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.), 2 том

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ИНФОРМАТИЗАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА

международная научно-практическая конференция посвящённая памяти заслуженного деятеля науки и техники Республики Казахстан, академику КАЕН Республики Казахстан, доктора юридических наук, профессора Каиржанова Елегена Изтлеуовича
(20 сентября 2024 г.), том 2

Алматы
2024

УДК 34:004
ББК 67:32.973
Қ54

Қ54 Қоғам мен мемлекетті ақпараттандыру және цифрландыру жағдайында қылмысқа қарсы іс-қимыл: халықар. ғыл.-тәж. конф. мат-ры (20.09.2024 ж.), 2 том = Противодействие преступности в условиях цифровизации и информатизации общества и государства: мат. межд. науч.- практ. конф. (20.09.2024 г.), том 2. – Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2024. – 110 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 Құбайыржановқа 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», посвященная памяти заслуженному деятеля науки и техники Республики Казахстан, академику КАЕН Республики Казахстан, академика КАЕН Республики Казахстан, доктора юридических наук, профессора Каиржанова Елегена Изтлеуовича, организованного кафедрой уголовного права и криминологии Алматинской академии МВД Республики Казахстан им. М. Есбулатова.

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

УДК 34:004
ББК 67:32.973

ISBN 978-601-360-139-7

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

10.00-10.10	**ДИЛЬБАРХАНОВА** **Жанат Рахимжанқызы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының уақытша м.а., полиция полковнигі	Алғыс сөз
10.10-10.20	**БИМОЛДАНОВ** **Ержан Малайұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары полиция полковнигі	Алғыс сөз
10.20-10.30	**СУЛЕЙМЕНОВ** **Адлет Даулетханович** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасы бастығының орынбасары. полиция подполковнигі	«Көлеңкелі Интернеттің кейбір ерекшеліктері туралы».
10.30-10.40	**САРСЕНБАЕВА** **Ботагоз Булатовна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы Академиясының Қылмыстық процесс және криминалистика кафедрасының профессоры з.ғ.к., полиция майоры	«Қылмыстық сот ісін жүргізуді цифрландыру жағдайында дәлелдемелерді трансформациялау».
10.40-10.50	**ДЮСЕМБАЕВА** **Динара Рамазановна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық процесс және криминалистика кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі	«Интернет желісін пайдалану арқылы жасалатын есірткі қылмыстарына қарсы іс-қимыл».
10.50-11.00	**АЛМАЗҚЫЗЫ** **Карлыгаш** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқылмысқа қарсы іс-қимыл жөніндегі мамандарды даярлау орталығының аға оқытушы-әдіскері полиция подполковнигі	«Киберқауіпсіздікті қамтамасыз етудің Нормативтік-құқықтық аспектілері».
11.00-11.10	**БЕЙСЕНБАЙ** **Әлия Бейсенбайқызы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының аға оқытушы-әдіскері, полиция майоры	«Цифрлық кеңістікті дамыту және киберқылмыс».
11.10-11.20	**ҚҰЛМАН** **Ернұр Ерланұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының оқытушы-әдіскері полиция лейтенанты	«Мобильді қосымшалардың қауіпсіздігі және мобильді қауіптерге қарсы тұру».
11.20-11.30	**КУРБАНОВ**	«Жасанды интеллект

	Ролан Диасович Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасының аға оқытушысы полиция майоры	киберқауіпсіздікті қамтамасыз етудегі технология ретінде».
11.30-11.40	**ШАЙСУЛТАНОВ** **Самат Даулетович** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі	«Дамудың тарихи аспектілері, тенденциялары интернеттегі алаяқтық»..
11.40-12.00	**ТАСБУЛАТОВ** **Руслан Ермекович** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнынан кейінгі білім беру факультетінің ғылыми-педагогикалық магистратурасының 2 курс магистранты полиция капитаны	«Сандық қылмыстардың қылмыстық-құқықтық аспектілері».
12.00-12.10	**БАТЫРХАН** **Темірлан Мейірханұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ғылыми-педагогикалық магистратурасының магистранты полиция капитаны	«Интернет-алаяқтықтың кең таралған түрлері мен тәсілдерін ашу мен тергеудегі жедел-іздестіру және тергеу іс-шараларының тактикалық ерекшеліктері».
12.10-12.20	**БЕЙСЕНБІ** **Арна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі білім беру факультетінің ҒПМ 2 курс магистранты полиция аға лейтенанты	«Қоғамдағы орын алып жатқан кибербуллингтің зардаптары».
12.20-12.30	**ЖАНДЫҒУЛОВА** **Шолпан Ерланқызы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі білім беру факультеті ғылыми-педагогикалық магистратурасының 1 курс магистранты полиция лейтенанты	«Ақпараттық жүйелердің немесе телекоммуникация желілерінің құрамы және құрылымы».
12.30-12.40	**БЕЙСЕНАЛИЕВ** **Бауыржан Нуралыулы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнынан кейінгі білім беру факультеті докторантурасының 1-курс докторанты полиция подполковнигі	«Қылмыстық процестің үш буынды моделін енгізу шеңберінде киберқылмысқа қарсы іс-қимыл».
12.40-12.50	**ШАУХАР** **ДАНИЯР ҚАНАТҰЛЫ** Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының жоғары оқу орнынан кейінгі білім беру факультетінің ғылыми-педагогикалық магистратурасының 1 курс магистранты полицияның аға лейтенанты	«Қылмыстық процестің үш буынды моделін енгізу шеңберінде киберқылмысқа қарсы іс-қимыл».

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

10.00-10.10	**ДИЛЬБАРХАНОВА** **Жанат Рахимжановна** Временно и.о. начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова полковник полиции	Приветственное слово
10.10-10.20	**БИМОЛДАНОВ** **Ержан Малаевич** Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова полковник полиции	Приветственное слово
10.20-10.30	**СУЛЕЙМЕНОВ** **Адлет Даулетханович** Заместитель начальника кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	«О некоторых особенностях теневого интернета». «Deep web и dark net».
10.30-10.40	**САРСЕНБАЕВА** **Ботагоз Булатовна** Профессор кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., майор полиции	«Трансформация доказывания в условиях цифровизации уголовного судопроизводства».
10.40-10.50	**ДЮСЕМБАЕВА** **Динара Рамазановна** Старший преподаватель кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., подполковник полиции	«Противодействие наркопреступлениям, совершаемым с использованием сети интернет».
10.50-11.00	**АЛМАЗҚЫЗЫ** **Карлыгаш** Старший преподаватель-методист Центра по подготовке специалистовпо по противодействию киберпреступности Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	«Нормативно-правовые аспекты обеспечения кибербезопасности».
11.00-11.10	**БЕЙСЕНБАЙ** **Әлия Бейсенбайқызы** Алматинская академия МВД Республики Казахстан им. М. Есбулатова Старший преподаватель-методист Центра подготовки специалистов по противодействию киберпреступности майор полиции	«Развитие цифрового пространства и киберпреступность».
11.10-11.20	**ҚҰЛМАН** **ЕРНҰР Ерланұлы** Преподаватель-методист Центра подготовки специалистов по противодействию киберпреступности Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции	«Безопасность мобильных приложений и противодействие мобильным угрозам».

11.20-11.30	**КУРБАНОВ** **Ролан Диасович** Старший преподаватель Кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции	«Искусственный интеллект как технология в обеспечении в сфере кибербезопасности».
11.30-11.40	**ШАЙСУЛТАНОВ** **Самат Даулетович** Старший преподаватель кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., подполковник полиции	«Исторические аспекты развития, тенденции интернет-мошенничества».
11.40-12.00	**ТАСБУЛАТОВ** **Руслан Ермекович** Магистрант 2 курса научно-педагогической магистратуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции	«Уголовно-правовые аспекты цифровых преступлений».
12.00-12.10	**БАТЫРХАН** **Темірлан Мейірханұлы** Магистрант научно-педагогической магистратуры Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции	«Тактические особенности оперативно-розыскных и следственных мероприятий в раскрытии и расследовании распространенных видов и способов совершения интернет-мошенничества».
12.10-12.20	**БЕЙСЕНБІ** **Арна** Магистрант 2 курса НП факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции	«Последствия киберзапугивания в обществе».
12.20-12.30	**ЖАНДЫҒУЛОВА** **Шолпан Ерланқызы** Магистрант 1 курса научно-педагогической магистратуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции	«Состав и структура информационных систем или сетей телекоммуникаций»..
12.30-12.40	**БЕЙСЕНАЛИЕВ** **Бауыржан Нуралыулы** Докторант 1-го курса докторантуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	«Противодействие киберпреступности в рамках внедрения трехзвенной модели уголовного процесса».
12.40-12.50	**ШАУХАР** **ДАНИЯР ҚАНАТҰЛЫ** Магистрант 1 курса научно-педагогической магистратуры факультета послевузовского образования Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова старший лейтенант полиции	«Противодействие киберпреступности в рамках внедрения трехзвенной модели уголовного процесса».

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

Аты-жөні, тегі	Лауазымы
ДИЛЬБАРХАНОВА Жанат Рахимжанқызы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының уақытша м.а., полиция полковнигі
БИМОЛДАНОВ Ержан Малайұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы бастығының орынбасары полиция полковнигі
СУЛЕЙМЕНОВ Адлет Даулетханович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасы бастығының орынбасары полиция подполковнигі
САРСЕНБАЕВА Ботагоз Булатовна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы Академиясының Қылмыстық процесс және криминалистика кафедрасының профессоры з.ғ.к., полиция майоры
ДЮСЕМБАЕВА Динара Рамазановн а	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының қылмыстық процесс және криминалистика кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі
АЛМАЗҚЫЗЫ Карлыгаш	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқылмысқа қарсы іс-қимыл жөніндегі мамандарды даярлау орталығының аға оқытушы-әдіскері полиция подполковнигі
БЕЙСЕНБАЙ Әлия Бейсенбайқызы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының аға оқытушы-әдіскері, полиция майоры
ҚҰЛМАН Ернұр Ерланұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы Киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының оқытушы-әдіскері полиция лейтенанты
КУРБАНОВ Ролан Диасович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасының аға оқытушысы полиция майоры
ШАЙСУЛТАНОВ Самат Даулетович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жедел-іздестіру қызметі кафедрасының аға оқытушысы з.ғ.м. полиция подполковнигі
ТАСБУЛАТОВ Руслан Ермекович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнынан кейінгі білім беру факультетінің ғылыми-педагогикалық магистратурасының 2 курс магистранты полиция капитаны
БАТЫРХАН	Қазақстан Республикасы ІІМ М. Есболатов атындағы

Темірлан Мейірханұлы	Алматы академиясының ғылыми-педагогикалық магистратурасының магистранты полиция капитаны
БЕЙСЕНБІ Арна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі білім беру факультетінің ҒПМ 2 курс магистранты полиция аға лейтенанты
ЖАНДЫҒУЛОВА Шолпан Ерланқызы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы жоғары оқу орнынан кейінгі білім беру факультеті ғылыми-педагогикалық магистратурасының 1 курс магистранты полиция лейтенанты
БЕЙСЕНАЛИЕВ Бауыржан Нуралыулы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнынан кейінгі білім беру факультеті докторантурасының 1-курс докторанты полиция подполковнигі
ШАУХАР ДАНИЯР ҚАНАТҰЛЫ	Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының жоғары оқу орнынан кейінгі білім беру факультетінің ғылыми-педагогикалық магистратурасының 1 курс магистранты полицияның аға лейтенанты

