықшылықтары болып табылады. Бірақ жаһандық желінің дамуымен бірге ХХІ ғасырдың экономикалық қауіптерінің бірі болып табылатын кибер алаяқтық қарқынды дамып келеді. аталған фишингтен басқа, киберкеңістікте алдау мен алаяқтық жасаудың басқа жолдары бар, мысалы, жалған Интернет-дүкендердің болуы, қара инфобизнес, казино және заңсыз букмекерлер, кликфрод.

Жалған Интернет – дүкендердің ерекшелігі, олар әдетте жүз пайыз алдынала төлеммен жұмыс істейді. Тауарды толығымен төлеп, ақша аударымын жасай отырып, жәбірленуші күтілетін тауарды ала алмайтынын болжау қиын емес. Алаяқтықтың бұл түрі тек тауарларды сатуға ғана емес, сонымен қатар әртүрлі қызметтерді ұсынуға да қатысты болуы мүмкін – жоқ қызметтерді қашықтан ұсыну (бақылау, басқа жазбаша жұмыстар жазу, жобаларды жасауға көмектесу, сәуегейлік, бүлінуді жою және т.б.). Кейіннен сайт иесі оны бұғаттайды немесе

домен атауын өзгертеді. Қара бизнес жәбірленушіге эксклюзивті және сирек кездесетін, бірақ іс жүзінде әртүрлі сайттарда ашық түрде қамтылған ақпаратты әр түрлі формада (кітаптар, фотосуреттер, бейне файлдар) сатумен сипатталады. Кликфрод сонымен қатар Интернеттегі алаяқтықтың бір түрі болып табылады. Қажетті ақпаратты іздеу кезінде пайдаланушы кездейсоқ немесе қызығушылық нәтижесінде қалқымалы жарнамалық терезені нұқып, содан кейін зиянды сайтқа түседі. Мұндай сайттан шығу және оны жабу үшін шабуылдаушы белгілі бір ақша сомасын аударуды сұрайды.

Сондай-ақ, қазіргі уақытта Интернет желісінде жалған қайырымдылық сияқты алаяқтықтың бұл түрі кең таралған. Бұл алаяқтықтың мәні мынада: шабуылдаушылар фотосуреттер мен ақпаратты қолдана отырып, мысалы, көмекке мұқтаж балалар, аштыққа ұшыраған жануарлар, қайырымдылық қорларының ресми сайттарынан көмек сұрап, спам түрінде жиі көмек сұрап айқайлаған хабарландырулар жібереді. Әрине, мұндай жолмен алынған ақша ешқандай көмекке бағытталмайды. Мұндай жағдайларда пайдаланушылар қайырымдылық қорлары ешқашан спам түрінде немесе күмәнді сайттарда жарнамаларды ілу түрінде маңызды ақпаратты таратпайтынын есте ұстауы керек. Сонымен қатар, мұндай қылмыскерлер үшін ең қауіпсіз алаяқтықтың жеке түрі бар. Алаяқтар үшін қауіпсіздік пен қолайлылық-алдауды, алаяқтық фактісін ашу нәтижесінде мұндай жәбірленуші кінәлілерді жазалау үшін ешқашан құқық қорғау органдарынан көмек сұрамайды. Алаяқтықтың бұл түріне заңсыз есірткі, қару-жарақ жеткізу туралы ұсыныстар, тіпті тапсырыс бойынша кісі өлтіру сияқты қызмет көрсету туралы ұсыныстар кіреді.

Қорытындылай келе, банк карталарының иелері мен Интернет желісін пайдаланушылар банкоматты адамдар көп жиналатын жерлерде, ұялы байланыста, күмәнді интернет – дүкендердегі Қызметтерді пайдаланған кезде абай болу керек, бейтаныс сайттарға сақтық танытуы керек. Халық үшін жаппай қолма-қол ақшасыз төлемдерге ауыртпалықсыз көшуге қаржылық сауаттылықтың жаппай артуы ықпал ететін болады, сонымен қатар бұл жосықсыз онлайн-ойыншыларды жоюға көмектеседі. Қорытындылай келе, ХХІ ғасырда екенін атап өткім келеді. алаяқтық бір орында тұрмайды, бірақ техникалық прогресті дамыта отырып, уақытпен қатар жүреді. Ақпараттық технологиялардың жаңа нысандары мен құралдарын жетілдіру және пайда болу барысында алаяқтықтың, бөтеннің мүлкін ұрлаудың барлық жаңа әдістері мен тәсілдері ойлап табылуда. Осылайша, ақпараттық технологиялар ғылым мен техниканың әртүрлі салаларында жаңа ақпаратты іздеу және адамның дамуы жолдарын ғана емес, сонымен бірге қылмыстың, әсіресе алаяқтықтың жаңа және өнертапқыштық түрлерін жасау құралы болып табылады. Демек, мұндай қылмыс түрлерімен күресу әдістері олардың даму деңгейіне сәйкес келуі керек, тіпті әлдеқайда кәсіби болуы керек.

Әдебиет

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. к.ю.н., – 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.



АКИМЖАНОВ

Талгат Курманович

директор научно-исследовательского института права университета «Туран»,
научный сотрудник НИЦ Алматинской Академии МВД
Республики Казахстан им. М. Есбулатова, д.ю.н., профессор

**КИБЕРПРЕСТУПНОСТЬ – КАК ИСТОЧНИК УГРОЗЫ
НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН**

Как известно, проблема противодействия преступности тесно связана, как правило, с неготовностью правоохранительных органов к своевременному реагированию на происходящие изменения в качественных и количественных изменениях данного социального негативного явления.

А криминальный мир напротив, успешно развивается совершенствуется, приобретая все новые формы деятельности недоступные и порой не совсем доступные правоохранительным органам, одним из которых является киберпреступность.

По мнению известных ученых криминологов в современном обществе наблюдается серьезное противоборство между преступностью и государством [1, с. 26].

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.

И, как указывают ведущие ученые, что в борьбе с преступностью, необходимо преодолеть отставание правоохранительной системы в сфере использования технических средств информации, связи и транспорта. Но главное-это пересмотр общей стратегии борьбы. [1, с. 26]

По мнению ученых, современный период развития можно охарактеризовать как переход от постиндустриального общества к обществу информационному. Его невозможно сегодня представить без интенсивных информационных обменов и развивающихся информационных систем. Информационные потоки постепенно становятся рычагами управления общественными процессами [2, с. 13].

Однако, указанный процесс цифровизации, коснулся не только современного общества, но и его вечного спутника, то есть самой преступности, которая является порождением этого общества и его неотъемлемой частью, о чем достаточно убедительно изложено в последних работах известного российского ученого криминолога Овчинского В.С. [3; 4; 5; 6.]

Являясь одним из новых и наиболее опасных видов современной преступности киберпреступность постепенно стала захватывать все новые пространства в нашем обществе, угрожая не только правам и законным интересам граждан, общественных и государственных органов, но и посягая на информационную безопасность, являющейся самостоятельной частью национальной безопасности страны и представляющей согласно ст.4 Закона РК от 6 января 2012 года №527-IV «О национальной безопасности Республики Казахстан» как состояние защищенности информационного пространства Республики Казахстан, а также прав и законных интересов человека и гражданина, общества и государства в информационной сфере реальных и потенци-

альных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны [7, с. 54].

В последние годы Республика Казахстан столкнулась с новым видом преступлений совершенные в сфере высоких технологий, так называемыми мошенничествами с использованием информационной системы, то есть киберпреступлениями.

Масштабы киберпреступности растут не только в Казахстане, но и по всемирно во всем мире.

Основными объектами преступного посягательства становятся граждане, государственные органы, банковские организации, крупные промышленные предприятия. Ежегодно численность кибер атак на информационные сети стремительно растет.

Особенно рост киберпреступности по данным Комитета по правовой статистике и специальным учетам Генеральной Прокуратуры РК имел место на 25 процентов в Республике Казахстан в период пандемии (2019-2020 годы), в то время, когда наблюдался спад общей преступности на 20-25 процентов, так как было дано указание всем жителям страны ограничить передвижение и находиться по месту жительства.

Приведем статистику мошенничества по годам за последние 7 лет. Так, по данным Комитета по правовой статистике и специальным учетам Генеральной Прокуратуры РК мошенничество в 2017 году мошенничество составило 27 487, в 2018 году – 29282 уголовных правонарушений, в 2019 году 32286 фактов мошенничества, в 2020 году – 33853 факта мошенничества, в 2021 году – 41083 факта мошенничества, в 2022 году-43499 факта мошенничества, в 2023 году – 44786 фактов мошенничества. Как видим имеет место устойчивая тенденция роста мошенничества за последние годы.

Киберпреступность – это сложное понятие, охватывающее множество незаконных действий, направленных на Информационно-коммуникационные технологии (ИКТ) и (или) использующих ИКТ при совершении преступления.

Киберпреступность имеет наступательную тенденцию. По мнению ученых В.С. Овчинского и Ю.Н. Жданова отличительная черта нашего времени – это окончательное стирание границ и различий между реальностью и виртуальностью, между миром вещей и миром информации, между деятельностью онлайн и офлайн, между социальной средой и киберсредой. Уже в ближайшие годы подавляющее большинство экономически мощных государств и значительная часть развивающихся стран полностью перейдут в цифровой мир. Вся полиция, по сути, будет киберполицией.[4, с. 16]

Выделяют две особенности киберпреступности: а) характеризуется высокой латентностью (практически невидима); б) системно связана со всеми другими видами преступлений и направлена против всех объектов уголовно-правовой защиты.

Киберпреступление – это противоправная деятельность лиц, которые взламывают безопасность информационной либо сетевой системы и в дальнейшем используют ее в своих преступных целях. Взломщиков такой системы называют – хакерами.

Виды киберпреступлений:

- 1) Киберпреступления против прав и свобод человека и гражданина, прав и законных интересов юридических лиц;
- 2) Киберпреступления в сфере экономики и банковской деятельности
- 3) Киберпреступления против общественной безопасности.
- 4) Киберпреступления против государства.

Киберпреступность по своей природе это не только самостоятельный вид преступности, но и реальная угроза национальной безопасности Республики Казахстан.

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.

Неслучайно, в ст. 4 Закона Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 28 де-

кабря 2018 года) к одному из видов национальной безопасности наряду 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 [7, 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 [2, 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 [8, 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 [7, 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, определяемое функционирование [9, 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» [10, 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» [11, с. 66].

Митрохин В.И., считает, что безопасность есть мера защищенности среды жизнебытия, чести, достоинства, ценностей личности, социальных групп, государства, общества, цивилизации в целом [12, с. 22.].

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 [9, с. 19 ; 13, с. 10].

В ст. 6 Закона Республики Казахстан «О национальной безопасности Республики Казахстан» закреплён 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 [7, с. 54].

Как нам представляется борьба с киберпреступностью 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 [14, 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, друзь-

ями, родственниками и другими людьми, люди становятся психологически интернет-зависимыми [8, с. 383].

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

Об этом описано в работе известного российского ученого криминолога В.С.Овчинского «Криминология цифрового мира» [3.], по мнению которого 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 [3, с. 22]. В.С. Овчинский достаточно точно изложил и аргументировал всю процедуру и механизм цифровизации криминального мира в современных условиях всеобщей цифровизации.

Казахстанский законодатель при разработке нового УК РК 2014 года предусмотрел новую главу 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК [15, с. 122-127], 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).[16, с. 302].

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 новой Концепции правовой политики Республики Казахстан на период с 2021 по 2030 годы, разработка которой ведется в настоящее время.

Литература

1. Кудрявцев В.Н. Стратегии борьбы с преступностью. – М.: Юристъ, 2003. – С. 352 .
2. Информационное право: учебник для бакалавров / отв. Ред. И.М. Рассолов. – Москва: Проспект, 2016. – С. 352.
3. Овчинский В.С. Криминология цифрового мира : учебник для магистратуры / В.С. Овчинский. – М.: Норма: ИНФРАМ, 2018. – С. 352.
4. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. – М.: Международные отношения, 2020. – С. 288.
5. 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.
6. Ларина Е.С. Овчинский В.С. Технологии, меняющие мир. Преимущества и риски цифровой революции. – М.: Книжный мир, 2022. – С. 616.
7. Правоохранительные органы: Сборник законодательных актов. – Алматы: ЮРИСТ, 2019. – С. 256 .
8. 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 .
9. Степашин С.В. Безопасность человека и общества (политико-правовые вопросы): Монография. СПб.: СПб ЮИ МВД России, 1994, – С. 23-28.
10. Казаков НД. Безопасность и синергетика (опыт философского осмысления)//Безопасность. Информационный сборник Фонда национальной и международной безопасности. 1994. №4, – С. 62-67.
11. Лесков МА. Гомеостатические процессы и теория безопасности // Безопасность. Информационный сборник. 1994. №4(20), – С. 66-72.
12. Митрохин В.И. Концептуальные основы стратегии национальной безопасности России // Социально-политический журнал. 1995. №6, – С. 22-40.
13. Комиссаров В.С. Преступления, нарушающие общие правила безопасности (понятия, система, общая характеристика): Автореферат. дис. ...д-ра юрид. наук. – М. МГУ. 1997. – С. 52
14. Конституция Республики Казахстан. Практическое пособие. – Алматы: ТОО «Издательство «Норма-К», 2024. – С. 48.
15. Уголовный кодекс Республики Казахстан: Практическое пособие.- Алматы: «Издательство «Норма-К», 2024. – С. 280.
16. Уголовное право Республики Казахстан: Особенная часть в 2-т.: Учебник для вузов. Отв. Ред. И.И. Рогов, К.Ж. Балтабаев, А.И. Коробеев. – Алматы: Жеті Жарғы, 2016. – С. 500.



ШАЯХМЕТОВА

Жанна Бекполовна

профессор кафедры уголовно-правовых дисциплин
Атырауского университета им. Х. Досмухамедова к.ю.н.

РАЗРАБОТКА ЭФФЕКТИВНЫХ ТЕХНОЛОГИИ В ПРЕДУПРЕЖДЕНИИ КИБЕРПРЕСТУПНОСТИ

В рамках нашей страны границы социальной инженерии набирают значение в связи с постоянной динамикой киберландшафта и цифровых технологий, повышения осведомленности общества о кибербезопасности, обновление методов кибератак.

Можно предположить, что для дальнейшего прогноза данного тренда осведомленность населения является важнейшим критерием в рамках мер по обеспечению кибербезопасности РК. Создание в этом направлении профилактических мероприятий разъяснительная работа с гражданами станут эффективным инструментом в соблюдении цифровой гигиены и сохранности персональных данных в период 2024-2026г.

Необходима возможность обсуждения актуальных тем, таких как новые угрозы, методы атак, инструменты и технологии, что поможет быть в курсе последних трендов в области кибербезопасности, в том числе таких, как отсутствие фиксированной цены у интернет-ресурса или критериев по оценке цифровых рисков [1].

Следует отметить, что основной вызов заключается не только в защите от кибератак, но и в разработке эффективных стратегий предотвращения и реагирования на них.

Это требует сбалансированного подхода, включая усиление технических мер безопасности, разработку международных норм и соглашений в области кибербезопасности, а также повышения осведомленности и обучения в области кибергигиены для пользователей.

Несмотря на стремительный прогресс в области биотехнологий, люди часто испытывают чувство неловкости, однако точное определение интеллектуальных или этических проблем, которые они вызывают, может оказаться непростой задачей. Это понятие равных прав коренится в убеждении, что все мы разделяем фундаментальную человеческую сущность, которая превосходит видимые различия, такие как цвет кожи, физическая привлекательность и даже интеллект. Если мы вступаем на путь возвышения себя до высшего состояния, это поднимает вопросы о правах, которые могут отстаивать эти усовершенствованные существа, и о том, как эти права будут соотноситься с правами индивидуумов, которые остаются неизменными. Потенциальные технологические возможности для самоизменения человека остаются неопределенными, что подчеркивает важность скромного подхода к пониманию нашей вражденной человеческой природы [2].

Крайне важно, чтобы мы ориентировались в новом технологическом мире с тщательным вниманием и приверженностью защите основных прав человека.

В условиях цифровизации общества преступления, предметом которых выступают личные данные, особенно актуальны для изучения. Однако теоретическая разработанность темы находится лишь на начальной стадии, а сам термин «identity theft» появился сравнительно недавно.

О недостаточной теоретической разработанности темы, в частности, свидетельствует отсутствие корректного разграничения, таких категории англосаксонской правовой системы, как «использование идентификационных данных» («identitytheft») и «мошенничество использованием личных данных» («identitytraud»).

В научных исследованиях отмечается непоследственность использования данных терминов на международном и национальном уровнях. Анализ доктринальных источников и нормативных правовых актов показал, что рассматриваемые категории нередко используется в качестве синонимов.

В отечественной правовой доктрине феномен использования идентификационных данных лица («identitytheft») именуется «Кражей личности», «хищением» личных данных или «кражей идентичности», что также не совсем корректно [3].

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 правила, не лишает потерпевшего возможности их использования. Соответственно, личность не может быть «украдено».

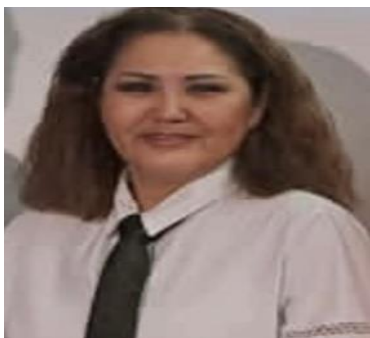
Существует еще один недостаток обозначения термином «кража» не правомерного завладения личными данным. Так, в случаях кражи в традиционном понимании собственник имущества выступает единственным потерпевшим, однако зачастую помимо лицо, личная информация которого незаконно используется, нарушаются права и законные интересы третьих лиц, вступающих в правоотношения со злоумышленником, а также различных и 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 [4].

Л. Лопуки утверждает, что рассматриваемое преступление имеет как минимум двух потерпевших: физическое и юридическое лицо, вступающее в правовые отношение 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 преступление 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 рассматриваемое преступление деяние более конкретно называть «незаконным использованием идентификационных (личных) данных лица».

Литература

1. Журнал Заңгер 7(276) 2024
2. Fukuyama F. Transhumanism //Foreign policy. – 2004. – №.144. – С. 42-43.
3. Генкин А.С., Путинцева И.К., Хищение личных данных в США: масштабы проблемы, финансовые, правовые и репутационные риски // Страхование дело. 2016.№9. – С. 11
4. Богданова Д.А. О некоторых последствиях кражи идентичности // Новые информационные технологии в образовании и науки: Материалы X международнойнаучной – практической конференции. – С. 376



СЕРАЛИЕВА

Алия Мажитовна

Абай атындағы Қазақ ұлттық педагогикалық университеті, қауымдастырылған профессор (доцент), з.ғ.к.,



БАЙМАГАМБЕТОВА

Зульфия Мажитовна

Әл-Фараби атындағы Қазақ ұлттық университетінің аға оқытушысы, философия докторы (PhD)



КАЗИЕВА

Асель Негметовна

Абай атындағы Қазақ ұлттық педагогикалық университетінің аға оқытушы, э.ғ.к.

ШЕТ ЕЛДЕРДІҢ МАТЕРИАЛДАРЫ БОЙЫНША ЧИПТЕУ МӘСЕЛЕЛЕРІ

Цифрлық технологиялардың (қашықтықтан сауда жасау; мемлекеттік қызметтер көрсету; мультимедиялық сүйемелдеу; банктік, сақтандыру, күзет, білім беру, пошталық, фискалдық және басқа да көптеген сервистер) көмегімен халыққа қызмет көрсетудің басым жолдарының спектрі күн сайын кеңеюде. Цифрландыру құралдарының бірі криптографиялық ақпаратты (деректерді) тасымалдайтын арнайы чиптерді материалдық объектілер құрылымына біріктіру болып табылады [1, 238 б.].

Осыған байланысты кейбір елдерде азаматтардың қауіпсіздігін арттыруға және мемлекеттік қызметтерді тиімдірек көрсетуге бағытталған халықты чиптеу мәселесі белсенді түрде талқылануда. Этимологиялық тұрғыдан «чип (ағылш. chip – жұқа пластина) есептеу жүйелерін жобалау үшін қолданылатын микросхема немесе кристаллға жағылған электронды модуль» [2, 751 бет]. «Чиптеу» деп адамның терісінің астына ақпараттық коды бар арнайы электронды мини-құрылғыны имплантациялау процесі түсініледі. Ондағы ақпарат дәл осы мақсат үшін жасалған арнайы сканерлер арқылы оқуға арналған. Мұндай имплантация медициналық операция болып табылмайды және іс жүзінде пирсингпен салыстыруға болады. Бірақ қазіргі уақытта адам мұны тек өзі немесе онымен айналысатын таныстарының көмегімен жасай алады [3, 22-бет].

Чиптеудің мәні Еуропалық Одақтың 2005 жылдың наурыз айында қабылданған құжатында айқын көрсетілген (Еуропалық топтың ғылымдағы этика және жаңа технологиялар бойынша №20 қорытындысы, 5-ші бөлім): «Қазіргі қоғам адамзатқа әсер етуі керек өзгерістермен бетпе-бет келді. Міне, прогрестің келесі кезеңі – бейнебақылау мен биометрияны, сондай-ақ адам ағзасына енгізілген әртүрлі электронды құрылғылар, тері астындағы чиптер

мен смарт тегтер арқылы бақылаудың нәтижесінде адам тұлғасының өзгеретіні соншалық, олар барған сайын желілік тұлғаларға айналып келеді. Олар үнемі қадағаланатын және бағаланатын қозғалысқа, әдеттер мен байланыстарға мүмкіндік беретін сигналдарды мезгіл-мезгіл қабылдап, жібере алуы керек. Бұл адам автономиясының мәні мен мазмұнын өзгертуі керек. Бұл жағдайда адамның қадір-қасиеті туралы түсінік өзгереді. Дене өзгерген сайын онымен бірге болатын іргелі, табиғи жеке құқықтардың кейбір бұзылуы оның қадір-қасиетін, сондай-ақ конституциялық құқықтары мен бостандықтарын төмендетпейді» [4].

Н.С. Бегалиевтің пікірінше, халықты чиптеу мәселесі көп қырлы мәселе болып табылады, соның салдарынан келесілерді бөліп көрсету қажет:

- азаматтардың конституциялық құқықтарын, бостандықтары мен мүдделерін қорғау;
- канондық (діни) нормалар мен көзқарастар;
- жазасын өтеп жатқан адамдарды қамауда ұстаудың пенитенциарлық құралы;
- техникалық сүйемелдеу;
- медициналық қамтамасыз ету;
- құқық бұзушылықтардың криминологиялық профилактикасы және криминалистикалық сәйкестендіру. [1, 239-240 б.].

Х.А. Алекперов қылмысты қашықтықтан бақылау жүйесін (ҚҚБ) «... адам ағзасына имплантацияланған жаһандық позициялау микрочипіне (GPS) негізделетін бағдарлама» құруды ұсынады, [5, б. 28].

М.Р. Мұқановтың пікірінше мұның бәрі сәйкестендірудің осы әдісін қолданудың ерекшеліктеріне негізделген.

1) Әмбебаптық.

Қазіргі уақытта чиптеу адамдарға, әртүрлі жануарларға, жүндерге және ағаштарға сыналған. Сонымен қатар, чиптеуді қолдану мүмкін емес объектілер жоқ, өйткені нақты жағдайларға байланысты қолданылатын чиптер мен сканерлеу құрылғыларының технологияларының айтарлықтай әртүрлілігі бар. Бірегейлігі чиптегі ақпарат іс жүзінде кез-келген болуы мүмкін және тапсырмаға байланысты өзгеруі мүмкін. Мұндай ақпаратты белгілі бір объектінің сәйкестендіру мәселелерін шешу үшін криминалистиканың нақты қажеттіліктерін ескере отырып, чипке енгізуге болады.

2) Ең төменгі қаржылық шығындар.

Чиптерді жасаудың өзі, контрафактіліктен қорғаудың жоғары деңгейін сақтай отырып, салыстырмалы түрде төмен бағаға ие. Қажет болған жағдайда тізілімді жүргізу және қажетті объектілер туралы қолда бар мәліметтерді құрылымдау мақсатында бағдарламалық қамтамасыз етуді пайдалану да елеулі шығындарды талап етпейді. Шығындардың негізгі бөлігі құқық қорғау органдары қызметкерлерінің қажеттіліктері үшін қажетті мөлшерде сканерлеу құрылғыларын сатып алумен байланысты.

3) Нақты уақыт режимінде орналасу мүмкіндігі.

Көптеген жағдайларда қолданылатын чиптеу технологиясы бірнеше ондаған метрден аспайтын минималды қателікпен ізделетін объектінің орнын анықтауға мүмкіндік береді. Бұл жағдайда чиптеу технологиясы объектінің орналасқан жерін GPS және ГЛОНАС жүйелерін чиптің өзіне сәйкес параметрлерді орнату арқылы орнатады. Осылайша, құқық қорғау органдарының қызметкерлеріне объектілердің қозғалысын нақты уақыт режимінде, тіпті олардың орналасқан жерінен жүздеген немесе мыңдаған шақырым қашықтықта бақылау мүмкіндігі беріледі.

4) Чиптің қолайсыз факторларға салыстырмалы тұрақтылығы.

Ауа-райы жағдайлары немесе ұзақ қашықтыққа тасымалдау чиптің жұмыс мүмкіндіктеріне ешқандай әсер етпейді. Сонымен қатар, микросхема тірі ағзаға еніп, уақыт өте келе тері астына ауысқан жағдайда да (көбінесе 5 см-ден аспайды), биологиялық объект мұндай таңбалауды қолдану тиімділігінің нашарлауына жол бермейді. Әдетте, бір чип организмнің өзі үшін толық қауіпсіздікте және ыңғайсыздық сезімі болмаған кезде биологиялық объектінің бүкіл өмір сүру кезеңіне жеткілікті [6, 112-113 б.].

Қазақстанда халықты чиптеуге қатысты түпкілікті шешімдер әлі де талқылану сатысында және тәуекелдер мен артықшылықтарды талдау қоғамның пікірін қалыптастыруда және осы технологияны енгізу туралы шешім қабылдауда маңызды рөл атқарады.

Чиптеу мәселелері бойынша шет елдерге салыстырмалы талдау жүргізейік.

Америка Құрама Штаттарында адамдарды чиптеу процесі негізінен медициналық сәйкестендіру және пациенттердің медициналық ақпаратын басқару сияқты медициналық мақсаттарда қолданылады. 2030 жылы нарық көлемі орта есеппен 6,3%-ға 138,8 млрд АҚШ долларына өседі деп болжануда [7].

Кейбір компаниялар өз қызметкерлеріне ғимараттар мен компьютерлік жүйеге оңай қол жеткізу үшін чип орнату мүмкіндігін ұсынады. Осындай компаниялардың бірі – «Three Square Market», ол 2017 жылы өз қызметкерлеріне үй-жайлар мен техникалық ресурстарға қол жеткізу үшін ерікті чиптеуді ұсынды [8].

Алайда, чиптерді жеке мақсатта қолдану әлі де бейресми және деректер қауіпсіздігі мәселелеріне байланысты халық арасында біршама қарсылық тудырады.

Швеция – адамдарды чиптеудегі алдыңғы қатарлы елдердің бірі. Көптеген шведтер дүкендерде төлеу, есіктерді ашу және электрондық жүйелерге қол жеткізу сияқты күнделікті жағдайларда пайдалану үшін өз еркімен чиптерді енгізу туралы шешім қабылдады. Бұл транзакция уақытын қысқартуға және чиптелген адамдар үшін өмір сүру деңгейін жақсартуға әкелді. Дегенмен, Швецияда бүкіл халықты кең және міндетті түрде чиптеуді енгізу заңды негізге ие емес және мемлекеттік саясат болып табылмайды. Швеция жеке бостандықтар мен деректердің құпиялылық ережелерін, сондай-ақ Еуропалық Одақтың халықаралық келісімдері мен заңнамасы шеңберіндегі міндеттемелерді ұстанады [9].

ҚХР-да халықты чиптеу процесі «Ақылды қала» жаһандық жобасы аясындағы тұлғалардың профильдеу жүйесімен тікелей байланысты, мұнда белгілі бір тұлғаның қозғалысы оның әлеуметтік белсенділігін талдау, индикативтік көрсеткіштерді есепке алу және қорытынды баллдарды жинақтау мақсатында таратушы құрылғылармен (порталдармен) тіркеледі. Кейіннен жиынтық ұпайлар жеке тұлғаны және оның елді мекен тұрғындарының иерархиялық жүйеде сәйкесінше орналасуын сипаттай алады [10].

Қазақстанда дербес деректерді қорғау және киберқауіпсіздік тетігін жетілдіру бойынша жұмыстар жүргізілуде. Құқықтық, ұйымдастырушылық, техникалық, әлеуетті дамыту және халықаралық ынтымақтастық шаралары пысықталуда. Ең алдымен, бұл технологияны енгізу процедураларын мұқият әзірлеу, чиптердің функционалдық сипаттамаларын нақты анықтау және оларда сақталған ақпаратты бақылау қажет. Сонымен қатар, чиптеу процесінде жеке деректердің қауіпсіздігін қамтамасыз ету тетіктеріне көп көңіл бөлінуі керек. Чиптерге рұқсатсыз қол жеткізу немесе деректерді сақтау жүйесіне зиянкестер заңсыз кірген жағдайда, жеке тұлғалар туралы ақпарат жалпыға қолжетімді болуы мүмкін деген қауіп бар. Болашақта адам біздің елімізде чиптің тасымалдаушысы бола алатындығын ескере отырып, халық арасында Цифрлық сауаттылық пен кибер сауаттылық деңгейін арттырудан бастау маңызды болып көрінеді [11, 12 б.].

2022 жылы Қытайдағы бет-әлпетті тану жүйесінен құпия ақпарат таратылып кетті. Бағдарламалық жасақтама жасаушылардың бірнеше ай бойы жіберген қателігіне байланысты миллиондаған Қытай азаматтарының құпия ақпараттары бар үлкен мәліметтер базасы (800 миллион жазбалар) көпшілікке қол жетімді болды. 2021 жылдың ортасында Apple Inc. және Meta Platforms Inc. компаниялары хакерлердің шабуылына ұшырады, олар құқық қорғау органдарының қызметкерлері ретінде көрініп, пайдаланушылардың жеке деректеріне нұқсан келтірді. 2022 жылдың қыркүйегінде ҰҚШҰ-ның ресми сайтына DDos шабуылы орын алып, нәтижесінде ресурстың қолжетімділігі бұзылып, белгілі бір ақпараттық хабарламаларды өзгертуге рұқсат етілмеген әрекеттер тіркелді. 24 сағат ұзақтығында сайт пайдаланушылар үшін қолжетімсіз болды. АҚШ-та 2022 жылдың 10 қазанында елдегі ең ірі 14 әуежай да қолжетімсіз болып шықты. Ресейлік хакерлерден құралған Killnet тобы бұл оқиға үшін жауапкершілікті өз мойнына алып, бұрын бұл нысандарды өз мақсаттары деп жариялаған. Болашақта адам елімізде чиптің тасымалдаушысы бола алатынын ескерсек, халық арасында цифрлық

сауаттылық пен киберсауаттылық деңгейін арттырудан бастау маңызды болып көрінеді. Цифрлық сауаттылықты арттыру жұмыстары «Цифрлық Қазақстан» бағдарламасы аясында да жүргізілді, бағдарламаның бір бағыты адами капиталды дамыту болды [12].

Халықты чиптеу жобасының оң қасиеттерін атап өтіп, Х.Д. Аликперов әлемде жыл сайын жүздеген мың адамдар із-түзсіз жоғалып кетеді, ал кейінірек анықталғандай, олардың көпшілігі қабырғаға сылап тасталған, көмілген, өртенген, суға батып кеткен" деп орынды көрсетті [5, 26-бет]. Біз халықты чиптеуді адам ұрлауға, киднепингке, кісі өлтіруге, еңбек құлдығына, адам денесінің мүшелерін алуға және т.б. қарсы профилактикалық құрал ретінде қарастыра отырып, осы көзқараспен толық бөлісеміз.

Осылайша, бұл мәселеде чиптеуді қолданудың халықаралық тәжірибесін зерттеу қажет деп санаймыз:

- хабар-ошарсыз жоғалған адамдарды іздестіру;
- тірі адамдар мен мәйіттерді сәйкестендіру;
- жеке тұлғаның орналасқан жерін анықтаумен байланысты жедел, тергеу және сот-сараптамалық міндеттерді шешу;
- адамдарды пенитенциарлық мекемелерде ұстауға қолайлы жағдайлар жасау;
- азаматтардың Қазақстан Республикасының мемлекеттік шекарасы арқылы өтуін бақылау;
- демографиялық жағдайды мониторингілеу бойынша міндеттерді шешу;
- арнайы контингентке техникалық қолдау көрсету («қиын жасөспірімдер», Альцгеймер синдромынан зардап шегетін адамдар).

Әдебиет

1. Бегалиев Н.Е. О Перспективности или нецелесообразности введения института чипирования населения //Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. №4. – С. 238-244.
2. Егорова Т.В. Қазіргі орыс тілінің шетел сөздерінің сөздігі. – М.: Аделант, 2014. – 800 б.
3. Семенова Л.В., Перминова В.А. Цифрлық экономика мен денсаулық сақтаудағы чиптеуді зерттеу// Sciences of Europe # 41, (2019). – Б.22-24. // [Электрондық ресурс]. – Қолжетімділік режимі: <file:///C:/Users/HP/Downloads/issledovanie-chipizatsii-v-tsifrovoy-ekonomike-i-zdravoohranenii.pdf> (өтініш берген күні: 12.08.2024).
4. Ғылымдағы және жаңа технологиялардағы этика бойынша Еуропалық топтың №20 қорытындысы [Электрондық ресурс]. Қолжетімділік режимі: http://www.kongord.ru/Index/A_tma_05/ethicsofchips.html (өтініш берген күні: 20.08.2024).
5. Аликперов Х.Д. Глобальный дистанционный контроль над преступностью: Допустимость, возможности, издержки //Криминология: вчера, сегодня, завтра. – №3 (42) 2016. – С. 26-33.
6. Муканов Р.С. Чипирование осужденных, состоящих на профилактическом учете, как склонных к совершению побега //Меры противодействия совершению некоторых видов правонарушений посредством чипирования отдельных категорий лиц: Материалы международной научно-практической конференции – г. Алматы: КазНПУ имени Абая, издательство ТОО «Лантар books», 2023. – С. 111-115.
7. «Global Medical Implantable Chips Market Size, Share & Trends Analysis Report by Application (Drug Delivery, Vital Sign Monitoring), by Region (North America, Europe, APAC, LATAM, MEA), and Segment Forecasts, 2021-2028» // [Электрондық ресурс]. – Қолжетімділік режимі: <https://www.linkedin.com/pulse/implantable-medical-devices-market-research-report-covering-patil> (күні өтініштер 22.08.2024).
8. «Прецедент: Three Square Market компаниясы АҚШ-та бірінші болып қызметкерлерге аутентификация чиптерін имплантациялайды» // Электрондық ресурс]. – Қолжетімділік режимі: <https://digital.report/pretsedent-kompaniya-three-square-market-pervoy-v-ssha-vzhivit-sotrudnikam-chipyi-dlya-autentifikatsii/> (қол жеткізілген күні 26.08.2024).

9. Джурова А.И., Сементелли А. (2023), «Кто-то наблюдает за мной: представление слежки как поведения, направленного на поиск ренты», Международный журнал социальной экономики, Vol. 50 №1. – С. 58-72.

10. Степушева Л.А. Еуропа тұрғындары чиптерді тері астына имплантациялай бастады // [Электрондық ресурс] – Қолжетімділік режимі: <https://www.pravda.ru/news/world/1403854/1403854-europetech/>. Жарияланды: 29.12.2018 (өтініш берген күні: 28.08.2024).

11. Абильдинова К.М., Олейник Ю.В., Аканова Г.К. Чипирование населения: оценка рисков и перспектив для кибербезопасности // Меры противодействия совершению некоторых видов правонарушений посредством чипирования отдельных категорий лиц: Материалы международной научно-практической конференции – г. Алматы: КазНПУ имени Абая, издательство ТОО «Лантар books», 2023. – С. 9-16.

12. Киберкеңістіктегі ахуалға шолу / Кибердайгест. – «ГТС» АҚ, 2022// [Электрондық ресурс] – Қолжетімділік режимі: URL: <https://sts.kz/wp-content/uploads/2023/01/dajdzhest-2023-god.pdf> (өтініш берген күні: 27.08.2024).



ТОГАЙБАЕВА

Шолпан Серикбаевна

профессор кафедры «Юриспруденция» Кокшетаусского университета
им. Абая Мырзахметова, к.ю.н.



ТОГАЙБАЕВ

Амир Ихсанович

старший преподаватель кафедры
«Юриспруденция» Кокшетаусского
университета им. Абая Мырзахметова, к.ю.н.



КАРАКУШЕВ

Салимгерей Имангалиевич

заведующий кафедры «Юриспруденция»
Кокшетаусского университета
им. Абая Мырзахметова, к.ю.н.

УЖЕСТОЧИТЬ НАКАЗАНИЕ ДРОППЕРАМ

Борьба с киберпреступностью – одна из важных составляющих в реализации Плана нации «100 шагов», предложенного Главой государства.

Из года в год число виртуальных правонарушений (хакерство, электронные хищения, осуществление преступных связей через электронную почту, перевод капиталов, добытых незаконным путем) растет, что побуждает органы МВД активно бороться с данным видом правонарушений.

В Генеральной прокуратуре с участием уполномоченных государственных органов (МЦРИАП, МВД, КНБ, АФМ, Нацбанк) и мобильных операторов обсуждены вопросы взаимодействия в сфере противодействия интернет-мошенничеству и преступлениям, совершаемым посредством сетей телекоммуникаций.

Между тем проблема с преступными атаками на мобильные приложения «WhatsApp» и «Telegram» всё ещё не устранена.

В этой связи АО «Казахтелеком» и крупнейшие сотовые операторы (АО «Кселл», ТОО «Мобайл Телеком-Сервис» (Теле2/Алтел), ТОО «Кар-Тел») выразили готовность к сотрудничеству и выработке необходимых технических решений для заслона киберпреступности.

Молодые люди и пенсионеры в поисках легкого заработка и доверия к рекламе целенаправленно либо без полного понимания негативных последствий вовлекаются в мошенничество. Ими оформляются банковские карты и счета для вывода или транзита похищенных денежных средств. Лицо, участвующее в такой схеме и оказывающее посреднические услуги в цепочке манипуляций с украденными деньгами, именуется «дроппером».

Надо сказать и о том, что старое поколение привыкло верить рекламе. Доверие признак старого поколения, воспитание того времени. Так и попадают на различные уловки мошенников.

Полиция Казахстана завалена заявлениями по обману по якобы инвестированию по гос. программе «Казмунайгаз».

Приведем пример.

В инстаграме в августе месяце 2024 года была реклама о том, что глава государства Казахстана - Касым-Жомарт Кемелевич Токаев говорит о совместной государственной программе, где необходимо внести инвестиции в эту программу. Это государственная программа гарантирует выплату за вложения.

Показывают видео с участием нашего главы государства. При этом сроки вложения ограничены. После рекламы появляется сайт внизу рекламы где необходимо нажать и выйдет анкета для заполнения. После заполнения заявления – анкеты Вам звонят на сотовый телефон и говорят о перспективах вложения инвестиций (денег) и о том, как будут идти начисления. После на вашем сотовом телефоне появляется приложение и можете видеть ваши вложения. Но самое интересное вы можете видеть кроме ваших вложений и еще 50 долларов. Когда вы спросите о том, что вы не добавляли 50 долларов, они скажут, что это от компании.

Но до этого они спрашивают сколько вы хотите вложить денег. Примерно 90 000 тенге. Они говорят вам номер сотового телефона куда вы должны скинуть и имя на кого вы скидываете. (Например, Иванов Константин). Вы сбрасываете им. Затем они говорят с вами свяжется менеджер их компании.

Он вам позвонит. Будет говорить, что он будет вам помогать с трудностями. Будет вам говорить о том, куда направлены деньги и сколько вы будете иметь прибыли.

На следующий день вы идете и в банке спрашиваете была ли такая компания – акция по гос. программе. Вам отвечают нет. И банк дает вам сайт «Казмунайгаза» и звоните. Этой акции нет. Соответственно вы понимаете что Вас обманули. Вы идете в полицию писать заявление.

Когда вы приходите в банк «Каспий» и просите не переводить перечисленные деньги и предъявляете им перевод через Каспий, они говорят не имеем права напишите заявление в полицию и они дадут запрос. Выяснилось, что деньги могут переводиться в течении трех дней. Этот менеджер периодически звонит Вам. Полиция рекомендует не брать трубку.

Ответственность за умышленное соучастие в мошеннических действиях наступает по статьям 28 и 190 Уголовного кодекса и предусматривает до 10 лет лишения свободы.

Что касается материальной ответственности, то уже есть факты взыскания с дропперов полной суммы обналиченных ими средств путем признания денежной массы неосновательным обогащением (статья 953 ГК РК)».

Так, постановлением судебной коллегии по гражданским делам Верховного Суда Республики Казахстан удовлетворен иск гр.Т. о взыскании с «дропперов» свыше 20 млн тенге.

Судом установлено, что гр.Т., введенная в заблуждение мошенниками, перечислила вышеуказанную сумму на счета и карты четырех казахстанцев. Последние, в свою очередь, не в полной мере осознавая преступность происхождения поступивших денег, по ранее достигнутой договоренности перевели их неустановленным лицам. Учитывая, что «дропперы» не приняли мер для выяснения оснований поступления денег и перечислили их иным лицам, суд расценил эти действия как распоряжение ими по своему усмотрению, а потому обязал вернуть полученное неосновательное вознаграждение [1].

Наиболее часто мошенниками используется схема незаконного завладения денежными средствами граждан путем понуждения их к оформлению онлайн займов на различных мобильных платформах, в т.ч. банков, и последующего перевода полученных заемных средств на счета других граждан – дропперов.

Анализ проведен путем изучения судебных актов, размещенных на сервисе «Судебная практика», и, по ориентировочным данным, в 2023 году рассмотрено более 200 дел анализируемой категории.

Проведенный анализ показал, что от граждан, попавших в такие ситуации, в основном поступали две категории исковых требований:

- о взыскании суммы неосновательного обогащения;
- о признании договора банковского займа недействительным.

По первой категории исков в качестве ответчиков указывались непосредственно дропперы, т.е. физические лица, на чьи банковские счета истцами переводились заемные средства.

Наибольшее количество исков поступило в суды г.Алматы, Астаны, Восточно-Казахстанской, Костанайской областей.

Такие иски, в основном, удовлетворены.

Вместе с тем практика разрешения таких споров в судах первой и апелляционной инстанции противоречивая.

Принимая решения, большинство судов исходили из конкретных обстоятельств дела и, удовлетворяя иски, придерживались следующей практики.

При отсутствии определенных законом правовых оснований ответчики при поступлении в их распоряжение имущества в виде денег, принадлежащих другим гражданам, должны были принять соответствующие меры и выяснить правомочность своих действий по дальнейшему их использованию, в т.ч. на покупку иностранной валюты, криптовалюты и др.

С момента фактического распоряжения поступившими на счета денежными средствами ответчики несут ответственность за свои действия и их доводы о нахождении под влиянием обмана и заблуждения не должны принимались судами во внимание, пока приговором суда не будет подтверждено отсутствие в действиях ответчиков признаков уголовно-наказуемого деяния, в том числе соучастия, пособничества в мошеннических действиях.

Формальный факт последующего перечисления ответчиками денежных сумм третьим лицам не принимался в качестве основания для отказа в иске.

Ответчики должны были осознавать риски совершаемых собственных действий, понимать, что могут быть вовлечены в противозаконные схемы и знать, что несут либо будут нести ответственность, пока не докажут свою невиновность.

Суды указывали, если приговором суда будет установлена вина иных лиц и непричастность ответчиков к противоправным действиям, последние в регрессном порядке могут взыскать ущерб с виновных лиц.

При этом материалы досудебного расследования для суда гражданской юрисдикции юридической силы не имеют, что вытекает из нормы ч.3 ст.76 ГПК.

Основным мотивом отказа в удовлетворении исков суды указывали, что переводы на счета других лиц денежных средств, полученных по банковским договорам займа, осуществлялись истцами самостоятельно.

Требования неизвестных лиц о переводе сумм займов неоднократно траншами на разные банковские счета должны были вызвать сомнения, при должной осмотрительности и предосторожности сами истцы могли предотвратить незаконные действия злоумышленников.

Истцы, как и ответчики, а также все иные граждане, должны осознавать риски совершаемых собственных действий и понимать, что могут стать жертвами мошенничества.

Приведен пример на сайте Верховного суда РК.

Судебная коллегия по гражданским делам Верховного Суда рассмотрела кассационное ходатайство Истца о пересмотре судебных актов местных судов по гражданскому делу о взыскании суммы неосновательного обогащения.

Женщина обратилась в суд с иском к четырем ответчикам о взыскании суммы неосновательного обогащения, мотивируя тем, что она, действуя по указанию неизвестных лиц, оформила кредит, в дальнейшем продала по заниженной стоимости свою квартиру другому лицу и все полученные денежные средства перевела на карточные счета ответчиков.

Управлением полиции района возбуждено уголовное дело по факту мошенничества, постановлением от 20 сентября 2023 года женщина признана потерпевшей.

Местные суды в удовлетворении иска отказали, мотивируя тем, что в действиях неизвестных лиц усматриваются признаки мошенничества, соответственно, возмещение причиненного преступлением материального ущерба потерпевшему подлежит разрешению в рамках уголовного дела. Истец обжаловала судебные акты в кассационную коллегия.

Коллегией установлено, что до продажи квартиры истцу позвонил неизвестный, представившись сотрудником полиции, сообщил, что неизвестные лица пытаются завладеть ее квартирой.

В последующем, истец была переключена на другое лицо, представившееся специалистом НацБанка. По ее указанию, женщина подала заявки на получение заемных средств в банках второго уровня, которые в последующем перевела ответчикам.

Под влиянием указанных лиц, истец продала принадлежащую ей квартиру. Вырученные денежные средства направлены на расчетный счет одного из ответчиков.

Согласно статье 953 Гражданского кодекса лицо (приобретатель), которое без установленных законодательством или сделкой оснований приобрело или сберегло имущество (неосновательно обогатилось) за счет другого лица (потерпевшего), обязано возвратить последнему неосновательно приобретенное или сбереженное имущество, за исключением случаев, предусмотренных статьей 960 ГК.

Обязанность, установленная пунктом 1 настоящей статьи, возникает также, если основание, по которому приобретено или сбережено имущество, отпало впоследствии.

Правила настоящей главы применяются независимо от того, явилось ли неосновательное обогащение результатом поведения приобретателя имущества, самого потерпевшего или третьих либо следствием события.

Представленными доказательствами в виде квитанции банков второго уровня установлено, что истец перевела четырем ответчикам денежные средства в сумме свыше 19 млн тенге.

Коллегия пришла к выводу, что по делу имеется неосновательное обогащение ответчиков, так как установлен факт поступления на их карточные счета денежных сумм от истца, при этом ответчики не доказали законные основания для получения этих сумм.

Поскольку после поступления денег ответчики не приняли мер для выяснения оснований их поступления, то последующие их действия по перечислению денег иным лицам коллегия расценила как распоряжение ими по своему усмотрению [2].

Какие принимают меры полиция и суды по противодействию этим фактам.

Полиция рассылает в инстаграм ролики по недопущению мошенничества, в частности участковые полиции ведут работу с населением на участке. Следователи возбуждают уголовные дела.

Необходимо и другим органам вести активную работу. Закрывать сайты при ежедневном просмотре инстаграм незамедлительно.

Мы полагаем, что необходимо вести чаще телепередачи по данным фактам.

Мы полагаем ужесточить наказание недобросовестных получателей денег.

Литература

1. Дропперов В. Казахстане будут привлекать к уголовной ответственности. Роза Нургалиева. 5 мая 2024г. // <https://golos-naroda.kz/31785-dropperov-v-kazakhstane-budut-privlekat-k-ugolovnoi-otvetstvennosti-genprokuratura-1714866832/>

2. Верховный Суд: Дропперы должны возмещать вред от мошеннических действий. // <https://sud.gov.kz/rus/news/verhovnyy-sud-dropper-dolzhen-vozmeshchat-vred-ot-moshennicheskikh-deystviy>



СУЛТАНОВ

Салимжан Исаевич

Экономикалық-құқықтық технологиялар мен қызмет көрсету салалары мектебінің
қауымдастырылған профессоры Еуразиялық технологиялық университеті, з.ғ.к.

ҚЫЛМЫСТЫҚ ІСТЕРДІ АЛҚАБИЛЕРДІҢ ҚАТЫСУЫМЕН ҚАРАУДЫҢ ЕРЕКШЕЛІКТЕРІ

Қылмыстық істер бойынша алқабилердің қатысумен қараудың ерекшеліктеріне Қазақстан Республикасының Қылмыстық-процестік кодексінде (әрі қарай ҚР ҚПК) өз алдына жеке бір бөлім берілген ҚР ҚПК Ерекше бөлігінің 14-бөлімі «Істер бойынша алқабилердің қатысуымен іс жүргізу» деген атаумен белгіленіп, келесі тарауларды қамтиды:

- 1) жалпы ережелері (65-тарау);
- 2) сот отырысын тағайындау ерекшеліктері (66-тарау);
- 3) сот талқылауыны қатысу үшін алқабиге кандидаттарды іріктеу (67-тарау);
- 4) алқабилер қатысатын соттың істі талқылау ерекшеліктері (68-тарау);
- 5) алқабилердің қатысуымен қаралған істер бойынша заңды күшіне енген үкімдерді, қаулыларды қайта қарау жөніндегі іс жүргізу ерекшеліктері (69-тарау);
- 6) алқабилердің қатысуымен қаралған істер бойынша заңды күшіне енген үкімдерді, қаулыларды қайта қарау жөніндегі іс жүргізу ерекшеліктері (70-тарау) [1].

ҚР ҚПК 7-бабының 3-тармағына сәйкес, алқаби – соттың қылмыстық істі ҚР ҚПК белгіленген тәртіппен қарауына қатысуға шақырылған және ант қабылдаған Қазақстан Республикасының азаматы болып табылады.

«Алқабилер туралы» Қазақстан Республикасының 2006 жылғы 16 қаңтардағы N121 Заңының 1-бабы 1-тармағында алқабиге осыған ұқсас анықтама келтірілген, «алқаби – соттың қылмыстық істі заңда белгіленген тәртіппен қарауына қатысуға шақырылған және ант қабылдаған Қазақстан Республикасының азаматы» [2].

Сондай-ақ, аталмыш заңның көрсетілген бабының 2-тармағында «алқабиге кандидат» болатын тұлғаға анықтама берілген, алқабиге кандидат – бұл ҚР ҚПК сәйкес кейіннен алқабилерді іріктеу рәсіміне қатысу үшін алқабиге кандидаттардың бірыңғай тізіміне енгізілген Қазақстан Республикасының азаматы [2].

Қылмыстық істерді алқабилердің қатысуымен жүргізудің қазақстандық моделінің ерекшеліктеріне кейбір авторлар да назар аударады. Сот билігін жүзеге асырудағы әлемдік тәжірибеде, кейбір шет мемлекеттерде шешімді алқабилер кәсіби судьясыз өздері қабылдауы мүмкін немесе «шеффен» түрінде постановление приговора профессиональными судьями в единой коллегии с присяжными заседателями үкімнің қаулысын кәсіби судья алқабилердің алқасымен біріге отырып шығарады. Қазақстандық модель шет мемлекеттерде қолданылатын осы екі түрлі модельден де өзгешелігімен ерекшеленеді [4].

ҚР ҚПК 2-бөлімінде қылмыстық процеске қатысатын мемлекеттік органдар мен адамдар туралы, олардың құқықтары мен міндеттері, құзыреттері мен өкілеттіктері туралы айтылады. Бірақ, бұл бөлімде қылмыстық процеске қатысатын адам ретінде тартылатын алқаби мен алқабиге кандидат туралы көрсетілмеген. Аталмыш бөлімге тиесілі 10-тарауда қылмыстық процеске қатысатын өзге де адамдар ретінде сот отырысының хатшысын, аудармашыны, куәні, куәгерді, сарапшыны, маманды, сот приставын, медиаторды қарастырады.

Ал, алқабиге байланысты мәселелерді зерделеу үшін жоғарыда көрсеткеніміздей, ҚР ҚПК Ерекше бөлігінің 14-бөліміне жүгінеміз.

Алқабиге және алқабиге кандидатқа берілген анықтамаларға сәйкес, сондай-ақ қылмыстық-процестік заңның ережелеріне орай, алқабиге кандидаттарға келесі негізгі талаптар қойылуы тиіс:

- 1) Қазақстан Республикасының азаматы;
- 2) жиырма бес жасқа толған жеке тұлға;
- 3) қылмыстық сот өндірісінің тілін жеткілікті білетін;
- 4) қылмыстық істе мүддесі жоқ;
- 5) қылмыстық процесте оның басқа мәртебесі жоқ адам.

Жоғарыда көрсетілген «Алқабилер туралы» заңның 10-бабында алқабиге кандидаттарға қойылатын талаптар көсетілген, осы баптың 1-және 3-бөліктеріне сәйкес, алқабиге кандидаттардың тізімдеріне келесі адамдар енгізілмейді және Алқабиге кандидаттардың тізімдерінен алып тасталуы тиіс:

- алқабилердің тізімдерін жасау кезінде жиырма бес жасқа толмағандар;
- өтелмеген не алынбаған сотталғандығы барлар;
- сот әрекетке қабілетсіз немесе әрекет қабілеті шектеулі деп таныған адамдар;
- судьялар, прокурорлар, тергеушілер, адвокаттар, мемлекеттік қызметшілер мен әскери қызметшілер, сондай-ақ құқық қорғау органдарының қызметкерлері;
- психикалық, мінез-құлықтық, оның ішінде психикаға белсенді әсер ететін заттарды тұтынуға байланысты бұзылушылықтарының (ауруларының) себебі бойынша денсаулық сақтау ұйымдарында есепте тұрған адамдар енгізілмейді;
- қылмыстық іс бойынша сот ісі жүргізілетін тілді білмейтін адамдар;
- өздерінің дене кемістігі немесе психикалық кемістігі салдарынан алқабидің міндеттерін атқаруға қабілетсіз адамдар;
- алпыс бес жастан асқан адамдар;
- діни қызметшілер өздерінің жазбаша өтініші бойынша алып тасталады [2].

ҚР ҚПК 640-бабына сәйкес, төрағалық етушінің алқабиге кандидаттарды істі қарауға қатысудан көрсетілгендерден бөлек басқа себептер бойынша босатуы мүмкін, мысалы:

- үш жасқа толмаған балалары бар әйелдерді;
- қызметтік міндеттерін орындаудан аландатылуы қоғамдық және мемлекеттік мүдделерге едәуір зиян келтіруі мүмкін адамдарды (дәрігерлер, мұғалімдер, әуежолдарының ұшқыштары және басқалар);
- сот отырысына қатыспау үшін дәлелді себептері бар өзге де адамдарды, олардың ауызша немесе жазбаша өтініші бойынша, процеске қатысушылармен талқыламастан, алқаби міндеттерін атқарудан босатуы мүмкін.

Қылмыстық істердің барлығы алқабилердің қатысумен қарала бермейтіндігін ескерген жөн. ҚР ҚПК 631-бабында істердің алқабилер қатысатын сотқа соттылығы көрсетілген. Соған сәйкес, сот алқабилердің қатысуымен аса ауыр қылмыстар туралы істерді қарайды. Енді, аса ауыр қылмыстарға қандай қылмыстарды жатқызуға болатындығын ескерсек, онда Қазақстан Республикасының Қылмыстық кодексіне (әрі қарай ҚР ҚК) жүгінген жөн. ҚР ҚК 10-бабы 5-бөлігіне сәйкес, жасалғаны үшін ҚР ҚК он екі жылдан астам мерзімге бас бостандығынан айыру немесе өмір бойына бас бостандығынан айыру түріндегі жаза көзделген қасақана жасалған іс-әрекеттер аса ауыр қылмыстар деп танылады [3]. Қылмыстық құқық бұзушылықты қылмыстың аса ауыр санатына жатқызу үшін екі шарттың болуын талап етеді: 1) іс-әрекет кінәнің қасақана нысанында жасалғаны; 2) ҚР ҚК Ерекше бөлігінде көрсетілген бапқа немесе оның бөлігіне тиесілі көзделген жазаның түрі бас бостандығынан айыру және ол он екі жылдан астам мерзімнен кем болмауы тиіс.

Оның өзінде, аса ауыр қылмыс болып саналғанына қарамастан, кейбір аса ауыр қылмыстарды қылмыстық-процестік заңнама алқабилердің қатысуымен қарауына тыйым салады. ҚР ҚПК 631-бабының 1-бөлігі, келесі жағдайларда жасалған аса ауыр қылмыстарды соттың алқабилердің қатысуымен қарауына тыйым салады:

- 1) төтенше ахуал жағдайларында және жаппай тәртіпсіздіктер барысында жасалған адам өлтіру;
- 2) бейбітшілікке және адамзат қауіпсіздігіне қарсы, конституциялық құрылыс негіздеріне және мемлекет қауіпсіздігіне қарсы қылмыстар;
- 3) террористік және экстремистік қылмыстар;
- 4) соғыс уақытында немесе ұрыс жағдайында жасалған әскери қылмыстар;
- 5) қылмыстық топ құрамында жасалған қылмыстар;
- 6) кәмелетке толмағандардың жыныстық тиіспеушілігіне қарсы аса ауыр қылмыстар туралы істер.

Сондай-ақ, қарастырылып жатқан ҚР ҚПК 631-бабының 1-бөлігінде аса ауыр қылмыс санатына жатпайтын кейбір қылмыстарды сот алқабилердің қатысуымен қарау мүмкіндігі көрсетілген. ҚР ҚК 116 (екінші және үшінші бөліктерінде), 125 (үшінші бөлігінің 1) тармағында), 128 (төртінші бөлігінің 1) тармағында), 132 (бесінші бөлігінде), 135 (төртінші бөлігінің 1) тармағында), 146 (екінші және үшінші бөліктерінде), 160, 163, 164 (екінші бөлігінде), 168, 249 (екінші бөлігінде), 317 (төртінші бөлігінде), 335 (төртінші бөлігінде), 337 (төртінші және алтыншы бөліктерінде), 345 (төртінші бөлігінде), 345-1 (төртінші бөлігінде), 346 (бесінші және алтыншы бөліктерінде), 380-1 (екінші бөлігінің 6) тармағында)-баптарында көзделген қылмыстар туралы қылмыстық істерді де сот алқабилердің қатысуымен қарайды [1].

Біз бұдан алқабилердің қатысуымен қарастырылуы мүмкін қылмыстық істердің шеңбері едәуір кеңетілгенін аңғарамыз. Қылмыстық-процестік заңнамада тікелей тыйым салынғанын бөлек аса ауыр қылмыстардың барлығы дерлік, сондай-ақ ауыр қылмыс емес болмаса да, кейбір қылмыстардың алқабилердің қатысуымен қаралуы мүмкін екені нақты көрсетілген.

ҚР ҚПК 634-бабының 2-бөлігіне сәйкес, сотқа дейінгі тергеп-тексеруді жүзеге асыратын адам тергеу әрекеттерін жүргізу аяқталғаннан кейін күдіктіні істің барлық материалдарымен таныстыру кезінде оған соттың істі алқабилердің қатысуымен қарауы туралы өтінішхат беру құқығын, сондай-ақ алқабилер қатысқан соттың үкіміне шағым жасау және шағымды қарау ерекшеліктерін қоса алғанда, осындай өтінішхатты қанағаттандырудың құқықтық салдарын түсіндіруге міндетті.

Қылмыстық істер бойынша қылмыстық сот ісін алқабилердің қатысуымен жүргізу тікелей күдіктінің немесе айыпталушының қалауына тәуелді болады. Бұл үшін күдікті, айыпталушы өз ісін соттың алқабилердің қатысуымен қарауы туралы өтінішхат беруі тиіс.

ҚР ҚПК 635-бабына сәйкес, сот алқабилердің қатысуымен қарастырылуға жататын қылмыстық істер бойынша алдын ала тыңдау өткізу күдіктінің, айыпталушының істі алқабилердің қатысуымен қарау туралы өтінішхатының болуына немесе болмауына қарамастан міндетті. Егер, қылмыстық іс алқабилердің қатысуымен қарастырылуы мүмкін санатқа жататын болса, онда алдын ала тыңдау міндетті болады.

ҚР ҚПК 635-бабының 3-бөлігіне сәйкес, істің барлық материалдары танысу үшін ұсынылған кезде, сондай-ақ келесі кезеңде, оның ішінде сотта істі алдын ала тыңдауда, бірақ сот басты сот талқылауын тағайындағанға дейін күдіктінің, айыпталушының істі соттың алқабилердің қатысуымен қарауы туралы өтінішхат мәлімдеуге құқығы бар. Күдікті немесе айыпталушы істі соттың алқабилердің қатысуымен қарауы туралы өтінішхатты соттың басты сот талқылауын тағайындағанға дейін беруі тиіс.

ҚР ҚПК 632-бабына сәйкес, қылмыстық істер жөніндегі мамандандырылған ауданаралық сотта және қылмыстық істер жөніндегі мамандандырылған ауданаралық әскери сотта алқабилер қатысатын сот бір судьяның және он алқабидің құрамында әрекет етеді. Әдетте, судья төрағалық етеді және үкім шығармас бұрын дауысқа салынады және барлық дауыс тең екендігін және судьяның да дауысы ескерілетінін білген жөн.

ҚР ҚПК 654-бабының 1-бөлігі алқабилер қатысатын соттың шешуіне жататын сұрақтардың мазмұнын айқындайды, соған сәйкес сотталушы жасады деп айыпталып отырған іс-әрекеттердің әрқайсысы бойынша мынадай:

- 1) іс-әрекеттің орын алғаны дәлелденді ме;

2) бұл іс-әрекетті сотталушының жасағаны дәлелденді ме;

3) бұл іс-әрекеттің жасалуына сотталушы кінәлі ме, – деген үш негізгі сұрақ қойылады.

Бұл кезде қойылатын сұрақтардың мазмұны заңгерлік терминдерсіз, қарапайым, жалпыға түсінікті болатындай етіп құралуы тиіс және әрбір алқабидің қойылған сұрақтардың мазмұнын түсінгеніне көз жеткізген абзал.

ҚР ҚПК 656-бабының 4-бөлігінде көрсетілгендей, Судья мен алқабилердің әрқайсысы дауыс беру құпиясын қамтамасыз ете отырып, сұрақ парағында қойылған және шешілуге жататын әрбір сұраққа бюллетеньге жауап жазады. Жауап міндетті түрде жауаптың мәнін ашатын («ия, дәлелденді», «жоқ, дәлелденген жоқ», «ия, кінәлі», «жоқ, кінәсіз») түсіндірме сөзі немесе сөз тіркестері болатын мақұлдаған «ия» немесе құптамаған «жоқ» дегенді білдіруге тиіс. Судья мен алқабилер өз бюллетеньдерін дауыс беруге арналған жәшікке салады.

ҚР ҚПК 656-бабының 9-бөлігіне сәйкес, егер қойылған негізгі сұрақтардың кез келгеніне берілген құпталмаған жауапқа дауыс берушілердің алтауы және одан да көбі дауыс берсе, ақтау кесімі қабылданған болып есептеледі.

ҚР ҚПК 656-бабының 12-бөлігіне сәйкес, он бес жылдан астам мерзімге бас бостандығынан айыру түріндегі жаза, егер осындай шешімге дауыс берушілердің сегізі және одан да көбі дауыс берсе, тағайындалуы мүмкін.

ҚР ҚПК 656-бабының 13-бөлігіне сәйкес, өмір бойына бас бостандығынан айыру судья мен алқабилердің бірауызды шешімі болған кезде ғана тағайындалуы мүмкін.

Әдебиет

1. Қазақстан Республикасының Қылмыстық-процестік кодексі
<https://adilet.zan.kz/kaz/docs/K1400000231>

2. «Алқабилер туралы» Қазақстан Республикасының 2006 жылғы 16 қаңтардағы N121 Заңы https://adilet.zan.kz/kaz/docs/Z060000121_

3. Қазақстан Республикасының Қылмыстық кодексі
<https://adilet.zan.kz/kaz/docs/K1400000226>

4. Г.Ж. Сулейменова. Казахстанский суд с участием присяжных заседателей, профессор кафедры уголовного процесса и криминалистики Казахской гуманитарно-юридической академии, кандидат юридических наук https://online.zakon.kz/Document/?doc_id=30061557

5. 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. – С. 148.

6. Уголовное право России. Общая часть: Учебник / Под ред. В.П. Ревина. – М.: Юстицинформ. 2016. – С. 580., – С. 185.

7. Қазақстан Республикасы Жоғарғы Сотының «Кәмелетке толмаған адамдардың қылмыстық құқық бұзушылықтары және оларды қылмыстық құқық бұзушылықтар мен қоғамға қарсы өзге де іс-әрекеттер жасауға тарту жөніндегі істер бойынша сот практикасы туралы» 2002 жылғы 11 сәуір N6 нормативтік қаулысы
https://adilet.zan.kz/kaz/docs/P02000006S_/history

8. «Зорлау және өзге де сексуалдық сипаттағы зорлық-зомбылық әрекеттермен байланысты қылмыстарды саралаудың кейбір мәселелері туралы» Қазақстан Республикасы Жоғарғы Сотының 2007 жылғы 11 мамырдағы N4 Нормативтік қаулысы
https://adilet.zan.kz/kaz/docs/P07000004S_



DAYETOVA

Aida Asylbekovna

PhD doctoral student, 1st-year specialty
«8D12301-Law Enforcement Activities», Almaty
Academy of the Ministry of Internal Affairs of the
Republic of Kazakhstan named after M. Yesbulatov,
Police Lieutenant Colonel



BAISEITOVA

Aliya Temirhanovna

Head of the Postgraduate Education Faculty,
Almaty Academy of the Ministry of Internal Affairs of
the Republic of Kazakhstan named after
M. Yesbulatov, Doctor of Law, Associate Professor
(Docent), Police Colonel

**SOME ISSUES RELATED TO VIOLATION OF RULES OF FLIGHT SAFETY
OR AIR TRANSPORT OPERATIONS IN THE REPUBLIC OF KAZAKHSTAN**

The aviation industry of the Republic of Kazakhstan plays a key role in the development of the national economy, enhancing international integration, improving the country's transport accessibility, and boosting tourism. Kazakhstan, with its vast territory and strategic location between Europe and Asia, recognizes the importance of developing its aviation infrastructure.

In address to the people of Kazakhstan, President Kassym-Jomart Tokayev highlighted the importance of developing air hubs, creating conditions for expanding cargo air transportation, and focusing on developing domestic air routes, particularly in tourist areas, by involving small aircrafts. The President also emphasized: «Law and order must prevail in our society. This is a basic condition for ensuring both public and individual safety. Only in this way will we create a Just, Clean, and Safe Kazakhstan. To achieve this strategic goal, we must create favorable external conditions for the peaceful and sustainable development of the country» [1].

The relevance of the research topic stems from the fact that, in the current context of aviation industry development, violations in air transport continue to occur and remain one of the most serious problems threatening aviation safety.

Nature and Scope of the Study Aircraft accidents are rare events, but they cost a lot of money. In addition to the financial costs, aviation accidents may also demand an enormous social toll. These costs are less tangible. The grief arising from the loss of relatives and friends and the costs to society resulting from the loss of skilled and valued workers are not readily quantifiable (FSF, 2002) [2].

Law enforcement agencies work within the framework of current legislation and take appropriate measures to combat violations in air transport. Kazakhstan became integrated into the global air transport system by joining the International Civil Aviation Organization (ICAO) in 1992. On July 2, 1992, the Supreme Council of Kazakhstan ratified the Convention on International Civil Aviation, adopted in Chicago, USA, in 1944 [3], which provided the standards and recommended practices of ICAO.

In addition, the Republic of Kazakhstan has acceded to international conventions that establish the following concepts of illegal acts in air transport:

1. Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo, 14 September 1963, «Tokyo Convention 1963») [4], art. 1:

– *Offenses and any acts, whether criminal or not, that may threaten or endanger the safety of the aircraft or the persons or property on board, or acts that jeopardize order and discipline on board;*

2. Convention for the Suppression of Unlawful Seizure of Aircraft (The Hague, 16 December 1970, «The Hague Convention 1970») [5], Art. 1:

– *Unlawful seizure of aircraft;*

3. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal, 23 September 1971) («Montreal Convention 1971») [6], Art. I:

– *Acts of violence against persons on board in-flight aircraft;*

– *Destruction of an aircraft in service or causing damage to that aircraft which renders it inoperable or which may endanger its safety in flight;*

– *Placement of or commitment of an action that leads to placement on an aircraft in service, by any means whatsoever, of a device or substance which is likely to destroy such aircraft or to cause damage to it which renders it inoperative or to cause damage to it which is likely to endanger its safety in flight;*

– *Destruction of or damage to air navigation equipment or interference with its operation if any such act is likely to endanger the safety of aircraft in flight;*

– *Knowingly providing false information that endangers flight safety;*

4. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Montreal, 24 February 1988, «Montreal Protocol 1988») [7], Art. II:

– *Acts of violence against individuals at airports serving international civil aviation, that causes or can potentially cause serious harm or death;*

– *Destruction or serious damage to equipment and structures of an airport serving international civil aviation, or to aircrafts located at the airport that are not in operation, or disruption of airport services.*

In the Criminal Code of the Republic of Kazakhstan, offenses related to air transport are defined in Chapter 14, «Transport Criminal Offenses» [8]. These regulations are blanket in nature, referring to laws and regulations from other areas of law. The primary legal act is the Law of the Republic of Kazakhstan «On the Use of the Airspace of the Republic of Kazakhstan and Aviation Activities» [9].

Procedures for investigating aviation accidents and incidents are regulated by the Rules for Reporting and Investigating Aviation Accidents and Incidents in Civil and Experimental Aviation [10]. Nonetheless, there are certain challenges in disclosing and investigating such criminal cases:

– For example, during the investigation of criminal violations of safety regulations in railway, air, sea, or river transport (Article 344 of the Criminal Code of Kazakhstan), the usage of standard professional experience by investigators is insufficient to select the optimal investigation methodology, apply individual skills and proven investigative tactics because this category of cases involves specific and multifaceted circumstances across various fields [11, p. 349] (*meteorology, medicine, airport operations, navigation services, aviation psychology, airline operations, ground services, and more*).