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

ФИО	Должность
ДИЛЬБАРХАНОВА Жанат Рахимжановна	Временно и.о. начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова полковник полиции
БИМОЛДАНОВ Ержан Малаевич	Заместитель начальника Алматинской академии МВД Республики Казахстан им. М. Есбулатова полковник полиции
СУЛЕЙМЕНОВ Адлет Даулетханович	Заместитель начальника кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
САРСЕНБАЕВА Ботагоз Булатовна	Профессор кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. М. Есбулатова к.ю.н., майор полиции
ДЮСЕМБАЕВА Динара Рамазановна	Старший преподаватель кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., подполковник полиции
АЛМАЗҚЫЗЫ Карлыгаш	Старший преподаватель-методист Центра по подготовке специалистовпо по противодействию киберпреступности Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
БЕЙСЕНБАЙ Әлия Бейсенбайқызы	Алматинская академия МВД Республики Казахстан им. М. Есбулатова Старший преподаватель-методист Центра подготовки специалистов по противодействию киберпреступности майор полиции
ҚҰЛМАН ЕРНҰР Ерланұлы	Преподаватель-методист Центра подготовки специалистов по противодействию киберпреступности Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции
КУРБАНОВ Ролан Диасович	Старший преподаватель Кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции
ШАЙСУЛТАНОВ Самат Даулетович	Старший преподаватель кафедры оперативно-розыскной деятельности Алматинской академии МВД Республики Казахстан им. М. Есбулатова м.ю.н., подполковник полиции
ТАСБУЛАТОВ Руслан Ермекович	Магистрант 2 курса научно-педагогической магистратуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции
БАТЫРХАН Темірлан Мейірханұлы	Магистрант научно-педагогической магистратуры Алматинской академии МВД Республики Казахстан

	им. М. Есбулатова капитан полиции
БЕЙСЕНБІ **Арна**	Магистрант 2 курса НП факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции
ЖАНДЫҒУЛОВА **Шолпан Ерланқызы**	Магистрант 1 курса научно-педагогической магистратуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова, лейтенант полиции
БЕЙСЕНАЛИЕВ **Бауыржан Нуралыулы**	Докторант 1-го курса докторантуры факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
ШАУХАР **ДАНИЯР ҚАНАТҰЛЫ**	Магистрант 1 курса научно-педагогической магистратуры факультета послевузовского образования Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова старший лейтенант полиции

СУЛЕЙМЕНОВ
Адлет Даулетханович
заместитель начальника кафедры оперативно-розыскной деятельности
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова подполковник полиции

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ТЕНЕВОГО ИНТЕРНЕТА DEEP WEB И DARK NET

Краткое описание: Для многих обывателей термины Deep Web и Dark Net (Дип Веб и Даркнет) звучат как нечто непонятное или скорее даже пугающее. СМИ, блоги, социальные сети часто описывают их как место, которое кишит наркоторговцами, киллерами, хакерами, нелицензионным контентом и т.п. Однако Даркнет как концепция приватной сети зародился еще в далеком 1970 году, а сегодня многие ресурсы в темной паутине посещают не только хакеры и преступники, но также журналисты, активисты, простые пользователи из стран, где интернет фильтруется спецслужбами. Но как и любое благое изобретение Дарнет можно использовать и не в благородных целях. В Даркнете безусловно есть площадки, где собираются киберпреступники, покупаются и продаются украденные конфиденциальные денные, различные малвари, нелицензионный контент.

Ключевые слова: Deep Web, DarkNet, браузер, Tor, поисковик, теневой Интернет, глубокая паутина, тайная вики (тайная вики), криптовалюта, биткойин, хакер, информационные технологии, киберпреступления, цифровые технологии.

В данной публикации мы постараемся более подробно рассказать о Deep Web, DarkNet что это такое, в чем разница и законно ли подключаться к скрытому интернету, а также о его использовании на хакерском поприще.

Большинство маркетологов говорят, что лучшее место, чтобы спрятать тело, – вторая страница Google. Однако это еще не далеко. Есть чёрное цифровое кладбище, называемое «Deep web». Это место, до которого Google дотянуться не способен.

Что это вообще такое Deep Web, он заработал репутацию зловещей бездны незаконной и вызывающей беспокойство деятельности, о которой можно услышать в СМИ. Но это место называется Dark Net. Термины «Deep Web» и «Dark Net» часто используются как синонимы, однако это не совсем верно. Даркнет – это лишь крошечная часть deep web'а, составляющая всего 0.01% от него. Все страшное, которые вы слышали о deep web, относились к Dark Net [1].

По большей части, контент в глубоком интернете очень похож на контент обычных сайтах, которые можно найти в Google.

Deep Web – это просто контент, который вы не сможете найти через поисковую систему. К этому контенту относится, например, личная информация в вашей учетной записи в какой-

нибудь социальной сети, ваши сообщения на электронной почте, закрытые страницы частных сайтов и т.д.

То, что мы можем найти в поиске, называется surface web, или «поверхностный интернет». Отличия между поверхностным и глубоким интернетом заключается в том, что некоторая защита препятствует к свободному доступу информации из deep web, а к surface web может получить доступ любой пользователь.

Более 96% контента находится в deep web, т.е. это большая часть информации, к которой мы получаем доступ в интернете только после аутентификации: банковский счет, электронная почта, аккаунт в социальной сети. Представьте только, если бы любой мог получить доступ к этой информации, просто погуглив ваше имя. Ваша личная информация была бы доступна всему миру [2].

Веб-сайты не позволяют индексировать защищенные страницы, потому что лишь определенные лица должны иметь доступ к информации, размещенной на них.

Понятие «скрытой сети», что такое – Даркнет. Термин Dark Net или «Тёмная паутина» в общем понимании обозначает совокупность веб-сайтов, видимых публично, но при этом имеющих скрытый IP-адрес сервера, на котором они размещаются. Такие сайты общедоступны для всех веб-пользователей, однако выяснить, кто является их автором, очень сложно. Так же стоит сказать что на подобные сайты невозможно попасть, используя популярные поисковые системы.

По сути Dark Net это частная сеть, в которой соединения устанавливаются только между доверенными пирами, иногда именующимися как «друзья», и чаще всего с использованием нестандартных протоколов и портов. Dark Net отличается от других распределенных одноранговых сетей, так как файлообмен происходит анонимно (вследствии того что IP-адреса русурсов недоступны публично), и следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

В виду этого Dark Net часто воспринимается как инструмент для осуществления коммуникации в запрещённых сообществах, подпольях, а так же для ведения незаконной деятельности. В более общем смысле термин Dark Net может быть использован для описания некоммерческих «узлов» сети Интернета или относится ко всем «подпольным» Интернет-коммуникациям и технологиям, которые в большинстве своем связаны с незаконной деятельностью или инакомыслием.

Можно встретить сравнение Dark Net и технологий 2p2-обмена применяемых, к примеру для распространения торрентов.

Так, наиболее распространенные на сегодняшний день файлообменники, например, BitTorrent, на самом деле не являются даркнетами, поскольку пользователи могут связываться с кем угодно в сети [3].

Почти все известные даркнеты децентрализованы и следовательно, считаются одноранговыми. Так же, многие даркнеты требуют установки специального программного обеспечения для получения доступа к сети.

Поговорим о истории возникновения Dark Net. Термин «Dark Net» имеет давнюю историю и появился еще на заре компьютерных технологий в 1970-х годах. В контексте сетевой безопасности данный использовался для обозначения сетей, изолированных от ARPANET. Даркнеты могли получать данные от главной сети ARPANET, но имели такие адреса, которые не появлялись в списках сетей и не отвечали на запросы извне [4].

В современном понимании, термин Dark Net получил широкое распространение благодаря публикации «The Darknet and the Future of Content Distribution», опубликованной в 2002 году, группой сотрудников Microsoft в лице Питера Биддла, Пола Инглэнда, Маркуса Пейнаду и Брайана Уиллмана [5].

Авторы данной публикации выдвинули идею Dark Net основанную на трёх предположениях:

Любой объект, предназначенный для широкого распространения, будет доступен определённой части пользователей с разрешением на копирование.

Пользователи будут копировать объекты, если это возможно и если они этого захотят.

Пользователи соединены каналами с высокой пропускной способностью.

Итак, термин Dark Net – это файлообменная сеть, которая возникает при появлении общедоступных данных, согласно предположению 1, и при распространении этих данных, согласно предположениям 2 и 3.

С тех пор этот термин часто заимствовался и в том числе использовался в таких крупных СМИ как Rolling Stone и Wired.

Специфика Даркнета, как правило, Даркнет используется в определнных случаях, например, таких как:

Неприкосновенность частной жизни и страх политических репрессий

Преступления в сфере информационных технологий

Распространение файлов, защищённых авторскими правами.

Даркнет и анонимные узлы TOR. Практически все сайты, находящиеся в Тёмной паутине, скрывают свою принадлежность, используя инструмент шифрования Tor [6].

TOR для тех кто не знал. Tor (The Onion Router) – свободное и открытое программное обеспечение для реализации луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Так с помощью Tor пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования шифрованных распределённых сетей серверов – узлов. Технология Tor обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом.

Tor позволяет скрыть вашу личность и «подменить» ваше местоположение. В случае, когда в управлении сети Tor находится вебсайт, эффект наблюдается тот же, что и в ситуации с конечным пользователем. Для того, чтобы посетить сайт в Тёмной паутине, который использует инструмент шифрования Tor, веб-пользователь должен также использовать Tor.

Вернемся к даркнетам. Важно сказать, что не все сайты Тёмной паутины используют Tor. Некоторые используют альтернативные сервисы, как, например, I2P, но принцип действия остаётся абсолютно таким же: пользователь должен использовать такой же инструмент шифрования, как и целевой сайт, и, что очень важно, знать, где найти сайт, чтобы посетить его посредством введения конкретного URL. Одним из самых известные примеров сайта Тёмной паутины остается Silk Road («Шёлковый путь»). Ранее Silk Road долгое время являлся анонимной торговой площадкой для покупки-продажи наркотиков.

Кстати, нужно помнить, что пользователи Tor встречают и некоторые неудобства, например такие как:

Так вы можете невольно стать соучастником масштабных преступлений и деятельности хакеров, так как ваш ПК становится частью сети, что используется другими хостами.

Tor разрабатывался военными и спецслужбами, что не исключает его использование в своих целях, несмотря на раскрученный бренд про 100% безопасность и анонимность использования.

Это создает неудобства при пользовании «белыми» сервисами, например, почтой. Суть в том, что при работе с Tor у вас постоянно меняется IP-адрес, что приводит к отключению сервисов, которые воспринимают это как попытку внешнего взлома.

Google часто блокирует поисковые запросы через Tor, поскольку считает, что это хакерская активность.

Белая сторона Даркнета. Компания Trend Micro опубликовала отчет из которого можно сделать вывод, что не все, что используется в Даркнете плохо. А именно:

– на сайты в скрытой сети заходят не только злоумышленники, но и добропорядочные граждане, в том числе журналисты и пользователи из стран с диктаторскими режимами;

– в торговом ассортименте подпольных магазинов преобладают не сильные, а слабые наркотики, которые и так легализованы на некоторых территориях.

Многие страны лишены того, что соответствовало бы первой поправке к Конституции США. Так сеть Darknet предоставляет всем желающим возможность свободно высказывать свои мысли, не боясь цензуры или преследования. По данным Tor Project, анонимные Hidden Services служат убежищем для диссидентов из Ливана, Мавритании и стран, которые накрыла Арабская весна. Тут же размещаются и зеркала сайтов, вызывающих страх и ненависть у правительств некоторых стран и глобальных корпораций – GlobalLeaks, Indymedia и Wikileaks.

Trend Micro в своем отчете так же отмечает ещё несколько особенностей даркнета. Например, никто не может оценить его размер. Вполне вероятно, что там гигантское количество страниц, но невозможно сказать, сколько из них доступны в каждый момент времени. Информационный ландшафт очень быстро меняется: сайты появляются и исчезают.