– investigators typically lack the necessary knowledge in aircraft operation and maintenance, to obtain which they require assistance from specialists such as pilots, air traffic controllers, navigators, engineers, and aviation doctors who possess such knowledge [12, p. 18]. There are serious challenges in selecting highly qualified and independent specialists to involve them in the inspection of the crime scene and other investigative actions, as well as in the expert examinations;

– at the initial stage of the investigation, it is often difficult to give the correct legal qualification to the event that occurred. It may contain elements of various crimes: violation of rules of traffic safety or operation of rail, air, sea or river transport (*Article 344 of the Criminal Code of the Republic of Kazakhstan*), a terrorist act (*Article 255 of the Criminal Code of the Republic of Kazakhstan*), sabotage (*Article 184 of the Criminal Code of the Republic of Kazakhstan*), intentional destruction or damage to property (*Article 202 of the Criminal Code of the Republic of Ka-*

zakhstan). At the same time, there may be no obvious data indicating the specific illegality of the event under investigation [13, p.349];

– as for aviation violations, at this moment, the aviation accident investigation agencies do not have any specialized departments where they can conduct an objective and complete study of aircraft parts and components, substances and materials, fuel, etc. Therefore, they are objectively examined at enterprises in Kazakhstan whose main activity is not related to the investigation of aviation accidents, or they are sent for examination to specialized institutions outside the Republic of Kazakhstan [14];

According to an Analysis of the State of Civil Aviation Flight Safety in Kazakhstan by «Aviation Administration of Kazakhstan» JSC, the number of aviation accidents were: in 2017 – 8 accidents (11 *fatalities*), in 2018 – 6 accidents, in 2019 – 4 accidents (18 *fatalities*), in 2020 – 2 accidents, in 2021 – 7 accidents, in 2022 – 2 accidents, in 2023 – 3 accidents (6 *fatalities*) [15, p.8].

The most frequent violations in air transport are: flight pattern deviations – 41.5%, flight and crew requirements – 18%, piloting technique – 32.8%, air traffic control rules – 3.7%, airport safety regulations – 4%. Violation of rules of traffic safety or transport operation, poor-quality repair of vehicles, tracks, signaling and communication equipment may be considered a crime if they result in the following consequences: accidents with people, crashes, accidents or other serious consequences [16, p.340].

According to A.Sh. Gabdrakhmanov: «the current situation, in addition to socio-economic causes, is explained by the lack of a comprehensive scientific approach to solving the problem of ensuring traffic safety, insufficient scientific development of modern legal means of combating accidents in transport, and serious omissions in the organization of the work of law enforcement agencies to prevent it» [17, p.].

The circumstances presented highlight the undoubted relevance, theoretical and practical significance of the development of this topic, due to the judicial and legal reform being carried out in the Republic of Kazakhstan and the objective demand for scientifically based analysis of issues of combating offenses in aviation transport.

References

1. Tokayev Kassym-Jomart. «A Just Kazakhstan: Law and Order, Economic Growth, Social Optimism» Address to the People of Kazakhstan // Internet resource: <https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-spravedlivyy-kazahstan-zakon-i-poryadok-ekonomicheskij-rost-obshchestvennyy-optimizm-285014>. – 2024 (accessed 07.09.2024);
2. Flavio Mendonca. «Criminalization of Aircraft Accidents» // Internet resource: [PDF] Criminalization of Aircraft Accidents (researchgate.net). – June 2009 (accessed 07.09.2024);
3. Convention on International Civil Aviation, adopted in Chicago, USA, 07.12.1944 // Internet resource: [https://ru.wikipedia.org/wiki/ Конвенция_о_международной_гражданской_авиации](https://ru.wikipedia.org/wiki/Конвенция_о_международной_гражданской_авиации) (accessed 08.09.2024);
4. Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft (Tokyo, 14.09.1963) // Internet resource: https://www.un.org/ru/documents/decl_conv/conventions (accessed 09.09.2024);
5. Hague Convention for the Suppression of Unlawful Seizure of Aircraft (Hague, 16.12.1970) // Internet resource: https://www.un.org/ru/documents/decl_conv/ (accessed 10.09.2024);
6. Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal, 23.09.1971) // Internet resource: https://www.un.org/ru/documents/decl_conv/ (accessed 11.09.2024);
7. Montreal Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Montreal, 24.02.1988) // Internet resource: https://www.un.org/ru/documents/decl_conv/conventions/airports.shtml (accessed 11.09.2024);
8. Criminal Code of the Republic of Kazakhstan dated 03.07.2014 – No. 226-V (amended on 09.09.2024) // Internet resource: <https://online.zakon.kz> (accessed 12.09.2024);

9. Law of the Republic of Kazakhstan dated 15.07.2010 – No. 339-IV «On the Use of the Airspace of the Republic of Kazakhstan and Aviation Activities» (as amended on 17.07.2024) // Internet resource: <https://online.zakon.kz> (accessed 13.09.2024);
10. Order of the Minister of Investment and Development of the Republic of Kazakhstan dated 27.07.2017 – No. 505. «On the Approval of the Rules for Reporting and Investigating Aviation Incidents and Accidents in Civil and Experimental Aviation» (as amended on 15.05.2023) // Internet resource: <https://online.zakon.kz> (accessed 13.09.2024);
11. Shiryayeva I.A. «Features of Investigating Crimes Committed in Air Transport» // Forum of Young Scientists 11(51), 2020. – Pp. 347-351 // Internet resource: <http://forum-nauka.ru> (accessed 13.09.2024);
12. Mitrofanova A.A. «On the Criminalistic Interpretation of the Concept of 'Aviation Incident'» // Russian Investigator, 2017, No. 5 – Pp. 16-19.
13. Kirikbaev S.K. Application of specialized knowledge of experts of the Forensic Examinations Center of the Ministry of Justice of the Republic of Kazakhstan in the investigation of aviation accidents // Internet resource: www.zakon.kz (date of access 09/14/2024);
14. Dayetova A.A. «Problems in the Investigation of Aviation Accidents in the Republic of Kazakhstan» // Materials of the International Scientific Conference of Students and Young Scientists «Farabi Álemi» III International Farabi Readings (11-13.04.2016) / Under the general editorship of K.N. Shakirov. – Almaty: Kazakh University, 2016. – Pp. 181-183. ISBN 978-601-04-1909-4;
15. «Analysis of the State of Safety of Civil Aviation Aircraft Flights in the Republic of Kazakhstan for 2023» // Internet resource: analiz-sostoianiia-bezopasnosti-poletov-za-2023-god-2.pdf (caa.gov.kz) (accessed 14.09.2024);
16. Chuchaev A.V. «Transport Crimes: Problems of Mechanism, Qualification, and Punishment» – PhD diss. in Law. – Moscow, 1990. – 511 p;
17. Gabdrahmanov A.Sh. «Crimes Against Transport Safety and Operation (Criminal Law and Criminological Aspects)» – PhD diss. in Law. – Kazan, 2007. – 190 p.



МАРАТ

Айгүл Маратқызы

профессор кафедры уголовного права и криминологии Алматинской академии МВД
Республики Казахстан им. М. Есбулатова, з.г.к.

О ЛИЧНОСТИ ИНТЕРНЕТ-МОШЕННИКА

Одной из центральных категорий криминологической доктрины является категория «личность преступника». Общеизвестно, что объектом профилактического воздействия, объектом предупредительной деятельности – является личность преступника.

В науке уголовного права под личностью преступника (субъектом уголовного правонарушения) понимается физическое вменяемое лицо, достигшее к моменту совершения уголовного правонарушения определенного, указанного в законе возраста. Поэтому о личности преступника говорят, когда имеют в виду субъекта уголовного правонарушения, то есть лицо, совершившее уголовное правонарушение, что нашло свое подтверждение в обвинительном приговоре суда, вступившем в законную силу.

По мнению С.С. Молдабаева, личность преступника включает в себя не только признаки, присущие субъекту преступления, – возраст, вменяемость, физическая сущность лица как человеческого индивида, социальные связи и проявления, отношение к существующим социальным ценностям, психологические особенности.

В криминологии же личность – это «социальное лицо» человека, то, кем он стал в процессе социального развития, формирования и деятельности в обществе, а под «личностью преступника» понимается «социальное лицо» человека, совершившего преступление. Личность преступника, то есть личность человека, виновного в совершении общественно опасного деяния, запрещенного законом под угрозой привлечения к уголовной ответственности, выражает его социальную сущность, сложный комплекс характеризующих его свойств, связей, отношений, его нравственный и духовный мир, взятые в развитии, во взаимодействии с социальными условиями, с психологическими особенностями, в той или иной мере повлиявшими на совершение им преступления.

Проведенный анализ научной литературы позволяет прийти к выводу о том, что в структуре личности преступника традиционно принято выделять три подсистемы: социально-демографические признаки, социальные функции личности, а также нравственно-психологические характеристики. Перечисленные структурные признаки в совокупности образуют единый комплекс взаимосвязанных и взаимообусловленных элементов, образующих личность преступника и раскрывающих ее криминологическую сущность.

Нам интересны некоторые аспекты криминологической сущности личности интернет-мошенника. В основе социально-демографической характеристики личности мошенника лежат его пол, возраст, социальное положение, образование, наличие семьи, гражданство. Как спра-

ведливо отмечает, Р.И. Дремлюга, «комплекс элементов, раскрывающих социально-демографическую характеристику личности мошенников, позволяют выявить наличие определенных отклонений в системе социализации мошенников и служат информационной основой для общесоциальной и специально-криминологической профилактики хищений» [4, с. 63].

Высокий процент совершения мошенничества лицами мужского пола обусловлен психологической устойчивостью, социально-активной ролью в обществе, обладанием теоретическими знаниями и практическими навыками в сфере информационных технологий с целью достижения результатов в криминальной сфере.

Рассматривая аналитические данные, представляется важным отметить, что наиболее многочисленной возрастной группой являются осужденные по анализируемым категориям уголовных правонарушений от 30-49 лет, от 25-29 лет и от 18-24 лет. Возрастной диапазон совершения уголовных правонарушений за период с 2020 и первое полугодие 2024 г. варьируется от 30 до 49 лет, что составляет 61,1% (при этом от 14 до 17 лет – 1,7%; от 18 до 24 лет – 15,2%; от 25 до 29 лет – 14,9%; от 50 и старше – 7,1%). Поскольку способы мошенничества характеризуются сложностью, изощренностью совершения, преступникам необходимо иметь достаточно высокий профессиональный уровень в сфере информационных технологий.

Динамика анализируемых категорий уголовных правонарушений, совершаемых лицами в возрасте от 18 до 24 лет, во многом обусловлена тем, что рассматриваемый возрастной промежуток характеризуется вступлением в осознанную жизнь, социализацией. К рассматриваемой возрастной группе относятся выпускники школы, обучающиеся в различных учебных заведениях, а также те, кто не продолжил обучение после получения общего среднего образования. Представляется важным отметить, что на сегодняшний день анализируемой возрастной группе присущ низкий уровень ответственности перед обществом, вследствие чего, преступность, характерная для нее криминальная субкультура воспринимаются ими как нечто «романтическое». Кроме того, вследствие минимального уровня личных доходов анализируемая категория лиц фактически, психологически, материально зависят от своих родителей (законных представителей, довольно часто находятся в состоянии психологического дискомфорта, обусловленного не только сравнением себя с более обеспеченными сверстниками, но и фактически не имеют возможности повысить свой социальный статус посредством повышения уровня своих доходов посредством применения противозаконных методов и средств.

Оценивая уровень образования анализируемой категории преступников, представляется важным отметить, что они обладают высоким уровнем технических компетенций, что существенно упрощает им возможность совершения уголовных правонарушений и сокрытия следов их совершения. Помимо наличия высокого уровня образования и технической компетентности, анализируемая категория преступников характеризуется стремлением к саморазвитию, предопределяющему процесс выявления в существующих системах (как компьютерных, так и социальных) пробелов и несовершенств, что дает им реальную возможность увеличивать свои преступные доходы.

От характерных особенностей личности современного интернет-мошенника преимущественно зависит тот вид мошенничества, на котором он специализируется. Изучение образовательного уровня личности преступника, являясь одним из основных показателей интеллектуального уровня, находится во взаимосвязи с методом и способом совершения общественно опасного деяния, поскольку особенностью рассматриваемой категории преступлений является осведомленность лиц об особенностях и недостаточной защищенности финансово-кредитной деятельности, обладание профессиональными навыками в сфере информационных технологий.

Среди лиц, причастных к совершению интернет-мошенничества в период с 2020 года по июнь 2024 года, преобладают лица со средним профессиональным образованием – 40,4%; общим средним – 36,8%, начальным и основным общим образованием – 19,6%, доля лиц с высшим профессиональным образованием составляет – 3,2%. Следует отметить, что у руководителей организованных групп или преступных сообществ при совершении рассматриваемой категории уголовных правонарушений преобладает фактор проявления высокоинтеллектуальных способностей. Образовательный уровень, выступающий важнейшим элементом социальной

характеристики, связанный с уровнем нравственного развития человека, реализацией его целей по обеспечению ресурсов материального и нематериального характера в мотивации преступного поведения, требует наличия высокого профессионализма и узкой специализации в данной сфере.

Так, на наш взгляд, «криминологический портрет личности мошенника, совершающего мошенничество с использованием сети интернет, может быть представлен следующим образом: «мужчины, преимущественно, в возрасте от 18 до 35 лет, проживающие в городах, чаще имеющие среднее профессиональное и общее среднее образование, являющиеся приверженцами субкультуры интернет-мошенников, которая подразумевает под собой общение на различных закрытых форумах, владеющих терминологией (жаргонизмами) интернет-мошенников».

Немаловажную роль в определении характера поведения преступника играет его семейное положение. В большинстве случаев лица, совершающие мошенничества с использованием электронных средств платежа, не состоят в браке, поскольку семейное положение воздействует на формирование личностных качеств, стимулируя на законопослушное поведение, социальный контроль над личностью.

По данным исследования отечественных ученых, при совершении уголовных правонарушений рассматриваемой категории для большинства лиц доминирующей является корыстная мотивация, обусловленная конечной целью получение денежных средств незаконным путем. Для достижения данной цели возникает необходимость овладения профессиональными навыками, знаниями, приобретения практического опыта в банковской и информационной сфере. Однако для некоторых преступников мотивом выступает самоутверждение и своеобразный фанатизм [5, с. 69]. Группа с корыстными интересами наиболее опасна для общества и государства. По имеющимся сведениям, представители указанной группы совершают около 79%, 7 всех преступлений, которые связаны с мошенничеством в сети Интернет в особо крупных размерах. При совершении профессиональных технических действий, они подкрепляются экономическими или юридическими знаниями [6, с. 162].

Среди наиболее ярких нравственно-психологических черт, характеризующих мошенника, особое внимание необходимо обратить на его склонность ко лжи. Данное качество исходит из самой сути мошенничества как преступления и связано главным образом со способом совершения общественно опасного деяния. Обман либо злоупотребление доверием предполагают безнравственное лживое поведение мошенника, который вводит в заблуждение потерпевшего относительно своих намерений. Феномен лжи активно изучается психологической наукой, которая определяет ее как сознательное искажение реальности и подмену действительных фактов, которые встраиваются в межличностные отношения.

Следующим особенным нравственно-психологическим качеством, характеризующим личность мошенника, является ярко выраженный артистизм в поведении, коммуникабельность является одной из самых существенных характеристик личности мошенника, которая заключается в его способности и желании общения с другими людьми, достаточной легкости установления контакта с ними, сопровождается при этом доброжелательностью, активностью и настойчивостью, используется для извлечения преступным путем материальной выгоды и сокрытия своих общественно опасных намерений.

Таким образом, особенностями личности интернет-мошенников являются следующие: преимущественно лица мужского пола, с каждым годом доля лиц от 20 до 40 лет возрастает, имеющие среднее профессиональное, среднее техническое образование и хорошие технические навыки, корыстолюбивые, азартные, любящие риск, владеющие компьютерной терминологией, которая непонятна большинству людей (не специалистам), часто замкнуты, имеют небольшой круг общения, предпочитают виртуальный мир, считают себя гениями, пренебрежительно относятся к своим жертвам, ведут малоподвижный образ жизни, обладают логическим мышлением, творческим подходом при решении поставленных задач, аналитическим складом ума, часто при наличии неопровержимых доказательств их вины начинают активно сотрудничать со следствием.

Личность интернет-мошенника по сей день остается одной из важных и сложных криминологических проблем.

Литература

1. Молдабаев С.С. Проблемы субъекта преступления в УП РК: Автореф. дис. докт. юрид. наук. – Алматы 1998, – С. 9.
2. Криминология: Учебник для юридических вузов/ Под общей редакцией д.ю.н., профессора А.И. Долговой. – М.: Издательская группа ИНФРА М – НОРМА, 1997, – С. 274.
3. Личность преступника. / В.Н. Кудрявцев, Н.Н. Кондрашков, Н.С. Лейкина и др... – М.: Юрид. лит, 1975, – С. 21.
4. Дремлюга Р.И. Интернет-преступность. – Владивосток: изд-во Дальневосточного университета, 2008. – С. 63.
5. Шестаков Д.А. Криминология: учебник для вузов. – М.: «Юридический Центр Пресс», 2019. – С. 400.
6. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М., 2014. – С. 336.



БАТЫРБАЕВ

Адылхан Кошкенович

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
қылмыстық құқық және криминология кафедрасының профессоры, з.ғ.к.,

ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ КРИМИНОЛОГИЯЛЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ СТРАТЕГИЯЛЫҚ БАҒЫТТАРЫ

Қоғамның цифрлық экономикасы мен цифрлық трансформациясының дамуымен криминологиялық қауіпсіздікті қамтамасыз ету мемлекеттің ұлттық қауіпсіздігінің маңызды бағыттарының біріне айналды.

Сонымен қатар, цифрлық технологиялардың қарқынды дамуы мен енгізілуі қылмыстық жағдайдың өзгеруіне, криминогендік факторлардың деңгейінің жоғарылауына ықпал етті, бұл мемлекеттен криминологиялық қауіпсіздік жағдайына, оның ішінде маңызды инфрақұрылым объектілерінің қауіпсіздігіне назар аударуды талап етеді [1].

Осыған байланысты цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз етудің ұлттық стратегиясының негізгі бағыты жеке тұлғаны, қоғамды және мемлекетті аталған стратегияның мақсаты болып табылатын цифрлық ортадағы қылмыстық қол сұғушылықтардан қорғау болуға тиіс.

Оның тұжырымдамалық ережелері Қазақстан Республикасының Конституциясы, [2] Қазақстан Республикасының ұлттық қауіпсіздігі туралы заңы, [3] ведомстволық нормативтік актілерді бақылау нәтижелері және оның жағдайы мен тенденцияларын, сондай-ақ жүргізілген әлеуметтік зерттеулердің нәтижелерін ескере отырып, цифрлық технологиялар саласындағы криминологиялық жағдайды зерттеу маңызды болып табылады.

Цифрлық технологиялар саласындағы қылмыстық жағдайға жүргізілген талдау цифрлық салада жасалған қылмыстар санының өскенін айғақтайды. Бұл түрдегі қылмыстардың саны ғана өзгерген жоқ, сонымен қатар қылмыс объектілері, қылмыс құралдары мен қарулары жаңартылды. Сонымен қатар, виртуалды ортада қылмыс жасаудың жаңа құралдары пайда болды.

Зерттеу барысында алынған қылмыс туралы статистикалық мәліметтер қылмыстың осы түрінің қолайсыз тенденциясын көрсетеді, бұл криминологиялық қауіпсіздік деңгейін арттырады. Осылайша, меншікке қарсы қылмыстардың, экстремистік және террористік бағыттағы қылмыстардың, оның ішінде терроризм мен экстремизмді қаржыландырудың, қылмыстық шыққан активтерді заңдастырудың, есірткінің заңсыз айналымының, зияткерлік меншік саласындағы қол сұғушылықтардың өсуінің, Қазақстанның маңызды ақпараттық инфрақұрылымына әсер етудің, виртуалды валютаны (криптовалютаны) пайдалана отырып жасалатын қылмыстардың және трансұлттық ұйымдасқан қылмыстың өсу қаупі сақталуда.

Криминологиялық қауіпсіздіктің қолайлы деңгейін сақтау үшін криминологиялық қауіпсіздіктің негізгі қағидаттарына сүйену қажет, атап айтқанда:

– цифрлық трансформация жағдайында цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету кезінде сақталуы үшін мыналар қажет болатын заңдылық қағидаты:

1) саладағы құқықтық қатынастарды құқықтық реттеудің заманауи тетігін құру мақсатында Қазақстан заңнамасын тексеру:

а) цифрлық технологиялар;

б) криминологиялық қауіпсіздікті қамтамасыз ету;

2) Қазақстан Республикасының қылмыстық заңнамасының мониторингі. Қылмыстық-құқықтық ресурс криминологиялық қауіпсіздікті қамтамасыз ету қызметінде үлкен маңызға ие. Біріншіден, қылмыстық заңнамаға мониторинг жүргізу қажет, бұл оның қоғамдық қатынастардың цифрлық трансформациясы кезеңіне сәйкестігін анықтауға мүмкіндік береді; екіншіден, қылмыстық-құқықтық нормаларды криминализациялау немесе декриминализациялау талап етілетін шекараларды нақты айқындауға, содан кейін ғана қылмыстық заңнаманы жетілдіру туралы сөз жүргізуге мүмкіндік береді.

3) жасалып жатқан қаржы операцияларының мониторингі, оның нәтижелері күдікті қаржы операцияларының жасалуын уақтылы ескертуге және оларды бұғаттауға мүмкіндік береді. Цифрлық технологияларды әзірлеу және пайдалану қажет, оларды енгізу оларды осындай операцияларды лезде бұғаттау үшін пайдалануға мүмкіндік береді;

4) цифрлық трансформация жағдайында өзектілігі айқын болатын криминологиялық сараптама туралы мәселені қарауға оралу қажет. Ақпараттық-цифрлық қатынастар саласында жасалатын іс-әрекеттер үшін қылмыстық жауаптылықты регламенттеу мәселелерін қарауға қабылдау және өзі қарау ерекше тәсілді талап етеді. Мұнда басты ерекшелігі-сараптаманы цифрлық технологиялар, криминология, математика саласындағы мамандар жүргізуі керек.

«Цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету қауіп-қатерлерді болжау, табу, тежеу, болғызбау, оларды болдырмау және олардың салдарын жою жөніндегі құқықтық және ұйымдастырушылық-техникалық және өзге де іс-шаралардың арқасында іске асырылуы мүмкін» деген авторлармен келісу керек. Сонымен бірге мұндай қызметті жүзеге асыру үшін қажет:

а) цифрлық технологиялар саласындағы қауіпсіздіктің ұйымдық- құқықтық негіздерінің заңдық құрамдас бөлігінен басқа, қылмыс жасау кезінде пайдаланылуы мүмкін технологиялардың техникалық сипаттамаларын білуді күнделікті қызметінде пайдалана алатын құқық қорғау органдарының қызметкерлерін тиісті даярлау. Бұл, өз кезегінде, кәсіптік даярлау жүйесінде оқытылатын пәндердің оқу жоспарларын өзгертуді, жаңа пәндерді енгізуді, оның ішінде қызметкерлердің біліктілігін арттыру үшін, осындай мамандарды оқытудағы тәсілдерді өзгертуді талап етеді.

Біліктілікті арттырудың жаңа бағдарламалары бойынша дайындық ПО оқу орындарында «цифрлық криминология», «ақпараттық-телекоммуникациялық және цифрлық технологиялар саласында жасалатын қылмыстарға қарсы іс-қимылды ұйымдастыру», «криптовалютаны пайдалану арқылы жасалатын қылмыстарға қарсы іс-қимыл» сияқты және осы бағыттағы пәндер енгізіу;

б) құқық қорғау органдары қызметкерлерінің цифрлық технологиялармен (таратылған тізілімдер (блокчейн) технологиялары, үлкен деректерді өңдеу (BigData), жасанды интеллект және т.б.) жарақтандырылуы, оларды пайдалану цифрлық қылмыстардың ашылу деңгейін арттырады, әртүрлі санаттармен профилактикалық жұмыстың бағыттарын анықтау үшін қажетті деректердің көп мөлшерін зерделеу арқылы алынған ақпарат көлемін арттырады. Трансұлттық ұйымдасқан қылмыс өкілдерінің қылмыстық әрекеттерін анықтау және жолын кесу жөніндегі қызметте жасанды интеллект және үлкен деректерді талдау (BigData) технологияларын қолдануға ерекше үміт артылады, бұл олардың құқыққа қайшы әрекеттеріне уақтылы ден қоюға мүмкіндік береді. Шынында да, бұл жағдайда қылмыстардың көп бөлігі виртуалды ортада жасалады, бұл олардың жасалуына қатысы бар адамдарды уақтылы анықтау деңгейін және қылмыстардың ашылуын тездетеді.

Цифрлық кеңістікте шекараның болмауына байланысты трансұлттық цифрлық қылмысқа қарсы іс-қимыл саласындағы халықаралық ынтымақтастық пен өзара іс-қимылға ерекше назар аудару қажет.

Аталған салада криминологиялық қауіпсіздікті қамтамасыз етуде криминологиялық тәуекелдер мен қауіптер деңгейін төмендетуге маңызды орын бөлінуге тиіс. Осы мақсатта қажет:

- цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету жүйесінің тиімді жұмыс істеуі үшін жағдайлар мен кепілдіктер жасауға қабілетті дербес, тұтас және орнықты цифрлық қауіпсіздік жүйесін құру және нығайту;

- жалпы қылмыстың, сондай-ақ цифрлық технологияларды пайдалана отырып, сондай-ақ цифрлық технологияларға қатысты жасалатын қылмыстардың алдын алуды нормативтік құқықтық реттеуді жетілдіру;

- криминологиялық қауіпсіздікті қамтамасыз ету жөніндегі қызметтің жүйелілігі мен кешенділігі;

- террористік және экстремистік әрекетке, сыбайлас жемқорлыққа, есірткінің, қарудың заңсыз айналымына, цифрлық технологияларды пайдалана отырып жасалатын адам саудасына, сондай-ақ адам мен азаматтың құқықтары мен бостандықтарына бағытталған өзге де қылмыстық әрекетке, «қоғамның материалдық және рухани құндылықтарына, мемлекет инфрақұрылымының аса маңызды және (немесе) ықтимал қауіпті объектілеріне» қарсы іс-қимыл [4];

- криминологиялық қауіпсіздік қатерлеріне кешенді және уақтылы ден қою мақсатында Интерполдың, Еурополдың қылмыстық сот ісін жүргізу тәртібімен өзара іс-қимыл және ынтымақтастық жөніндегі барлық арнайы мүмкіндіктерді тиімді пайдалану. Бұл ретте «қылмыстың алдын алу жөніндегі бірлескен жұмысты ұйымдастыру үшін ұлттық заңнаманы, мемлекеттің, оның құзыретті органдары мен азаматтық қоғамның рөлін ескеру қажет» [5].

Цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету жөніндегі қызмет құқық қорғау органдарының ведомствоаралық және ведомствоішілік деңгейде өзара іс-қимылы кезінде табысты болуы мүмкін. Бұл ретте өзара іс-қимыл ақпараттық қауіпсіздікті тікелей қамтамасыз ететін ұйымдармен, қаржы мекемелерімен, ұялы байланыс операторларымен және интернет-провайдерлермен де жүзеге асырылуға тиіс. Алайда, оның тиімділігі оны құқықтық реттеу кезінде ғана мүмкін болады, сонымен қатар цифрлық қылмысқа қарсы тұру үшін қажетті ақпаратты анықтау, бекіту, талдау тәртібін бекіту. Шешімдерді жедел қабылдау мақсатында қысқа мерзімде маңызды ақпаратпен алмасу шарттары мен мүмкіндіктерін анықтау маңызды болып көрінеді;

- профилактикалық әсердің үздіксіздігі принципі, оның ішінде виктимологиялық профилактика. Виктимологиялық профилактиканы жоққа шығаруға болмайды. Бұл ретте оны криминологиялық насихаттауды жүзеге асыруға бағытталған инновациялық технологияларды пайдалана отырып жүзеге асыру қажет.

Цифрлық трансформация жағдайындағы басты міндет-цифрлық және телекоммуникациялық технологияларды пайдалана отырып жасалатын қылмыстар туралы халықтың хабардарлығын арттыру, өйткені аталған технологиялар саласындағы білімнің жеткіліксіз деңгейі, азаматтардың, әсіресе аға буын мен жасөспірімдердің шамадан тыс сенімділігі аталған салада жасалатын қылмыстардың өсуіне алып келеді.

Бұл мәселені шешу үшін азаматтармен ағарту жұмыстарын жүргізу, сондай-ақ оларды зерттелетін саладағы қолданыстағы қылмыстық схемалар туралы хабардар ету қажет. Мұндай ақпарат құқық қорғау органдарының ресми интернет-ресурстарында, мемлекеттік мекемелердің ақпараттық стендтерінде, қоғамдық көлікте орналастырылады, алайда халық оны әрдайым байқай бермейді және қабылдай бермейді.

Профилактиканың тиімділігін арттыру және азаматтарға профилактикалық ақпаратты жеткізу үшін орынды болып көрінеді:

- түрлі БАҚ, сондай-ақ мессенджерлердің мүмкіндіктерін пайдалана отырып, аталған салада виктимологиялық профилактика бағдарламасын әзірлеу;

- цифрлық технологияларды пайдалана отырып жасалатын қылмыстардың қылмыстық-құқықтық негізін түсіндіре отырып, аудиторияны кеңейте отырып, халықпен жүйелі түрде ағарту жұмыстарын жүргізетін құқықтық топтар құру үшін түрлі мессенджерлерді пайдалану;

- халықты қылмыстар туралы ақпараттандыру үшін вебинарларды белсенді жүргізу, бұл ретте азаматтарды қылмыстың осы түрінің қауіптілігі, олардың жекелеген түрлерінің таралуы,

осындай қылмыстың құрбаны болу қаупін төмендету тәсілдері және адамға қатысты аталған салада қылмыс жасалған жағдайда іс-әрекеттер туралы хабардар ету;

- кәмелетке толмағандарда цифрлық гигиенаны қалыптастыруға бағытталған іс-шаралар өткізу, яғни ақпараттық қауіпсіздіктің негізгі ережелері туралы хабардар ету;

- азаматтарға қатысты осы қылмыстарды жасау қаупін төмендететін мінез-құлық ережелері туралы жадынамалар дайындау және тарату және оларды адамдар көп жиналатын орындарға тарату;

- ПО қызметкерлерінің халықпен кездесулерін ұйымдастыру, оның барысында азаматтарды қылмыстың осы түрінің қауіптілігі, олардың түрлерінің таралуы, аталған салада қылмысқа ұшырау қаупін төмендететін мінез-құлық ережелері және адамға қатысты осындай қылмыс жасалған жағдайлардағы іс-әрекеттер туралы хабардар ету.

Пайдалану кезінде халық үшін қарапайым қауіпсіздік ережелерінің қажетті тізбесін дайындау:

- Интернет желілері, олардың ішінде ұсынбау: Интернет желісінің тексерілмеген көздерінен бағдарламалық өнімдерді жүктеуді жүзеге асыру, бағасы немесе сапасы бойынша тиімді ұсыныстары бар жарнамалық сілтемелерді, сондай-ақ үлкен бонустар ұсыныстарын пайдалану, белгісіз адресаттардан хат-хабарлармен танысу, онлайн-дүкендерде, жеке кабинеттерде тіркелу кезінде жеңіл (оңайлатылған) парольдерді пайдалану. Сонымен қатар, ешқашан электрондық пошта мекенжайларының деректерін, банк карталарының нөмірлерін, туған күнін пайдаланбаңыз; әрқашан сайттардың, олардың мекен-жайларының және т.б. шындығын тексеріңіз.;

- әлеуметтік желілерді ұсынбау, оның ішінде: бейтаныс пайдаланушылармен қарым-қатынас жасау, күмәнді ұйымдарда төлқұжат деректерін қалдыру, несие немесе басқа ұйымдардың парольдері бар банк карталарының деректерін телефон арқылы әртүрлі сылтаулармен беру, түрлі делдалдық қызметтерді ұсынатын тұлғаларға ақша аударымдарын жіберу және т.б.

Алдын алу іс-әрекетінде халықты қылмыстық көріністерден қорғау тәсілдеріне үйретуге үлкен мән беріледі:

- азаматтардың өмірін, денсаулығын, құқықтарын, бостандықтары мен заңды мүдделерін қылмыстық көріністерден қорғаудың басымдығы қағидаты. Осыған байланысты жеке тұлғаға ерекше назар аудару керек, өйткені оны криминологиялық қорғау мемлекет үшін басым болып табылады, «сонымен бірге қазіргі жағдайда жеке тұлғаның криминологиялық қауіпсіздігі ұлттық қауіпсіздікті қамтамасыз ету жүйесінде ең осал болып көрінеді» [6].

Мұндай қауіпсіздікті қамтамасыз етудің негізгі міндеттерінің бірі адамның, қоғамның және мемлекеттің өмірлік маңызды және басқа да маңызды мүдделерін қылмыстық қол сұғушылықтар мен қауіптерден қорғаудың қолайлы деңгейі болып саналуы керек. Бұл жағдайда қылмыстың өсуіне және оның криминологиялық қауіпсіздікті қамтамасыз ету саласындағы жеке тұлғаның мүдделері үшін ықтимал және нақты қауіптілігіне әсер ететін криминогендік сипаттағы факторлардың жиынтығын ескеру қажет [7].

Алайда, ең алдымен, криминологиялық қауіптердің осы сипатынан халықтың қорғалу деңгейін зерттеу қажет.

Қауіпсіздік, егер криминологиялық қауіпсіздік контекстінде қарастырылса, «көптеген семантикалық реңі бар, бірақ «қауіпсіздік» ұғымына қатысты оны кез-келген қауіптен қорғалған күй ретінде қарастыру керек» деген құқықтық категория болып табылады [8].

Сонымен қатар, қорғаудың өзін анықтау азаматтың өмірлік маңызды мүдделерді қылмыстық және қылмыстық сипаттағы жағымсыз факторлардан қорғау жағдайын қабылдауына байланысты. Сонымен қатар, жеке тұлғаның қылмыстық қауіптер мен тәуекелдерден қорғалуын қамтамасыз ету мемлекетке жүктелген және бұл міндет басым болып табылады.

Цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету жөніндегі қызметте криминологиялық жағдайдың мониторингіне ерекше рөл бөлінуге тиіс, оның нәтижелері криминологиялық қауіпсіздіктің нақты жай-күйін, сондай-ақ цифрлық технологиялар саласындағы заңдылықтарды айқындауға, оның өткен және қазіргі жай-күйін талдауға, қылмыстың аталған түрін болжауға, қылмыс көрсеткіштерін, экономикалық, саяси және «әлеуметтік процестерді» белгілеуге мүмкіндік береді. теріс әлеуметтік құбылыстар",

қылмысқа әсер етеді, бұл криминологиялық қауіптердің деңгейін анықтауға және цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету субъектілері қызметінің тиімділігіне баға беруге мүмкіндік береді.

Зерттелетін қылмыс түрінің өсу тенденцияларын және осы қылмыстарды анықтауға байланысты проблемаларды ескере отырып, мониторинг жүргізу кезінде олардың кідірісі мен ұйымдастырылу деңгейіне назар аудару қажет.

Мониторингтің бұл түрі жасанды интеллект және үлкен деректерді талдау технологиясы сияқты цифрлық технологияларды пайдалана отырып жүзеге асырылуы тиіс, оларды қолдану ақпараттық деректердің үлкен массасын зерттеуге мүмкіндік береді. Мониторинг нәтижелеріне сүйене отырып, жақын арада қылмыс және оның түрлері туралы болжам беріледі. Айта кету керек, мұндай жұмыс тұрақты негізде жүргізілуі керек. Ішкі істер органдарының практикалық қызметінде болжау фрагменттелген және формальды түрде жүзеге асырылады. Көбінесе зерттеулер белгілі ережелерге иллюстрациялық сипатқа ие, эмпиризмге бейімділік, теориялық талдаудың болмауы [9] байқалады.

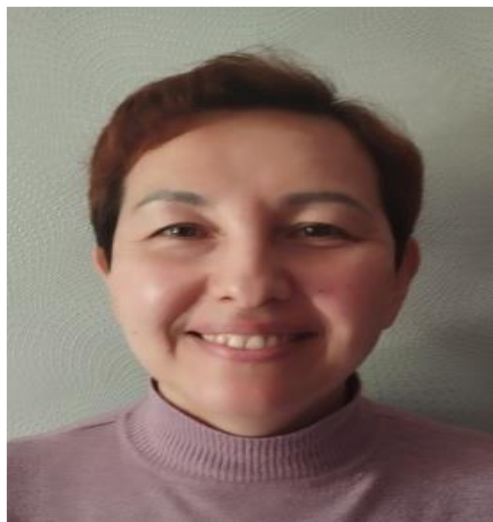
Ерекше назар аударуды қажет ететін келесі бағыт – цифрлық технологиялар, соның ішінде жасанды интеллектті пайдалану. Бұл салада мамандар мен сарапшылар болмаса жасау мүмкін емес. Өйткені, оны қолдану қауіпсіздік және Цифрлық бизнес саласындағы сараптамалық білімді, сондай-ақ қылмыстық мақсатта қорғау мен пайдалануды талап етеді. Алайда, аталған салада мамандардың болмауы және оның қылмыскердің қолдануына қол жетімділігі айқын.

Корпоративтік ақпараттық-цифрлық жүйелерді жаңғыртуды жүргізу олардың хакерлік шабуылдардан қорғалуына айтарлықтай әсер етеді және цифрлық технологиялар саласындағы қылмысқа қарсы іс-қимылда күш-жігерді біріктіруге ықпал ететін болады.

Осылайша, қазіргі цифрлық әлемнің дамуына байланысты мемлекеттердің ұлттық қауіпсіздігінің маңызды аспектілерінің бірі цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз ету болады.

Әдебиет

1. Глотина И.М. Киберпреступность: основные проявления и экономические последствия // Вопросы экономики и права. 2014. №8.
2. Қазақстан Республикасының Конституциясы. Конституция 1995 жылы 30 тамызда республикалық референдумда қабылданды https://adilet.zan.kz/kaz/docs/K950001000_
3. Қазақстан Республикасының ұлттық қауіпсіздігі туралы Қазақстан Республикасының 2012 жылғы 6 қаңтардағы №527-IV заңы
4. Конев Д.А. Современные подходы к деятельности по обеспечению криминологической безопасности в сфере цифровых технологий // Философия права. 2020. №4 (95).
5. Владимир Колокольцев выступил на XIV Конгрессе ООН по предупреждению преступности и уголовному правосудию. URL: <https://xn--b1aew.xn--p1ai/news/item/2334440>
6. Колоткина О.А., Минникес И.А., Ягофарова И.Д. Право личности на криминологическую безопасность: понятие, содержание, место в системе национальной безопасности Российской Федерации // Всероссийский криминологический журнал. 2018. №4. Т. 12.
7. Лапин А.А. Научное обеспечение криминологической безопасности в системе международного правоохранительного сотрудничества // Гуманитарные, социально-экономические и общественные науки. 2016. №11.
8. Остапенко О.В. Незаконное производство лекарственных и медицинских изделий: проблемы квалификации // Аграрное и земельное право. 2021. №4.
9. Афанасьева О.Р., Гончарова М.В., Шиян В.И. История криминологического прогнозирования в системе органов внутренних // Актуальные проблемы юриспруденции: сборник статей по материалам VII Международной научно-практической конференции. – Новосибирск, 2018.



КУРМАНОВА

Гульнара Сагиндыковна

профессор кафедры профессионально-психологической подготовки и управления ОВД
Алматинской академии МВД Республики Казахстан им. М. Есбулатова,
к.ю.н., полковник полиции в запасе

**К ВОПРОСУ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО
БЕСПЕЧЕНИЯ КРИМИНОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ ЛИЧНОСТИ
ОТРУДНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ,
СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ**

Проблема изучения личности преступника в современной криминологической науке занимает одно из центральных мест. «Нельзя объективно рассматривать причины преступности и конкретных преступлений, а также выработать эффективные меры профилактики, не изучив личность преступника» [1, с. 52]. В данном контексте следует заметить, что эффективное изучение личности лица, совершившего преступление, зависит от особенностей учета преступности в целом, а также определенной ее части, к примеру, преступности сотрудников правоохранительных органов.

Некоторые ученые под личностью преступника понимают совокупность социально значимых свойств, влияющих в сочетании с внешними условиями (ситуацией) на преступное поведение [2, с. 82], другие считают, что «личность преступника представляет собой единство социального и индивидуального, врожденного и приобретенного, связь между которыми носит диалектический характер» [3, с. 159].

Ряд ученых считают, что «личность преступника – наиболее широкое и емкое понятие, выражающее социальную сущность лица, сложный комплекс характеризующих его признаков, свойств, связей, отношений, его нравственный и духовный мир, взятые в развитии, во взаимодействии с социальными и индивидуальными жизненными условиями и в той или иной мере определившие совершение преступления» [4, с. 21]. Но личность преступника это не только социальный тип, но психологический, то есть, система взаимодействующих между собой социальных и психических черт, свойств и качеств субъекта общественных отношений [5 с. 119].

К примеру, И.И. Карпец сомневался в необходимости введения в криминологическую науку понятия «личности преступника», так как оно (понятие), как правило, сводится к лицу, нарушившему уголовный закон, а для этого вполне достаточно традиционного и очень точного по своему содержанию понятия «субъект преступления». [6, с. 102]. Но «теоретическое отрицание общего определения личности преступника означает, по существу, отказ от сведения индивидуального к социальному и по логике вещей лишает криминологическую теорию мето-

логической опоры. Без общего определения личности преступника вряд ли возможна выработка криминологических и социально-психологических характеристик по отдельным группам преступников» [7, с. 28-29].

По нашему мнению, объективно личность преступника отличается от личности неправопоступника наличием факта совершенного преступления, но это не означает, что не следует учитывать сформировавшиеся черты, свойства и качества субъекта, определившие выбор преступного поведения. Их знание имеет значение при профилактике преступлений.

Из приведенного выше видно, что в целом понятие «личности преступника» в научной литературе еще дискуссионно, но одновременно достаточно освещено. И данные определения, на наш взгляд, приведены в той степени, в какой необходимы для изучения понятия личности сотрудника правоохранительных органов, совершившего преступление.

На наш взгляд, личность сотрудника правоохранительных органов, совершившего преступление, существенно отличается от «личности преступника» не только личностными особенностями, свойствами, качествами, но и наличием специфических особенностей, присущих только рассматриваемому типу. Это ни в коем случае не говорит о выделении особого или специфического типа «личности преступника». Но чтобы перейти к более детальному рассмотрению данного вопроса, нам необходимо дать понятие личности сотрудника правоохранительных органов.

Правоохранительный орган – государственный орган, обеспечивающий соблюдение и защиту прав и свобод человека и гражданина, законных интересов физических и юридических лиц, государства, реализующий политику государства по противодействию преступности и иным правонарушениям в соответствии со своей компетенцией, наделенный специальными полномочиями по обеспечению законности и поддержанию общественного порядка, выявлению, предупреждению, пресечению, расследованию правонарушений, исполнению судебных решений по уголовным делам. К правоохранительным органам относятся органы прокуратуры, внутренних дел, государственной противопожарной службы, антикоррупционная служба и служба экономических расследований, осуществляющие свою деятельность в соответствии с законодательными актами Республики Казахстан [8].

Для более детального изучения, мы остановимся на исследовании понятия «личность сотрудника органов внутренних дел»

Структура любой личности – как субъекта общественных отношений, состоит из трех основных элементов [5, с. 119]:

1. социальный статус, включающий в себя совокупность признаков, отражающих место человека в системе общественных отношений (пол, возраст, уровень образования, социальное положение);
2. социальные функции, отражающие реальные проявления личности в основных сферах деятельности (профессионально-трудовой, социокультурной, социально-бытовой);
3. нравственно-психологические установки, отражающие отношение человека к его проявлениям в основных видах деятельности (отношение к государству, закону, правопорядку, социальным ценностям, конституционным обязанностям и др.) [5, с. 119].

Структура личности сотрудника правоохранительных органов, помимо трех выше перечисленных компонентов, по нашему мнению, включает в себя: правовой статус сотрудника правоохранительных органов и специфику прохождения службы в правоохранительных органах. Если три первых элемента составляют структуру любой личности, то правовой статус и особенности прохождения службы в этих органах, являются специфическими и свойственными только рассматриваемому типу личности. На примере органов внутренних дел, как самом крупном правоохранительном органе, мы рассмотрим правовой статус сотрудников ОВД и особенности прохождения службы.

Слово статус [лат. Status] – с латинского языка переводится как состояние, положение. Таким образом, правовой статус – это правовое положение физических либо юридических лиц. Как правило, правовой статус составляют права и обязанности.

Впервые в Казахстане была исследована проблема правового статуса работников правоохранительных органов Жалбуровым Е.Т. По его мнению, правовой статус работников правоохранительных органов представляет собой юридическое закрепление положения данной категории служащих в системе государственной службы. Он раскрывается через установление их служебных прав и обязанностей (полномочий), ответственности. Структура правового статуса работников правоохранительных органов с позиции широкого подхода включает следующие элементы: гражданство и правосубъектность; полномочия (совокупность служебных прав и обязанностей); юридическую ответственность во всех проявлениях; различного рода гарантии. Ядром в исследуемом правовом статусе являются государственно-властные полномочия, а также юридическая ответственность работников правоохранительных органов [9, с. 13-83].

Гражданство Республики Казахстан – это устойчивая политико-правовая связь лица и Республики Казахстан, т.е. принадлежность лица к государству.

Гражданство Республики Казахстан – это устойчивая политико-правовая связь лица и Республики Казахстан, т.е. принадлежность лица к государству. Согласно нормам Закона Республики Казахстан «О правоохранительной службе», на службу в органы внутренних дел принимаются граждане Республики Казахстан, достигшие восемнадцатилетнего возраста, способные по своим личным, моральным, деловым, профессиональным качествам, состоянию здоровья и физическому развитию, уровню образования выполнять возложенные на них должностные обязанности [8].

Обозначенные нами определения гражданства и правосубъектности, в рамках исследуемой проблемы, на наш взгляд, являются обязательными требованиями к поступающим на службу в ОВД и выступают как необходимые условия для приобретения правового статуса сотрудника органов внутренних дел, т.е. не могут одновременно являться его элементами.

Государственно-властные полномочия представляют собой определенную государством и закрепленную законодательно совокупность служебных обязанностей и прав сотрудников правоохранительных органов, в целях выполнения возложенных на них задач и функций в пределах своей должностной компетенции. Таким образом, должностные лица правоохранительных органов уполномочены государством от его имени (имени государственного органа, где проходят службу) разрешать в пределах своей компетенции возникающие социально-правовые вопросы и ситуации, принимают по ним решения в форме правовых актов и в необходимых случаях, применяя государственное принуждение. При этом, наличие власти (влажности) является обязательным условием [9, с. 40-41]. Законные требования сотрудников ОВД обязательны для исполнения всеми гражданами и должностными лицами.

За невыполнение или ненадлежащее выполнение своих служебных обязанностей сотрудники органов внутренних дел несут в соответствии с законодательством дисциплинарную, уголовную и иную ответственность. В целом юридической ответственности работников правоохранительных органов присущ повышенный характер [9, с. 128]. Другими словами, сотрудник органов внутренних дел, нарушая законность, подрывает доверие граждан, не только к самому правоохранительному органу, в котором он служит, но и подрывает авторитет государства в целом.

Принимая во внимание выше отмеченное определение правового статуса работников правоохранительных органов, и результаты проведенного нами исследования, можно сформулировать следующее: в структуру правового статуса работников правоохранительных органов входят государственно-властные полномочия и юридическая ответственность. Данное определение приемлемо и для органов внутренних дел. Соответственно, правовой статус является элементом структуры личности сотрудника органов внутренних дел.

Следующим структурным элементом личности сотрудника органов внутренних дел является специфика прохождения службы в органах внутренних дел, которая, на наш взгляд, заключается в следующем:

1. Особый порядок правового регулирования службы определен Законами Республики Казахстан «О правоохранительной службе», «Об органах внутренних дел Республики Казах-

стан». Они регулирует основной порядок и условия прохождения службы сотрудниками органов внутренних дел, их права, обязанности и ответственность.

2. Лицам, состоящим на службе или в кадрах органов внутренних дел, присваиваются специальные звания рядового и начальствующего состава.

3. Служба в органах внутренних дел – особый вид государственной службы граждан Республики Казахстан, связанный с выполнением ими служебных обязанностей и служебного долга перед государством и народом Казахстана.

4. Каждый сотрудник органов внутренних дел в индивидуальном порядке принимает Присягу на верность народу Казахстана.

5. Сотрудники органов внутренних дел обеспечиваются форменным или специальным обмундированием, им выдаются служебные удостоверения и жетоны установленного образца.

6. Сотрудники органов внутренних дел имеют право на ношение, хранение и применение огнестрельного и иного оружия, специальных средств. Они также вправе применять физическую силу, в том числе боевые приемы борьбы самбо, в порядке, установленном законом.

7. Сотрудникам органов внутренних дел запрещается состоять в партиях, профессиональных союзах, выступать в поддержку какой-либо политической партии. Их деятельность не совместима с депутатским мандатом, занятием иной оплачиваемой деятельности, кроме преподавательской, научной или иной творческой деятельности; осуществлением предпринимательской деятельности, вхождением в состав руководящего органа или наблюдательного совета коммерческой организации. Также запрещается организация забастовок и участие в их проведении. Принятие данных ограничений фиксируется в письменной форме под роспись сотрудника.

8. На службу в органы внутренних дел принимаются граждане Республики Казахстан достигшие 18 лет. Определены возрастные цензы приема граждан на службу в органы внутренних дел: на должности рядового и начальствующего состава не старше 35 лет. Установлен предельный возраст нахождения на службе в органах внутренних дел в зависимости от имеющегося специального звания.

9. Для сотрудников органов внутренних дел законодательством предусмотрены социальные и правовые гарантии.

Вышеперечисленные особенности не исчерпывают полную специфику прохождения сотрудниками службы в органах внутренних дел, но на наш взгляд, являются достаточными для раскрытия структурного элемента личности сотрудника.

Служба в ОВД требует от сотрудника неукоснительного соблюдения служебного долга, требований Присяги, высокого чувства ответственности, воспитанности, работоспособности, дисциплинированности, выдержки и самообладания. Высокие требования предъявляются к культурному уровню, наличию моральных и нравственных качеств. Таким образом, сотрудником органов внутренних дел является гражданин Республики Казахстан, имеющий специальное звание и занимающий определенное должностное положение, принявший на себя ограничение некоторых прав, обладающий государственно-властными полномочиями по охране общественного порядка и обеспечению общественной безопасности, защите прав, свобод и законных интересов человека и гражданина, общества и государства от преступных и иных противоправных посягательств, за невыполнение или ненадлежащее выполнение которых несет юридическую ответственность.

Соответственно, личность сотрудника правоохранительных органов, совершившего преступление, представляет собой лицо, состоящее на службе или в кадрах данного органа, имеющее специальное звание, обладающее государственно-властными полномочиями и совершившее преступление.

Как говорилось выше, личность сотрудника правоохранительных органов, совершившего преступление, может значительно отличаться от других категорий преступников. Сотрудники правоохранительных органов обладают специальными познаниями уголовного и уголовно-процессуального права, криминалистической техники и оперативно-розыскной деятельности, психологии и других спецдисциплин, владеют приемами рукопашного боя, которые могут и

порой используют при совершении преступлений, в частности насильственного характера. Тем более значительная доля преступлений, совершенных ими, тем или иным образом связана с их служебным положением, к тому же обозначенные нами правовой статус и специфика прохождения службы, как структурные элементы личности сотрудника правоохранительных органов, ставит в особое положение рассматриваемую нами категорию лиц по сравнению с другими видами преступников.

Некоторые российские исследователи рассматривают криминологическую характеристику личности сотрудников, совершивших преступления, в зависимости от вида совершаемых ими преступлений. Например, Варыгин А.Н. различает «профессиональные» преступления, к которым относит должностные и преступления против правосудия; и общеуголовные преступления [10, с. 12]. На наш взгляд, сотрудник правоохранительных органов все 24 часа в сутки является сотрудником правоохранительных органов, и это объясняется не только порядком оплаты труда. К примеру, ч.1 статьи 19 Закона Республики Казахстан «Об органах внутренних дел Республики Казахстан» гласит: «Сотрудники органов внутренних дел на всей территории Республики Казахстан независимо от занимаемой должности, времени в случае обращения к ним с заявлением или сообщением об уголовном или административном правонарушении либо в случае непосредственного его обнаружения обязаны принять меры по пресечению противоправных деяний, оказанию помощи нуждающимся в ней, охране места происшествия, а также информировать ближайшие органы внутренних дел» [11]. Соответственно и данное положение можно применить к факту совершения сотрудниками преступлений, конечно, оно не может иметь значения для квалификации преступления и назначения наказания, но имеет значение для криминологической характеристики личности сотрудника правоохранительных органов, совершившего преступление.

Кроме того, преступления совершаемые сотрудниками, имеют большой общественный резонанс. Ведь представитель власти, лицо, уполномоченное государством, защищать права, свободы и законные интересы граждан, общества и государства, не выполняя свои обязанности и при этом нарушая закон, не вызывает не только доверия и уважения, но и обычной приязни. Этому еще и способствуют средства массовой информации, которые порой непроверенную, а зачастую и недостоверную информацию «выпускают» в эфир и печать, при этом «смачно» муссируя «сплетни и слухи» о злодеяниях и кознях отдельных сотрудников правоохранительных органов. И для рядового гражданина не имеет значения, совершено ли сотрудником преступление в сфере его профессиональной деятельности или вне ее, в его глазах правоохранительный орган и его сотрудники будут олицетворяться с беззаконием и несправедливостью, произволом и вседозволенностью, и гражданин, чувствуя свою незащищенность, будет меньше доверять и самому государству.

Поэтому изучение личности сотрудника правоохранительных органов, совершившего преступление, с учетом обозначенных нами структурных элементов его личности - правового статуса и специфики прохождения службы, необходимо нам не только для более глубокого криминологического познания изучаемой категории лиц, но и для эффективного противодействия преступным проявлениям среди сотрудников правоохранительных органов. Кроме этого, позволит определить и наметить пути совершенствования отбора, обучения и расстановки кадров на службу в правоохранительные органы, в том числе и органы внутренних дел.

Бесспорно, совершение сотрудниками ОВД преступлений это феномен для современной концепции статуса полицейского, и необходимо проводить эффективную превенцию уголовных деликтов данных лиц. И в связи с этим, возникает много проблем исследовательского характера. Мы не будем доказывать в данной статье ценность и важность изучения личности сотрудника, совершившего уголовное правонарушение. Но для этого, на наш взгляд, необходимо усовершенствовать проводимый учет лиц, совершивших уголовные правонарушения, в данном случае – сотрудников правоохранительных органов, результаты которого послужат основой для научных исследований.

В связи со сказанным выше и в целях совершенствования информационно-аналитического обеспечения научных криминологических исследований личности преступни-

ков, в том числе и по нашей проблематике, мы предлагаем разработать дополнительную форму учета, путем внесения изменений в соответствующий приказ Генерального Прокурора Республики Казахстан [12], либо путем разработки отдельного нормативного правового акта:

– отдельный статистический учет лиц – сотрудников правоохранительных органов, совершивших уголовные правонарушения, с отражением информации по следующим разделам:

1) социально-демографический – пол, возраст, образование (с обязательным указанием учебного заведения, если оно является ведомственным ВУЗом), семейное положение т.п.;

2) уголовно-правовой – вид уголовного правонарушения, мотивация, форма вины, индивидуальный или групповой характер, вид наказания;

3) специфический, это особенности, присущие сотрудникам правоохранительных органов – специальное звание, стаж службы в правоохранительном органе, занимаемая должность на момент совершения уголовного правонарушения, стаж в данной должности и службе; объективные связи совершенного уголовного правонарушения со служебной деятельностью; характеристики по служебной деятельности; наличие дисциплинарных взысканий;

4) виктимологический – характеристики и особенности жертв (возраст, пол и т.д.), характер отношений между потерпевшим и преступником.

Литература

1. Криминология. – Алматы: ТОО «Издательство «Норма-К», – 2004, – С. 336.
2. Алексеев А.И. Криминология. Курс лекций. 2-е изд., испр. и доп.. – М.: ЦЮЛ «Щит», 2001. – С. 332.
3. Джекебаев У.С., Рахимов Т.Т., Судакова Р.Н. Мотивация преступления и уголовная ответственность. – Алма-Ата, 1987. – С. 192.
4. Личность преступника. – М., «Юридическая литература», 1975. – С. 272.
5. Криминология: Учебник / Под ред. проф. Н.Ф. Кузнецовой, проф. В.В. Лунеева. – 2-е изд., перераб. и доп. – М.: Волтерс Клувер, 2004. – С. 640.
6. Карпец И.И. Проблема преступности. – М., «Юридическая литература», 1969. – С. 168.
7. Джекебаев У.С. О социально-психологических аспектах преступного поведения (на материалах криминологического изучения хищения социальистического имущества). Издательство «Наука» Казахской ССР, – Алма-Ата. 1971. – С. 202.
8. Закон Республики Казахстан «О правоохранительной службе» // <https://adilet.zan.kz/rus/docs/Z1100000380/z110380.htm> (дата обращения 12 сентября 2024 года)
9. Жалбуров Е.Т. Правовой статус работников правоохранительных органов Республики Казахстан (сравнительно-правовой анализ). Дисс...канд. юрид. наук, – Алматы, 1999. – С. 141.
10. Варыгин А.Н. Преступность сотрудников органов внутренних дел и проблемы воздействия на нее. Дисс... докт. юрид. наук. – Саратов, 2003. – С. 392.
11. ЗРК ОБ ОВД // <https://adilet.zan.kz/rus/docs/Z1400000199> (дата обращения 12 сентября 2024 года)
12. Приказ Генерального Прокурора Республики Казахстан от 27 февраля 2018 года №29 «Об утверждении Правил ведения и использования специальных учетов лиц, совершивших уголовные правонарушения, привлекаемых к уголовной ответственности, лиц, привлеченных к уголовной ответственности за совершение уголовного правонарушения и дактилоскопического учета задержанных, содержащихся под стражей и осужденных лиц» // <https://adilet.zan.kz/rus/docs/V1800016667> (дата обращения 12 сентября 2024 года)



ЗУЛЕЕВА

Айнагуль Жанилбековна

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
қылмыстық құқық және криминология кафедрасының аға оқытушысы,
ф.ғ.д. (PhD), полиция подполковнигі

СЫБАЙЛАС ЖЕМҚОРЛЫҚҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ОҢ ҮРДІСТЕР

Қазақ мемлекеті дамуының алдыңғы кезеңдерінде жетістіктерге қол жеткізілді жалпы мойындалған нәтижелер, бұл мәселеде айқын оң үрдістер байқалды нығайту және дамыту табыстың кепілі болатын сыбайлас жемқорлыққа қарсы күрес осы Сыбайлас жемқорлыққа қарсы стратегияны қазіргі даму кезеңінде іске асыру елдер.

Қазақстан ТМД елдерінің ішінде алғашқылардың бірі болып «Сыбайлас жемқорлыққа қарсы күрес туралы» Заңды қабылдады мұнымен күресудің жағымсыз құбылыстарын, мақсаттарын, міндеттерін, негізгі принциптері мен тетіктерін анықтады.

2001 жылдан бастап күрес жөніндегі мемлекеттік бағдарламалар іске асырылуда сыбайлас жемқорлықтың себептерін жою бойынша нақты шаралар және сыбайлас жемқорлық көріністерінің туындау жағдайлары қабылдануда.

Қазақстанда кәсіби мемлекеттік аппаратты қалыптастыру үшін негіз, есептілік, ашықтық және меритократия қағидаттарына негізделіп 1999 жылдан бастап қолданыста болған және бекітілген «Мемлекеттік қызмет туралы» Заң Мемлекет басшысы 2005 жылы мемлекеттік қызметшілердің Ар намыс кодексін құрдых [1].

Сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы құқық қорғау функциялары реттеуші және реттеуші органдарды біріктіретін мемлекеттік орган құрылды. Ол шақырылмаған сыбайлас жемқорлыққа қарсы саясатты қалыптастыру және іске асыру ғана емес, сонымен қатар мемлекеттік органдардың, ұйымдар мен субъектілердің қызметін үйлестіру сыбайлас жемқорлықтың алдын алу мәселелеріндегі квазимемлекеттік сектор. Сонымен қатар, сыбайлас жемқорлық қылмыстар қызметін анықтауға, жолын кесуге, ашуға және тергеуге бағытталған. Бұл ретте жаңадан құрылған орган үшін басымдық алдын алу-профилактикалық қызмет болып табылады.

Жазаның бұлтартпаушылық принципі сәтті жүзеге асырылуда. Шенеуніктер атқаратын лауазымдары мен дәрежелеріне қарамастан, сыбайлас жемқорлық әрекеттерін заңға қайшы жасаған әрекеттері үшін заңның барлық қатаңдығы бойынша жауапкершілікке тартылуда [2].

Қылмыстық-құқықтық саясат лауазымды тұлғалардың сыбайлас жемқорлық қылмыстар жасағаны үшін қатаң жауапкершілігін қамтамасыз етеді.

Сыбайлас жемқорлық қылмыстары үшін қатаң жауапкершілік қажеттілігі Қазақстан Республикасының құқықтық саясатының 2010 жылдан 2020 жылға дейін тұжырымдамасында көрсетілген.

Мұндай қағидаттық тәсіл жаңа Қылмыстық кодексте көрсетілген. Сонымен, сыбайлас жемқорлық қылмыс жасау, шартты түрде соттауға тыйым салынып, мемлекеттік қызметте лауазымдарды атқару құқығына өмір бойы тыйым салу енгізілді, ал адамдар, алғаш рет сыбайлас жемқорлық қылмыс жасаған кезде тұлғаның белсенді өкінуіне байланысты тек соттың қалауымен жауапкершіліктен босатылуы мүмкін.

Сыбайлас жемқорлыққа қарсы заңнама тәркілеу жөніндегі нормалармен басшылар үшін қылмыстық жолмен алынған мүлікті, дербес жауапкершілікті сыбайлас жемқорлыққа қарсы іс-қимыл туралы толықтырылды. Онда осындай маңызды ұғым бекітілген, «мүдделер қақтығысы» ретінде.

Бұл ретте мемлекеттік қызметшілердің жауапкершілігін күшейтумен қатар, олардың әлеуметтік кепілдіктері де жетілдірілуде [3].

Мемлекеттік аппараттың және жалақысын кезең-кезеңімен, тұрақты арттыру мемлекеттік қызметшілердің өз міндеттерін адал және әділ негізде орындауы үшін жағдай жасау. Мемлекеттік аппараттың жалақысын кезең-кезеңімен, тұрақты арттыру мемлекеттік қызметшілердің әлеуметтік әл-ауқатын арттыруға және олардың өз міндеттерін адал және әділ негізде орындауы үшін қолайлы жағдай жасалуда.

Құқық қорғау органдарын одан әрі жаңғыртудың мемлекеттік бағдарламасында 2020 жылға дейінгі кезеңге арналған жүйелер және кадр саясатының тұжырымдамасында құқық қорғау органдарын арттыруға бағытталған шаралар көзделіп құқықтық тәртіп органдарына деген сенім деңгейі өсуіне, әртүрлі мінез-құлық және құзыреттілігі жоғары деңгейлі персоналды қалыптастыруға жұмыс жүргізіліп жатыр.

Азаматтардың құқықтары мен заңды мүдделерін қорғау ісіндегі рөлде сот жүйесіне деген сенімді арттыруға, оны нығайтуға ерекше көңіл бөлінеді. Судьялар корпусын қалыптастыру тетігін жетілдіру, электрондық сот ісін жүргізу, оның ашықтығы мен қолжетімділік деңгейін арттыру бойынша шаралар қабылданды.

Барлық жерде ақпаратқа қол жетімділік кеңейтіліп, оған келесі шаралар ықпал етті электрондық үкіметті, сондай-ақ мемлекеттік және жеке құрылымдардың интернет-ресурстарды қалыптастыру.

Мемлекеттік органдар есебінен веб-сайттар, сенім телефондары сыбайлас жемқорлық туралы мағлұматтарды кедергісіз хабарлауы үшін азаматтарға жағдайлар жасалды.

«Мемлекеттік қызмет көрсету туралы заңының» және «Рұқсаттар мен хабарламалар туралы» заңдарының қабылдануымен көрсетілетін қызметтердің сапасын арттыру үшін жағдайлар жасалған.

Жүргізілген жұмыстың нәтижесі жыл сайын бұзушылықтар санының, оның ішінде мемлекеттік қызмет көрсету мерзімдері (2012 жылмен салыстырғанда 8,7 есе) және шағымдар оларды көрсету сапасына (25%-ға), сондай-ақ автоматтандырылған қызметтер үлесін ұлғайтуға (2 еседен астам) және халыққа қызмет көрсету орталықтары арқылы көрсетілетін қызметтер 51%) төмендеуіне әкелді.

Мемлекеттік бюджет қаражатын тиімді және ашық игеру мақсатында сатып алуды автоматтандыру деңгейі мен бәсекелестік ортаны қалыптастыру артып келеді.

Экономиканың мемлекеттік емес секторында мыналар кәсіпкерлік қызметті жүргізу, жұмысқа орналастыру және жұмыспен қамтуды қамтамасыз ету халық саны арттыру үшін қолайлы жағдайлар жасалған.

Жалпы аталған шараларды қабылдау Қазақстан сыбайлас жемқорлыққа қарсы іс-қимылда Орталық Азия өңірі мен ТМД елдері арасында жетекші орындардың бірін иелену деңгейі бойынша мүмкіндік берді.

Сыбайлас жемқорлық күрделі, тарихи өзгермелі, теріс әлеуметтік құбылыс болып табылатын, тіптен өздеріңіз білетіндей, адам дамуының алғашқы кезеңдерінде өркениеттерден бұрын пайда болды.

Сыбайлас жемқорлық проблемасы барлық елдерде бар, ол әлеуметтік-экономикалық прогрессті артқа тартып, тек өзіне тән көріністері мен ауқымымен ерекшеленеді.

Әмбебап және жан жақты анықтаманың жоқтығына қарамастан сыбайлас жемқорлық әрекеті, оған ең алдымен шенеуніктердің теріс пайдалануы, жеке пайда алу үшін билік немесе лауазымдық позиция, және ең көп әдетте шенеуніктерге пара беру, пайдалану оның кең таралған түрлері болып танылады.

Сонымен бірге тиімді және жүйелі қарсылықтың негізгі шарттары сыбайлас жемқорлық билік органдарының қоғамға есеп беруі және бақылауында болуы танылады, сот төрелігінің тәуелсіздігі мен әділдігі, баяндауда айқын және күрделі емес заңдарды, мемлекеттің кадр саясатындағы меритократияны, ашықтықты қолдану мемлекеттік рәсімдер және қоғамдағы сыбайлас жемқорлыққа төзбеушілік [4].

Жалпы, алғашқы нәтижелерді қорытындылай келе сыбайлас жемқорлыққа қарсы іс-қимылды жүзеге асыру Қазақстанның стратегиясында мыналарды атап өткен жөн

Біріншіден, сенім қалыптастыру жұртшылықты Қазақстан Президентінің сыбайлас жемқорлыққа қарсы саясатына әлеуметтік жағынан айтарлықтай нығайды мемлекеттік органдардың қолдауы.

Екіншіден, сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы жүйелі заңнамалық өзгерістер сыбайлас жемқорлық құқық бұзушылықтардың алдын алу жүйесін нығайту үшін елеулі құқықтық негіздер қалыптастырды.

Үшіншіден, кадр саясатын сапалы қайта қарау мемлекеттік қызмет, құқық қорғау, сот органдары, квазимемлекеттік сектор төмендеуіне жағдай жасады мемлекеттік қызметкерлердегі сыбайлас жемқорлық деңгейі басқару.

Төртіншіден, мемлекеттік органдардың ашықтығын арттыру жұртшылықтың легитимділігімен үйлеседі

Бесіншіден, белсенді қатысу жұртшылықты сыбайлас жемқорлыққа қарсы шараларға және насихаттауға сыбайлас жемқорлыққа қарсы мәдениет қоғам сыбайлас жемқорлыққа төзбеушілік атмосферасын нығайтуға мүмкіндік берді [3].

Қазақстан-2030» Стратегиясы іс жүзінде болашақ сыбайлас жемқорлыққа қарсы саясаттың негізін қалады және сыбайлас жемқорлыққа қарсы күресте табысты нәтижелерге жету үшін шешімін күшейтті. Қазақстандық мемлекет дамуының алдыңғы кезеңдерінде жалпы мойындалған нәтижелерге қол жеткізілді, сыбайлас жемқорлыққа қарсы іс-қимыл ісінде айқын оң үрдістер байқалды, оларды күшейту және дамыту ел дамуының қазіргі заманғы кезеңінде осы Сыбайлас жемқорлыққа қарсы стратегияны табысты іске асырудың кепілі болады. Қазақстан ТМД елдерінің арасында алғашқылардың бірі болып осы келеңсіз құбылыспен күрестің мақсатын, міндеттерін, негізгі қағидаттары мен тетіктерін айқындаған «Сыбайлас жемқорлыққа қарсы күрес туралы» Заңды қабылдады. 2001 жылдан бастап Сыбайлас жемқорлыққа қарсы күрес жөніндегі мемлекеттік бағдарламалар іске асырылуда, олардың шеңберінде сыбайлас жемқорлық көріністері пайда болуының себептері мен жағдайларын жою жөніндегі нақты шаралар қабылдануда. 1999 жылдан бастап қолданыстағы Заң және 2005 «Мемлекеттік қызмет туралы» жылы Мемлекет басшысы бекіткен Мемлекеттік қызметшілердің Ар-намыс кодексі Қазақстанда есеп берушілік, ашықтық және меритократия қағидаттарында құрылған кәсіби мемлекеттік аппаратты қалыптастыру үшін негіз жасады [5].

Мемлекеттік қызмет пен сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы реттеуші және құқық қорғау функцияларын біріктіретін арнайы мемлекеттік орган құрылды. Ол мемлекеттік қызметті ұйымдастыру мен өткеру және мемлекеттік аппараттазалығына мониторинг жүргізу мәселелерін реттеуге ғана арналған емес, оған сыбайлас жемқорлықтың алдын алу және оның профилактикасы, сондай-ақ сыбайлас жемқорлық қылмыстар жасаған адамдарды қылмыстық қудалау функциясы да берілген. Бұл ретте алдын алу-профилактикалық қызмет жаңа құрылған орган үшін басымды болып табылады. Жаза бұлтартпастылығы қағидаты табысты іске асырылуда.

Сыбайлас жемқорлық іс-әрекеттерін жасағаны үшін әшкереленген шенеуніктер атқарып отырған қызметтері мен шендеріне қарамастан, заңның барынша қатаңдығы бойынша жауапты болады. Қылмыстық-құқықтық саясат сыбайлас жемқорлық қылмыстарды жасағаны үшін лауазымды адамдардың қатаң жауапкершілігін қамтамасыз етеді.

Сыбайлас жемқорлық қылмыстары үшін қатал жауапкершілік қажеттілігі Қазақстан Республикасының 2010 жылдан 2020 жылға дейінгі кезеңге арналған құқықтық саясат көзделген тұжырымдамасында Осындай қағидаттық тәсіл жаңа іске асырылған. Мәселен, Қылмыстық кодекс те сыбайлас жемқорлық қылмыстарын жасаған адамдарға мерзімнің ескіруі қолданылмайды, шартты түрде соттауға тыйым салынған, мемлекеттік қызметте лауазымға орналасу құқығына өмір бойына тыйым салу енгізілді. Сыбайлас жемқорлыққа қарсы заңнама қылмыстық жолмен алынған мүлікті тәркілеу, сыбайлас жемқорлыққа қарсы іс-қимыл үшін басшылардың дербес жауапкершілігі жөніндегі нормалармен толықтырылды. Онда «мүдделер қақтығысы» деген маңызды ұғым бекітілген [6].