Если посмотреть на ассортимент магазинов, то там преобладает марихуана и фармацевтические средства вроде виагры. Так называемая «фарма» – давний предмет купли-продажи на полулегальных сайтах, которые существуют и в открытой Сети. Так же в списке присутствуют видеоигры, аккаунты к разным сайтам, грибы [7].

Даркнет и хакеры. Все в том же отчете Trend Micro упоминает известный факт, что даркнет используется для установки командных серверов в ботнетах и других зловредах. По своей природе Скрытая сеть естественным образом подходит для этого. Один из примеров malware, которая пропускает трафик через Tor, – известный троян-шифровальщик Cryptolocker.

В июне 2016 года специалисты «Лаборатории Касперского» подготовили отчет и рассказали о подпольной торговой площадке xDedic, на которой злоумышленники продают доступ к взломанным серверам со всего мира. Тогда ресурс, работавший в обычном интернете, а не в зоне .onion, быстро исчез с радаров и прекратил свою деятельность. Теперь исследователи компании Digital Shadows сообщают, что xDedic вернулся в строй, но перебрался в даркнет.

Каким образом попадают в DarkNet. К темной сети (darknet) вы не сможете получить доступ через стандартный браузер (Google Chrome, Safari и т.п.), для этого вам нужно специальное программное обеспечение для шифрования, например, браузер Tor.

Tor сохраняет анонимность, скрывает местоположение и засекречивает передачу данных пользователей, поэтому DarkNet, как правило, используют для преступной деятельности. Согласно исследованию двух экспертов по угрозам кибер-разведки, более половины сайтов из даркнета предлагают незаконные продукты или услуги. И отследить кого-то из преступников, их деятельность попросту невозможно.

Но несмотря на то, что правоохранительным органам почти невозможно поймать преступников, анонимность даркнета полезна для пользователей с точки зрения этики.

Пользователь не оставляет цифрового следа в даркнете. Это спасает политических осведомителей, активистов и журналистов, которые живут в репрессивных странах, где введена цензура и за негативное мнение может последовать наказание. Они используют темную сторону интернета, чтобы заявить о своем истинном мнении, не боясь, что их личность будет раскрыта.

Даркнет имеет две крайности: он защищает людей, чью свободу пытаются ограничить, но с другой стороны он создает огромное поле для незаконной деятельности. Это наводит на один вопрос.

Законен ли Даркнет. Доступ к темной сети не является чем-то незаконным. Несмотря на то, что люди совершают незаконные действия на просторах темного веба, использование его для доступы к скрытому контенту не противоречит закону. На самом деле, Tor, самое популярное программное обеспечение для доступа в даркнет, был создан ВМС США, в настоящее время финансируется правительством США [8].

Они поддерживают Tor, потому что он защищает частную жизнь активистов, которые пытаются поменять тиранические режимы своих стран. От этой технологии зависит жизнь и свобода этих людей.

Почему люди имеют неправильно представление о Deep Web. Глубокая поутина по ошибке связана с незаконной деятельностью даркнета. Это не просто рынок наркотиков и прочих незаконных предметов (это описание даже отдаленно неверно). Deep Web в основном безвреден и необходим нам для защиты нашей личной информации и конфиденциальности. Он играет огромную роль в нашей повседневной жизни.

Литература

1. https://zen.yandex.ru/media/applespbevent/darknet-deep-web-chto-eto-takoe-v-chem-raznica-i-zakonno-li-podkliuchatsia-k-skrytomu-internetu-5b4f182246ae1500a9379bbf
2. https://zen.yandex.ru/media/applespbevent/
3. https://ru.wikipedia.org/wiki/BitTorrent_(программа)
4. https://ru.wikipedia.org/wiki/ARPANET
5. https://ipiskunov.blogspot.com/2016/08/darknet.html
6. https://www.torproject.org
7. https://ru.wikipedia.org/wiki/WikiLeaks
8. https://safe.cnews.ru/news/top/anonimnaya_set_tor_na_60_finansiruetsya

САРСЕНБАЕВА
Ботагоз Булатовна
профессор кафедры уголовного процесса и криминалистики
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова к.ю.н., майор полиции

ТРАНСФОРМАЦИЯ ДОКАЗЫВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Введение. Доказывание в уголовном судопроизводстве строится на ряде констант, обусловленных самой природой данной деятельности. Эти константы формировались на протяжении истории развития уголовного судопроизводства и имеют место в современном уголовном процессе разных стран и разных исторических типов. К их числу следует отнести тесную связь уголовного судопроизводства с уголовных правом в силу того, что судопроизводство является единственной легальной формой применения норм уголовного права к единичному уголовному правонарушению.

Правоприменительный характер, как другая константа уголовного судопроизводства, требует по каждому уголовному делу сначала установить фактическую основу совершенного уголовного правонарушения: познать, что фактически произошло в реальной жизненной ситуации, кто это совершил, есть ли вина и каковы ее формы, т.е. познать все юридически значимые фактические обстоятельства, позволяющие правильно применить нормы уголовного права. Для этого требуется особая процессуально правовая технология познавательной деятельности, чтобы правильно установить фактическое проявление всех признаков конкретного состава преступления в частном случае совершения правонарушения, а также всех процессуально значимых фактических обстоятельств (времени, места, обстановки, ситуации, результатов и пр.).

Познавательная деятельность в уголовном судопроизводстве начинается с момента обнаружения преступления и сопровождает всю дальнейшую процессуальную деятельность в отношении конкретного лица. Для ее осуществления вовлекаются и иные заинтересованные субъекты, чье право нарушено преступлением. Также возникает необходимость взаимодействовать с иными лицами, привлекаемыми в качестве свидетелей, понятых, специалистов, экспертов, переводчиков и т.д.

Еще одной константой является требование правильности и достоверности, предъявляемое к процессуальному познанию. Познающие субъекты процесса не имеют права на ошибку: привлечение к ответственности невиновного, привлечение не за то преступление, которое было совершено, без учета тяжести преступления и личности виновного является незаконным во всех правопорядках. И, наконец, презумпция невиновности, как константа уголовного судопроизводства, требует своего опровержения посредством доказанности всех фактических обстоятельств дела вне разумных сомнений. Это предполагает проверку и познание не только об-

винительных, но и оправдательных; не только уличающих, но и оправдывающих обстоятельств и аспектов совершенного деяния.

Поскольку уголовное судопроизводство это деятельность, осуществляемая при взаимодействии людей, она прежде всего вырабатывает социальные технологии и формирует определенный набор методов, средств, приемов такого взаимодействия, обеспечивая достижение целей данной деятельности.

Социальная технология формируется в зависимости от целей судопроизводства, поэтому технология инквизиционного процессуального познания существенно отличается от технологии современного. В современном процессе различаются технологии познания, например, в англо-саксонском уголовном процессе, строящемся на теории уголовного иска, и континентальном, строящемся на принципе публичности. Наиболее успешные социальные технологии познания получают процессуально правовое регулирование и становятся нормами доказательственного права. Эти правовые предписания превращают социальную технологию в процессуально-правовую, придавая легальность результатам познания и в известной мере обеспечивая правильность познания.

Появление цифровых технологий и их тотальное проникновение в сферу социальных отношений не может не затронуть право в целом и уголовно-процессуальное познание и доказывание, в частности.

Основная часть. Вторжение цифровых технологий в уголовное судопроизводство не ждет специального разрешения законодателя и фактически, хотя и фрагментарно, уже присутствует в нем. Цифровые технологии существенно меняют делопроизводство, облегчая работу с процессуальными документами и возможности оперативной связи между различными субъектами процесса. Электронные базы данных позволяют получать информацию, имеющую юридическое значение при производстве по делу.

Использование цифровых устройств при проведении следственных действий, например, видеозаписи, фотографирования, получения локализации нахождения средств связи и пр. позволяет получать информацию, во-первых, быстрее, во-вторых, с большей точностью, в третьих, с возможность более детального ее изучения (качество изображений, возможность их увеличения, фиксации более мелких деталей). Как эти технологии влияют на процессуальное доказывание? По мнению Л.В. Головко, цифровизация уголовного судопроизводства может быть сопоставлена с общим техническим развитием: гусиное перо, которым писались процессуальные документы в 18-19 веке, было успешно заменено пишущими машинками в веке 20 м, а теперь последние заменяются компьютерами, но это не меняет обозначенные выше константы процессуального познания и доказывания. Увы, это не так. Цифровые технологии проникают значительно глубже и требуют весьма серьезного изучения и прогноза возможных и необходимых трансформаций процессуального познания и доказывания как на уровне теоретических представлений, так и на уровне процессуального регулирования [1].

На данный момент такие трансформации уже проявляют себя в силу того, что сама преступная деятельность также проходит свою «цифровизацию». Появляются новые методы совершения преступлений, давно известных уголовному законодательству. Использование цифровых технологий преступниками требует новых навыков, правил, специальных знаний как для их выявления, так и для их расследования, раскрытия, получения достаточных и достоверных доказательств для их судебного разрешения [2].

Например, использование цифровых технологий при совершении мошенничества и похищениях таким способом денежных средств со счета потерпевшего или незаконный оборот наркотических и иных запрещенных веществ без контакта покупателя и продавца, через социальные сети. Эти и многие иные преступления, которые совершаются в физическом мире, оставляют следы. Выявление таких следов и их процессуальное закрепление позволяет получать привычные доказательства, хотя расследование таких преступлений сопровождается необходимостью учитывать особенности цифровых технологий. Например, при расследовании дел о незаконном обороте наркотиков следователь, традиционно, проводит осмотр места «закладки товара» и действует по правилам осмотра места происшествия, фиксируя различного рода «физические» следы: общий вид места, окружающую среду, возможные следы обуви, от-

печатков пальцев или иные микро следы, оставляемые и преступником, сделавшим эту «закладку», и «покупателем», приходившим забрать ее. Следователь будет производить и допросы фигурантов дела, возможных свидетелей; проводить экспертизы и пр.

Однако существенную роль в расследовании таких преступлений начинают играть цифровые технологии. Например, анализ соцсетей помогает выявлять и адреса, с которых предлагается такого рода «товар», и поступающий запрос на приобретение такого «товара». Наличие цифровых видеокамер позволяет отследить и выявить лиц, которые находились в районе «закладки-покупки». Цифровые системы проведения платежей позволяют выявлять счета, криптокошельки, иные формы цифровых расчетных операций конкретных лиц и устанавливать как продавца, так и покупателя в этих незаконных операциях. Существенную роль в раскрытии разного рода преступлений играют различного рода видеокамеры, размещенные на улицах города, в общественных местах, торговых точках, в подъездах жилых домов [3].

Такого рода видеозаписи оформляются и изымаются; осматриваются и приобщаются к делу в порядке ст.118 УПК РК. Суд исследует их в совокупности со всеми иными доказательствами и учитывает при принятии решения по делу. Следует признать, такого рода видеозаписи нередко дают более точную информацию, чем, например, свидетельские показания. Они позволяют уточнять и детализировать обстоятельства преступного правонарушения, но нередко такие технические источники информации позволяют установить и невиновность лица, привлекаемого к ответственности.

Цифровая видеозапись позволяет следователю создавать цифровую модель происшествия, чтобы понять, например, можно ли было избежать столкновения в данном дорожно-транспортном происшествии (ДТП), кто из водителей и как нарушил правила. Можно констатировать, что в расследовании преступлений, которые совершаются в физическом мире, цифровая техника дает значительно больше возможностей для более точного познания и доказывания фактических обстоятельств преступления. Трансформация регулирования доказывания по таким уголовным делам будет происходить путем уточнения процессуального порядка использования различных видов цифровой техники, получения и хранения цифровой информации. Однако понятие доказательства в этих ситуациях сохраняет свою природу следа, оставленного преступлением в объективной реальности, и свою информационную природу как фактических данных, имеющих значение для производства по данному делу [4].