Бұл ретте мемлекеттік қызметшілердің жауапкершілігін күшейтумен қатар олардың әлеуметтік кепілдіктері де жетілдірілуде. Мемлекеттік аппараттың еңбекақысын кезең-кезеңмен, үнемі көтеріп отыру мемлекеттік қызметшілердің әлеуметтік өзін-өзі сезінуін арттыруға және олардың өз міндеттерін адал және әділ негізде орындауы үшін жағдайлар жасауға арналған. Құқық қорғау жүйесін одан әрі жаңғыртудың 2020 жылға дейінгі кезеңге арналған мемлекеттік бағдарламасы мен Құқық қорғау органдарының кадр саясаты тұжырымдамасында құқық тәртібі органдарына деген сенім деңгейін арттыруға, мінсіз жүріс-тұрыспен және құзыреттіліктің жоғары деңгейімен ерекшеленетін персоналды қалыптастыруға бағытталған шаралар көзделген. Сот жүйесіне деген сенімді арттыруға, азаматтардың құқықтары мен заңды мүдделерін қорғау ісінде оның рөлін күшейтуге ерекше көңіл бөлінуде. Судьялар корпусын қалыптастыру тетігін жетілдіру, электрондық сот ісін жүргізуді дамыту, оның ашықтығы мен қолжетімділік деңгейін арттыру жөнінде шаралар қабылданды.

Жер-жерде ақпаратқа қолжетімділік кеңейтілді, оған электрондық үкіметті, сондай-ақ мемлекеттік және жекеше құрылымдардың интернет-ресурстарын қалыптастыру жөніндегі шаралар ықпал етті. Азаматтардың сыбайлас жемқорлық фактілері туралы кедергісіз ақпарат алуы, оның ішінде мемлекеттік органдардың сенім телефондары мен веб-сайттары арқылы кедергісіз ақпарат алуы үшін жағдайлар жасалды.

Елдің инвестициялық тартымдылығын күшейту, оның бәсекеге қабілеттілігін арттыру мақсатында кәсіпкерлік қызметті, халықтың сапалы және тез арада мемлекеттік қызметтерді алуын қиындататын әкімшілік кедергілер жойылуда. Заңның және «Мемлекеттік көрсетілетін қызметтер туралы» «Рұқсаттар мен Заңның қабылдануымен көрсетілетін мемлекеттік қызметтердің хабарламалар туралы» сапасын арттыру үшін жағдайлар жасалды, рұқсаттар саны мен қызметтің лицензияланатын түрлері күрт азайды.

Мемлекеттік қызметтерді көрсетудің тиімділігін бағалау және оның сапасын сыртқы бақылау жүйесі қалыптастырылды. Атқарылған жұмыстың нәтижесінде мемлекеттік қызметтерді көрсетудің мерзімдерін бұзу саны (2012 жылмен салыстырғанда 8,7 есеге) және оларды көрсету сапасына шағымдардың саны (25%-ға) жыл сайын төмендеп келеді, сондай-ақ автоматтандырылған қызметтердің үлесі (2 еседен астам) және халыққа қызмет көрсету орталықтары арқылы көрсетілетін қызметтердің үлесі (51%-ға) ұлғайды.

Мемлекеттік сатып алуларды автоматтандыру деңгейі артуда, бұл бәсекеге қабілеттіортаның қалыптасуына, бюджет қаражатының ашық және тиімді игерілуіне ықпал етеді. Экономиканың мемлекеттік емес секторында кәсіпкерлік қызметті жүргізу, жұмысқа орналасу және халықты жұмыспен қамтамасыз ету үшін қолайлы жағдайлар жасалды. Тұтастай алғанда, аталған шаралардың қабылдануы Қазақстанға сыбайлас жемқорлыққа қарсы қызмет деңгейі бойынша Орталық Азия өңірінде де, ТМД елдері арасында да көшбасшы орындардың бірін алуға мүмкіндік берді.

Дегенмен, қол жеткізген табыстарға қарамастан, сыбайлас жемқорлыққа қарсы шараларды жетілдіру және қордаланған мәселелермен күресу бойынша жұмысты жалғастыру қажет.

Тәсілдер мен әдістерді үнемі жаңартып отыру, сондай-ақ мемлекеттік органдар, бизнес пен азаматтық қоғам арасындағы өзара іс-қимылды нығайту болашақта сыбайлас жемқорлықпен сәтті күресудің кепілі болып табылады.

Осылайша, сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы оң үрдістер жүйелі өзгерістер мен ұжымдық күш-жігер неғұрлым әділ және ашық қоғамды қалыптастыруға ықпал ететініне сенім үшін негіз жасайды.

Әдебиет

1. Қазақстан Республикасының мемлекеттік қызмет туралы Заңы 23.11.2015, №416-VҚРЗ
2. Алауханов Е. Антикоррупционная правовая политика/ Е. Алауханов. – Аламты: Зан әдебиеті, 2009. – С. 254.
3. ҚР Президентінің 2010-2020 жылға дейінгі кезеңге арналған тұжарымдамасы. Қазақстан Республикасының қылмыстық кодексі 24.08.2009 ж. №858
4. Байменов А.М. Государственная служба: Международный опыт. Казахстанская модель / Байменов А.М. – Астана: Фолиант, 2000. – С. 152
5. Қазақстан Республикасы Сыбайлас жемқорлыққа қарсы күрес іс қимыл туралы 18.11.1998 ж. №410 заңы.
6. Қазақстан Республикасының қылмыстық кодексі 3.07.2014 №226-V ҚРЗ



БАПАНОВ

Мағжан Талғатұлы

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы қылмыстық құқық және криминология кафедрасының аға оқытушысы, з.ғ.м., полиция майоры



БАПАНОВА

Тогжан Талгатқызы

Заң колледжі арнайы пәндер оқытушысы, философия докторы (PhD)

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАРСЫ ІС-ҚИМЫЛДА ЗАҢНАМАНЫ ЖЕТІЛДІРУ ЖОЛДАРЫ

Жоғары технологияларды пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды зерттеу, тиімді алдын алу және ашу олардың егжей-тегжейлі криминологиялық сипаттамаларын зерделеусіз мүмкін емес.

Криминологиялық сипаттама деп қылмыстың қасиеттерін, заңдылықтарын, факторлары мен салдарын (оның жеке түрі немесе түрі), сондай-ақ қылмыскердің жеке қасиеттерін сипаттау түсініледі. Жоғары технологияларды қолдану арқылы жасалған қылмыстық құқық бұзушылықтар туралы айтатын болсақ, жәбірленушінің жеке басын және оның Виктимологиялық сипаттамасын зерттеу керек.

Жоғары технологияларды қолдана отырып, қылмыстың қасиеттері мен белгілерін зерттеу көптеген себептерге байланысты өте қиын. Олардың біріншісі және негізгісі-бұл заңға қайшы әрекеттердің осы тобы үшін ғылымда бірыңғай, қалыптасқан терминологиялық аппараттың болмауы. Қазіргі уақытта Қазақстан Республикасының Қылмыстық кодексінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар тобы ғана бөлек бекітілгендіктен, ресми статистикада осы әрекеттерді талдау деректері ғана бар. Алайда, егер қылмыс құбылысын жоғары технологияларды пайдалана отырып, компьютерлік құрылғының көмегімен жасалған кез келген құқыққа қайшы әрекет ретінде түсіндіретін болсақ, ҚР ҚК 7-тарауының норма белгілеріне түсетін және түспейтін қылмыстық құқық бұзушылықтардың елеулі шеңберін зерттеу қажет.

«Компьютерлік ақпарат саласындағы қылмыстар», ал компьютерлік технологияларды қолдану арқылы жасалған, бірақ басқа баптар бойынша ескерілген әрекеттер қарастырылмайды. Осылайша, криминологтар компьютерлік қылмысты зерттеуге, тек ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар туралы деректермен жұмыс істеуге немесе бейресми деректер мен өз зерттеулерінің нәтижелерін пайдалануға мәжбүр.

Тағы бір себеп-жалпы қылмыстың, оның ішінде компьютерлік технологияларды қолданудың кідірісінің жоғары деңгейі. В.В. Лунеев атап өткендей, «Жасырын қылмыс деңгейі бүгінде нақты қылмыстың 70-80% құрайды... қылмыс жасаған адамдардың шамамен 5% ғана қылмыстық жауапкершілікке тартылады» [1, 7-бет]. Статистикалық мәліметтер компьютерлік технологияларды қолдану арқылы жасалған қылмыстардың көп бөлігін көрсетпейді. В.Г. Степанов – Егиянц мұндай қылмыстардың кідірісін 85-99% деңгейінде анықтайды, М.В. Старичков кідіріс деңгейін шамамен 99,7-99,8% деп атайды [2, 74-112 ББ]. Мұның себептері жәбірленушілер тарапынан оларға қатысты құқыққа қайшы әрекет жасау кезінде тиісті реакцияның болмауы да, компьютерлік технологияларды пайдалана отырып, көптеген қылмыстардың жасырын сипаты да болып табылады. Мысалы, шабуылдаушы араласудың ізін қалдырмай, заңмен қорғалатын құпияны қамтитын ақпараты бар файлды көшіре алады. Осылайша, қылмыс іс жүзінде байқалмай қалады.

Сонымен қатар, компьютерлік қылмыстардың көпшілігі бірнеше әрекеттерді орындау арқылы жасалады ұқсас құрамы бар эпизодтар. Мысалы, қылмыскер Банктің желісін бұзады және көптеген салымшылардың шоттарынан аз мөлшерде ақша алады, ал ресми статистика бұл жағдайда тек бір заңсыз әрекетті қарастырады.

Тергеу практикасын және қылмыстық құқық бұзушылықтардың жаңа түрлерінің пайда болуын ескере отырып, Қазақстан Республикасының Қылмыстық кодексіне "ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар" деген 7-тарау енгізілді, онда Қазақстан Республикасының бұрын қолданыста болған Қылмыстық кодексіне қарағанда 9 құрам бар (ҚР ҚК 227 және 227-1-баптары).

Қылмыстық құқық бұзушылықтардың ең көп таралған түрлері-қорлау, әлеуметтік желілерде жала жабу, зиянды бағдарламаларды тарату арқылы ақпаратқа заңсыз қол жеткізу, контрафактілік жұмыстарды тарату, ақпараттық технологияларды қолдану арқылы ұрлау.

Криминалистикалық сипаттаманы ғылыми әзірлеу процесі қылмыстық әрекеттің объективті заңдылықтарын көрсетудің нақты мысалы болғандықтан, белгілі бір элементті криминалистикалық сипаттамаға енгізу процесі объективті түрде қажет, заңды болуы керек, осыған байланысты мобильді телекоммуникация саласындағы қылмыстық құқық бұзушылықтарды криминалистикалық сипаттамаға енгізу қажеттілігі негізделеді. жасау кезінде шағылысу процесіне табиғи түрде қатысатын элементтер кез келген қылмыстық құқық бұзушылық, атап айтқанда, бұл белгілер, қылмыстық құқық бұзушылықты жасау тәсілін, оны қолданудың типтік салдарын, болжамды қылмыскердің жеке басын, қылмыстық құқық бұзушылықтың себептері мен мақсаттарын, қылмыстық құқық бұзушылықты жасау орны, уақыты мен жағдайын сипаттайтын.

Криминалистикалық сипаттаманың элементтері арасындағы статикалық және статистикалық байланыстарды талдау нәтижелері бойынша олардың негіздемесі криминалистикалық сипаттамамен орындалатын міндеттерге бейімделген және криминалистикалық сипаттамаға енгізілген деректерді толықтыру, нақтылау және пайдалану жөніндегі қызметті ғылыми ұйымдастыруға бағытталған әдістер жүйесі, криминалистика әзірлеген және қарызға алған әдістер мен әдістер негізінде мүмкін болады деген қорытынды жасалады.

Мұның бәрі ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін қылмыстық жауаптылықты реттеуге байланысты мәселелерді кешенді және егжей-тегжейлі зерделеу қажеттілігін алдын ала анықтайды.

Біз отандық криминологиялық ғылым Ақпарат және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасының негізгі белгілерін қалыптастыруда айтарлықтай кешігіп келе жатқанын атап өтеміз. Бұл позицияны қалыпты деп тану мүмкін емес және теориялық ойлауды қажет етеді.

Ақпарат және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасының негізгі құрамдас бөліктерін тұжырымдай отырып, автор 1) қылмыстық құқық бұзушылықтардың криминологиялық маңызды белгілерін, 2) криминологиялық жағдайды ашатын деректерді, 3) қылмыстық құқық бұзушылықтардың

алдын алу жөніндегі қызметтің ерекшелігін айқындайтын белгілерді қамтитын сыналған теориялық модельге сүйенеді. Бірінші топқа қылмыскердің жеке қасиеттері, қылмыстық құқық бұзушылықтың себептері мен мақсаты, жәбірленушінің жеке басының қасиеттері жатады. Екіншісіне-қылмыстық құқық бұзушылықтар статистикасы, қылмыстық құқық бұзушылықтардың әлеуметтік жағдайлары туралы мәліметтер. Үшіншісіне-қылмыстық құқық бұзушылықтардың себептері, қылмыстық құқық бұзушылықтардың салдары, қылмыстық құқық бұзушылықтардың тетігі, қылмыстық құқық бұзушылықтарға ықпал ететін мән-жайлар.

Деректерді электрондық өңдеу техникасы дамыған сайын қылмыстық құқық бұзушылықтар саласы кеңейіп келеді, өйткені компьютерлер әр түрлі техникалық өнімдерге енуде. Тиісінше, автор киберқылмыстың жалпы тенденциясын атап көрсетеді-ол кем дегенде аппараттық және техникалық тасымалдаушылармен және көп жағдайда ақпараттық технологиялармен байланысты қылмысқа айналады. Сонымен, қазіргі уақытта «компьютерлік қылмыс» (CIBER CRIME) термині компьютерлік қылмыстан кейінгі немесе мультимедиялық қылмысты қамтыды.

Киберқылмыстың криминологиялық сипаттамасын ұсына отырып, зерттелетін қылмыстық құқық бұзушылықтарды жасау әдістерінің мазмұнына назар аудару керек, отандық және шетелдік криминологиялық ғылымда киберқылмыстарды жасау тәсілдерін, олардың нақты атаулары мен жіктелуін сипаттау мәселелерінде белгілі бір ұғымдар жоқ екенін атап өткен жөн. Бұл мәселе ғылым үшін соншалықты Жаңа, ол тек түсіну және теориялық даму сатысында. Өртүрлі техниканың құралдарын пайдалана отырып жасалған қылмыстық құқық бұзушылықтар бойынша нақты қылмыстық істердің нәтижелерін талдау, сондай-ақ арнайы әдебиеттерді зерделеу негізінде қылмыскердің әртүрлі ниеттермен компьютерлік техниканың құралдарына қол жеткізуге бағытталған белгілі бір технологиялық әрекеттерді қолдану әдісі негізгі жіктеу белгісі ретінде әрекет етеді деген қорытындыға келеміз. Тиісінше, қылмыстық құқық бұзушылық жасау тәсіліне байланысты келесідей топтастыруға болады: ақпарат алу; ақпаратты ұстап алу; компьютерлік техника құралдарына рұқсатсыз қол жеткізу; деректерді және басқару топтарын манипуляциялау; кешенді әдістер.

Қылмыстық құқық бұзушылықтың дербес криминологиялық сипаттамасы ретінде біз оны жасау жағдайын анықтаймыз, ол арқылы (криминологиялық мағынада) қылмыстық құқық бұзушылық жасалғанға дейін және жасалған кезде өзара әрекеттесетін объектілердің, құбылыстардың және қоршаған ортаның орнын, уақытын, заттай, табиғи-климаттық, өндірістік, тұрмыстық немесе өзге де жағдайларын сипаттайтын процестердің жүйесін түсінеміз. Ақпараттандыру және байланыс саласында қылмыстық құқық бұзушылықтар жасау жағдайы бірқатар маңызды факторлармен сипатталады. Ең алдымен, бұл қылмыстық құқық бұзушылықтар кәсіби қызмет саласында жасалатынын атап өткен жөн. Қылмыскерлер, әдетте, компьютерлер мен оның құрылғыларын басқару саласындағы арнайы дағдыларды ғана емес, сонымен қатар тұтастай алғанда ақпараттық жүйелердегі ақпаратты өңдеу саласындағы арнайы білімді, сондай-ақ тиісті қаржылық, банктік және егжей-тегжейлі ақпараттық технологиялардағы қажетті арнайы білімді меңгереді. Осы қылмыстық құқық бұзушылықтардың барлығы әрдайым кәсіби дайындық барысында адамдарға белгілі болатын кәсіби қызметтің белгіленген тәртібін бұзумен байланысты, сондықтан бұл әрекеттерді бағалау кезінде ниет мәселелері біржақты шешілуі мүмкін.

Қылмыстық құқық бұзушылықтардың келесі криминологиялық сипаттамасы-ақпараттандыру және байланыс саласында қылмыстық құқық бұзушылық жасаған қылмыскердің жеке басы. Компьютерлік қылмыстық құқық бұзушылықтар туралы арнайы заң әдебиеттерінде салыстырмалы түрде жақында терминдер пайда болды: «ХАКЕР» – компьютерлік жүйелер мен желілер бойынша маман; «КРЭКЕР» – бағдарламалық жасақтаманы бұзудың негізгі мақсаты болып табылатын хакер; «ФРИКЕР» – қазіргі уақытта компьютерлік желіні білдіретін телефонияны заңсыз және стандартты емес пайдалану жөніндегі маман. Тиісті атаулар пайда болды «ХАКИНГ», «КРЭКИНГ», «ФРИКИНГ» – бұл маманның жұмысына қажет арнайы бағдарламалық жасақтама мен жабдықтардың жиынтығы.

Қылмыстық құқық бұзушылықтардың маңызды криминологиялық сипаттамасы қылмыстық құқық бұзушылықтың себебі болып табылады. Компьютерлік қылмыстық құқық бұзушылықтардың ең көп тараған себептері ретінде, қылмыстық істерді зерттеу көрсеткендей, қызығушылық немесе ойын-сауық, авантюризм, біреудің өзіне деген расположыласына жетуге тырысу, тану, өзін-өзі көрсету, кек алу, вандализм, жеке немесе қаржылық пайда, ақша. Қазіргі уақытта қылмыстық құқық бұзушылықтардың негізгі себептері материалдық пайда алу болды.

Тіркелген қылмыс қылмыстық статистиканың негізгі статистикалық көрсеткіші болып табылады, бірақ қылмыстың ресми есептілікте ескерілмейтін бөлігін де ескеру қажет. Сыртта тіркелген құқық қорғау органдары қалдырған қылмыстық құқық бұзушылықтардың жиынтығы ретінде анықталған жасырын (жасырын) қылмыс деп аталады. Бұл көптеген жағдайларда анық емес жағдайларда жасалатын жекелеген қылмыстық құқық бұзушылықтардың ерекшелігіне байланысты. Компьютерлік қылмыстық құқық бұзушылықтар оларды ашудың техникалық күрделілігіне байланысты ең жасырын санатқа жатады.

Әлемдік өркениет дамуының қазіргі кезеңінде индустриалды қоғамнан ақпараттық қоғамға көшу байқалады. Ақпарат кез келген басқа құндылық сияқты заңсыз әрекеттерден тиісті қауіпсіздік шараларын қабылдауды талап ететін қоғамдық ресурстардың маңызды түріне айналады. Бұл процесс ақпараттық қауіпсіздікті қамтамасыз ету проблемасын Қазақстан Республикасының ұлттық қауіпсіздігінің құрамдас бөліктерінің бірі ретінде өзектендіреді. Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі құралдары құқықтық шаралар болып табылады, олардың құрамдас бөлігі қылмыстық қол сұғушылықтардың ақпараттық қоғамдық қатынастарға қолжетімділігін шектеуге бағытталған қылмыстық-құқықтық шаралар болып табылады. Ақпараттың әлеуметтік құндылығын қоғамдық қатынастарды дамытудың негізгі бағыты ретінде тану проблеманы криминологиялық талдау және ақпараттық қауіпсіздікті жүзеге асыру үшін тиісті шаралар қабылдау қажеттілігін анықтайды.

Ақпараттық қауіпсіздікті қамтамасыз етудегі маңызды мәселе ақпаратты заңсыз қол жеткізуден қорғау мәселесі болып табылады. Бұл проблеманың болуы заңмен қорғалатын неғұрлым құнды ақпараттың заңсыз қол жеткізуден қорғалуы, сондай-ақ заңмен қорғалатын ақпаратқа заңсыз қол жеткізу, әдетте, елеулі қоғамдық қауіпті салдарға, атап айтқанда оның құпиялылығын, тұтастығы мен қолжетімділігін бұзуға әкеп соқтыруы болып табылады.

Сонымен қатар, ақпаратты заңсыз қол жеткізуден қорғаудың қазіргі заманғы шаралары белгілі бір тасымалдағыштардағы (компьютерлік ақпарат) ақпаратты қорғаудың басымдығына негізделген, бұл осы тәсілдің ақпараттық заңнаманың ережелеріне сәйкес келмеуіне байланысты ақпаратты заңсыз қол жеткізуден қорғаудың нақты жүйесінің болмауына әкеп соғады. Бұл жағдайлар ақпараттық қатынастар саласында криминологиялық қорғау шараларын әзірлеу қажеттілігінің себебі болып табылады, оның құрамдас бөліктерінің бірі заңмен қорғалатын ақпаратқа заңсыз қол жеткізу болуы керек. Бұл жағдайда ақпаратты қорғау дәрежесі тасымалдаушының қасиеттерімен емес, оның мазмұнымен анықталуы керек.

Мұның бәрі заңмен қорғалатын ақпаратқа заңсыз қол жеткізуден тұратын қылмыстық құқық бұзушылықтардың жаңа жалпы құрамының элементтерін егжей-тегжейлі әзірлеуді талап етеді.

В.П. Числиннің пікірінше, «ақпараттық қауіпсіздікті қамтамасыз етудің қылмыстық-құқықтық шаралары, жауапкершіліктің басқа түрлерімен салыстырғанда қылмыстық жауапкершіліктің неғұрлым қатандығына байланысты, кез-келген ақпараттың заңсыз қол жетімділігінен емес, тек заңмен қорғалатын ақпараттан қорғауға бағытталуы мүмкін» [3, 38-49 ББ.]. Демек, ақпараттың бұл түрін қылмыстық-құқықтық реттеу саласына жатпайтын ақпараттық ресурстардың басқа массивінен ажырату мәселесі туындайды.

Екі ұшты презентация заңмен қорғалатын және барлық құжатталған ақпаратты қамтитын ақпарат ұғымын тым кең түсіндіруге мүмкіндік береді. Ақпараттық заңнаманың нормаларына сүйене отырып, ақпаратты заңмен қорғалатын санатқа жатқызу критерийлері анықталды.

Негізгі криминологиялық тұжырымдама детерминация ұғымы болып табылады, ол болмыстың маңызды ерекшеліктерінің бірін – заттардың, құбылыстар мен процестердің жалпыға ортақ байланысын, өзара тәуелділігі мен өзара тәуелділігін көрсетеді.

Л.А. Судареваның пікірінше, «компьютерлік қылмыс саласындағы маңызды детерминанттар: 1) қоғам дамуының жалпы төмен мәдени және экономикалық деңгейіне байланысты объективті себептер мен жағдайлар; 2) компьютерлік қылмыс жасаушыларға әсер ететін әлеуметтік-психологиялық факторлар: төмен әлеуметтік мәртебе; төмен жалақы деп санау керек; жоғары кәсіби деңгей» [4, б. 11].

Жоғарыда айтылғандарға байланысты Қазақстан Республикасына тән ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды жүйелеуді жүргізу қажет екенін атап өткім келеді, оларды жасау мақсаты бойынша қылмыстық құқық бұзушылықтарды мынадай топтарға бөлу ұсынылады:

1) басқа біреудің есептік атаулары мен парольдері арқылы Интернеттің компьютерлік желісіне заңсыз қол жеткізу;

2) ұялы байланыстың «қосарланған» телефондарын пайдалану;

3) компьютерлік ақпаратқа рұқсатсыз қол жеткізу: а) көшіру; б) модификациялау; в) жою немесе бұғаттау;

4) электрондық бақылау-касса машиналарының фискалдық жадын өзгерту;

5) компьютерлік ақпаратқа заңсыз қол жеткізу жолымен ақшалай қаражат пен материалдық құндылықтарды ұрлау;

6) Еңбек жанжалдарына байланысты ақпаратты жою, бұғаттау немесе өзгерту;

7) контрафактілік даналарды көшіру және пайдалану мақсатында компьютерлерге арналған бағдарламаларды қорғаудың бағдарламалық-техникалық құралдарын еңсеру;

8) компьютерлер үшін зиянды бағдарламаларды тарату.

Қорытындылай келе, әмбебап хакерлік жүйені құру мүмкін емес сияқты, мүлдем тұрақты қорғаныс жүйесін құру мүмкін емес деп айтуға болады. Сондықтан, қорғаныс жүйесін қолданған кезде оның қолданылу аясын және әртүрлі біліктілік пен жабдықтағы зиянкестердің әсеріне қарсы тұру қабілетін нақты көрсету қажет. Компьютерлік қылмыс мәселесін әзірлеу және онымен күресу әдістерін табу-бұл уақыт пен тәжірибе мәселесі. Аталған проблемаларды жан-жақты зерттеу қажеттілігі тергеу практикасының қажеттілігімен де, қылмыстық-құқықтық және сот-медициналық теорияны одан әрі жетілдіру, олардың компьютерлік қылмысқа қарсы күрестің тиімділігіне әсерін күшейту міндеттерімен де байланысты.

Әдебиет

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.



ТУРГУНБАЕВА

Альбина Маратқызы

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
қылмыстық құқық және криминология кафедрасының оқытушысы, з.ғ.м., полиция капитаны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ КИБЕРҚЫЛМЫС ДИНАМИКАСЫНЫҢ ЕРЕКШЕЛІКТЕРІ ЖӘНЕ ОНЫҢ АЛДЫН АЛУ МӘСЕЛЕЛЕРІНЕ ӘСЕРІ

Мақалада 2018-2021 жылдар аралығында Қазақстан Республикасындағы ақпараттандыру және байланыс саласындағы қылмыстың жай-күйін ашатын статистикалық деректерге талдау жүргізілді. Интернет-алаяқтықпен байланысты құқық бұзушылықтарға ерекше назар аударылады. Елдегі киберқылмыстың жай-күйі туралы түсінік қалыптастыратын негізгі көрсеткіштер талданды. Кибернетикалық қылмыс саласында тіркелген құқық бұзушылықтар санымен қатар, өндірістегі қылмыстық істердің; сотқа жіберілген қылмыстық істердің; тоқтатылған сотқа дейінгі тергеулердің санына талдау жүргізілді. Алынған деректерді талдау негізінде осы саладағы қылмыстардың жекелеген түрлерінің алдын алу жөніндегі қызметтің тиімділігі туралы қорытынды жасалды, бірақ интернет-алаяқтықтың алдын алу мен жолын кесудің теріс тенденциясы анықталды. Осыған байланысты ақпараттандыру және байланыс саласындағы қылмысқа қарсы іс-қимыл мәселелерінде құқық қорғау органдары мен сот жүйесінің қызметін жетілдіру жөніндегі шараларды күшейту ұсынылады.

Ішкі істер органдарының практикалық қызметінің мазмұны нақты басқару шешімдерін қабылдауға да, қолда бар күштер мен құралдарды бөлуге және үйлестіруге де әсер ететін қолданыстағы Қылмыстық жағдаймен анықталады. Осыған байланысты Ішкі істер органдары үшін қылмыстың ағымдағы жай-күйін және оның өзгеру динамикасын талдау әрқашан өзекті болып табылады. Қазіргі жағдайда киберқылмыс деп аталатын ақпараттық технологиялар саласындағы қылмыстық іс-шаралар қарқын алуда. Бүгінгі таңда интернет күнделікті өсіп келе жатқан кеңістікті білдіреді, онда пайдаланушыларға ақпарат іздеуден гөрі көп мүмкіндіктер беріледі. Қылмыстық жоспарларын жүзеге асыру үшін интернет-ресурстарды пайдалана отырып, қылмыстық элементтер де өз жағдайларын жіберіп алмайды, олар қылмыстық заңмен тыйым салынған әрекеттерді жасайды. Көптеген киберқылмыскерлер компьютерлік және смарт технологияларды тек пайдаланушы ортасына ғана емес, сонымен қатар банктік және төлем жүйелеріне де ену үшін пайдаланады. Хакерлер дербес деректерді, инсайдерлік ақпаратты, коммерциялық құпияны және қорғалатын басқа да мәліметтерді жинау мақсатында смартфондарды, гаджеттерді және әртүрлі ақпараттық базаларды қорғауды бұзады заңмен. Осыған байланысты профилактикалық және алдын алу қызметінің маңызды элементі ақпараттық қауіпсіздікті қамтамасыз ету болып табылады. Бұл аспектіні қазақстандық және шетелдік авторлар көрсетеді [1, 60-бет; 2, 40-бет; 3, 67-бет; 4, 26-бет; 5, 399-бет; 6, 645-бет]. Алайда, бұл мәселе жеке зерттеуді қажет етеді және ұсынылған мақаланың тақырыбынан асып түседі.

Біздің міндетіміз – «киберқылмыс» ұғымының мағынасын анықтау және оның негізгі түрлерінің динамикасын талдау. Киберқылмыс сияқты қылмыстық құқық бұзушылықтың

көптеген анықтамалары бар. Анықтаманың өзіндік ерекшелігін талап етпестен, жеке авторлардың зерттеулерінде көрсетілген көзқарастарды қорытындылай келе [7-10], біз осы мәселе бойынша өз көзқарасымызды тұжырымдадық. Сонымен, біздің ойымызша, киберқылмыс деп киберкеңістікте компьютерлік жүйелер немесе компьютерлік желілер, сондай-ақ компьютерлік жүйелер немесе желілер шеңберіндегі киберкеңістікке қол жеткізудің басқа құралдары, сондай-ақ компьютерлік жүйелерге, компьютерлік желілерге немесе компьютерлік деректерге қарсы жасалған қылмыстық құқық бұзушылықтардың жиынтығын түсіну керек.

Киберқылмыс – бұл шекарасы жоқ және оны шешуді талап ететін, оның ішінде жазалау санкцияларымен қатар алдын алу және профилактикалық аспектіні көздейтін қылмыстық-құқықтық шараларды қолдану арқылы жаһандық проблема екенін атап өткен жөн.

Киберқылмыстың әлемдік ауқымын бағалай отырып, әлемнің әртүрлі аймақтарында 40 миллионға жуық киберқылмыскерлер жұмыс істейді деп айту керек, олардың әрекеттері миллиардтаған долларға бағаланады [11].

Аталған жағдайлар таңдалған тақырыптың өзектілігін анықтайды, өйткені киберқылмыстар санының өзгеруін зерттеу оларға қарсы іс-қимыл шараларын іске асырудың тиімділігін бағалауға және елдегі киберқылмыстың жай-күйі туралы қорытынды жасауға және киберқылмысқа қарсы күресті жетілдірудің одан әрі бағыттарын анықтауға мүмкіндік береді.

Мақалада 2018-2021 жылдар аралығындағы Қазақстан Республикасындағы (ҚР) киберқылмыс динамикасы, Қылмыстық кодекстің 7-тарауында көзделген қылмыстық құқық бұзушылықтарды талдаумен қатар (ҚР ҚК 205, 206, 207, 208-баптары және т. б.) ҚР ҚК 190-бабының 2-бөлігінің 4-тармағында көзделген іс-әрекет зерттелді. Бұл тәсіл ақпараттық жүйені пайдаланушының көмегімен қылмыс жасау тәсілі киберқауіпсіздік мәселелерімен тікелей байланысты екендігіне байланысты [12; 13; 14].

Статистикалық деректерді талдау көрсеткендей, 2018 жылдан 2021 жылға дейінгі кезеңде Қазақстан Республикасында ақпараттандыру және байланыс саласында 364 қылмыстық құқық бұзушылық және 43911 интернет-алаяқтық жасалған [15] (кесте. 1).

Кесте 1

2018-2021 жылдар аралығында тіркелген киберқылмыстар туралы ақпарат

Қылмыстық құқық бұзушылық түрі	Барлығы ЕҚДБ-да тіркелген				Барлығы
	2018	2019	2020	2021	
ҚР ҚК 190-бабының 2-бөлігінің 4-тармағы «ақпараттық жүйені пайдаланушының сенімін алдау немесе теріс пайдалану жолымен жасалған алаяқтық»	517	7769	14220	21405	43911
Ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге заңсыз қол жеткізу (205-бап)	28	59	71	46	204
Ақпаратты заңсыз жою немесе өзгерту (206-бап)	13	6	12	9	40
Ақпараттық жүйенің немесе ақпараттық-коммуникациялық желінің жұмысын бұзу (207-бап)	5	6	4		15
Ақпаратты заңсыз иемдену (208-бап)	11	16	8	9	44
Ақпаратты беруге мәжбүрлеу (209-бап)	1				1
Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату (210-бап)	4	4	4	4	16
Қолжетімділігі шектеулі электрондық ақпараттық ресурстарды заңсыз тарату (211-бап)	7	8	8	5	28
Заңсыз мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін қызметтер көрсету (212-бап)	1	2			3
Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абонентті сәйкестендіру құрылғысын заңсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды жасау, пайдалану, тарату (213-бап)	2	7	2	1	12
Барлығы	589	7877	14325	21479	44274

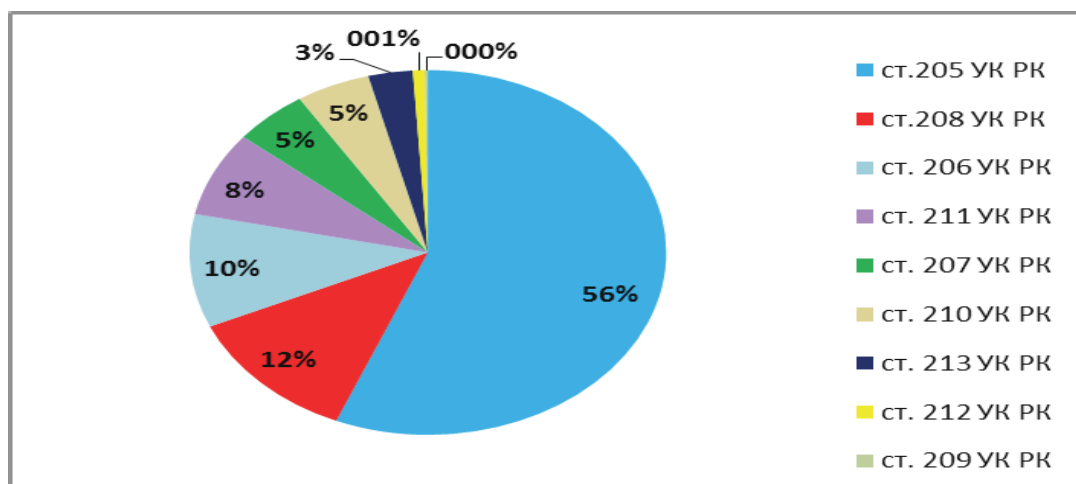
Жоғарыда келтірілген мәліметтерден қылмыстық құқық бұзушылықтардың ең көп тіркелуі интернет-алаяқтыққа байланысты істер бойынша байқалады. Жалпы, ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтар бойынша жыл сайын айтарлықтай тіркеледі интернеттегі алаяқтық туралы істерге қарағанда фактілер аз (кесте. 1). Неғұрлым егжей-тегжейлі зерттеу үшін, сондай-ақ тіркелген қылмыстық істердің сандық арақатынасындағы жеткілікті үлкен алшақтыққа байланысты, Интернет-алаяқтықтан бөлек, ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтарды талдаған жөн.