Сохранится и требование к достаточности доказательств, потому что цифровое доказательство должно находить подтверждение в остальных доказательствах, собранных по делу, в совокупности своей позволяя следователю, государственному обвинителю и суду сформировать в своем сознании непротиворечивый и полный образ совершенного преступления как фактическую основу для отыскания и применения адекватной уголовно правовой нормы.

Принципиально иная ситуация доказывания возникает при совершении преступлений, порожденных самим процессом цифровизации: это так называемые «компьютерные» преступления [5].

Развитие уголовного права уже выделяет новые виды преступлений, совершаемых исключительно посредством цифровой техники и в цифровой среде. В УК РК, например, появилась Глава 7. «Уголовные правонарушения в сфере информатизации и связи», куда вошли такие преступления, как «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций» (ст.205); «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» (ст. 210) и др. подобные.

Если обычные преступления совершаются в социальной среде и проявляют себя так или иначе в форме жизненного события, то компьютерные преступления совершаются в цифровой среде, в которой выделяются три уровня информационных отношений: технический (сетевой), программный (сервисный) и информационный (собственно информация, присутствующая в сети) [6].

Для компьютерных преступлений характерно то, что:

а) они не существуют вне цифровой среды, поскольку их нет в реальном мире, значит нет и привычных для нас «аналоговых» следов, типа: удар-повреждение;

б) они осуществляются в мире цифровой информации, но способны захватывать любой из указанных выше уровней: технический, повреждая компьютер или в целом сеть; программный, нарушая, искажая, уничтожая программу, или информационный, искажая, блокируя циркулирующую информацию, создавая ложную информацию;

в) они выражены цифровым языком, поэтому требуют не перевода с цифрового на разговорный язык, а специальной интерпретации-объяснения значения, смысла, действия и последствий цифрового знака или цифровой записи;

г) они и информация о них не существуют вне цифрового носителя, поэтому если уничтожается носитель, уничтожается и информация и само существование преступления. [7]. И эта ситуация требует существенной трансформации практически всех представлений о доказывании в уголовном судопроизводстве: иного определения предмета доказывания; понимания, что доказательство – это не только фактические, но еще и цифровые данные, требующие собственного процессуального порядка их обнаружения, собирания и использования; что следственные действия по их собиранию, проверке и оценке невозможны без специалиста по цифровым технологиям во взаимодействии со следователем и иными участниками процесса на всех этапах работы с цифровой информацией и, очевидно, другие уточнения и теоретических представлений, и правового регулирования.

Прежде всего требуется трансформация существующих уголовно-правовых представлений о признаках каждого их составов компьютерного преступления, только после этого можно будет формулировать предмет доказывания по таким делам. Представляется, что для применения нормы уголовного права в этих случаях, как минимум, потребуется устанавливать, на каком из цифровых адресов произошел несанкционированный сбой и в чем он выразился: в повреждении технической аппаратуры, или программы, или вторжении в информацию.

Возможно, это позволит предположить, что могло иметь место преступное вторжение. Далее возможно технически удастся проследить, с какого адреса пришла вредоносная программа или информация. И только через сопоставление технических (сетевых) манипуляций может быть будет установлен и субъект этого преступления. Это усложняет задачи и проблемы доказывания.

Во первых, преступление совершается вне реального мира, не очевидно для всех кроме преступника, следовательно, его трудно выявлять обычными способами.

Во-вторых, оно не оставляет того, что можно было бы идентифицировать как след, который можно изъять, зафиксировать, приобщить к материалам дела. Возможно, информация, выраженная языком цифрового кода или алгоритма, будет понята специалистом как свидетельствующая о намеренном вредоносном действии с точки зрения техники или технологии. Однако это еще не свидетельствует о преступности совершенного деяния, ибо язык цифр требует преобразования в человеческий, единственный, на котором можно описать признаки состава преступления. Сейчас много внимания уделяется проблеме создания машиночитаемого права [8]. Эта проблема уже достаточно успешно решается. Но вот обратной логической операции, когда машина могла бы сказать человеку, что то или иное цифровое действие является преступным, пока еще нет.

В уголовном судопроизводстве есть два субъекта, которые предназначены для оказания содействия следователю и суду: специалист, который привлекается, когда возникает необходимость в использовании неких специальных знаний для оказания содействия следователю (ч.1 ст.80, ч.2.1 ст.221 УПК РК), и переводчик, который призван переводить текст с одного языка на другой (ч.1 ст.81 УПК РК). Однако в настоящее время их правовое положение не пригодно для выявления и расследования компьютерного преступления.

Специалист действует только в рамках задач, поставленных следователем, но следователь не может знать, посредством каких знаков, кодов, символов может проявить себя вредоносный характер цифрового действия, поэтому он не сможет конкретизировать задачу. Одновременно специалист, не знающий признаков данного состава преступления, не знает, а что в воспринимаемой им цифровой (кодовой) информации, собственно, необходимо следователю ввиду того, что будет иметь правовое значение. Переводчик также не приспособлен к такой ситуации. Цифровой язык не создан для свободного социального взаимодействия людей. Он создан для

взаимодействия «человек машина» и человек создает нечто искусственное, формально алгоритмичное для передачи команд машине и получения ее реакции. Чтобы выявить правовые смыслы в таком взаимодействии необходим не переводчик, а интерпретатор. Он должен понимать смысл и назначение каждой цифровой команды-кода; знать, какую реакцию машины это порождает; уметь объяснить человеческим языком весь процесс взаимодействия «человек-машина-человек». Поэтому трансформация доказывания по уголовным делам о компьютерных преступления необходима и неизбежна, однако она требует профессионального взаимодействия и совместных исследований юристов со специалистами в области цифровых технологий.

Литература

1. Руководящие принципы Комитета министров Совета Европы в отношении электронных доказательств в гражданском и административном производстве: приняты Комитетом министров 30 января 2019г., на 1335-м заседании заместителей министров // URL: https://www.coe.int/ru/web/portal/-/committeeof ministers-adopts-guidelines-on-electronic-evidence-in-civil-and-administrative-proceedin-1.

2. Маршалл Ангус М, Цифровая экспертиза: Цифровые доказательства при расследовании уголовных дел. Чичестер, Великобритания: Вайли-Блэквелл. 2008. электронная книга. ISBN: 9780470517758 и др.

3. Иккерт А.В. К вопросу о современном состоянии законодательства в сфере использования технических средств фиксации административных правонарушений в области дорожного движения // Актуальные вопросы юридической науки. 2019. №4 (4). – С. 24.

4. Шейфер С.А. Доказательства и доказывание по уголовным делам: Проблемы теории и правового регулирования. – М.: Норма, 2009.

5. П.С. Пастухов. Основы теории электронных доказательств. Монография /под ред. С.В. Зуева. – М.: Юрлитинформ. 2019. – С. 31-62.

6. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / под ред. акад. РАН Б. Н. Топорнина. Санкт-Петербург: Юридический центр Пресс, 2001. – С. 663; Волков Ю.В., Уровневое регулирование цифровых отношений / Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под : ред. Бегишева И.Р., Громовой Е.А., Залоило М.В., Филиповой И.А., А.А. Шутовой. В 6 т. Т. 1. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – С. 81-86.

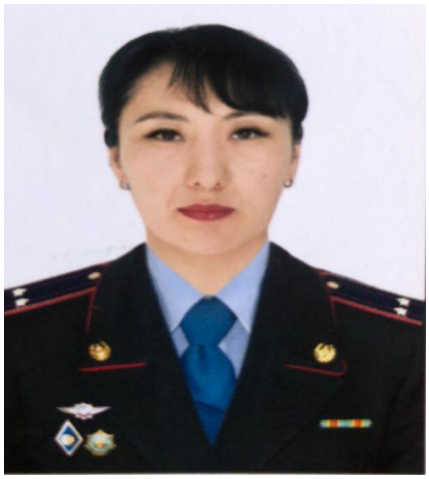
7. Основы теории электронных доказательств: монография /под ред. Зуева С.В.. – М.: Юрлитинформ. 2019. – С. 25-26, 28, 30.

8. Хабриева Т.Я., Черногор Н.Н. Будущее права. Наследие академика Степина В.С. и юридическая наука. Москва: ИНФРА-М, 2020; Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. №4. – С. 735-749.

9. Маршалл Ангус М, Цифровая экспертиза: Цифровые доказательства при расследовании уголовных дел. Чичестер, Великобритания: Вайли-Блэквелл. 2008. электронная книга.

10. Волков Ю.В, Уровневое регулирование цифровых отношений / Цифровые технологии и право: сборник научных трудов I Международной научно практической конференции (г. Казань, 23 сентября 2022 г.) / под: ред.. Бегишева И.Р, Громовой Е.А., Залоило М.В., Филиповой И.А., Шутовой А.А. В 6 т. Т. 1. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – С. 81-86.

11. Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. №4. – С. 735-749.



ДЮСЕМБАЕВА
Динара Рамазановна
старший преподаватель кафедры уголовного процесса
и криминалистики Алматинской академии
МВД Республики Казахстан им. М. Есбулатова
м.ю.н, подполковник полиции

ПРОТИВОДЕЙСТВИЕ НАРКОПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

В своем Послании народу, глава Государства дал поручение правоохранительным органам «поставить мощный заслон на пути распространения наркотических веществ среди наших граждан, особенно среди молодежи» [1].

В последние годы противодействие наркопреступлениям, совершаемым с использованием сети интернет, стало одним из ключевых направлений правоохранительных органов. Это обусловлено быстрым развитием цифровых технологий, широкой доступностью интернет – сервисов, а также растущим влиянием даркнета, что и привело к созданию новых каналов для незаконного оборота наркотиков. Платформы в даркнете, криптовалютные транзакции и мессенджеры предоставляют преступникам высокий уровень анонимности, что значительно усложняет процесс выявления и пресечения их деятельности. Эти условия создают серьезные вызовы для правоохранительных органов Казахстана и других стран, где фиксируется рост количества преступлений, связанных с распространением наркотических средств в интернете.

Значимым шагом в решении данной проблемы стало одобрение Главой государства инициативы МВД о создании Департамента по противодействию «киберпреступности». Новое подразделение МВД уже приступило к работе, сосредоточив усилия на борьбе и профилактике правонарушений в сети Интернет и социальных сетях, включая противодействие наркопреступности. Для этого оперативные службы оснащены современным оборудованием и программно-аппаратными комплексами, которые в автоматическом режиме позволяют выявлять случаи распространения наркотиков через социальные сети, мессенджеры и другие онлайн-платформы.

В рамках совершенствования законодательства введен новый состав преступления (статья 299-1 УК РК) – реклама и пропаганда наркотиков, который охватывает распространителей «граффити-рисунков» и другой информации о незаконном обороте наркотиков. [2]

Кроме того, Уголовный кодекс был дополнен новыми составами преступлений, связанными с использованием информационно-коммуникационных технологий. Склонение к потреблению наркотиков и их сбыт через Интернет отнесены к категориям тяжких и особо тяжких преступлений соответственно.

При этом, ситуация осложняется тем, что традиционные методы борьбы с наркопреступлениями недостаточно эффективны для противодействия цифровым схемам. Необходимы новые подходы, включающие киберследственные технологии, анализ криптовалютных транзакций, а также усиленное международное сотрудничество. Современные примеры противодействия интернет – наркопреступлениям демонстрируют важность координации усилий между странами, поскольку преступные сети зачастую пересекают границы, что требует единого подхода и обмена информацией.