Сонымен, киберқылмыс динамикасын зерттей отырып, ҚР ҚК 7-тарауында көзделген ең көп таралған қылмыстық құқық бұзушылықтардың үштігіне мыналар кіретінін атап өткен жөн:

- 1) ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге заңсыз қол жеткізу (ҚР ҚК 205-бабы), оның тіркелу пайызы қаралып отырған қылмыстық құқық бұзушылықтардың жалпы процентінің 56% құрайды;
- 2) ақпаратты заңсыз иемдену (ҚР ҚК 208-бабы), оны тіркеу пайызы 12%;
- 3) тіркелу пайызы 10% құрайтын ақпаратты заңсыз жою немесе өзгерту (ҚР ҚК 206-бабы).

Ең аз таралған қылмыстарға барлық басқа қылмыстық құқық бұзушылықтар кіруі керек, өйткені олардың тіркелу пайызы 1-ден 8%-ға дейін (сурет. 1.)

Бұл ретте, 2019-2020 жылдары қаралатын іс-әрекеттерді жалпы тіркеудің байқалып отырған өсуіне қарамастан (50%-ға), 2021 жылы ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтарды тіркеу көрсеткіші 2018 жылғы белгілерге оралды.



Сурет. 1. 2018 жылдан 2021 жылға дейінгі кезеңде ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтарды тіркеудің пайыздық мәндері.

Қарастырылып отырған барлық қылмыстық құқық бұзушылықтар бойынша тіркеудің өсуі (2019 және 2020 жж.) және одан кейінгі төмендеуі (2021ж.) байқалады, бұл біздің ойымызша, тіркеудің кезекті секірісінен кейін жүргізілетін қылмыстардың алдын алу және алдын алу шараларымен түсіндіріледі.

Интернет-алаяқтыққа келетін болсақ, оларды тіркеу ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтардың жалпы санынан бірнеше есе көп. Сонымен қатар, 2018 және 2021 жылдардағы көрсеткіштерді салыстыра отырып, біз қылмыстардың 40 еседен астам өскенін байқаймыз (сурет. 2) [16].



Сурет. 2. 2018-2021 жылдар аралығында интернет-алаяқтықтарды тіркеу фактілерінің өсуі

Интернеттегі алаяқтықты тіркеудің өсуін байқай отырып, бір жағынан, осы әрекеттердің алдын алу және алдын алу бойынша жүргізіліп жатқан шаралардың жеткіліксіздігі және тиімділігінің аздығы туралы қорытынды жасауға болады; екінші жағынан, азаматтардың сенімділігі мен құқықтық сауатсыздығы туралы, алаяқтық мобильді қосымшалардың бақылаусыз таралуы, қаржылық интернет-пирамидалардың ашық жарнамасы туралы, төлем интернет-платформаларының қолданыстағы киберқорғау шараларының тиімділігі аз, Киберқауіпсіздік бойынша мамандардың жетіспеушілігі және т.б.

Қарастырылып отырған барлық әрекеттерді тіркеу көрсеткіштерімен қатар, киберқылмыс динамикасын сипаттайтын тағы бір элемент-ашылу коэффициенті. Қазақстан Республикасында бұл көрсеткіш интернет-алаяқтық туралы істер бойынша 31,65% – РК және ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылық жасау фактілері бойынша басталған барлық қылмыстық істер бойынша 72,7% – по құрайды. Бұл көрсеткіш сотқа жіберілген қылмыстық істердің және іс жүргізу тоқтатылған қылмыстық істердің пайызынан қалыптасады. Айта кету керек, деректерді талдау және пайыздық арақатынасты есептеу кезінде ЕҚДБ-да белгілі бір кезеңде тіркелген қылмыстық істердің саны емес, іс жүргізудегі қылмыстық істердің, оның ішінде өткен жылдардағы қылмыстық істердің саны ескерілді, бұл дәлірек динамиканы көрсетеді.

Кесте 2

Өндірістегі, сотқа жіберілген және 2018-2021 жылдары тоқтатылған, интернет-алаяқтық фактілері бойынша басталған қылмыстық істердің саны,және пайыздық көрсеткіш

фактілері бойынша басалан қылмыстық істердің саны және пайыздық көрсеткіші												
Интернеттегі алаяқтық	2018			2019			2020			2021		
	Өндірісте барлығы	Сотқа жіберілді	Аяқ	Өндірісте барлығы	Сотқа жіберілді	Аяқ	Өндірісте барлығы	Сотқа жіберілді	Аяқ	Өндірісте барлығы	Сотқа жіберілді	Аяқ
	535	127	142	8210	669	1581	15058	1683	1950	23351	3054	2858
	Ашылу пайызы			Ашылу пайызы			Ашылу пайызы			Ашылу пайызы =25%		
Ашудың жалпы пайызы=31,65%												

Кесте 3

ҚР ҚК 7-тарауында көзделген, іс жүргізудегі, сотқа жіберілген және тоқтатылған қылмыстық құқық бұзушылық фактілері бойынша қылмыстық істердің саны 2018-2019 жж. және олардың ашылуының пайыздық көрсеткіші

Қылмыстық құқық бұзушылық	2018				2019			
	Өндірісте барлығы	Сотқа жіберілді	Аяқ	ашылу%	Өндірісте барлығы	Сотқа жіберілді	Аяқ	ашылу%
Барлығы	168	6	83	52,9%	147	11	92	70%
ҚР ҚК 205-бабы	89	1	29	33,7%	77	0	42	54,5%
ҚР ҚК 206-бабы	31	3	18	67,7%	14	1	13	100%
ҚР ҚК 207-бабы	7	0	7	100%	8	2	2	50%
ҚР ҚК 208-бабы	15	1	5	40%	22	7	13	91%
ҚР ҚК 209-бабы	1	0	0	0%	1	0	1	100%
ҚР ҚК 210-бабы	7	0	7	100%	4	1	3	100%
ҚР ҚК 211-бабы	14	1	13	100%	13	0	10	77%
ҚР ҚК 212-бабы	1	0	0	0%	2	0	1	50%
ҚР ҚК 213-бабы	3	0	3	100%	7	0	7	100%

Кестелерде келтірілген деректерді талдау келесілерді анықтауға мүмкіндік береді:

1) ақпараттандыру және байланыс саласында жасалған құқық бұзушылық фактілері бойынша тергеп-тексерілетін қылмыстық істерді ашудың ең жоғары пайызы (75-тен 100%-ға дейін) баптарда көзделген іс-әрекеттерге келеді:

– 2018 жылы ҚР ҚК 207, 210, 211 және 213;

– 2019 жылы ҚР ҚК 206, 209, 210, 213;

– 205, 207, 208, 211, 213 ҚР ҚК 2020 ж.;

– 2021 жылы ҚР ҚК 212-бабынан басқа барлық қылмыстық құқық бұзушылықтар бойынша.;

2) ақпараттандыру және байланыс саласында жасалған құқық бұзушылық фактілері бойынша тергеп-тексерілетін қылмыстық істерді ашудың ең аз пайызы (75%-ға дейін) баптарда көзделген іс-әрекеттерге келеді:

– 2018 жылы ҚР ҚК 205, 206, 208, 209;

– 2019 жылы ҚР ҚК 205, 207, 212;

– 2020 жылы ҚР ҚК 206, 210;

– 2021 жылы ҚР ҚК 212;

– ашудың нөлдік пайызы тек 2018 жылғы 209 және 212-баптар бойынша, тағы да 2020 және 2021 жылдардағы ҚР ҚК 212-бабы бойынша байқалады.;

– интернет – алаяқтықпен байланысты қылмыстық құқық бұзушылықтар бойынша ашудың ең жоғары проценті келесі үш жыл ішінде (2019-2021 жж.) 2018 жылы ғана байқалады. Ашылудың ең төменгі пайызы 2020 жылға келеді (24%).

Аталған тұжырымдар жалпы алғанда, ҚР ҚК 7-тарауының баптарында көзделген қылмыстық құқық бұзушылықтарды жасау фактілері бойынша алдын алу және алдын алу бойынша жеткілікті тиімді жұмыс жүргізіліп жатқанын, оның нәтижелері қылмыстық құқық бұзушылықтарды ашудың жоғары пайызы және оларды жасау фактілерін қысқарту болып табылатынын айғақтайды.

Сонымен қатар, келесі қылмыстық құқық бұзушылықтарды назардан тыс қалдыруға болмайды:

– зиянды компьютерлік бағдарламаларды құру және пайдалану (ҚР ҚК 210-бабы). Осы құқық бұзушылықты тіркеу талданатын кезең бойы тұрақты, бұл осы қылмыстық құқық бұзушылықтардың алдын алу жөніндегі жұмыстың жеткіліксіздігін көрсетеді;

– интернет-ресурстарды орналастыру үшін қызметтер ұсыну,

– заңсыз мақсаттарды көздейтін (ҚР ҚК 212-бабы), оның ашылу пайызы нөлдік көрсеткішке ие.

Осыған байланысты жоғарыда аталған қылмыстық құқық бұзушылықтарды анықтау және олардың алдын алу жөніндегі жұмысты жандандыру қажет.

Тиісінше, жүргізілген зерттеу нәтижелері ҚР ҚК 7-тарауында көзделген қылмыстық құқық бұзушылықтар бөлігінде белгілі бір оң динамиканы көрсетеді, алайда интернет-алаяқтықтарды тіркеумен және ашумен байланысты жағдай көп нәрсені қалайды.

Себептердің басым көпшілігі, жоғарыда айтылғандай, объективті сипатта болғанына қарамастан, анықталған теріс үрдіс интернет-алаяқтыққа қарсы күрес жөніндегі шараларды жетілдіру, тергеу органдары қызметінің тиімділігін арттыру және осы әрекеттердің алдын алу және алдын алу бойынша нәтижелі жұмыс жүргізу қажеттігін тағы да дәлелдейді.

Әдебиет

1. Баширов А. Қазақстан Республикасындағы ақпараттық қауіпсіздік мәселелері / / қазіргі заманның өзекті мәселелері. 2015. №4 (10). 59-61 бет.

2. Хан Т.А., Жиенбеков Ж.Е. ақпараттық қауіпсіздікті қамтамасыз ету жүйесі / / қазіргі заманның өзекті мәселелері. 2016. №2 (12). 37-43 бет.

3. Жетпісов А.Ж. қылмыстарды анықтауға және ашуға байланысты қызмет саласындағы ақпаратты қорғау қажеттілігі туралы // қазіргі заманның өзекті мәселелері. 2018. №3 (21). Б. 68-72.

4. Новичков В.Е., Пухтин И.Г. Ресей Федерациясының маңызды ақпараттық инфрақұрылымына заңсыз әсер еткені үшін қылмыстық жауапкершілікті енгізудің әлеуметтік-құқықтық негіздемесі // құқық қорғау органдарындағы Психопедагогика. 2018. №2 (73). 25-29 бет.
5. Шабуров А.С., Зонова В.Э., Рыжук Н.С. ақпарат қауіпсіздігін қамтамасыз ету жөніндегі талаптарға сәйкес сыни ақпараттық инфрақұрылымды қорғау // Инновациялық технологиялар: теория, құралдар, практика. 2018. Т.1. 397-403 ББ.
6. Курбатов Н.М. Ресей Федерациясының маңызды ақпараттық инфрақұрылымының қауіпсіздігін қамтамасыз етудің құқықтық және ғылыми негіздерін қалыптастыру туралы // удмурт университетінің хабаршысы. Серия: Экономика және құқық. 2019. Т. 29. №5. 644-654 ББ.\
7. Герке Марко. Киберқылмысты түсіну: құбылыс, міндеттер және заңнамалық жауап. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime> 2014r. pdf (қол жеткізілген күні: 08.02.2022);
8. Михайлов Б.П., Хазов Е.Н., Богданов А.В. және т.б. қылмыстық іздестіру бөлімшелерінің киберқылмысқа қарсы іс-қимылының ерекшеліктері: оқу құралы. – М.: Бірлік-Дана, 2016. 151 б.
9. Кияутин В.Г., Новиков А.П. киберқылмыспен, кибертерроризммен және адам трафигімен күресті құқықтық реттеу: Еуропалық Одақтың тәжірибесі. – Бішкек; – Мәскеу: Қырғыз-Ресей Славян университеті, 2010. 240 б.
10. Хан Т.А., Нұркеев А.Ж. компьютерлік қылмысты анықтаудың заманауи тәсілдері және компьютерлік қылмыстардың ерекшеліктері / Алтай мемлекеттік университетінің жаңалықтары. 2017. №6 (98). 105-111 ББ.
11. Ресей электрондық коммуникациялар қауымдастығы (РАЭК). Жаһандық киберқауіптер: цифрлық инфрақұрылымды қауіпсіз дамыту мүмкін бе? URL: (<http://raec.ru/live/raec-news/9471/>) (өтініш берген күні: 09.02.2022).
12. Ақпараттық портал «Zakon.kz» интернет-алаяқтар қазақстандықтарды қалай алдайды. URL: <https://www.zakon.kz/4927774-kak-internet-moshenniki-obmanyvayut.html> (өтініш берген күні: 09.02.2022).
13. «Tengrinews» жаңалықтар порталы. Қазақстанда интернет-алаяқтықтардың саны күрт өсті (22.01.2021 ж.бастап). URL: <https://tengrinews.kz/crime/kolichestvo-internet-moshennichestv-rezko-vozroslo-454633/> (қол жеткізілген күні: 09.02.2022).
14. А. Горбунова ИМ-де Қазақстандағы интернет-алаяқтықтың ең танымал түрлері туралы айтты / Forbes Kazakhstan. URL: https://forbes.kz/process/probing/samyie_populyarnyie_vidyi_internet-moshennichestva_v_kazahstane_nazvali_v_mvд (қол жеткізілген күні: 09.02.2022).
15. Статистикалық деректер-2018-2021 жылдардағы қылмыстық құқық бұзушылықтар туралы мәліметтер. URL: <https://qamqor.gov.kz> (өтініш берілген күні 09.02.2022).
16. Алмазов А. киберқылмыс-Қазақстан Республикасының қауіпсіздігіне жаңа Қылмыстық қатер / Қазақ ұлттық университетінің хабаршысы. Серия заңды. 2018. Т. 88, №4. 142-151 ББ.



ЕРГАЛИЕВА

Кулянда Сагиповна

старший преподаватель, кафедры уголовно-правовых дисциплин
Атырауского университета им. Х. Досмухамедова, м.ю.н.

СОВРЕМЕННЫЕ ПОДХОДЫ ПРОФИЛАКТИКИ БЫТОВОГО НАСИЛИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

Проблема бытового насилия на сегодняшний день актуальна не только в Казахстане, но и во всем мире. Согласно официальным данным Комитета по статистике Министерства Национальной экономики Республики Казахстан, в среднем по регионам более 17% женщин в возрасте от 18-75 лет подвергались физическому или сексуальному насилию, 21% – психологическому насилию, 7% – экономическому. Более половины жертв бытового насилия считают, что физическое и сексуальное насилие оказало большое отрицательное влияние на их здоровье в дальнейшем. Зловредность негативных последствий насилия трудно, а зачастую невозможно оценить. Как определить цену унижений и мучений человека, ставшего жертвой насилия в семье? Помимо физических, психических и моральных страданий жертва насилия испытывает чувство незащищенности, что, в свою очередь, порождает неверие в собственность государства обеспечить конституционные права, и, в частности, личную безопасность своих граждан. В такой ситуации одно лишь декларирование Конституцией любого государства прав и свобод человека и гражданина как высших ценностей недостаточно. Нужны конкретные меры. Вместе с тем, то, что испорчено семьей и в семье, очень трудно, зачастую, невозможно «исправить» с помощью других институтов социального контроля [1].

Исследования показали, что от 20 до 70% женщин, подвергшихся жестокому обращению в семье, никогда не говорили об этом другому человеку до того, как их опросили при проведении исследования. Те же, кто обращается за помощью, чаще идут к родственникам, друзьям, чем в учреждения, только меньшинство обращается в милицию.

С зарождением гражданского общества начало изменяться отношение к женщине. Стал повышаться ее социально-правовой статус и укрепляться защита ее прав и свобод. Однако это сложный и долговременный процесс, требующий постоянного стимулирования. Обыденное создание консервативно, а правовые системы о современизируются, приводятся в соответствие потребностям и гражданского общества тоже медленно.

Проблема насилия против женщин должна рассматриваться в контексте широкой проблематики насилия вообще. Она «неявляется характерной исключительно для российского общества. этой проблеме большое внимание уделяют вся мировая общественность и правительства зарубежных стран».

Декларация ООН «Об искоренении насилия в отношении женщин» выделяет три основные сферы жизнедеятельности, в которых распространено насилие в отношении женщин, – это «семья», «работа, учеба» и «досуг».

Не умаляя актуальности проблемы насилия против женщин в сферах работы, учебы и досуга, можно с уверенностью сказать, что насилие против женщин в семье достигло таких мас-

штабов, что подрывает основы жизнедеятельности не только самой семьи, но и разрушает фундамент безопасности нашего общества.

По данным официальной статистики, в каждой четверг той российской семье совершается насилие. Анонимные опросы свидетельствуют, что каждая вторая женщина является жертвой насилия [2].

Насилие в семье ложное социальное явление, а потом у различных формы, в которых оно проявляется. Так, в законопроекте «Об основах социально-правовой защиты от насилия все-мье» указывается, что оно может иметь формы физического, психического, сексуального воз-действия и принуждения. Такое деление может показаться спорным, поскольку «в доктрине уголовного права насилие подразделяется на физическое и психическое», а в законе под термином «насилие», как утверждает Л.Д. Гаухман, подразумевается вообще только физическое насилие.

Однако в рамках криминологической характеристики данного социально-правового явле-ния выделение разнообразных форм насилия позволяет более глубоко рассмотреть все его ас-пекты. Кроме того, следует учитывать, что в международных правовых актах и рекомендациях по защите женщин от насилия используется указанная трехчленная градация форм насилия.

На сегодняшний день до сих пор нет объективной полной картины распространенности насилия в семье, так как в нашей стране учет подобных преступлений не налажен. Отсутствие официальной статистики не случайно. Из-за специфики семейных отношений, в силу объек-тивных и субъективных причин эти преступления являются высоколатентными. Насилие ста-рательно скрывается жертвами от окружающих, которые, в свою очередь, воспринимают его как личное дело каждой семьи. Правоохранительные же органы неохотно принимают заяв-ления и возбуждают уголовные дела по фактам семейного насилия [3].

Многие юристы, педагоги, психологи, социологи отмечают влияние социальной среды на формирование личности несовершеннолетнего преступника. Особое место отводится воздей-ствию микросреды, в том числе семьи. Как показывают данные исследований, большинство несовершеннолетних преступников воспитывались в семьях с социально-негативными свойствами.

Социально негативные свойства семьи отличаются большим разнообразием: воспитание детей в условиях неполной семьи, одним родителем; наличие в семье судимых родственников (родителей, братьев, сестер, бабушек, дедушек); злоупотребление спиртными напитками чле-нами семьи, скандалы, драки, сексуальная распущенность; тяжелое материальное положе-ние, плохие жилищные условия, отсутствие отдельной комнаты для детей, нужда в пита-нии, одежде; низкая правовая культура, правовой нигилизм родителей и других членов семьи; грубость, жестокость, насилие в семье, воспитание детей в условиях эмоционального голода.

По данным профессора В.Н. Кудрявцева, около 35% подростков правонарушителей вос-питывались в неполной или распавшейся семье; в 30% семей таких подростков имели место пьянство, драки, скандалы; 7% взрослые сами совершали преступления, а в 11% отмечалось с их стороны пренебрежительное отношение к труду; в 20% - безразличное отношение к воспи-танию подростков. В результате проведенного А.И. Лебедевой исследования установлено, что каждый четвертый подросток, совершивший преступление или правонарушение, воспитывался в не полной семье.

Профессор Д.А. Шестаков в своих исследованиях обнаруживает у каждого третьего взрослого преступника связь между его преступными наклонностями и негативным влиянием, испытанным им в родительской семье [4].

По мнению профессора Г.А. Аванесова, безнравственность, вирусы потребительства, нера-зумных запросов, эгоизма, карьеризма, пьянства и даже антиобщественного (преступного поведения) чаще всего заражают человека у истоков сознательной жизни – главным образом, в семье.

Ненормальный моральный климат в семье по степени своего воздействия оказывает-ся чрезвычайно опасным для ее членов, особенно для несовершеннолетних и малолетних детей, которым наносится невосполнимый ущерб.

Неблагополучная обстановка в семье и проявление домашнего насилия в отношении несовершеннолетних оказывает негативное воздействие на формирование их личности. В Рос-

сии нет реально действующей программы, способствующей укреплению семьи противодействию домашнему насилию. В качестве сравнительного анализа необходимо отметить активно работающие Великобритании программы, направленные на укрепление семьи, которые преследуют цель устранить, либо значительно ослабить действие семейных факторов риска, связанных отсутствием заботы о детях, жестоким отношением к детям, конфликтами между родителями и детьми. В целом эти программы охватывают детей всех возрастов начиная с младенчества и заканчивая периодом взросления (додостижения 21года-официальный возраст совершеннолетия). Проблема остается нерешенной, безнаказанность приводит к вопиющим случаям бытового насилия с причинением тяжкого вреда здоровью. Предварительный анализ действующих норм позволил прийти к следующим выводам:

во-первых, необходимо усовершенствовать работу государственных кризисных центров для помощи жертвам семейного насилия и оказать дополнительную поддержку не правительственным кризисным центрам;

во-вторых, усовершенствовать применение защитного предписания, запретив совместное проживание жертвы и агрессора, установив запрет на преследование, телефонные звонки психологическое воздействие на жертву.

Совместное проживание заметно снижает эффективность защитного предписания;

в-третьих, в качестве меры принуждения следует дополнительно ввести общественные работы, на мой взгляд, в данной ситуации они были бы более эффективны, чем профилактические беседы или наложение штрафов [5].

в-четвертых, согласно Резолюции, Общественного совета по вопросам деятельности органов семейно-бытовые конфликты возникают на фоне алкогольного или наркотического опьянения.

В этой связи рекомендуется увеличить число центров детоксикации и временной адаптации для правонарушителей.

Министерству здравоохранения необходимо разработать методику проведения психологической коррекционной работы с агрессорами, усовершенствовать методику принудительного лечения от алкоголической и наркотической зависимости. Со стороны медицинских организаций следует оказывать содействие полиции и своевременно сообщать о фактах бытового насилия.

Литература

1. Фатеев А. Противодействие насилию в семье: законодательный опыт Украины // Ученые записки. Серия Право. Криминологические проблемы управления социальным и процессам и в современной России. – Ростов-на-Дону. 2006. – С. 82-83.
2. Гишинский Я.И. Институт семьи в системе «Девиантность – социальный контроль». Криминология: вчера, сегодня, завтра. Труды Санкт-Петербургского криминологического клуба. – СПб., 2002. – С. 40.
3. Насилие и его влияние на здоровье. Доклад о ситуации в мире. ВОЗ. – М., 2003. – С. 101-102.
4. Сидоренко Т.А. О насилии против женщин в семье // Криминологическая характеристика убийств. – М., 1997. – С. 95.
5. Ермакова Л. Признание проблемы-основа ее решения / Специальный выпуск журнала. «Если хочешь быть здоров. – Екатеринбург, 2000. – С. 20.



ҚҰЛАЖАНОВА

Аяжан Нүсіпжановна

Еуразия Технологиялық Университеті, экономикалық-құқықтық технологиялар және қызметтер мектебінің аға оқытушысы, з.ғ.м.

ҰЙЫМДАСТЫРЫЛҒАН ҚЫЛМЫСТЫҢ ҚЫЛМЫСТЫҚ ҚҰҚЫҚТЫҚ АСПЕКТІЛЕРІ

Қазіргі таңда Қазақстан саяси және қоғамдық өмірдің барлық салаларында түбегейлі реформалардың алдында тұр. Социализм мен жоспарлы экономикадан құқықтық және нарықтық экономикаға көшу заңнамаға өзгерістер енгізуді қажет етті. Қылмыстық құқық реформалары қылмыстың жаңа, аса қауіпті түрлерінің пайда болуына байланысты ерекше назар аударуды талап етті.

Қазіргі уақытта бұрынғы КСРО аумағында, атап айтқанда, Қазақстан аумағында мемлекеттің саяси тұрақтылығы мен ұлттық қауіпсіздігіне қатер төндіретін ұйымдасқан қылмыс дамығанын айта аламыз. Сонымен қатар, мемлекеттің экономикалық қауіпсіздігіне де қатер төнді, өйткені қылмыстық топтар заңсыз қаражат алған оларды заңдастыруға кірісті, бұл өз кезегінде көлеңкелі экономика мен сыбайлас жемқорлықтың дамуына әкелді.

Ұйымдасқан қылмыспен күрес Қазақстан Республикасының басым бағыттарының біріне айналуы тиіс, өйткені оның қоғамдық қауіптілігі мен ауқымы әлдеқайда ауыр болуы мүмкін трансұлттық ұйымдасқан қылмысқа айналу қаупі бар.

Ұйымдасқан қылмысқа қарсы күресте қылмыстық құқық жетекші рөл атқаратыны даусыз, өйткені қылмыстық құқық арқылы мемлекет іс-әрекеттің қылмыстылығы мен жазалануын анықтайды. Қылмысқа қарсы күрес саласындағы қылмыстық саясат Қазақстанның ұлттық ерекшеліктерін ескере отырып, шет мемлекеттердің табысты тәжірибесіне сүйене отырып, мемлекеттің қаралып отырған мәселе бойынша ұстанымын бекітуі тиіс күшті қылмыстық-құқықтық институттарға негізделуі тиіс [1].

Бұл тәсіл өз кезегінде мемлекеттің қылмыстық саясатын, оның ішінде ұйымдасқан қылмысқа қарсы күрес саласындағы саясатын іске асыруға негіз болады. Айта кету керек, қазіргі уақытта Қазақстан Республикасының қылмыстық саясатының ерекшелігі Қазақстан Республикасының Қылмыстық кодексіне тиісті баптарды енгізу, сондай-ақ қылмыстық жауапкершілікті белгілеу арқылы ұйымдасқан қылмыстық әрекеттің қоғамдық қауіптілігін біріктіру болып табылады.

Қазіргі кезеңде ұйымдасқан қылмыспен күрес мәселелері осы заңсыз құбылыстың кең таралған және ауқымды сипатына байланысты өте өзекті болып табылады.

Ұйымдасқан қылмыстық әрекеттің заңды және заңсыз жұмыс әдістерінің үйлесімі бар заңды бірлестіктерге айналуы үлкен қоғамдық қауіп болып табылады, бұл өз кезегінде ұйымдасқан қылмыстық қауымдастықтар құрылымына мемлекеттік қызметкерлер мен құқық қорғау органдарының қызметкерлерінің қатысуының жоғары деңгейін анықтайды.

Ұйымдасқан қылмыстық бірлестіктер күнделікті өмірдің бір бөлігіне айналғанын мойындау керек, сондықтан қолданыстағы заңнаманы жетілдіруге, жаңа қылмыстық-құқықтық нормаларды әзірлеуге және табысты іске асыруға негізделген ұйымдасқан қылмысқа қарсы

күрестің арнайы қылмыстық-құқықтық институтын дамытудың өзекті қажеттілігі туындады. шет елдердің тәжірибесі.

Бүгінгі таңда қолданыстағы қылмыстық-құқықтық институттарды одан әрі тереңдету қажеттігі туындап отыр, олардың негізгісі қатысушылық институты болып табылады.

Айта кету керек, отандық қылмыскер үшін заңнама қылмыстық топтың құрамында қылмыс жасауды қатысу институтымен реттеумен сипатталады, ал қылмыстық топ тұрақты негізде адамдардың бірлестігінің болмауына байланысты ұйымдасқан қылмыстық әрекетке кірмейді және, сәйкес тұрақтылықтың сипатты белгісі.

Д.В. Савельев ұйымдасқан қылмыспен күресудің тиімді жүйесінің іргелі негізі құқықтық қызметтің тиісті деңгейі болып табылатынын дұрыс атап көрсетті [2].

Қатысу институты қылмыстық құқықтың орталық институттарының бірі бола отырып, көптеген зерттеулердің объектісі болды. Қылмыстық құқық ғылымында қатысудың нысандары мен түрлеріне қатысты әртүрлі гипотезалар бар. Құқық қорғау саласында, белгілі бір әрекеттің жазасы мен қоғамдық қауіптілігін анықтау барысында біртұтас көзқарастарды қалыптастыру осы мәселені шешуге байланысты.

Басқа ғалымдардың пікірінше, осы типтердің ішіндегі кіші түрлерді анықтау арқылы күрделі қатысушылықты, топтық қылмысты және қажетті қатысушылықты ажыратуға болады.

Біздің ойымызша, қатысушылықтың объективті белгілеріне сүйене отырып, қатысушылықтың екі түрін ажыратуға болады – қарапайым және күрделі.

Қарапайым қатысу деп бірлескен орындауды, ал күрделі қатысуды рөлдерді бөлу арқылы қатысуды түсінеміз.

Өз кезегінде серіктестер арасындағы субъективті байланыстың сипаттамаларына сүйене отырып, қатысушылықтың келесі формаларын ажыратуға болады:

- алдын ала келісімсіз адамдар тобы;
- алдын ала сөз байласу бойынша адамдар тобы;
- ұйымдасқан топ;
- қылмыстық қоғамдастық.

Бұл ретте ұйымдасқан топ пен қылмыстық қоғамдастық қылмыстық әрекеттің ұйымдасқан нысандары ретінде әрекет етеді [3].

Қазіргі уақытта ұйымдасқан қылмысқа қарсы күрестің кешенді қылмыстық-құқықтық институты ұйымдасқан топ туралы нормалармен, атап айтқанда, Қазақстан Республикасы Қылмыстық кодексінің 262-бабында «Ұйымдасқан топты, қылмыстық ұйымды құру және басқару, сондай-ақ оларға қатысу ретінде», Қазақстан Республикасы Қылмыстық кодексінің 263-бабы «Қылмыстық қоғамдастық құру және басқару, сол сияқты оған қатысу», Қазақстан Республикасы Қылмыстық кодексінің 264-бабы «Қылмыстық қоғамдастықты құру және басқару».

Жоғарыда аталған баптарда ұйымдасқан қылмыстық әрекетке қарсы күрестің негізгі ережелері қамтылған.

Осы баптарда көрсетілген барлық қылмыстар қоғамдық қауіптіліктің жоғары дәрежесімен сипатталады және мемлекетке, қоғамға және жеке адамға елеулі қауіп төндіреді.

Ұйымдасқан қылмыстық әрекет өзінің сапалық белгілерін оған қатысушылардың өзара әрекет ету әдісінен алады. Ұйымдасқан қылмыстың террористік ұйымдармен бірігуі қоғамға ерекше қауіп төндіреді.

Қатысу формасы оның сыртқы жағын білдіреді, ол екі немесе одан да көп тұлғаларды бір қылмыстық ұйымға біріктіру механизмін көрсетеді. Қылмыстық топтар мен қауымдастықтар субъектілердің бірлескен қылмыстық әрекетінің нысандарының бірі болып табылады, дегенмен ұйымдасқан қылмыстық әрекет қылмыстық топтардың жиынтығына қарағанда ауқымды құбылыс болып табылады.

Ұйымдасқан қылмыс – қылмыстың ерекше түрі жүйелілігімен, құрылымымен және ерекше функционалдық бағыттылығымен сипатталады.

Қарастырылып отырған ұйымдасқан сипаттағы қылмыстардың түрлері үшін мынадай белгілер тән: ұйымдасқан топ түрінде ғана қатысуда жасалған, ұйымшылдықтың жоғары дәрежесімен сипатталатын; ұйымдасқан қылмыстық топ құрылған кезден бастап қылмыс жасалды деп есептелетін қылмыстардың формальды құрамы.

Кез келген қылмыстық қауымдастықтың негізі ұйымдасқан сипаттағы топ болып табылады. Сонымен бірге бұл қылмыстық бірлестіктер өзіне тән объективті және субъективті белгілерімен ерекшеленеді.

Мысалы, бандаға тән белгілер қарулану мен ұйымшылдық, сондай-ақ ортақ мақсаттың болуы.

Объективті және субъективті белгілері бар ұйымдасқан топ қылмыстық қауымдастықтың құрылуына негіз болады.

Айта кету керек, барлық қылмыстық қауымдастықтың белгілері бірдей емес. Мысалы, банда қару-жарақпен, мақсатпен және ұйымшылдықпен сипатталады.

Айта кету керек, қылмыс жасау туралы алдын ала келісімге қатысты екі негізгі көзқарас бар. Осылайша, бірінші көзқарас бойынша, алдын ала пайда болуы объективті қастандық жүзеге асырылғанға дейін ғана мүмкін болады. Екінші көзқарас, алдын ала келісім қылмыс жасауға дайындалу сатысында жасалады [1].

Біздің ойымызша, алдын ала сөз байласудың ерекшелігі белсенді қылмыстық әрекет басталғанға дейін сыбайластар арасындағы қылмыстық әрекеттерді келісу түріндегі субъективті байланыстың пайда болуы болып табылады. Белсенді қылмыстық әрекет деп нақты қылмыстың объективтік жағының белгілерін қамтитын әрекеттерді жасауды түсінеміз.

Ұйымдастыру қылмыстық топ қатысушыларының іс-әрекеттерін өзара үйлестіру, сондай-ақ олардың арасындағы қарым-қатынасты анықтау туралы хабардар болуын білдіреді.

Өз кезегінде бұл байланыстардың беріктігі топ өзінің алғашқы қылмысын жасағанға дейін пайда болатын тұрақтылықты қалыптастырады.

Тұрақтылық ұйымдасқан топтың жоғары даму деңгейінде де жатыр. Бұл деңгей қылмыстық әрекеттерді жоспарлауға жауапты басшының – менеджердің болуымен анықталады.

Ұйымдасқан топтардың ерекшеліктерінің бірі – олардың назар аударуы белгілі бір қылмыстарды жасау және қылмыстық әмбебап деп аталатын нәрсенің болмауы.

Ұйымдасқан топтардың жетекшілері, әдетте, ең тәжірибелі қылмыскерлер болып табылады, олардың функциялары қылмыстық әрекеттерді жоспарлау, сыбайластар мен объектілерді, қылмыстық әрекеттің құралдарын іздеу болып табылады.

Ұйымдастыру белгісі ұйымдасқан топтың ерекше белгісі емес, өйткені ол алдын ала сөз байласуы бар топқа да тән. Ұйымдастыру-қылмыстық топтың тұрақтылығын құрудың негізі.

Қылмыстық топтың тұрақтылығы ұғымы қылмыстық құқық ғылымында ең көп зерттелген ұғымдардың бірі болып табылады, себебі бұл мәселені шешу қатысушылықтың аса қауіпті нысандарын анықтау үшін қажет [3].

Ұйымдастыру топтың қылмыстық әрекетін жоспарлаудан, оның бағыты мен белгілі бір қылмыстарды жасауға бағытталуынан тұрады.

Адамдар ұйымдасқан топқа кіргенде белгілі бір құқықтар мен міндеттер алады. Сонымен қатар мұндай құқықтар мен міндеттердің тізімі әр топта әртүрлі.