Преступные сообщества, занимающиеся сбытом наркотических средств и психотропных веществ с использованием сети Интернет, различных мессенджеров и других технических ресурсов, различаются по своим размерам, особенностям функционирования и другим аспектам. Несмотря на это, можно выделить общие для них черты и составить типовую иерархию преступников, входящих в указанные формирования. Актуальной представляется следующая классификация:

– организаторы;

– разработчики новых формул психоактивных веществ;

– контрабандисты;

– оптовые курьеры;

– «маркетологи», отвечающие за интернет-ресурсы;

– «закладчики», размещающие наркотики по тайникам, из которых после поступления оплаты запрещенное вещество забирает покупатель;

– «складмены», получающие оптовую партию у курьеров и распределяющие меньшие партии по «закладчикам»;

– «диспетчеры», являющиеся посредниками между покупателями и «закладчиками»;

– «кадровики», отвечающие за поиск и вербовку сотрудников;

– «кассиры», распределяющие денежные средства между членами группы;

– «промоутеры», занимающиеся размещением рекламных надписей (наклеек, трафаретов, плакатов, объявлений и т.д.) в различных местах;

– «коллекторы», взыскивающие долги с членов группы, а также возвращающие похищенные ими наркотические средства и психотропные вещества;

– «обналичиватели», переводящие электронные денежные средства или криптовалюту в наличные средства;

– «кураторы», непосредственно работающие с курьерами, «промоутерами», «диспетчерами», перечисляющие им зарплату, создающие отчет по каждому сотруднику и обеспечивающие безопасность «закладчиков»;

– «дропы», паспортные данные которых используются для проведения нелегальных операций, чтобы оставить лиц, совершающих преступления, анонимными [3].

Большинство подобных преступных сообществ функционируют в так называемом «Даркнете» (от англ. «Darknet», также известен как «Скрытая сеть», «Темная сеть», «Теневая сеть», «Темный веб») и в мессенджере «Telegram».

Даркнет – это скрытый сегмент интернета, доступный только через специализированные браузеры. Для безопасности пользователей сети даркнет полностью анонимен – для доступа к нему используется зашифрованное соединение между участниками. Самым распространенным из которых является «The Onion Router» (TOR). Данная программа представляет собой систему прокси-серверов, позволяющих устанавливать сетевое соединение, защищенное от слежения и от средств анализа интернет – трафика. Анонимность интернет – трафика обеспечивается применением распределенной сети прокси-серверов.

Даркнет стал одним из основных каналов для продажи наркотиков благодаря анонимности и возможности избегать правительственных ограничений. Например, на таких площадках, как Hydra и другие, преступники могут находить покупателей и совершать сделки, оставаясь анонимными.

В Казахстане, как и в других странах все большую популярность у потребителей запрещенных веществ набирает мессенджер «Telegram», хотя используется он и законопослушными гражданами для обмена сообщениями, получения информации и т.д. Сбытчиков и покупателей наркотиков эта площадка привлекает широким набором функций сохранения анонимности.

Сбыт запрещенных веществ с помощью мессенджера «Telegram» осуществляется обычно двумя способами:

1) прямой контакт покупателя и продавца посредством переписки в секретном чате, где они договариваются об условиях сделки, после чего происходит передача наркотика путем закладки;

2) покупка через чат-боты (программы, способные расшифровывать сообщения в мессенджерах и выполнять соответствующие действия на основе этих сообщений), в которых покупатель может выбрать товар, его количество, примерное местонахождение закладки.

Использование мессенджера «Telegram» связано не только с продажей наркотиков, но и с другими преступлениями, касающимися их незаконного оборота. В частности, значительное распространение получили каналы, группы и чат-боты, пропагандирующие употребление наркотических веществ, а также предоставляющие информацию о способах их изготовления и применения.

К числу современных методов совершения наркопреступлений относится использование криптовалюты, которая представляет собой цифровую валюту, обеспечивающую учет расчетных единиц через децентрализованную платежную систему. Криптовалюта не имеет материальной или электронной формы. Фактически, это набор данных, фиксирующих объем расчетных единиц в соответствующем информационном пакете.

Наиболее популярной криптовалютой остается биткойн, широко применяемый для нелегальных финансовых операций благодаря своей анонимности. Эта анонимность обусловлена отсутствием сведений о владельцах и получателях средств, а также невозможностью проверки существования адреса, на который направляются средства.

Использование криптовалюты в целях наркоторговли:

1. Анонимные транзакции, то есть преступные группы используют криптовалюту для покупки и продажи наркотиков, так как транзакции трудно отследить. Bitcoin и Monero, в частности, остаются основными криптовалютами в теневом секторе, где Bitcoin используется чаще из-за своей популярности, а Monero предпочитают за еще более высокий уровень анонимности.

Биткойн (Bitcoin) не является полностью анонимным, однако остается одной из самых распространенных криптовалют в наркоторговле, так как его использование проще, и он имеет большую ликвидность. Благодаря распространенности биткойна его легко обменять на фиатные деньги через обменники, что упрощает «отмывание» средств.

Монеро (Monero) – криптовалюта часто используемая в наркоторговле благодаря встроенным функциям для скрытия транзакций. Монеро обеспечивает высокий уровень приватности, скрывая информацию о транзакциях (например, сумму и адреса отправителя и получателя), что делает его популярным среди тех, кто занимается незаконной деятельностью.

Эфириум (Ethereum) – криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна (децентрализованных приложений), работающих на базе умных контрактов. Реализована как единая децентрализованная виртуальная машина. В некоторых случаях наркоторговцы используют сеть эфириума, особенно при применении смарт-контрактов для проведения сделок. Однако эфириум менее популярен в этой сфере из-за публичного характера блокчейна.

2. Оплата через даркнет. Большая часть нелегальных сделок с наркотиками проходит через даркнет, где продавцы требуют оплату в криптовалюте. Такой расчет – снижает риск раскрытия личности участников и защищает преступников от отслеживания традиционными банковскими системами. Платформы, такие как Hydra и другие даркнет-рынки, используют криптовалюты для покупки и продажи запрещенных веществ.

3. Использование миксинговых сервисов, которые применяются для того, чтобы замаскировать источник и назначение средств. Преступники часто используют сервисы микширования (так называемые «миксеры»), которые позволяют разбивать и смешивать криптовалютные транзакции. Это делает их почти невидимыми для отслеживания и затрудняет работу правоохранительных органов, которые пытаются отследить средства.

4. Мультиподписи и смарт-контракты, используются наркоторговцами для обеспечения сделок и гарантии выполнения обязательств между продавцом и покупателем. Такие методы повышают безопасность операций, так как доступ к средствам возможен только при согласии нескольких сторон.

Сети и рынки, использующих криптовалюты для наркоторговли:

1. Hydra – это крупнейший даркнет-рынок в России и странах СНГ, где пользователи совершают покупки наркотиков и других нелегальных товаров с оплатой в криптовалюте. Hydra активно использует Биткойн и Монеро, предлагая своим пользователям встроенные инструкции по анонимности.

2. The Silk Road и его преемники. Silk Road был одним из первых даркнет-рынков, использовавших криптовалюту для торговли наркотиками. После его закрытия появились многочисленные платформы-наследники, такие как Dream Market и AlphaBay, которые также предоставляли возможность покупать наркотики за Биткойн и Монеро.

В Казахстане в последние годы наблюдается рост использования криптовалюты в теневых операциях и наркоторговле. Как и в других странах, даркнет-рынки и частные Telegram-каналы становятся площадками, на которых проводятся сделки с наркотиками с использованием криптовалют. Правоохранительные органы Казахстана стараются контролировать эту сферу, но сложность в отслеживании анонимных транзакций в криптовалюте остаётся серьёзной проблемой.

Однако, разные страны по-разному регулируют использование криптовалют. В Германии биткойн признан расчетной денежной единицей, в Японии – законным платежным средством, облагаемым налогом на покупку. В Швейцарии биткойн регулируется как любая иностранная валюта, что делает страну привлекательной для криптовалютных операций. В то же время в Китае банковским учреждениям запрещены любые операции с биткойнами, однако для физических лиц таких ограничений нет.

Правовой статус криптовалюты в Казахстане, регулируется Законом Республики Казахстан «О цифровых активах в Республике Казахстан» от 06.02.2023 года.

Таким образом, криптовалюты играют важную роль в наркоторговле, предоставляя анонимность и защиту от отслеживания. Однако правоохранительные органы активно работают над разработкой новых инструментов и стратегий для борьбы с незаконной деятельностью в криптовалютных сетях.

Проблемой в борьбе с криптовалютной наркоторговлей является также недостаточная осведомленность правоохранительных органов о цифровой наличности. Сотрудники просто не обладают необходимыми знаниями о криптовалюте, не владеют навыками ее обнаружения и изъятия. На современном этапе обращение с криптовалютой и борьба с криптовалютной наркоторговлей требуют значительных знаний в областях изучения нескольких дисциплин, особенно связанных с программированием и информационными технологиями.

Министерство внутренних дел Казахстана активно использует технологии блокировки сайтов и аккаунтов, подозреваемых в продаже наркотиков. Это стало возможным благодаря внедрению системы анализа сетевого трафика и мониторинга социальных сетей. Такие технологии позволяют предотвращать распространение запрещенного контента и ограничивать доступ к нему [4].

Проблемы и перспективы в борьбе с наркопреступностью в интернете:

1. Отсутствие универсального правового регулирования. Различия в законодательных нормах разных стран часто затрудняют расследования трансграничных преступлений. Ано-

нимность в сети создает дополнительные барьеры для отслеживания нарушителей, что требует разработки новых инструментов для идентификации личностей в интернете.

2. Несогласованность в действиях национальных служб безопасности разных стран снижает эффективность борьбы с кибернаркопреступностью, поскольку интернациональный характер интернета требует более тесного сотрудничества между государствами, чтобы оперативно обмениваться информацией о наркосетях и подозрительных аккаунтах.

3. Использование современных технологий в отслеживании наркопреступлений таких как искусственный интеллект и анализ больших данных, представляют собой перспективные инструменты в борьбе с наркопреступлениями. Например, алгоритмы машинного обучения могут помочь выявлять шаблоны поведения в интернете и определять потенциальные угрозы [5].

Международный опыт борьбы с наркопреступлениями в сети интернет:

1.В России работает «Госнаркоконтроль», который использует методы анализа больших данных для выявления подозрительных транзакций и онлайн-активности. Использование аналитических технологий позволяет мониторить транзакции с криптовалютами и выявлять связи между торговцами наркотиками в интернете. В 2021 году эти технологии помогли раскрыть около 200 крупных онлайн-наркосетей [6].

2. США регулярно проводят международные операции по пресечению наркоторговли в интернете, такие как операция «Dark HunTor» в 2021 году, которая была направлена на выявление преступных группировок, использующих даркнет. Операция, проводимая ФБР совместно с Интерполом, привела к аресту более 150 человек и изъятию значительного количества наркотиков и оружия. Эта операция иллюстрирует важность международного сотрудничества для выявления преступных сетей [7].

3. Европол сотрудничает с социальными сетями и крупными онлайн-платформами для борьбы с наркоторговлей. Например, через платформу SIRIUS, Европол и национальные правоохранительные органы могут быстро обмениваться данными о преступной активности в интернете. В 2022 году Европол сообщил о 40% сокращении предложений о продаже наркотиков на крупных социальных платформах благодаря сотрудничеству с их администрацией [8].

4. В развивающихся странах, где инфраструктура для мониторинга интернет-преступлений ограничена, ООН активно содействует внедрению базовых технологий и обучению специалистов. Программы ООН позволили развивающимся странам, таким как Мексика и Таиланд, внедрить системы мониторинга трафика и обмениваться информацией с международными агентствами для выявления наркопреступлений [9].

Примеры Казахстана, России, США, Европейского союза и программ ООН демонстрируют многообразие методов, используемых в борьбе с наркопреступлениями в интернете. Использование технологий, международное сотрудничество и адаптация правовых норм являются основными подходами, обеспечивающими результативность противодействия наркоторговле в сети.

В целях повышения эффективности борьбы с криптовалютной наркоторговлей необходимо разработать ведомственные акты правоохранительных органов, в которых должна быть определена методика ее обнаружения и изъятия с последующим закреплением в УПК РК.