Топ неғұрлым үйлесімді және ұйымдасқан болса, соғұрлым оның мүшелерінің мінез-құлық ережелері қатаң болады. Ұйымдастыру қылмыстық қоғамдастыққа қатысушылар арасындағы тәртіпті, өзара жауапкершілікті және бағыныштылықты дамытуға ықпал етеді.

Қылмыстық қауымдастықтардың әлеуметтік қауіптілігі сонымен қатар олардың заңды және заңсыз әрекеттер элементтерін біріктіруінде, бұл оларға қомақты ақша табуға мүмкіндік береді [4].

Өз кезегінде, бұл қаржылар қылмыстық қауымдастықтың мемлекеттік құрылымдарға енуіне ықпал етеді, сонымен қатар мемлекеттік қызметкерлер мен құқық қорғау органдары қызметкерлерінің сыбайлас жемқорлықты анықтайды.

Сыбайлас жемқорлық қылмыстық қауымдастықтар ұзақ уақыт бойы құқық қорғау органдарының назарынан тыс қалып, ұзақ уақыт жұмыс істеуіне мүмкіндік береді.

Айта кету керек, бұрын қылмыстық қауымдастықтың жетекшілері қылмыс жасауға өздері қатыспағандықтан, қылмыстық жауапкершіліктен жалтарып келген.

Алайда қылмыстық заңнаманың дамуымен оларды қылмыстық қауымдастықты құру және оның қызметін басқару үшін жауапкершілікке тарту мүмкін болды.

Қылмыстық бірлестікті тану үшін заң шығарушы нақты анықтайды қылмыстық қоғамдастықтың ауыр немесе аса ауыр қылмыстар жасау түріндегі мақсаты болуы керек.

Ұйымдасқан қылмыс қоғамға қауіпті зардаптарының ауырлығына байланысты қылмыстың ең қауіпті түрлерінің бірі екені даусыз.

Мемлекет қабылдаған шараларға қарамастан, Қазақстан Республикасында ұйымдасқан қылмысқа қарсы күреске байланысты проблемалардың бар екенін мойындауға мәжбүрміз.

Ұйымдасқан қылмыспен күрес Қазақстан Республикасының басым бағыттарының біріне айналуы тиіс, өйткені оның қоғамдық қауіптілігі мен ауқымы әлдеқайда ауыр болуы мүмкін трансұлттық ұйымдасқан қылмысқа айналу қаупі бар.

Қылмыстық құқық ұйымдасқан қылмысқа қарсы күрес жүйесінің негізгі элементтерінің бірі болып табылады, сондықтан ұйымдасқан қылмысқа қатысты мәселелерді реттейтін қылмыстық-құқықтық институттарды одан әрі дамыту және нығайту қажет.

Қазақстан Республикасының қылмыстық саясаты соңғы онжылдықтарда заң шығарушының қылмыстық заңнаманы ізгілендіру мен адамдардың, ұйымдардың, қоғамның құқықтары мен заңды мүдделерін қылмыстық-құқықтық қорғауды қамтамасыз ету арасындағы тепе-теңдікті іздеуге байланысты күрделі жолдан өтті. Ұйымдасқан қылмысқа қарсы күрес саласындағы қылмыстық саясаттың негізгі бағыттарының бірі ұйымдасқан қылмыс саласындағы тұжырымдамалық аппаратты неғұрлым егжей-тегжейлі реттеу және соның нәтижесінде ұйымдық белгілері бар қылмыстық құқық бұзушылық белгілерін нақтылау болуы тиіс [5].

Ұйымдасқан қылмыс белгісінің өзі Қазақстан Республикасының қолданыстағы қылмыстық заңнамасында көзделген қылмысқа қатысудың түрлері мен нысандарының жеткілікті анық емес реттелуіне байланысты ғылыми пікірталастың нысанасы болып табылады, бұл белгіге белгілі бір дәрежеде тән. Сонымен қатар, қылмыстық заңмен тыйым салынған әрекеттерді жасауға тұлғалардың әрбір бірлестігі ұйымдасқан қылмыстың элементі болып табылмайды.

Қазақстан Республикасы Қылмыстық кодексінің Жалпы бөлімінің нормаларын түсіндіру және одан әрі жетілдіру қажеттілігімен қатар, Қазақстан Республикасы Қылмыстық кодексінің Ерекше бөлімінің нормалары да Қазақстан Республикасының Қылмыстық кодексінің нормаларын кеңейту және кеңінен қолдануды қажет етеді. квалификациялық белгілер жүйесіндегі ұйымдасқан қылмыс белгілері.

Сонымен қатар қылмыстық құқық ұйымдасқан қылмыспен күресуге қатысты барлық мәселелерді дербес шеше алмайды. Қылмыстық-құқықтық институттар бұл жүйенің негізі ретінде қызмет етеді, бірақ, анық, қылмыстық-құқықтық реттеу ұйымдасқан қылмысқа қарсы күрес жүйесінің барлық элементтерін құқықтық реттеумен осы жүйені қосымша реттеуді талап етеді.

Зерттеу нәтижесінде Қазақстан Республикасы 21-29 және 30-39 жас аралығындағы, орта және жоғары білімі бар Қазақстан Республикасының ер азаматтарының ұйымдасқан қылмыстық әрекеттерге қатысуымен сипатталады деген қорытындыға келді.

Әдебиет

1. Уголовный кодекс Республики Казахстан от 03.07.2014 г. №226-V. Справочная правовая система «Параграф».
2. Мауленов Г.С. Организованная преступность в Республике Казахстан и в зарубежных странах. – Астана, 2013. – С. 98.
3. Каиржанова С.Е. Преступность в сфере банковской деятельности: криминологический и уголовно-правовые проблемы. Автореф. дисс.на соиск. учен. степ. д.ю.н. – Астана, 2007. – С. 42.
4. Дамаскин О.В. Коррупция: Состояние, причины, противодействие. – М., 2000. – С. 304.
5. Абдиров Н.М. Казахстан в зеркале проблем организованной преступности и коррупции // Проблемы борьбы с коррупцией и организованной преступностью. – Караганда, 1998. – С. 86-111.



УСЕНБАЕВА

Асемгуль Узакбаевна

Еуразия Технологиялық Университеті,
Экономикалық-құқықтық
технологиялар және қызметтер мектебінің
аға оқытушысы, з.ғ.м.



ҚҰЛАЖАНОВА

Аяжан Нүсіпжановна

Еуразия Технологиялық Университеті,
Экономикалық-құқықтық
технологиялар және қызметтер мектебінің
аға оқытушысы, з.ғ.м.

**ҚОҒАМДЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ
ЖҮЙЕСІН ДАМУ**

Қауіпсіздік – адамның жетекші қажеттіліктерінің бірі. Қауіпсіздік сезімсіз адамның толыққанды өмір сүруі және оның жеке басының дамуы мүмкін емес. Қоғамдық қауіпсіздік азаматтардың өмірін, денсаулығы мен әл-ауқатын, қазақстандық қоғамның рухани-адамгершілік құндылығын және қоғамның тұтастығы мен тұрақтылығы үшін әлеуметтік қамсыздандыру жүйесін нақты және әлеуетті қатерден қорғаудың жай-күйін көрсетеді. Заңдылық пен құқық тәртібі деңгейінің төмендеуімен, оның ішінде қылмыстың өсуімен сипатталатын қоғамдық қауіпсіздікке төнетін қатер мемлекеттің тұрақты дамуына елеулі кедергі болады, экономикалық белгісіздікті арттырады, ұзақ мерзімді инвестицияға кедергі жасайды және заң үстемдігі қағидатына нұқсан келтіреді.

Сондықтан Қазақстан Республикасы ұлттық қауіпсіздігінің 2021-2025 жылдарға арналған стратегиясында құқық қорғау органдары мен сот жүйесі жұмысының тиімділігін арттыру, халықты барлық құқық бұзушылық түрінен қорғау мәселелерін қоса алғанда, азаматтардың, қоғам мен мемлекеттің қауіпсіздігі басты назарға алынды. Елдің әлеуметтік-экономикалық дамуының қазіргі кезеңі адам мен азаматтың құқықтары мен бостандығына, қоғамның материалдық және рухани құндылығына нұқсан келтіру мүмкіндігімен сипатталған қоғамдық қауіпсіздік үшін ықтимал тәуекелді ескеріп, қазіргі құқық бұзушылық профилактикасы субъектілерінің өзара іс-қимыл жасау тетігін өзгерту талап етіледі.

Әділетті Қазақстанның қауіпсіз және құқықтық қоғамын құру бағдары азаматтардың құқықтары мен бостандығын қорғауға бағытталған құқық үстемдігін қамтамасыз етуді, сондай-ақ құқық тәртібін қамтамасыз ету мәселесінде мемлекет пен қоғам арасындағы өзара қатынастың теңдестірілген моделін қалыптастыруды айқындайды.

Киберқылмысқа қарсы іс-қимыл бойынша жүйелі шаралар іске асырылады. Ол үшін халықаралық және ведомствоаралық өзара іс-қимылды күшейту, құқық қорғау органдары жұмысының жаңа форматын енгізу және халық арасында ауқымды ақпараттық түсіндіру жұмысын ұйымдастыру қажет.

Процестерді цифрландыруға және құқық тәртібін қамтамасыз ету саласында қазіргі заманғы IT-құралдарды ендіруге ерекше назар аударылады.

Осылайша, Тұжырымдаманы іске асыру 2029 жылға қарай халықтың қауіпсіздік деңгейінің, қорғалғанын сезінуінің және құқық қорғау органдарына деген сенімінің үнемі жоғарылай беруін қамтамасыз етуге мүмкіндік береді. Бұл ретте Қазақстанның елдегі құқық тәртібінің, сондай-ақ азаматтардың құқықтары мен бостандығын қорғау деңгейін сипаттайтын халықаралық рейтингтердегі позициясы жақсарады.

2024 жылдың 2 қыркүйек күні Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: құқық тәртібі, экономикалық өрлеу, қоғамдық оптимизм» атты Қазақстан халқына Жолдауында көптеген мәселелерді қамтыды. Жолдауда қоғамда заң мен тәртіп идеологиясын терең орнықтыру қажеттігін атап кетті. Цифрлық технологиялардың күнделікті өмірімізге жаппай енуі түрлі алаяқтардың көбеюіне әкеп соқтыруда. Оған бәріміз куә болып отырмыз. Сондықтан, қазір қаржы және экономика негіздерін білу, қарапайым цифрлық дағдыларды меңгеру аса маңызды болып тұр.

Бұл – бүкіл қоғамның және әр адамның қауіпсіздігін қамтамасыз етуге қатысты ең басты талап. Біз сонда ғана Әділетті, Таза және Қауіпсіз Қазақстанды құра аламыз. Осы стратегиялық мақсатымызға жету үшін еліміздің бейбіт өмір сүруіне және тұрақты дамуына қолайлы сыртқы жағдай қалыптастыруымыз қажет. Бұл – қазіргі аса күрделі геосаяси ахуал кезінде өте жоғары кәсібилікті талап ететін дипломатияның міндеті.

Қазақстан бейбіт және теңгерімді сыртқы саясатты қатаң ұстанып келеді. Еліміздің егемендігі мен тәуелсіздігін нығайту, шетелдегі азаматтарымыздың құқықтарын қорғау, ұлттық мүдделерімізді ілгерілету, экономикаға инвестиция тарту – дипломаттарымыздың басты міндеті. Қазақстан Біріккен Ұлттар Ұйымының Жарғысын қатаң ұстана отырып, көп жақты ынтымақтастық орнатуға қашанда дайын екенін паш етіп келеді. Еліміз халықаралық қауіпсіздік және тұрақтылық мәселелерін шешуге белсенді атсалысады.

Көптеген елде, тіпті кейбір дамыған мемлекеттердің өзінде қылмыс пен тәртіпсіздік өршіп тұрғанына қарамастан, біз соңғы жылдары қауіпсіз қоғам құру жолында едәуір жетістікке жеттік. Көшедегі, қоғамдық орындардағы қылмыс пен заңсыздық тыйылып келеді. Дегенмен арқаны кеңге салуға болмайтынын атап өтті [1].

Стратегия – Президент Қасым-Жомарт Тоқаевтың тапсырмасы бойынша енгізілетін мемлекеттік жоспарлаудың жаңа жүйесінің негізгі құжаттарының бірі. Осыған орай құжатта таяудағы бес жылда болуы мүмкін деп болжанып отырған негізгі сын-қатерлерге қарсы іс-қимылға баса мән берілген.

Сонымен қатар Қазақстан Стратегиясында ұлттық қауіпсіздікті нығайтудың негізгі басымдықтары айқындалды. Азаматтардың, қоғам мен мемлекеттің қауіпсіздігі бірінші орынға қойылған. Стратегияда адами капитал саласындағы қауіпсіздікті қамтамасыз етуге, ең алдымен, ұлттың зияткерлік әлеуетін сақтауға және ұлғайтуға назар аударылады. Биологиялық қауіпсіздікті қамтамасыз ету жөніндегі кешенді жұмыстармен бірге қоғамдық денсаулық сақтау ісін дамыту мәселесі де ұлттық қауіпсіздіктің базалық факторларының қатарына енгізілді. Аталған бағыт құқық қорғау органдары мен сот жүйесі жұмыстарының тиімділігін арттыруды, халықты құқық бұзушылықтардың барлық түрінен қорғауды қамтиды. Экономикалық қауіпсіздіктің міндеттері айтарлықтай түзетілді. Қауіпсіздікті қамтамасыз ету тұрақты өсудің жаңа моделіне көшуге, экономиканың технологиялық күрделілігін арттыруға, өнімділігі жоғары жұмыс орындарын ашуға және халықтың табысын арттыру үшін жағдай жасауға байланысты. Атап айтқанда, басты бағыттар азық-түлік қауіпсіздігі, қаржы жүйесінің тұрақтылығы, көлік-транзит саласындағы қатерлерді азайту болып табылады.

Ақпараттық қауіпсіздік саласында кибер қауіптерге қарсы іс-қимыл, қазақстандықтардың жеке деректерін қорғау, ақпараттық инфрақұрылым, стратегиялық нысандар және ұлттық ақпараттық кеңістіктің қорғалу деңгейін арттыру маңызды рөл атқарады.

Қорғаныс қабілетін қамтамасыз ету, ұлттық мүдделерді халықаралық аренада ілгерілету мәселелері ұлттық қауіпсіздіктің дәстүрлі бағыттарының қатарына жатады. Сонымен бірге олардың мазмұны жаңа аймақтық және жаһандық сын-қатерлерге, соның ішінде, гибридті және

асимметриялы сын-қатерлерге байланысты елеулі өзгерістерге ұшырады. Әрбір басым бағыт бойынша алдын алу тетіктері және қатерлердің алдын алу жөніндегі нақты шаралар әзірленді. Олар ұлттық қауіпсіздік тәуекелдерін басқару жөніндегі іс-қимыл жоспары арқылы іске асырылады, сондай-ақ, ұлттық жобаларға және мемлекеттік жоспарлау жүйесінің басқа да құжаттарына енеді.

Қазақстан Республикасының Ұлттық қауіпсіздік стратегиясы болып мемлекеттік жоспарлау жүйесінің ұлттық қауіпсіздікті қамтамасыз ету саласындағы негізгі проблемалар мен қауіп-қатерлерді, стратегиялық мақсаттар мен нысаналы индикаторларды, міндеттер мен нәтижелер көрсеткіштерін айқындайтын құжат танылады. Ұлттық қауіпсіздік дегеніміз адамның және азаматтың, қоғам мен мемлекеттің серпінді дамуын қамтамасыз ететін Қазақстан Республикасы ұлттық мүдделерінің нақты және ықтимал қауіп-қатерлерден қорғалуының жай-күйін айтамыз [2].

Интернет-ресурстар мен әлеуметтік желілерді пайдалану кезінде қауіпсіздік жағын елемеу жеке өмірдің қол сұғылмаушылығы үшін жоғары тәуекелге, көпшілікке қолжетімді дербес деректерді рұқсатсыз пайдалануға немесе модификациялауға, сондай-ақ қолжетімділігі шектеулі дербес деректердің жария болуына немесе олардың қылмыстық қоғамдастықтар немесе олар басқа мемлекеттердің аумағында сақталған кезде барлау құрылымдары үшін эксаумақтық қолжетімділігіне әкеледі.

Ақпараттық қауіпсіздік мәселелері бойынша құқықтық сауаттылықтың төмен болуы және тұрғындардың, АКТ саласы қызметкерлерінің және ұйымдар басшыларының арасында оны арттыруға қалыптасқан қажеттілігінің болмауы ақпараттық салада құқық бұзушылықтар мен қылмыстардың дамуы үшін жарамды негіз туғызады. Құқықтық шектеулер туралы білімнің болмауы басқа азаматтардың құқықтары мен бостандықтарын, авторлық және сабақтас құқықтарды иеленушілердің ақпараттық жасақтамаға құқықтарын бұзатын және ақпараттық ресурстардың жұмыс істеуіне әсер ететін әрекеттерді жасауға болады деген иллюзия туғызады [3].

Ақпараттық технологияларды қолдану арқылы тұрақты сауалнама жүргізіп тұру, сондай-ақ халықпен кездесу қоғамның көңіл-күйін бақылауға, проблемалы мәселелерді анықтауға және оларды шешу бойынша шаралар қабылдауға мүмкіндік береді. Сонымен қатар ПМ-нің азаматтық қоғамды дамыту тұжырымдамасын іске асыру шеңберінде қоғамдық тәртіп пен азаматтардың қауіпсіздігін қамтамасыз ету, заңға бағынатын мінез-құлықты насихаттау жөніндегі арнайы жобаларды іске асыру арқылы үкіметтік емес ұйымдармен, еріктілермен және жергілікті қауымдастықпен сындарлы ынтымақтастығы дамитын болады.

Азаматтардың құқықтық сауаттылығы деңгейін жоғарылатуға және өз құқықтары мен мүддесін қорғау дағдысын дамытуға, құқық бұзушылыққа төзбейтін белсенді азаматтық ұстанымын қалыптастыруға бағытталған мемлекеттің ақпараттық саясаты ұзақ мерзімді стратегияға айналады. Бұл жұмыс адамды мектепке дейінгі мекемелерден бастап өмірдің барлық кезеңінде сүйемелдейді. Тиісті іс-шаралар өмірдің барлық саласын қамтитын елдің стратегиялық құжаттарында бекітілген [4].

Жұртшылықтың қылмыстың алдын алудан хабардар болуын арттыру үшін барлық мемлекеттік органның кәсіби, ақпараттық-түсіндіру жұмысы қажет, бұл халыққа: азаматтардың өз мүлкін, денсаулығы мен өмірін сақтау, сондай-ақ тұрғылықты ауданында қауіпсіздікті қамтамасыз ету бойынша бастапқы шаралар қабылдауға тиіс екенін; көптеген қылмыс конъюнктуралық сипатта болатынын және зардап шегушілердің абайсыздығы мен ұқыпсыздығынан жасалатынын; азаматтар қарапайым және тиімді шараларды өз бетінше немесе көршілерімен бірлесіп қабылдау арқылы қылмыстың алдын ала алатынын ұғынуға көмектесуге тиіс.

Алайда қоғамдағы қауіпсіздікті қамтамасыз ету мәселелеріне қоғамның әрбір мүшесінің рухани мәдениетінің деңгейі әсер ететінін атап өткен жөн. Мұнда құқықтық мәдениет – оның құрамдас бөліктерінің бірі, ол мәдени және құқықтық тәрбие мен оқыту жүйесінің әсерінен қалыптасады. Бұл жерде баланың есейген сайын өз отбасында, мектепте, ортада қандай құндылықтарға ие болатыны маңызды. Күш-жігер нақты проблемаларды талдауға негізделген

және ықтимал зардап шегушілерге немесе құқық бұзушыларға бағытталған нысаналы ақпараттық науқанға бағытталуға тиіс.

Азаматтарды тұрғылықты аудандағы криминогендік ахуал және полицейлер қабылдап жатқан алдын алу шаралары туралы хабардар ету жеке қауіпсіздік пен мүліктің сақталуы үшін алаңдаушылықты азайтуға, сондай-ақ қоғамның белсенді мүшелерін құқық тәртібін сақтауға қатысуға ынталандыруға ықпал ететін болады. Полицияның қоғамдық санаға жағымды ықпал етуде, жауапты және белсенді іс-қимыл жасауының орнықты стереотипін қалыптастыруда (қоғамдық қауіпсіздікті қамтамасыз ету және қылмыстың алдын алу, салауатты, зорлық-зомбылықсыз өмір салтын және әлеуметтік бірлікті насихаттау мәселелері бойынша) бұқаралық ақпарат құралдарымен өзара іс-қимылына ерекше рөл беріледі.

Әдебиет

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: құқық тәртібі, экономикалық өрлеу, қоғамдық оптимизм» атты Қазақстан халқына Жолдауы 20234 жыл 2 қыркүйек // <https://kaz.zakon.kz/kogam-tynysy/6048484-asymzhomart-toaevty-azastan-khalyna-zholdauy-2024-toly-mtn.html>.

2. Қазақстан Республикасының Ұлттық қауіпсіздік стратегиясын әзірлеу, мониторингтеу, іске асыру, бағалау және бақылау жүргізу әдістемесін бекіту туралы Қазақстан Республикасы Ұлттық экономика министрінің 2021 жылғы 1 қыркүйектегі №82 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2021 жылғы 6 қыркүйекте №24227 болып тіркелді.

3. Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысы // <https://adilet.zan.kz/kaz/docs/P1700000407>.

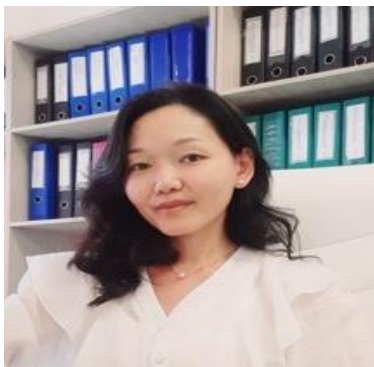
4. Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасын (құқық бұзушылық профилактикасы саласында) бекіту туралы Қазақстан Республикасы Үкіметінің 2023 жылғы 29 желтоқсандағы №1233 қаулысы // <https://adilet.zan.kz/kaz/docs/P2300001233>.



УСЕНБАЕВА

Асемгуль Узакбаевна

Еуразия Технологиялық Университеті,
Экономикалық-құқықтық
технологиялар және қызметтер мектебінің
аға оқытушысы, з.ғ.м.



БАТЫРБЕКОВА

Балнур Каримбаевна

Еуразия Технологиялық Университеті,
Экономикалық-құқықтық
технологиялар және қызметтер мектебінің
аға оқытушысы, з.ғ.м.

**ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ
ЦИФРЛЫҚ ИНФРАҚҰРЫЛЫМЫН ДАМУ**

2024 жылдың 2 қыркүйек күні Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: құқық тәртібі, экономикалық өрлеу, қоғамдық оптимизм» атты Қазақстан халқына Жолдауында көптеген мәселелерді қамтыды. Жолдауда қоғамда заң мен тәртіп идеологиясын терең орнықтыру қажеттігін атап кетті. Цифрлық технологиялардың күнделікті өмірімізге жаппай енуі түрлі алаяқтардың көбеюіне әкеп соқтыруда.

Жолдауда Қазақстанды қауіпсіз әрі жайлы елге айналдыру керектігі айтылды. Құқық қорғау органдарына және басқа да жауапты мекемелерге азаматтардың қауіпсіздігін барынша қамтамасыз ету жүктелді. Ішкі істер министрлігі ұсақ бұзақылық пен вандализмнен бастап, шетелдіктердің заңсыз көшіп келуіне және басқа да ауыр қылмыстарға қатаң тосқауыл қойып, дереу жолын кесуге міндетті. Құқықтық мемлекетте қылмыс әлеміне орын жоқ, қарақшылықты түп-тамырымен жою қажет. Түрлі экстремистердің, оның ішінде әсіре діншілдердің де елге іріткі салатын әрекеттеріне қатысты ұстаным дәл осындай болуға тиіс. Құқық қорғау органдары кәсібилік, батылдық және табандылық танытуы керек. Жол-көлік инфрақұрылымын жақсарту және интеллектуалдық жүйені енгізу арқылы жол қауіпсіздігін қамтамасыз етуге болады. Бұл – жергілікті ғана емес, республикалық жолдарға да қатысты мәселе. Осы салаға жауапты мекеме автокөліктердің техникалық жағдайына тиісті бақылау жасауы қажет. Көптеген елде, тіпті кейбір дамыған мемлекеттердің өзінде қылмыс пен тәртіпсіздік өршіп тұрғанына қарамастан, біз соңғы жылдары қауіпсіз қоғам құру жолында едәуір жетістікке жеткендігін атап кетті [1].

Сонымен қатар, қауіпсіздікті қамтамасыз етудің цифрлық инфрақұрылымын дамыту, Қазақстанда цифрландыру бағытын дамыту «электрондық үкімет» пен «Ақпараттық Қазақстан – 2020» қалыптастыру және дамыту жөніндегі мемлекеттік бағдарламалары арқылы өрбиді.

«Қазақстанның киберқалқаны» тұжырымдаманы іске асыру кезеңінде киберқауіпсіздікте белгілі бір нәтижелерге қол жеткізілді, атап айтқанда сапалы кәсіби қызметтер нарығы құрылды, осы мамандық бойынша білім беру гранттары ұлғайтылды, киберқауіпсіздік мәдениеті арттырылды, «электрондық үкіметтің» ақпараттандыру объектілеріне тәулік бойы мониторинг қамтамасыз етілді. Қажетті нормативтік құқықтық база қалыптастырылды, оның ішінде «электрондық үкімет» объектілері мен ақпараттандырудың аса маңызды объектілері

үшін талаптар белгіленді, бұл ретте киберқауіпсіздік жөніндегі талапты елемеген жағдайда тиісті тексерулер жүргізіледі [2].

Ішкі Істер Министрлігінің алдында тұрған міндеттердің бірі құқыққа қайшы әрекеттің жедел әрі сапалы алдын алуға және жолын кесуге қабілетті қазіргі заманғы техникалық жарактандырылған полиция құру болып табылады. Осыған байланысты қызметтің ашықтығы мен жеделдігін қамтамасыз ететін цифрлық технологияны ендіру жалғасатын болады. Полицияның және Ұлттық ұланның байланыс инфрақұрылымын одан әрі дамыту қажет. «Цифрлық полицей» жобасы шеңберінде полицейлерді жаңа буынның бейнетіркегішімен жарактандыру қажет. Бұл азаматтармен коммуникация кезінде көрсетілетін қызмет сапасын арттыруға және жанжалды жағдайдың туындауының алдын алуға мүмкіндік береді. Бақылауды және полицияның кешенді күштерін үйлестіруді жүзеге асыру мақсатында шағын қалаларда жедел басқару орталығын құру жұмысы жалғасаты болады. Қоғамдық жерлерді полицияның жедел басқару орталығы мен кезекші бөлімімен жалғасқан бейнебақылау камераларымен қамту «Бейнебақылаумен толық қамту» жобасының арқасында жүзеге асырылатын болады. Шешім қабылдаудың жеделдігін арттыру үшін ішкі істер органдарының жедел-қызметтік және талдамалық қызметі үшін ақпараттық кешен құру қажет. Байланыс инфрақұрылымын жақсарту қылмыстық сот ісіне қатысушылардың құқықтары мен бостандығын қорғауды қамтамасыз етіп, электрондық форматта сапалы тергеп-тексеруге жағдай жасайды.

Қазіргі заманғы ақпараттық-коммуникациялық технология полицияның қоғаммен әріптестік қатынас орнатуына, азаматтармен кері байланысты ұйымдастыруға ықпал етеді. Хабар қабылдаудың бірнеше арналы жүйесі арқылы азаматтардың полицияға арыздану форматы «102» мобильді қосымшасын немесе бейне- немесе аудиохабар жіберу үшін ПМ сайтында және әлеуметтік желіде орналастырылған чат-ботты пайдалануға мүмкіндік береді. Көші-қон саласында құқық бұзушылықтың алдын алу жүйесін құру мақсатында ықтимал тәуекел туралы алдын ала хабардар ету үшін жаңа ақпараттық жүйе ендірілетін болады.

Сонымен бір уақытта ықтимал қатерге жедел ден қоюға мүмкіндік беретін ақпараттық қауіпсіздікті қамтамасыз ету шаралары күшейтілетін болады. Стратегиялық жоспарлау мен дәлелді профилактиканы жүзеге асыру үшін полицияның институционалдық мүмкіндігін дамыту керек.

Дамыған елдер полициясының озық тәжірибесіне сүйеніп, полицияны трансформациялау жөніндегі міндеттерді тиімді іске асыру стратегиялық талдау және жоспарлау жұмысын қайта құруды талап етеді. Бұл: оларды дамыту сценарийін қоса алғанда, қоғамдық қауіпсіздіктің кең контекстін, қазіргі заманғы үрдіс пен қатерді талдауға; құбылмалы жағдайлар мен қоғам сұранысына сәйкес ұзақ мерзімді стратегиялық міндеттерді әзірлеуге, жоспарлауға және оларға қол жеткізуді бағалауға; құзырет, ресурс пен жарактандырылу деңгейінің стратегиялық міндеттерге қол жеткізу және тәуекелді басқару бойынша , жоспарларына сәйкестігі тұрғысынан жұмыс тиімділігін бағалауға (мықты және әлсіз тұстары) бағытталады.

«Нақты» деректер мен ғылыми тәсілдерге негізделген дәлелді талдау құқық бұзушылықтың алдын алу жөніндегі стратегиялық шешімдерді әзірлеуге негіз болады. Осы міндетті іске асыруды қолдау мақсатында Ақпараттық-коммуникациялық технология саласын және цифрлық саланы дамыту тұжырымдамасы шеңберінде мемлекеттік органдардың бүгінгі шашыраңқы ақпараттық жүйесін біртұтас жүйеге интеграциялау жүзеге асырылатын болады. Сонымен бір уақытта ақпарат қауіпсіздігі деңгейін арттыру бойынша шаралар қабылданады.

Ішкі Істер Министрлігінің талдамалық ресурсын орнықты дамыту үшін ведомстволық оқу орындарында мамандар даярлаудың ғылыми әлеуеті мен деңгейін жоғарылатуға бағытталған ведомстволық бағдарлама әзірленетін болады. Осы жұмыс шеңберінде: кадр даярлау және олардың біліктілігін арттыру тәсілдерін өзгерту; IT-салада дағдысы бар криминалогтардың кәсіптік өзегін құру үшін біліктілігі жоғары мамандарды тарту; халықаралық және ұлттық сарапшыларды тартып, ПМ-де ғылыми қызметтің тиімділігін талдау және деректер негізінде құқық бұзушылықтың дәлелді профилактикасына өту үшін ведомстволық ғылымның әлеуетін арттыру бойынша тұжырымдамалық пайымды әзірлеу; ПМ оқу орындарының қызметкерлерін

ғылыми қолданбалы зерттеудің қазіргі заманғы әдісі саласында сертификаттау (оның ішінде қолданыстағы онлайн-платформалар негізінде) болжанады.

Ішкі істер органдарының материалдық-техникалық жарақтандырылуын жақсарту шараларын іске асыру жаңа, технологиялы және құзыретті қазақстандық полицияға айнарудың міндетті шарты болып табылады. Елді мекендердің дамуы, жаппай урбанизация тұрғын секторының кеңеюіне серпін берді. «Жұртқа жақын» полиция қағидатын қамтамасыз ету шеңберінде полицияны материалдық-техникалық жарақтандыруды жақсарту мәселелері кезең-кезеңімен шешілетін болады. Белгіленген талаптарға сәйкес келетін ғимараттарды, қажетті цифрлық құралдарды, полицейлерге техникалық қызмет көрсету, дене шынықтыру даярлығы үшін инфрақұрылымды қоса алғанда, жұмыс және сапалы қызмет көрсету үшін ыңғайлы тұрмыстық жағдай жасау қажет. Өңірлердегі ведомстволық медициналық мекемелерді жаңғыртуға ерекше назар аударылатын болады. Азаматтардың құқықтары мен заңды мүддесін тиімді қорғауды қамтамасыз ету жөніндегі міндеттердің басымдығын ескеріп, бұл іс-шаралар бағдарламалық құжаттарға енгізілетін болады [3].

Мемлекеттік органдардағы ақпараттық қауіпсіздіктің жай-күйіне жауапты қызметкерлердің кәсібилігін арттыру және олар қабылдайтын шараларды тиісті түрде әмбебап ету, кәсіптік стандарттарды бейімдеу, сондай-ақ ақпараттық ресурстар мен жүйелердің қорғалуын бақылау параметрлері мен қорғау профильдерін жақсартатын тәжірибелік дағдылар мен техникалық білімдер бойынша талаптарды кеңейту қажеттігі туындап отыр.

Құқық қорғау органдарының ғылыми-зерттеу ұйымдарын неғұрлым күрделі киберқылмыстарды тергеуге тарту арқылы киберқылмыстылыққа қарсы іс-қимылға техникалық дайындық және кәсіби құзыреттіліктің жоғары деңгейін қалыптастыру және қолдау бойынша міндеттерді шешу қажет.

Отандық әзірлемелердің сұранысқа аса ие болмауы проблемасын жою, өйткені киберқауіпсіздік түптен келгенде отандық IT-саласының және электронды өнеркәсібінің даму деңгейіне байланысты. Мұның себептерінің бірі мемлекеттік органдарда олардың өнімдерін басым түрде пайдалану міндеттілігінің болмауы. Оларды қолдау шараларын белгілеу, оның ішінде мемлекеттік-жекешелік әріптестікті ынталандыру, бәсеке қабілеттілікті арттыру.

Ақпараттық қауіпсіздік жөніндегі уәкілетті орган жанынан Киберқауіпсіздік жөніндегі кеңес құрылуы тиіс, оның негізгі міндеттерінің бірі киберқауіпсіздік бойынша өзекті мәселелерді қарау, басшылыққа алынатын құжаттарды, нормативтік құқықтық базаны өзекті күйінде ұстау, отандық электрондық және софтверлік өнеркәсіп өнімін басым түрде пайдалануға ықпал ету, қоғамдық маңызы бар IT-жобаларға жария бағалау жүргізу болуы тиіс.

Жеке ақпараттық жүйелердің иелері мен меншік иелері өздерінің экономикалық мүмкіндіктеріне қарай, ақпараттық жүйелерді әзірлеудің, жасаудың, сынаудың және пайдаланудың стандартталған процестеріне сүйенуге ұмтылып, олардың ақпараттық қауіпсіздігін қамтамасыз етуге қажетті шаралар қарастыруы тиіс. Бұл үшін қажетті бағдар ретінде қызмет ете алатын техникалық стандарттар мен басқа да нормативтік-техникалық құжаттар бар.

Технологиялық процестерді басқарудың автоматтандырылған жүйелерінің қауіпсіздігін және ақпаратты қорғаудың ұлттық жүйесін қауіпсіз пайдалануды нормативтік-құқықтық және ұйымдастырушылық-техникалық қамтамасыз етуді, құқық қолдану практикасын, әдіснамалық базасын жетілдіру бойынша міндеттерін іске асыру үшін ұсынылады:

Мемлекеттік секторда заңнамамен және техникалық стандарттармен белгіленген ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды мүлтіксіз орындау, сондай-ақ киберқауіпсіздік үшін зиян келтірмей технологиялардың даму серпінін ескере отырып, оларға қажетті өзгерістерді жедел енгізу. Белгіленген талаптарды сақтау пәрменді мемлекеттік бақылау шараларымен қамтамасыз етілуі тиіс.