Подытоживая, можно отметить, что наркопреступность в интернете представляет собой одну из наиболее серьезных угроз для общества и требует комплексного подхода. Совмещение правовых, технических и международных мер позволит повысить эффективность противодействия наркопреступлениям. Однако для этого необходимо адаптировать законодательство к новым вызовам, улучшить международное сотрудничество и внедрить инновационные технологии для мониторинга и выявления преступной активности в сети.

Литература

1. Послание Главы государства народу Казахстана «Единство народа и системные реформы – прочная основа процветания страны» от 1 сентября 2021г.

2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК.

3. Насыров Р.Р. Некоторые вопросы противодействия незаконному обороту наркотиков в современных условиях / Насыров Р.Р., Васильев В.Г. // Вестник Уфимского юридического института МВД России. – 2017. – № 4. – С. 88-91.

4. Алиев М.И. Блокировка сайтов, распространяющих наркотики // Криминология Казахстана. – 2022.

5. Петров В.А. Использование аналитических технологий в борьбе с наркопреступлениями // Вестник криминологии. – 2023.

6. Петров В.А. Использование криптовалют в наркопреступлениях // Вестник права и общества. – 2023.

7. Johnson M., et al. Operation Dark HunTor: Tackling Darknet Narcotic Networks // Cyber Crime Journal. – 2022.

8. Smith A., Williams D. Collaboration between Europol and Social Media Companies // European Security Review. – 2021.

9. Кузнецов И.О. Программы ООН для развивающихся стран в борьбе с киберпреступностью // Современные технологии и право. – 2020.

АЛМАЗҚЫЗЫ
Карлыгаш
старший преподаватель-методист центра
по подготовке специалистовпо по противодействию киберпреступности
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова подполковник полиции

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Согласно Закону Республики Казахстан «О национальной безопасности Республики Казахстан», одним из видов национальной безопасности является информационная безопасность, под которой понимается – состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны [1].

Следует учесть, что кибербезопасность это часть информационной безопасности государства в целом. Под кибербезопасностью мы понимаем состояние защищенности прав и интересов человека и гражданина, общества и государства от реальных и потенциальных угроз в киберпространстве на фоне развития информационной сферы, в том числе информационно-коммуникативных технологий, нашей страны. Одним из первых шагов в рамках развития правовых средств обеспечения кибербезопасности было принятие 31 декабря 1998 года постановления Правительства Республики Казахстан №1384 «О координации работ по формированию и развитию национальной информационной инфраструктуры, процессов информатизации и обеспечению информационной безопасности», которое послужило платформой для дальнейшего совершенствования законодательной базы в данной сфере. Так, было принято 3 новых редакции законов Республики Казахстан «Об информатизации» (2003, 2007, 2015 годы) и несколько специализированных законов Республики Казахстан о внесении в них соответствующих изменений по вопросам электронных форматов представления информации (данных) в том числе, по вопросам информационно-коммуникационных сетей, «электронного правительства». В целях определения государственной политики в сфере обеспечения информационной безопасности, в том числе кибербезопасности, принимались различные основополагающие концептуальные документы. В 2006 году была принята первая Концепция информационной безопасности Казахстана [2].

Она базировалась на ряде нормативных правовых актов – Конституции Республики Казахстан, Законах Республики Казахстан «О национальной безопасности Республики Казахстан», «О государственных секретах», «О борьбе с терроризмом», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О противодействии экстремизму», Концепции развития конкурентоспособности информационного пространства Республики Ка-

захстан на 2006-2009 годы, а также Концепции информационной безопасности государств – участников СНГ в военной сфере. В 2011 году была принята вторая Концепция, в которой список нормативных правовых актов был дополнен следующими законами: «О техническом регулировании» (2004), «О лицензировании» (1995), «О средствах массовой информации», «О связи» (2004). Также были использованы положения Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности (2010) и Концепции сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности [3].

Концепции о конкурентоспособности информационного пространства и об информационной безопасности стран СНГ в военной сфере сюда не вошли. Необходимо отметить, что Концепция 2011 года в части юридической базы не эволюционировала – перечень законов расширился за счет тех, что могли войти еще в версию от 2006 года, причем все они, за исключением закона о СМИ, фактически не менялись. Это говорит об очень медленном реагировании законодательства на изменения в сфере информации, которые происходят ежегодно. При этом можно обозначить, что акцент делался именно на технической стороне защиты информации (данных). Можно предположить, что чиновники смотрят на социально-политические аспекты информационной безопасности достаточно узко – во внимание берутся в основном внешнеполитические угрозы (законодательство о национальной безопасности, о секретах, о борьбе с терроризмом) или же сфера СМИ. Тогда как эта сфера гораздо шире – здесь может быть использован потенциал законов о языках, о религиозной деятельности, о культуре, об Ассамблее народа Казахстана, об образовании и т. д. Это показало бы, что Концепция отражает комплексный подход.) [4, с. 15].

В Концепции 2011 года состояние информационной безопасности оценивалось угрозами, которые можно условно разделить на внутренние и внешние.

Внутренние угрозы:

1. Неконкурентоспособность отечественного контента.

2. Отсутствие отечественных информационных технологий приводит к вынужденному использованию иностранного оборудования и информационных систем.

3. Отсутствие адекватного правового, организационного и технического режима защиты персональных данных граждан, что создает предпосылки для злоупотребления персональными данными в криминальных целях, в том числе подделки документов.

4. Недостаточно эффективное функционирование системы защиты информации.

5. Проблема нехватки квалифицированных кадров в информационнокоммуникационной отрасли.

6. Сравнительно низкий уровень общей правовой и информационной культуры, в том числе, навыков безопасного использования киберпространства в казахстанском обществе.

7. Неправомерные действия государственных структур, приводящие к нарушению законных прав и интересов физических и юридических лиц, государства в информационной сфере.

Внешние угрозы:

1. Использование ведущими странами информационных войск.

2. Активное использование экстремистскими и террористическими организациями информационно-коммуникационных сетей для своей пропаганды.

3. Угроза компьютерных атак как метод террористической деятельности.

4. Киберпреступность.

5. Влияние глобальных СМИ.

На современной этапе развития информационной сферы Казахстана и в целях реализации основных направлений Послания Главы государства народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность», постановлением Правительства Республики Казахстан от 30 июня 2017 года №407 утверждена Концепция кибербезопасности («Киберщит Казахстан»). Согласно данной Концепции, под кибербезопасностью понимаются состояние защищенности информации в электронной форме и среды ее обработки,

хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации. В анализируемой Концепции также ставится акцент на техническую составляющую защиты общественных интересов в сфере информационной безопасности, в том числе кибербезопасности.

Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов:

1) конфиденциальность информации, которая означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем. Если доступ к информации получает неуполномоченное лицо, происходят несанкционированный доступ или нарушение конфиденциальности. Для некоторых видов защищаемых законом или владельцем типов информации конфиденциальность является одним из наиболее важных атрибутов (служебная информация, охраняемые законом виды тайн, персональные данные ограниченного доступа, например, сведения о клиентах банка, кредиторах, налоговые данные, сведения медицинских учреждений о состоянии здоровья пациентов и т.д.).

2) целостность информации – способность информации (данных) сохрняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к нарушению целостности. Особенно важна целостность данных, связанных с функционированием объектов критической информационно-коммуникационной инфраструктуры (например, автоматизированные системы управления воздушным движением, электро – энергоснабжения и так далее).

3) доступность информации определяется способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводят к потере доступности. Доступность – важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиентов путем предоставления информационно-коммуникационных услуг (информационные системы продажи железнодорожных и авиационных билетов, банковских услуг, распространение продукции Интернет-ресурсами и электронными СМИ в Интернете). Ситуацию, когда уполномоченный пользователь не может получить доступ к определенным услугам (чаще всего сетевым), называют отказом в обслуживании [5].

Кроме этого, в связи с развитием коммуникационных (сетевых технологий) также дополнительно выделяют еще два свойства информационной безопасности, связанные с личностью лица, управляющего или использующего информационную систему или электронный информационный ресурс с использованием сети удаленно: аутентичность и апеллируемость. Под аутентичностью понимается возможность достоверно установить автора юридически значимого действия с информацией или сообщения в сфере оказания информационно-коммуникационных услуг, например, в электронной коммерции, когда используются электронно-цифровая подпись или иной способ аутентификации. Апеллируемость (неотрекаемость) – возможность при отказе от авторства доказать, что автором действий с информацией в информационной системе или ресурсе является именно данный пользователь и никто другой путем регистрации совершаемых действий. Как известно, основами современных программно-технических средств безопасности являются, аутентификация и идентификация так как любые информационно-коммуникационные технологии-услуги и сервисы в основном рассчитаны на обслуживание субъектов-пользователей.

Аутентификация (установление подлинности) – проверка принадлежности к субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Идентификация – присвоение субъектам доступа к информационной системе или электронному ресурсу личного идентификатора, обеспечивающего установление подлинности и определение полномочий субъекта при его допуске в информационную систему, контроль полномочий в процессе сеанса работы и регистрацию действий [5]. Согласс-

но отмеченной выше Концепции кибербезопасности, под угрозой информационной безопасности понимается потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или компоненты информационной системы или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей. Наиболее распространенные угрозы информационной безопасности – это сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и так далее), неправильное хранение архивных данных, нарушения прав доступа к данным, некорректная работа пользователей и обслуживающего персонала, потери информации (из-за несанкционированного доступа или инфицирования вредоносными программами – компьютерными вирусами), компьютерная атака, под которой понимается целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно-аппаратных средств (или протоколов межсетевого взаимодействия) [5].

В целом, в Республике Казахстан организационно-правовые и технические основы системы мер по обеспечению информационной безопасности в области информатизации и связи (кибербезопасности) формировались и законодательно закреплялись как составляющие информационной безопасности и обеспечения безопасности информационного пространства и инфраструктуры связи в соответствии с Законом Республики Казахстан «О национальной безопасности». На наш взгляд, Концепция кибербезопасности, рассчитанная на 2017-2022 годы, учла многие стороны развития современного казахстанского общества. Так, различные вопросы обеспечения информационной безопасности нашли свое отражение и развитие в отечественном законодательстве: Уголовном кодексе, Кодексе «Об административных правонарушениях», законах «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», и в целом ряде подзаконных актов, разработанных в рамках реализации Закона Республики Казахстан «Об информатизации», вступившего в силу с 1 января 2016 года. Следует отметить, что новая редакция Уголовного кодекса Республики Казахстан, действующая с 01 января 2014 года, предусматривает отдельную главу, посвященную преступлениям, совершаемым в сфере информатизации и связи. С учетом квалифицирующих обстоятельств в ней содержится 38 составов преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций [6].

В Кодекс Республики Казахстан «Об административных правонарушениях» включен ряд составов административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе на должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде нарушения требований по эксплуатации средств защиты электронных информационных ресурсов, невыполнения Единых требований, неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, мер по их защите [7].

Благодаря централизации подключения к Интернету через Единый шлюз доступа к Интернету государственных органов существенно снижены угрозы несанкционированного доступа и вредоносного воздействия на электронные информационные ресурсы государственных органов. На ежедневной основе фиксируется и отражается более 180 миллионов атак различного уровня. Создана и совершенствуется система правовых, организационных, технических и криптографических мер защиты государственных секретов, обрабатываемых с использованием средств вычислительной техники. Наиболее чувствительная для безопасности государства информация в электронной форме передается только через сети телекоммуникаций специального назначения, физически отделенные от Интернета и использующие криптографические средства защиты информации.

В целом, с первых этапов становления вопросов информационной безопасности с учетом характера содержащейся информации дифференцированы правовые режимы общедоступных и конфиденциальных электронных информационных ресурсов и систем, установлены права и обязанности собственников, владельцев и пользователей по их защите. Но необходимо отметить, что характерная для последних десятилетий общемировая тенденция внедрения достиже-

ний информационно-коммуникационных технологий с темпами, существенно опережающими формирование культуры их использования, и укоренения общественных и производственных отношений, характерных для «информационного общества», в первую очередь, в вопросах обеспечения кибербезопасности, в Казахстане также находит свое подтверждение.

На сегодняшний день, в сфере обеспечения кибербезопасности Казахстана можно отметить такие угрозы как:

– низкая цифровая и правовая грамотность населения, работников сферы информационно-коммуникативных технологий, персонала и руководителей организаций по вопросам информационной безопасности;

– нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере информационно-коммуникативных технологий установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;

– непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

– действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

– деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру [5].

Таким образом, в целях обеспечения кибербезопасности, необходимо:

– направить усилия государства на формирование в казахстанском обществе устойчивых представлений о «кибергигиене» и привитии высокой производственной культуры создания и использования информационно-коммуникационных технологий на всех этапах жизненного цикла программных продуктов, информационных систем, программного обеспечения, технологических платформ, информационной и сетевой инфраструктуры, поддерживающего оборудования;

– проведение тренингов и обучающих практик по защите персональных данных и неприкосновенности частной жизни среди пользователей Интернета, в том числе несовершеннолетних и их родителей;

– необходимо в реализации образовательных и научно-исследовательских задач в сфере информационной безопасности важнейшую роль обозначить высшим учебным заведениям Казахстана, что позволит расширить технические возможности специальных государственных и правоохранительных органов по обеспечению информационной безопасности (в т.ч. кибербезопасности) государства и повысить уровень аналитического и научно-исследовательского сопровождения данных мероприятий.

В рамках повышения эффективности предупредительного потенциала в сфере превенции киберпреступности, следует отметить необходимость решения задач по закладыванию и поддержанию высокого уровня профессиональной компетенции и технической готовности специализированных подразделений путем постоянного повышения квалификации личного состава, расширения арсенала технических средств фиксации и криминалистических исследований «цифровых» доказательств с использованием результатов научно-исследовательских работ, проводимых отечественными учебными заведениями и исследовательскими учреждениями, в том числе, подведомственных специальным и правоохранительным органам Республики Казахстан. Следует обозначить, что обеспечение кибербезопасности является задачей всех субъектов, деятельность которых связана с использованием информационно-коммуникационных

технологий, поэтому сотрудничество в целях обеспечения информационной безопасности, будет способствовать защите интересов всех заинтересованных сторон в данной сфере.

Литература

1. Закон Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» // Сетевое издание «Zakon.kz» [Электронный ресурс] : Режим доступа: http://www. zakon. kz.

2. Концепция информационной безопасности Республики Казахстан до 2011 года // Информационная система «ПАРАГРАФ» [Электронный ресурс] : Режим доступа: https://prg.kz/

3. Концепция информационной безопасности Республики Казахстан до 2016 года // Информационная система «ПАРАГРАФ» [Электронный ресурс] : Режим доступа: https://prg.kz/

4. Сабитов Д. Информационная безопасность Казахстана: защита данных и смыслов. Институт мировой экономики и политики (ИМЭП) при Фонде Первого Президента Республики Казахстан / Д. Сабитов. – Астана – Алматы: Лидера Нации, 2015. – С. 68. 34

5. Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан») // Сетевое издание «Zakon.kz» [Электронный ресурс] : Режим доступа: http://www. zakon. kz.

6. Уголовный кодекс Республики Казахстан от 03 июля 2014 года №226 – V ЗРК // Сетевое издание «Zakon.kz» [Электронный ресурс] : Режим доступа: http://www. zakon. kz.

7. Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года №235-V ЗРК // Сетевое издание «Zakon.kz» [Электронный ресурс] : Режим доступа: http://www. zakon. kz.

БЕЙСЕНБАЙ
Әлия Бейсенбайқызы
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының
аға оқытушы-әдіскері полиция майоры

ЦИФРЛЫҚ КЕҢІСТІКТІ ДАМЫТУ ЖӘНЕ КИБЕРҚЫЛМЫС

Мақалада сандық кеңістік киберқылмыс тұрғысынан талданады. Сандық кеңістік қоғамдық өмірдің әр саласына енеді. Мемлекет үшін негізгі жүйе, елді және азаматтарды қылмыстық қол сұғушылықтан қорғауға қабілетті құқық қорғау органдары құқықтық жүйе болып табылады. Өзекті мәселелердің бірі киберқылмыстың әлемдік өсуі. Толыққанды болу үшін киберқылмысқа қарсы іс-қимыл тетіктерін әзірлеу қажет ақпаратты қорғау, кибершабуылдардың алдын алу шараларын күшейту.

Түйін сөздер: сандық кеңістік; киберкеңістік; киберқылмыс; инновация технологиясы; бопсалау; алаяқтық; ұрлық.

Цифрлық кеңістік қоғамдық өмірдің әр саласына енеді, нәтижесінде прогресс пайда болып қана қоймай, киберқылмыс пайда болады. Оның ерекшеліктері бар, соның арқасында ол шекаралар мен кеңістіктік шектеулер жоғалады. Осыған байланысты ақпараттық қауіпсіздікті қамтамасыз ету үшін белгілі бір шаралар қабылдау қажет.

Киберқылмыс интернет-беттерді бұзуға, зиянды бағдарламаларды таратуға және ақпараттық технологиялар арқылы виртуалды кеңістікте қылмыстық әрекеттерді жүзеге асыратын адамдардың заңсыз ақпаратқа негізделеді. Мұндай заңсыз әрекеттерді жүзеге асыру үшін компьютер маңызды рөл атқарады. Бұл шабуылдаушыларға ақпаратты ұрлауға, жоюға немесе бүлдіруге ғана емес, сонымен қатар компьютерлік вирустары бар зиянды сайттарды орналастыруға мүмкіндік беретін техникалық құрал. Қылмыстың бұл түрі, басқалардың бәрі сияқты, қоғамның ақпараттық қауіпсіздігіне қауіп төндіреді. Банк карталарынан ақша ұрлаудан басқа, киберқылмыскерлер адамның жеке деректерін ұрлауды үйренді, бұл ақпарат желіде жарияланған жағдайда оның беделіне орны толмас зиян келтіруі мүмкін. Киберқылмыс-бұл әрбір жеке интернет-пайдаланушының проблемасы ғана емес, оны кеңірек, әлеуметтік және тіпті халықаралық деңгейде қарастыру керек. Киберқылмыстың өсуінен тек жеке тұлғалар ғана емес, заңды тұлғалар да зардап шегеді; біздің заманымыздағы хакерлік шабуылдардың құрбаны-бүкіл елдер, мемлекеттер [4, 383 б.].

Мемлекет үшін елді және азаматтарды қылмыстық қол сұғушылықтан қорғауға қабілетті негізгі жүйе құқық қорғау органдарының жүйесі болып табылады. Ол неғұрлым дамыған болса, соғұрлым тиімді болады, бірақ барлық проблемаларды болдырмау үшін оны түзету мүмкін емес. Кейде туындаған мәселелердің шешімін табу өте қиын, сіз көптеген ақпаратты

өңдеп, бірқатар қадамдар жасауыңыз керек. Өзекті мәселелердің бірі-киберқылмыстың әлемдік өсуі [1-4].

Көптеген жүйелер сыртқы әсерлерден қорғаудың жоғары деңгейіне ие, бірақ бұл деректерді кибершабуылдардан 100% қорғау үшін әрдайым жеткіліксіз. Айта кету керек, интернет-алаяқтардың саны артып келеді, көптеген қылмыскерлер фишингпен, деректерді ұрлаумен, кибиотерроризм. Киберқылмыстың дамуы интернет-технологияларды жаппай қолданумен тығыз байланысты.

Киберқылмыспен күресуге бағытталған маңызды қадам 2001 жылы 23 қарашада Будапештте Еуропа Кеңесінің мүшелері қол қойған компьютерлік ақпарат саласындағы қылмыс туралы Конвенция қабылданды. Шын мәнінде, ұлттық деңгейде қолданылатын бұл Конвенция киберқылмыстық әрекеттерді құқықтық құдалау қажеттілігін бекіткен алғашқы құжат болды. Онда киберқылмыстың төрт негізгі түрі туралы айтылды: заңсыз қол жеткізу, заңсыз ұстау, деректерге араласу, жүйеге араласу. Алайда, өткен 20 жыл ішінде киберқылмыс жақсарды және біздің заманымызда фишинг, фарминг, есірткі кибер саудасы, кибертерроризм, әлеуметтік хакерлік (қарақшылық) және т.б. сияқты көптеген сорттар бар [2, 72 б.].

Интернет-технологияларды белсенді пайдалану шабуылдаушыларға ең аз із қалдырып және кез келген елдің аумағында бола отырып, қылмыстық әрекеттер жасауға мүмкіндік береді. Қысқа уақыт ішінде көптеген компаниялар қашықтан жұмыс істеуге көшті, ал деректерді қорғауға дайын болмады, сонымен қатар шектеулер қою әрқашан қылмыстың өсуіне әкеледі, бірақ көшеге шығу мүмкін болмағандықтан, қылмыс жаңа мүмкіндіктер іздей бастады және онлайн режимге көшті. Екінші фактор-қорқыныштың болмауы: қылмыскер ұсталмайтынына сенімді, өйткені ол физикалық із қалдырмайды және қылмыстың бұл түрінің ашылуы төмен. Қазіргі кезеңде зерттеушілер келесі мәселені шешуі керек: қажет емес ақпаратты алып тастау және мәселені зерттеуге көмектесетін біреуін таңдау, содан кейін киберқылмысқа қарсы тиімді шараларды әзірлеуге болады. Қазіргі уақытта жалған ақпараттың таралуына байланысты ақпарат өрісінің шамадан тыс жүктелуі байқалады. Интернет үлкен мүмкіндіктер беріп қана қоймай, белгілі бір тәуекелдерді тудырады [4; 5; 9].

Әдетте, кибершабуылдардың келесі мақсаттары бар:

– Бұл ақпаратты ұрлау және сату.

– Мемлекеттік органдардың жұмысына зиян келтіру.

– Террористік әрекеттер.

– Бопсалау.

– Алаяқтық.

– Ұрлық.

Киберқауіптерге қарсы іс-қимыл саласында барынша тиімді саясатты жүргізу үшін цифрландыру үдерісінің жетістіктері мен ресурстарын толық көлемде пайдалану қажет. Цифрландыру елдің ұлттық және ақпараттық қауіпсіздігін қамтамасыз ету саясатында маңызды рөл атқара алады. Цифрлық инновацияларды дұрыс енгізу және пайдалану Пайдаланушының жеке деректерін де, мемлекеттік деңгейдегі және маңызы бар құпия материалдарды да қорғау міндетін едәуір жеңілдетеді [18, 259 б].

Бұл саладағы ең перспективалы технологиялардың бірі блокчейн. Ол кибершабуылдарға қарсы күресте жаңа мүмкіндіктер ұсынады, мысалы, үшінші тұлғаларға ақпараттың ағып кету мүмкіндігінен деректерді қорғауды арттыру. Егер бұрын киберқылмыскерлер операцияны бір рет жасап, қажетті деректерді алу жеткілікті болса, енді блокчейн бұл процесті оған айтарлықтай қиындатады.

Тағы бір маңызды аспект-ақпарат алмасу процесін қорғау. Мысалы, WhatsApp сияқты мессенджерді қорғау үшінші тұлғалардың жеке хат алмасуына қол жеткізе алмайтындығына жүз пайыз кепілдік бермейтіні белгілі, өйткені шифрлау жетілмеген және әлсіз жағы бар (метадеректер бөлек жүйелерде сақталады). Хакерлердің кіруіне жол бермеу үшін метадеректерді бөлу және осылайша олардың жиынтық жарамсыздығына кепілдік беру арқылы желіні орталықсыздандыруға қабілетті блокчейн технологиясын қолдануға болады [10, 172 б].