Ақпараттық ресурстар мен жүйелердің иелерінің бейғамдық және салғырттық танытуына сенетін киберқылмыскерлер мен шетелдік техникалық компьютерлік барлаушылар қызметінің сипатын есепке ала отырып, ақпараттандыру объектілерінің қорғалу жай-күйін толық бағалау үшін қорғалуды бақылаудың техникалық құралдарымен ақпараттық жүйелер мен

ресурстардың жай-күйін тұрақты мониторингтеуге және ақпараттың таралу арналарын (осалдықтарды, вирустарды, троян бағдарламаларын, декларацияланбайтын функциялар мен белгілерді) анықтау бойынша жұмысты жүзеге асыруға ұмтылу қажет.

Жалпы ұлттық ауқымдағы қауіп-қатерлерді тиімді оқшаулау және оларды іске асырудың алдын алу үшін Бірыңғай талаптар мен қолданыстағы «Электрондық үкіметтің» ақпараттандыру объектілерінің ақпараттық қауіпсіздігін, қорғалуын және қауіпсіз жұмыс істеуін қамтамасыз етудің мониторингін жүргізу қағидалары негізінде мемлекеттік сектор үшін ғана емес, сонымен қатар жеке меншіктегі объектілер үшін де бағдар ретінде қызмет ететін басшылыққа алынатын құжаттар әзірлеуді көздеу қажет.

Азаматтар мен бизнестің мемлекеттік органдар көрсететін қызметтерге жоғары сенімін қамтамасыз ету мақсатында заңнамалық деңгейде бағдарламалық өнімдер, байланыс қызметтерін және өзге де ақпараттық-коммуникациялық инфрақұрылым жеткізушілері үшін кемінде үш жыл ішінде сатып алынатын өнімдерге, сатып алынатын өнімдер мен көрсетілетін қызметтерді міндетті техникалық қолдау жөніндегі шешімдерге келісімдерде, конкурстық құжаттамада және техникалық ерекшеліктерде көрсету үшін ақпараттық қауіпсіздік жөніндегі шаралар әзірлеу қажет [4].

Әдебиет

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: құқық тәртібі, экономикалық өрлеу, қоғамдық оптимизм» атты Қазақстан халқына Жолдауы 2023 жыл 2 қыркүйек // <https://kaz.zakon.kz/kogam-tynysy/6048484-asymzhomart-toaevty-azastan-khalyna-zholdauy-2024-toly-mtn.html>.

2. Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасын (құқық бұзушылық профилактикасы саласында) бекіту туралы Қазақстан Республикасы Үкіметінің 2023 жылғы 29 желтоқсандағы №1233 қаулысы // <https://adilet.zan.kz/kaz/docs/P2300001233>.

3. 2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы №269 қаулысы.

4. Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысы // <https://adilet.zan.kz/kaz/docs/P1700000407>.



КАЛИБАЕВА

Наргиз Бахытқызы

Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы
академиясының 2-курс докторанты полиция майоры

ЖЕКЕ ҚҰРАММЕН ТӘРБИЕ ЖҰМЫСЫНЫҢ ҰЙЫМДАСТЫРУШЫЛЫҚ-ҚҰҚЫҚТЫҚ ЖҮЙЕСІ

Қазіргі уақытта ақпарат тәрбие жұмысының құралы ретінде тиімді пайдаланылады, жеке тұлғаға әсер етудің маңызды факторы болып табылады. Тәжірибе көрсеткендей, қызметкерлерге ақпарат беру тек оқу процесін ғана емес, сонымен бірге тәрбие мен дамуды да сипаттайды. Бір нәрсені жақсы білетін адам өзінің білімі мен тәжірибесін тарата алады, демек, басқалармен қарым-қатынасын жақсы жаққа өзгерте алады. Заңдылық идеяларын, заңдылықты сақтау құндылықтарын тарата отырып, қызметкер қоғамның жағдайын өзгерте алады. Сонымен, бұл білімді ақпараттандыру және тарату қабілеті ішкі істер органдарының алға қойған міндеттерін тиімді орындау үшін қолданылатын тәрбие жұмысының маңызды құралы болып табылады.

Ақпараттық-насихаттық жұмыс – бұл ішкі істер органдарының жеке құрамын тәрбиелеу міндеттерін іске асыру құралы, қызметкерлерге қызметтік қызмет үшін қажетті ақпаратты ұсыну және түсіндіру, сондай-ақ қызметкерлерді мемлекеттік құқық қорғау саясатының дұрыстығына сендіру арқылы қызметкерлердің мемлекеттік-құқықтық дүниетанымын қалыптастыруға бағытталған. Жеке құраммен ақпараттық-насихаттық жұмысты ұйымдастыру және жүргізу тәрбие жұмысы бөлімшелеріндегі ақпараттық-насихаттық жұмыс секторына жүйелендірілген [1].

Ақпараттық-насихаттық жұмыс келесі негізгі міндеттерді шешуге бағытталған:

- жеке құрамның мемлекеттік-құқықтық көзқарасы мен сенімін қалыптастыру, қызметкерлердің моральдық-психологиялық жағдайына әсер ету арқылы қоғамдық-саяси өмірдің оқиғаларын, процестері мен құбылыстарын талдау мен бағалауға кәсіби көзқарасты қалыптастыру;

- жеке құрамды кез-келген жағдайда жедел-қызметтік міндеттерді сәтті орындауға жұмылдыру, қырағылық пен құқықтық іс-әрекетке дайын болу жағдайын сақтау, қызметкерлердің қызметтік міндеттерін орындауға оң көзқарас қалыптастыру;

- жеке құрамды жедел ақпараттандыру және осы негізде жағдайдың нақты жағдайларына қатысты жедел-қызметтік міндеттерді ойдағыдай орындау үшін қызметкерлерге қажетті кәсіби білімді, дағдыларды, іскерліктерді өзектендіру;

- қызметтік ұжымдарды саясаттандыруға, әсіресе ауқымды қоғамдық-саяси іс-шараларды дайындау және өткізу кезеңінде, сондай-ақ өңірдегі әлеуметтік-саяси және криминогендік ахуалдың шиеленісуіне жол бермеу;

– жеке құрамды Қылмыстық ортаның теріс ақпараттық-психологиялық әсерінен қорғауды қамтамасыз ету, қызметтік ұжымдарға көрінеу жалған ақпараттың, қауесеттердің, жала жабудың, дүрбелең көңіл-күйінің ену салдарын бейтараптандыру.

Ақпараттық-насихаттық жұмыстың міндеттерін іске асыру кезінде еліміздің жоғары басшылығының, Қазақстан Республикасының Ішкі істер министрінің құқықтық тәртіпті, заңдылықты, қылмыспен күресті қамтамасыз етуге бағытталған шешімдерін; қылмысқа қарсы күрестің өзекті мәселелерін, елде және аймақта қалыптасқан жедел және криминогендік жағдайды ескере отырып, ішкі істер органдарының жедел-қызметтік қызметінің міндеттерін түсіндіруге назар аударылады; ішкі істер органдары қызметкерлерінің батыл және батыл әрекеттерінің мысалдары, жедел-қызметтік қызметтің оң тәжірибесі.

Ақпараттық-насихаттық жұмыстың ерекшеліктері-белсенділік, өзектілік, жүйелілік, кешенділік, динамизм, табыстылық және эмоционалды қанықтылық. Ақпараттық-насихаттық жұмыстың тиімділігі үшін Ақпарат және қоғамдық байланыстар бөлімшелерінің мүмкіндіктерін, жаңа ақпараттық технологиялардың мүмкіндіктерін белсенді пайдалану қажет. Тәрбие жұмысының мүддесі үшін білім беру ұйымдарының ғалымдары мен профессор-оқытушылар құрамынан, дәстүрлі діни конфессиялардың, қоғамдық бірлестіктердің өкілдерінен, өнер және мәдениет қайраткерлерінен, ардагерлер ұйымдарының өкілдерінен қоғамдық дәріс топтары құрылуы мүмкін [2].

Ақпараттық-насихаттық жұмыс мазмұнының сыртқы аспектісі ішкі істер органдарының тәрбие аппараттарының бұқаралық ақпарат құралдарымен, мәдениет және өнер қайраткерлерімен, дәстүрлі діни конфессиялардың өкілдерімен, мемлекеттік билік және жергілікті өзін-өзі басқару органдарының, қоғамдық бірлестіктердің өкілдерімен, әскери іс-қимылдар мен ішкі істер органдарындағы қызметтің ардагерлерімен жеке құраммен тәрбие жұмысы мүддесінде өзара іс-қимылы болып табылады. Мұндай өзара іс-қимыл Ішкі істер органдарының имиджін азаматтардың қызметкерлерді стереотиптік қабылдауы ретінде қалыптастырады және сонымен бірге қызметкерлерді білім беру процесінің маңызды функциясы ретінде өзін-өзі тәрбиелеуге итермелейді. Ақпараттық-насихаттау жұмыстарының осындай саласының тәрбиелік іс-шаралары әртүрлі міндеттерді орындай алады:

- Қазақстан Республикасы ПМ-нің қылмысқа қарсы күрес, құқық бұзушылықтардың алдын алу және жолын кесу саласындағы қызметі туралы ақпаратты Азаматтарға жеткізу;
- ішкі істер саласын реттейтін Қазақстан Республикасының заңнамасындағы өзгерістер туралы қоғамды түсіндіру және ақпараттандыру;
- тұрғындардың ішкі істер органдарына көмек көрсету бойынша белсенді азаматтық ұстанымын қалыптастыру;
- қызметкерлердің ішкі істер органдарындағы қызметтің беделіне деген сенімін арттыру, жеке құрамға таңдаған кәсібі мен Қазақстан Республикасы ПМ-не қатыстылығы үшін намыс сезімін ояту.

Ақпараттық-насихаттық жұмысты жүзеге асыру кезінде бұқаралық ақпарат құралдарымен өзара іс-қимыл маңызды құрал бола алады. Мұндай өзара әрекеттесудің келесі мақсаттары болуы мүмкін:

- ішкі істер органдарының қызмет мүддесі үшін облыстық, өңірлік және жергілікті бұқаралық ақпарат құралдарымен өзара іс-қимылы;
- жастарды патриоттық, құқықтық тәрбиелеу және кәсіби бағдарлау мақсатында өзара іс-қимыл жасау;
- қоғамдағы қалыптасқан әлеуметтік-саяси жағдайды көрсететін қызмет мүдделері үшін қажетті аспектіде жеке құрамға ақпараттық-насихаттық Ықпал етудің жаңа, заманауи нысандарын бастамашылық іздестіру.

Бұқаралық ақпарат ағындарының ішкі істер органдары қызметкерлерінің құндылық бағдарларына педагогикалық әсері ішкі істер қызметкерлеріне кәсіби қызмет мақсатында және қандай да бір ақпаратты алудың өзекті қажеттіліктері мақсатында облыстық, өңірлік және жергілікті бұқаралық ақпарат құралдары ұсынатын ақпаратты бағдарлауға мүмкіндік беретін ақпараттық ортаны құрудан көрінеді.

Ақпараттық орта Ішкі істер органдары қызметкерлерінің мүдделеріне сәйкес әлеуметтік бағыттағы қызметтік қызметті жүзеге асыру үшін кәсіби және әлеуметтік белсенділігін қалыптастыруға ықпал етеді. Егер мұндай орта педагогикалық мақсаттар негізінде ақпараттық-насихаттау жұмысымен қалыптаспаса, онда қызметкердің қарым-қатынасы азаматтық, адамгершілік және кәсіби қасиеттерді тәрбиелеудегі тәрбие жұмысының мақсаттарына қайшы келуі мүмкін [3].

Ішкі істер органдары қызметкерлерінің ақпараттық артықшылықтарын қалыптастыру жөніндегі ақпараттық-насихаттық жұмыстың тәрбиелік әсері ақпараттық ағындарды: әсер ету мақсаттары негізінде модельдеуге; сандық және сапалық өлшеуге; реципиенттермен кері байланысты жүзеге асыруға; жеке педагогикалық міндеттердің сәттерін өзектендіре отырып, ақпаратты қарқынды ағындармен жоспарлы түрде бағыттауға болатындығымен сипатталады. Ақпараттық ортаны құру мақсатында тәрбие іс-шаралары мыналар болуы мүмкін бұқаралық ақпарат құралдарының материалдарын тиімді тарта отырып құрылуы тиіс. Ақпараттық-бағдарлаушы хабарламалар (шежіре, фактілер, айқындаушы ақпарат); басқарушының педагогикалық ықпалының ақпарат ағыны (мемлекеттік саясат тұрғысынан оқиғаларды түсініктемелер мен бағалау, қызметкерлердің топтық пікірін және жеке кәсіби қасиеттерін қалыптастыру); ақпарат теріс балама ақпарат көздерін, қауесеттерді, алыпсатарлықтарды, болжамдарды және негізсіз болжамдарды бейтараптандыру бойынша [4].

Осылайша, реттелген бұқаралық ақпарат ағындары ішкі істер органдары бөлімшелері қызметкерлерінің ақпараттық ортасын қалыптастырады, соның негізінде жеке құрамның моральдық-психологиялық жағдайына тиімді әсер етеді, ішкі істер органдары қызметкерлерінде патриотизм мен кәсіби этика нормаларын, ант беру талаптарын сақтауға деген ұмтылыс қалыптасады, Отанды қорғауға тұрақты моральдық және психологиялық дайындық қалыптасады және Отанды қорғауға тұрақты мотивация сақталады. Сондай-ақ, қылмыстық әлем туралы қажетті объективті және сенімді бағдарлаушы ақпаратты ұсыну және сонымен бірге осындай ақпараттың ақпараттық және психологиялық әсерін бейтараптандыру негізінде қызметтік міндеттерді орындау кезінде қолда бар ақпараттық қажеттіліктерді ескере отырып, қызметкерлерді әлеуметтік бағдарлау жүзеге асырылады.

Әдебиет

1. Сапарғалиев Ғ. ҚР Конституциялық құқығы. – Алматы 1998ж.
2. Баянов Е. Мемлекет және құқық негіздері. – Алматы 2002ж.
3. Сапарғалиев Ғ., Ибраева А. Мемлекет және құқық теориясы. – Алматы 1998ж.
4. Зиманов С. Конституция и Парламент РК. – Алматы 1996



САРБАСОВ

Алихан Ержанович

докторант 2-го курса Алматинской
академии МВД Республики Казахстан
им. М. Есбулатова, м.ю.н, майор полиции



АЙТКЕШ

Айбек Қанатұлы

преподаватель кафедры уголовного права и
криминологии Алматинской академии МВД
Республики Казахстан им. М. Есбулатова,
м.ю.н, м.э.н, майор полиции

СОВЕРШЕНСТВОВАНИЕ МЕЖГОСУДАРСТВЕННОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Будучи долгие годы постиндустриальным, общество, в начале нового тысячелетия становится все более информационным и цифровым. В условиях современного цифрового общества информационные данные представляют из себя важнейший и необходимый компонент его совершенствования и эффективного развития. При этом информационные данные становятся значимыми не только для отдельно взятых людей, но и в целом государств.

Сегодня любой житель планеты обладает правом обращения с информацией любыми законными способами. Для распространения информационных данных не существует границ, они представляют ценность для общества, а их защита представляется важнейшей деятельностью [1].

Вне всякого сомнения, с каждым годом цифровая сфера все более тесно переплетается с нашей повседневной жизнью. Поэтому наличие защищенного цифрового пространства является необходимым условием для оптимального использования возможностей, предоставляемых обществу цифровизацией. Несмотря на то, что цифровизация и информатизация общества благоприятствует инновационному росту, она одновременно несет риски для государственной безопасности, всех заинтересованных сторон. Ежегодно человечество получает все больше информации об угрозах и уязвимостях в цифровой сфере [2].

Согласно экспертным оценкам самые большие угрозы в информационной сфере исходят от террористических организаций и профессиональных преступников. Угрозы со стороны преступников-непрофессионалов (уровня простых пользователей интернет-услугами) в основном ограничиваются кражами конфиденциальной или иной необходимой информации, в то время как профессиональные преступники в основном сосредоточены на цифровом мошенничестве в целях конкуренции между бизнес-структурами, шпионаже, а также на краже информационных данных, обладающих высокой стоимостью [3]. В дополнение к перечисленным угрозам важно подчеркнуть, что человечество также сталкивается и с другими проблемами, возникающими в цифровой сфере, поскольку с каждым годом международный контекст кибербезопасности становится намного шире. В этой связи необходимо отметить, что кибербезопасность отдельных сфер и интересов не может быть обеспечена в одной стране изолированно от всего мирового сообщества и поэтому должна рассматриваться в совокупности всех глобальных телекоммуникационных сетей, а также социально-экономическими, полезными, возможностями, предлагае-

мых цифровизацией. Таким образом, из-за возросшей зависимости и уязвимости киберпродуктов и услуг цифровая устойчивость государств и обществ к киберугрозам в информационной сфере недостаточна и требует своего постоянного мониторинга и существенного совершенствования. Во всем мире финансовые потери из-за киберпреступности продолжают расти. По экспертным оценкам к 2025 году потери от киберпреступлений составит 10,5\$ трлн. Оценки стоимости киберпреступности в Азиатско-Тихоокеанском регионе различаются, но предполагаемые цифры около 81 миллиарда долларов США свидетельствуют о том, что это более серьезная проблема, чем любая страна может решить самостоятельно. Потери казахстанских компаний в результате кибератак составляют менее 800 тыс. тенге (42%). При этом каждая десятая организация теряла от 800 тыс. до 2,4 млн тенге, а в 5% сумма достигает более 8 млн тенге. Однако порой материальный ущерб – далеко не единственная проблема, с которой сталкиваются компании вследствие инцидента. Действия злоумышленников могут нанести серьезный ущерб репутации, что в некоторых случаях имеет большее значение для жизнедеятельности компании, чем финансовые потери [4].

При этом нельзя не отметить то, что, по мнению многих отечественных исследователей киберпреступности, материалы официальных статистических данных не могут в достаточной степени объективно отражать все характеристики (структуру, состояние, динамику и др.) рассматриваемого вида преступлений, совершаемых в нашей стране. Кроме того, уровень латентности рассматриваемых противоправных деяний составляет около 90% и выше [5]. Более того, рассматриваемая категория преступлений имеет достаточно высокий уровень латентности. В этой связи на сегодняшний день феномен киберпреступности имеет огромное влияние на все телекоммуникационные и интернет-системы и становится важнейшей и крупной криминальной проблемой современности. Все вышеперечисленное требует перехода к более решительным глобальным мерам в подходах к обеспечению кибербезопасности.

Не вызывает возражений утверждение отечественных специалистов о том, что современная киберпреступность является не только организованной, высокотехнологичной и причиняющей большой экономический вред, но также при этом обладает высоким латентным характером. Природа рассматриваемого вида преступности носит трансграничный и транснациональный характер на том основании, что киберпреступность не ограничивают государственные границы, а субъекты рассматриваемых преступлений в большинстве своем являющиеся высококлассными специалистами в сфере информационных технологий, по большей части становятся участниками организованных преступных групп [6]. В этой связи перечисленные особенности киберпреступности обязывают субъектов по ее противодействию совершенствовать международно-правовое сотрудничество по обмену различными информационными данными между правоохранительными органами иностранных государств и проводить совместные мероприятия в сфере борьбы с рассматриваемым явлением. Совершенствование международного сотрудничества в рассматриваемой сфере в обязательном порядке должно строиться с участием представителей всего мирового сообщества, что обуславливается как свойствами информационных данных, выступающих объектами киберпосягательств, так и совокупностью основных черт рассматриваемых противоправных деяний. Нельзя не согласиться с мнением международного эксперта в сфере законодательных основ противодействия киберпреступности Штайн Шьольберга, по мнению которого «киберпространство следует рассматривать в качестве пятого общего пространства, наравне с наземным, морским, воздушным и космическим, и оно также требует выработки особых правовых мер в сфере координации международного сотрудничества» [7]. Поэтому в современных условиях международная законодательная база должна способствовать адекватному и своевременному реагированию на новейшие вызовы и угрозы в сфере информационной безопасности. Совершенно понятно, что в современных условиях правовое регулирование борьбы с киберпреступлениями выступает в качестве базиса всего комплекса мер, связанного с противодействием преступности в информационной сфере. В этой связи международным сообществом были подготовлены нормативные правовые акты, направленные на борьбу с киберпреступностью, среди которых особая роль принадлежит региональным нормативно-правовым актам. Ряд положений, которые касаются борьбы с киберпре-

ступностью, также закрепила «Окинавская хартия глобального информационного общества 2000 г.», Глобальная программа кибербезопасности, которую в 2007г. утвердил Международный союз электросвязи, а также ряд других нормативных правовых актов. Сегодня международное сотрудничество стран в сфере противодействия рассматриваемой преступности строится на заключении многосторонних, региональных, двусторонних соглашений. Примером регионального международного соглашения в рассматриваемой сфере следует назвать Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности 2013г. Важно отметить, что «особая роль в консолидации международных усилий по решению важнейших вопросов в сфере информационной безопасности отводилась Конвенцией о преступности в сфере компьютерной информации 2001г., вступившей в силу 1 июля 2004г. дополнительному протоколу к ней от 28 января 2003г., который рассматривает вопросы в сфере уголовной ответственности относительно распространения информации расистского и ксенофобского характера». В ней содержится «подробная классификация киберпреступлений, указывается порядок по взаимодействию стран, чьи интересы пострадали в результате действий киберпреступников, и, кроме того, регламентируются вопросы по хранению и использованию личной информации клиентов интернет-провайдеров при расследовании преступлений [9].

В данной Конвенции «рассмотрены ключевые вопросы, среди которых уголовно-правовая характеристика преступлений в сфере компьютерной информации; уголовно-процессуальные особенности противодействия преступности, которые направлены на обеспечение сбора доказательств при расследовании компьютерных преступлений; а также вопросы международного сотрудничества в уголовно-процессуальной деятельности, направленного на сбор доказательств совершения таких преступлений за рубежом» [10].

По мнению одних некоторых исследователей в области борьбы с киберпреступностью, несмотря на то, что помимо рассматриваемой Конвенции существуют другие международные акты, однако при этом она представляет из себя «признанный международный договор, содержащий нормы как материального, так и процессуального (процедурные) права по противодействию киберпреступлениям и защите свободы, безопасности и прав человека в информационном пространстве» [11]. Ряд других правоведов, полагают, что в настоящее время Конвенция представляет собой устаревший и не отвечающий современным реалиям международный правовой акт из-за стремительных темпов освоения киберпространства и внедрения новейших цифровых технологий. Конвенция 2001г. освещает в большей степени понятийный и категориальный аппарат, определяющий перечень противоправных деяний в сфере киберпреступности, который с каждым годом все больше теряет актуальность. Данный документ был разработан в конце 1990-х гг., и ряда угроз в сфере информационного пространства просто не существовало либо о них не было известно широкой общественности [12]. Из сказанного следует, что на сегодняшний день все-таки сложилась некая основа правового регулирования противодействия киберпреступности. Между тем, по мнению многих отдельных специалистов, ситуация, связанная с выявлением киберпреступлений, свидетельствует о невысокой эффективности международно-правовой базы по борьбе с рассматриваемым феноменом. Из-за этого в настоящее время международное сотрудничество в борьбе с киберпреступностью все больше становится фрагментарным. Во многом такое положение дел объясняется отсутствием необходимой конвенции ООН, определяющей единые для большинства государств векторы борьбы с киберпреступностью, конвенции, которая в том числе бы перечисляла современные уголовно-правовые составы, предусматривающие санкции за совершение рассматриваемых преступлений, а также современный действенный системный комплекс мер по международному сотрудничеству в информационно-коммуникационной сфере.

При этом важно отметить, что в современных условиях необходимо активно противодействовать киберпреступности, которая все больше приобретает трансграничный характер [13]. Данная деятельность должна осуществляться на основе хорошо скоординированного международного сотрудничества мировых держав, и в первую очередь при эффективном взаимодействии их правоохранительных органов и служб. И только при таком глобальном подходе всего

мирового сообщества возможно реальное снижение рассматриваемых противоправных деяний. Кроме всего прочего, правительствам и бизнес-сообществу необходимо совершенствовать свои цифровые навыки и свою обязанность заботиться о своих клиентах. Это также включает в себя предложение безопасных продуктов и услуг в области информационных технологий. Компании и государственные органы должны нести ответственность за свою работу в этом направлении и практиковать прозрачность в отношении того, какие меры кибербезопасности они принимают и как они обрабатывают пользовательские данные. Государствам необходимо устанавливать рамки и стандарты, например, когда речь заходит о требованиях безопасности критически важных услуг и процессов. Освещая проблему совершенствования межгосударственного сотрудничества по обеспечению информационной безопасности, важно подчеркнуть, что во многих странах в настоящее время уже активно функционирует ряд государственных систем по защите государственных секретов и информации, а также по лицензированию функционирования предприятий в сфере защиты информационных данных [14]. Сегодня в государствах Европейского Союза на постоянной основе заняты организацией и проведением «крупномасштабных национальных, международных и транснациональных киберучений, которые способствуют повышению уровня специальной подготовки руководящих и подчиненных органов управления, сил и средств кибербезопасности по надлежащему обеспечению функционирования критически важных инфраструктурных объектов» [15]. Следует также отметить, что изучив положительный зарубежный опыт, в первую очередь необходимо развивать на политическом и техническом уровне дальнейшее сотрудничество по укреплению кибербезопасности со всеми международными организациями, в которых состоит наша страна, в том числе с теми, которые функционируют на территории государств – участников Содружества Независимых Государств (далее – СНГ). Сегодня регулирование международных отношений в киберпространстве становится серьезной проблемой. Поэтому нашей стране в первую очередь совместно с государствами – единомышленниками, выступающими союзниками РК в различных сферах деятельности, необходимо продвигать дорожную карту цифровой стратегической автономии. При этом нашей Республике необходимо укреплять сотрудничество в рамках международных организациях (ШОС, ОДКБ, СНГ и др.), а также оказывать поддержку менее защищенным странам, с их согласия, в наращивании их потенциала в области кибербезопасности, тем самым способствуя общей стабильности киберпространства, как на территории государств – участников СНГ, так и во всем мире. При этом наша страна в дальнейшем должна стремиться к тому, чтобы международные договоры не приводили к технологической или экономической зависимости заинтересованных сторон и к отчуждению персональных данных наших граждан или конфиденциальных данных администраций, источников дестабилизации киберпространства. Это будет включать в себя превращение РК в цифровую территорию, которая в наибольшей степени уважает основные права людей, создаст зоны доверия и экономического процветания. В сложившихся современных условиях киберпространство должно оставаться местом свободного выражения мнений для всех граждан, где злоупотребления могут быть предотвращены только в пределах, установленных законом, и в соответствии с нашими международными соглашениями. Развитие цифровых технологий не может быть устойчивым в киберпространстве, где государства не уважают передовой опыт, необходимый для сбалансированного перехода к цифровым технологиям, который выгоден всем странам, и где несколько экономических игроков монополизировали богатство, которое составляют цифровые данные, в частности персональные данные, истинные ресурсы для будущих поколений.

В этой связи важно, чтобы проводилась активная пропаганда и защита информации в телекоммуникационных сетях связи. Цифровой переход, носитель политических, социальных и экономических возможностей, далеко не во всех странах контролируется одинаково. Это наносит ущерб безопасности и развитию государств, которые менее защищены, и ослабляет всю цифровую среду на международном уровне [16]. В целях содействия надежному и устойчивому внедрению цифровых технологий во всех странах, и в частности в развивающихся, наша страна должна оказать помощь в укреплении потенциала стран, которые хотели бы повысить

устойчивость и безопасность своих информационных систем, особенно в том, что касается защиты критически важных инфраструктур и борьбы с киберпреступностью.

Для обеспечения долговечности и устойчивости проектов по укреплению потенциала, предпочтительно будет действовать на основе долгосрочных надежных партнерских отношений. Это действие также должно позволить нашей стране укрепить свою собственную кибербезопасность. Рост цифровых рынков во всем мире, а также связанные с этим императивы безопасности должны давать возможность дифференцировать цифровые продукты и услуги, уровень безопасности которых адаптирован к их использованию. Поддерживая инвестиции, инновации и экспорт, а также посредством государственных закупок государство должно создать благоприятную среду для отечественных компаний в цифровом секторе, предлагающих безопасные продукты и услуги, в том числе по борьбе с киберпреступностью. Участие в многосторонних переговорах по кибербезопасности (ООН, ОБСЕ и др.) будет способствовать укреплению глобальной базы обязательств по обеспечению национальной безопасности в соответствии с международным правом. Также необходимо укреплять двусторонние контакты, в частности в рамках межведомственного дипломатического диалога по вопросам, касающимся киберпространства, возглавляемого Министерством иностранных дел. Таким образом, современное киберпространство не только не является пространством без правил, но и регулируется действующим международным законодательством. Несмотря на это необходимая сегодня современная международная нормативная база по эффективной защите киберпространства все еще находится на стадии обсуждения международного сообщества. Однако дальнейшее отсутствие прогресса в переговорном процессе может нанести ущерб сохранению стабильного, безопасного глобального киберпространства, необходимого для развития современной цивилизации и надежной международной экономики цифровой эпохи.

Кроме того, в условиях нового тысячелетия межгосударственные меры по борьбе с кибербезопасностью должны играть более активную роль в цифровой сфере. С одной стороны, путем увеличения инвестиций в безопасность своих собственных сетей и услуг и, с другой стороны, путем объединения всех международных сторон по принятию коллективных мер международной безопасности и противодействия киберпреступности.

Литература

1. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № – 8. – С. 46-50.
2. Кобец П.Н. Совершенствование мер, осуществляемых органами внутренних дел в сфере информационно-психологического противодействия терроризму // Юридическая психология. – 2021.
3. Кобец П.Н. Выявление и мониторинг социальных сетей, используемых экстремистскими группировками, – важнейшая основа противодействия их преступной деятельности // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2017. – №2(42). – С. 13-19.
4. <https://lsm.kz/kazahstanskije-kompanii-teryayut-milliony-iz-za-hakerskih-atak>.
5. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: дис. ... канд. юрид. наук. – Иркутск, 2006. – С. 237.
5. Варданян А.В., Никитина Е.В. Расследование преступлений в сфере высоких технологий и компьютерной информации. – Москва: Юрлитинформ, 2007. – С. 312.
6. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. – 2016. – Т. 10. – № 2. – С. 369-378. – DOI 10.17150/1996-7756.2016.10(2).
7. Schjolberg S.A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime [Electronic resource] / Stein Schjolberg // Twelfth United Nations Congress on Crime

Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. – Mode of access. – URL: http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf. (дата обращения: 16.12.2021).

8. Харитошкин В.В. О мерах противодействия киберпреступности в международном и российском уголовном праве // Вестник Тверского государственного университета. Серия: Право. – 2019. – №3(59). – С. 111-117.

9. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – №2. – С. 17-25.

11. Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации: дис. ... канд. юрид. наук: 12.00.13. – Москва, 2014. – С. 174.

12. Атнашев В.Р., Яхьева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. – 2019. – №3(29). – С. 37-42.

13. Кобец П.Н. О современных информационных технологиях, используемых экстремистскими и террористическими группировками, и необходимости противодействия киберпреступности // Вестник развития науки и образования. – 2016. – №6. – С. 4-9.

14. Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. – 1999. – № – 5. – С. 3-5.

15. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. – 2015. – №3(11). – С. 2-14.

16. Поляков В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет // Известия Алтайского государственного университета. – 2016. – №3(91). – С. 142–144. – DOI 10.14258/izvasu(2016) 3-26.

**«Қоғам мен мемлекетті ақпараттандыру және цифрландыру
жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық
атты халықаралық ғылыми-практикалық конференция
қорытындысы бойынша
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.

Қазақстан Республикасы ПМ Мақан Есболатов атындағы Алматы академиясында (2024 жылғы 20 қыркүйек) әр елдің ғалымдарын, сарапшыларын 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
по итогам 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.

Конференция «Противодействие преступности в условиях цифровизации и информатизации общества и государства» проведенная в Алматинской академии МВД Республики Казахстан имени Макана Есбулатова (20 сентября 2024 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.

МАЗМҰНЫ

«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференцияның бағдарламасы.....	3
Программа международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»	6
«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық ғылыми-тәжірибелік конференцияның қатысушылар тізімі.....	9
Список участников международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»	10
БЕЙСЕНАЛИЕВ Б.Н., БИМОЛДАНОВ Е.М., КАИРЖАНОВА С.Е. Детерминанты (причины и условия) возникновения и развития торговли людьми.....	11
СОРОКУН Н.С. Выявление и устранение причин и условий совершения преступлений в сфере информационно-телекоммуникационных технологиях, как основа профилактики таких деяний	17
МЕЛЬНИК С.Л. Проблемные вопросы признания потерпевшим по коррупционным делам	21
РУСТЕМОВА Г.Р. Правовые риски цифровизации в законодательстве о здравоохранении.....	24
БАПАНОВ Т.А. Кибер алаяқтық: сипаттамасы және әдістері	30
АКИМЖАНОВ Т.К. Киберпреступность – как источник угрозы национальной безопасности Республики Казахстан	33
ШАЯХМЕТОВА Ж.Б. Разработка эффективных технологии в предупреждении киберпреступности	39
СЕРАЛИЕВА А.М., БАЙМАГАМБЕТОВА З.М., КАЗИЕВА А.Н. Шет елдердің материалдары бойынша чиптеу мәселелері.....	41
ТОГАЙБАЕВА Ш.С., ТОГАЙБАЕВ А.И., КАРАКУШЕВ С.И. Ужесточить наказание дропперам	46
СУЛТАНОВ С.И. Қылмыстық істерді алқабилердің қатысуымен қараудың ерекшеліктері	50
DAYETOVA A.A., BAISEITOVA A.T. Some issues related to violation of rules of flight safety or air transport operations in the republic of Kazakhstan	54

МАРАТ А.М. О личности интернет-мошенника	58
БАТЫРБАЕВ А.К. Цифрлық технологиялар саласындағы криминологиялық қауіпсіздікті қамтамасыз етудің стратегиялық бағыттары	62
КУРМАНОВА Г.С. к вопросу совершенствования информационно-аналитического беспечения криминологических исследований личности отрудника правоохранительных органов, совершившего преступление.....	67
ЗУЛЕЕВА А.Ж. Сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы оң үрдістер	73
БАПАНОВ М.Т., БАПАНОВА Т.Т. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимылда заңнаманы жетілдіру жолдары.....	78
ТУРГУНБАЕВА А.М. Қазақстан Республикасы киберқылмыс динамикасының ерекшеліктері және оның алдын алу мәселелеріне әсері.....	83
ЕРГАЛИЕВА К.С. Современные подходы профилактики бытового насилия в Республике Казахстан.....	89
ҚҰЛАЖАНОВА А.Н. Ұйымдастырылған қылмыстың қылмыстық құқықтық аспектілері	92
УСЕНБАЕВА А.У., ҚҰЛАЖАНОВА А.Н. Қоғамдық қауіпсіздікті қамтамасыз ету жүйесін дамыту.....	96
УСЕНБАЕВА А.У., БАТЫРБЕКОВА Б.К. Қауіпсіздікті қамтамасыз етудің цифрлық инфрақұрылымын дамыту	100
КАЛИБАЕВА Н.Б. Жеке құраммен тәрбие жұмысының ұйымдастырушылық-құқықтық жүйесі	104
САРБАСОВ А.Е. АЙТКЕШ А.Қ. Совершенствование межгосударственного сотрудничества в области противодействия киберпреступности.....	107
«Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл» атты халықаралық атты халықаралық ғылыми-практикалық конференция қорытындысы бойынша қарары	113
Резолюция по итогам международной научно-практической конференции «Противодействие преступности в условиях цифровизации и информатизации общества и государства»	114

Беттеу:
Б.Ю. Туренова

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу
және редакциялық-баспа жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 12 қараша 2024ж. жіберілді.
Пішімі 60x84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 9.
Таралымы 100.