Әрине, тек Blockchain технологиясы киберқылмыстық қызметті тоқтату үшін тиімді ақпараттық саясат жүргізу үшін жеткіліксіз болады. Бұл салаға жасанды интеллект ресурстары да қатысуы мүмкін [15, 127 б]. Мысалы, АҚШ-та әрбір полиция бөлімшесі кескін арқылы бетті тану бағдарламасымен жабдықталған. Бұл технология іс жүзінде белсенді қолданылады, бұл қылмыскерлерді іздеуді едәуір жеңілдетеді және шабуылдаушылардың портреттерін жасау процесін жеделдетеді [17, 53 б].

Қазіргі әлемде киберқылмыс қоғамға және оның ақпараттық қауіпсіздігіне үлкен қауіп төндіреді. Киберқылмыс жедел әрекет етуді және тиімді шешуді қажет ететін әлеуметтік мәселелер кешенін тудырады [12; 13; 14].

Ақпараттық технологияларды жетілдіре отырып, киберқылмыс адам өмірі мен қызметінің көптеген салаларында және тұтастай алғанда қоғамда көрініс табады. Қылмыстың осы түрінен қорғау халықаралық ынтымақтастық пен өзара іс-қимыл деңгейіндегі күш-жігердің корреляциясын болжайды [15; 16].

Ақпараттық құқық бұзушылықтар мен киберқылмыстарға қарсы тиімді саясат жүргізу үшін мынадай шаралар қолданылуы мүмкін:

1) желіде киберқылмыстарды анықтауға жәрдемдесетін технологияларды, сондай-ақ осы құқық бұзушылықтарға тергеу жүргізу тәсілдерін жетілдіру [14, 175 б];

2) киберқауіптерге қарсы тұру үшін блокчейн технологиясын барынша кеңінен қолдану;

3) жасанды интеллект ресурстарын дамыту және оларды киберқылмыстарды тергеу саласына дәйекті енгізу;

4) кибертерроризмнің барлық ықтимал нысандары мен көріністерінде оған қарсы мақсатты күрес.

Киберқылмыскерлер дамып келеді, сайттарды қорғаудың әлсіз жақтарын, қылмыс жасауға көмектесетін жаңа бағдарламалық жасақтаманы іздейді, ақпараттық жүйелер мен азаматтардың жеке беттері мен файлдарына ғана емес, сонымен қатар мемлекеттік органдарға, ірі кәсіпорындарға, банк саласына да кибершабуылдар жасайды. Осыған байланысты көптеген салалардың қалыпты жұмысы бұзылады, адамдардың өміріне қауіп төнеді немесе елеулі қаржылық шығындар туындайды. Қылмыскерлер құпия және құпия ақпаратты ұрлап, ақшаны әртүрлі тәсілдермен ұрлап, әртүрлі сипаттағы зиян келтіруі мүмкін [2; 5; 6; 9].

Мемлекет ықтимал қауіп-қатерлерге тез және қатаң жауап беруі керек, ең дұрысы қылмыс жасалғанға дейін де оларды көрсетуі керек. Бұл әсіресе мемлекеттік қауіпсіздікке қатысты мәселелерге қатысты. Мәселені шешудің бірнеше әдісі бар:

– Ақпарат жүйелерін бақылауды күшейту, тіпті олар шетелдік типтерге жатса да және ТМД-да орналасқан компьютерлерде тұрса да.

– Киберкеңістікте жасалған заңсыз әрекеттер үшін қылмыстық жазаны қатаңдату, сондай-ақ провайдерлерді ақпаратты сақтау ережелерін бұзғаны үшін жазалау, әсіресе бұл мемлекеттік немесе коммерциялық құпияны қамтитын ақпаратты ұрлауға немесе жариялауға әкеп соқтырса.

– Қызметкерлердің білімі мен біліктілігін арттыру, олармен ақпараттық қауіпсіздік саласындағы сауаттылықты арттыратын тұрақты іс-шаралар өткізу.

– Зиянды бағдарламалар мен кибершабуылдардан қорғауға қабілетті антивирустар мен басқа да бағдарламалық жасақтама әзірлейтін компанияларды қаржыландыруды арттыру.

Тек жоспарлы және қажырлы жұмыс киберқылмыс деңгейін едәуір төмендетуге, деректерді қылмыстық қол сұғушылықтан сенімді қорғауды қамтамасыз етуге көмектеседі.

Әдебиет

1. Дауров А.И. Қазіргі кездегі киберқылмыспен күрес жағдайына әсер ететін факторлар. Ресей заңнамасындағы олқылықтар. 2021. Т. 14. №4. 155-158 бб.

2. Карцхия А.А., Макаренко Г.И. Қазіргі киберқауіпсіздік пен қарсылықтың құқықтық аспектілері киберқылмыс / киберқауіпсіздік мәселелері. 2023. №1 (53). 58-74 бб.

3. Солоненко К.М. Ресей Федерациясындағы киберқылмыс: Қазіргі даму тенденциялары және оған қарсы әрекет / құқық саласы. 2022. №4. 67-77 б.

4. Маныч Е.Г. Ресейдегі киберқылмыс: негізгі криминологиялық көрсеткіштер және оның қазіргі заманғы көрсеткіштері тенденциялар / XXI ғасырдағы мемлекет және құқық. 2021. №1. 56-60 б.

5. Теуважуков А.Х. Кибер кеңістікте жасалған қылмыстарды анықтау мен алдын-алудың кейбір мәселелері / қолданбалы зерттеулер журналы. 2023. №4. 152-155 бб.

6. Хисамова З.И., Бегишев И.Р. Пандемия жағдайындағы цифрлық қылмыс: негізгі трендтер // Бүкіләлемдік криминологиялық журнал. 2022. Т. 16. №2. 185-198 бб.

7. Швыряев П.С. Ресейдегі киберқылмыс: қоғам мен мемлекет үшін жаңа сынақ / Мемлекет басқару. Электрондық хабаршы. 2021. №89. 184-196 бб.

8. Шикула И.Р., Куркин Е.Н. Күрестің негізгі әдістері және қарсы күрес туралы / Халықаралық эксперименттік білім журналы. 2023. №1. 37-41 б.

9. Шхагапсоев З.Л. Тиімді ашуға және тергеуге кедергі келтіретін кейбір факторлар туралы киберкеңістікте жасалған қылмыстар / экономикалық қауіпсіздік хабаршысы. 2021. №2. – 258 б.

10. Антониан Е.А., Аминов И.И. Блокчейн-кибертерроризмге қарсы іс-қимыл технологиялары // 2019. №6 (103). 170-175 б.

11. Волынская О.В. Киберқылмыспен күресте құқықтық ой мен перспективаны дамыту қылмыстық іс жүргізу // Ресей ІІМ Мәскеу университетінің хабаршысы. 2020. №3. 72-74 б.

12. Даненьян А.А. Киберкеңістікті халықаралық құқықтық реттеу / Білім беру және құқық. 2020. №1. 261-269 б.

13. Кумышева М.К., Геляхова Л.А. Ресейдегі және әлемдегі киберқылмыс туралы мәселеге олқылықтар // Ресей заңнамасы. 2018. №4. 383-385 б.

14. Мартьянов Н.Р. Қазіргі кезеңдегі киберқылмыстарға қарсы қылмыстық-құқықтық күрес // Мемлекеттік қызмет және кадрлар. 2020. №1. 175-177 б.

15. Тимофеев А.В. Қазіргі заманғы контекстегі жасанды интеллекттің мәні мен мәселелері ғылыми және философиялық идеялар / / Мәскеу мемлекеттік облыстық газеті университет. Серия: Философиялық ғылымдар. 2020. №2. 127-133 б.

16. Тарасик Н.М. Киберқылмыспен күрестің құқықтық негіздерін талдау // химия және химия технологиясындағы жетістіктер. 2016. №5(174). 66-68 б.

17. Тишутина И. Глобалдық цифрландыру жағдайындағы қылмыстарды ашу мен тергеудің жаңа мүмкіндіктеріне / Тула мемлекеттік университетінің жаңалықтары. Экономикалық және заң ғылымдары. 2019. №4. 46-55 б.

18. Шинкарецкая Г.Г., Берман А.М., Цифрландыру және ұлттық қауіпсіздікті қамтамасыз ету мәселесі // Білім және құқық. 2020. №5. 254-260 б.

19. Горбунов А.С. Мемлекеттің ақпараттық қауіпсіздігі контекстіндегі тұлға / Сібір мұғалім. 2017. №5 (114). 64-68 б.

ҚҰЛМАН
Ернұр Ерланұлы
Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы киберқылмысқа қарсы іс-қимыл бойынша
мамандарды даярлау орталығының оқытушы-әдіскері
полиция лейтенанты

МОБИЛЬДІ ҚОСЫМШАЛАРДЫҢ ҚАУІПСІЗДІГІ ЖӘНЕ МОБИЛЬДІ ҚАУІПТЕРГЕ ҚАРСЫ ТҰРУ

Цифрлық дәуірде мобильді құрылғылар біздің күнделікті өміріміздің ажырамас бөлігіне айналды. Смартфондар мен планшеттер тек қарым-қатынас пен ойын-сауық үшін ғана емес, сонымен қатар жұмыс, қаржылық операциялар және жеке ақпаратты сақтау үшін де қолданылады. Мобильді қосымшалардың функционалдығы артқан сайын, осы құрылғыларға бағытталған қауіптер саны да артып келеді.

Мобильді қосымшалардың қауіпсіздігі әзірлеушілер үшін де, пайдаланушылар үшін де маңызды аспектке айналады. Платформаға қарамастан-iOS немесе Android – мобильді құрылғылар әртүрлі шабуылдарға ұшырайды, бұл құпия деректердің ағып кетуіне, қаржылық шығындарға немесе құрылғының дұрыс жұмыс істемеуіне әкелуі мүмкін.

Кілтті сөздер: қауіпсіздік, мобильді қосымшалар, әлеуметтік медиа, хакерлер, қорғау.

Қазіргі әлемде мобильді құрылғылар күнделікті өмірімізде ажырамас бөлігі болған кезде, мобильді қосымшалардың қауіпсіздігі мәселелері барған сайын маңызды бола түсуде. Смартфондар мен планшеттерде жеке фотосуреттерден бастап банк карталарының деректері мен корпоративтік ақпаратқа дейінгі жеке және құпия ақпараттың үлкен көлемі бар. Бұл оларды киберқылмыскерлер үшін тартымды нысанға айналдырады, олар үнемі шабуылдардың жаңа әдістерін әзірлеп, осалдықтарды пайдаланады. Осыған байланысты мобильді қосымшаларды әзірлеушілер, ақпараттық қауіпсіздік мамандары және соңғы пайдаланушылар ағымдағы қауіптер мен олардан қорғану әдістері туралы хабардар болуы қажет.

Мобильді қосымшалардың қауіпсіздігіне негізгі қауіптердің бірі – деректердің жылыстауы. Бұл әртүрлі жолдармен болуы мүмкін, соның ішінде қорғалмаған желілік қосылымдарды ұстап алу, қосымшаның немесе операциялық жүйенің өзіндегі осалдықтарды пайдалану, сондай-ақ құрылғыны жоғалту немесе ұрлау нәтижесінде. Деректердің жылыстауы жеке пайдаланушылар үшін де, ұйымдар үшін де ауыр салдарға әкелуі мүмкін. Пайдаланушылар үшін бұл қаржылық шығындарға, жеке басын ұрлауға немесе құпиялылықты бұзуға әкелуі мүмкін. Ұйымдар үшін салдары одан да ауыр болуы мүмкін, оның ішінде беделге нұқсан келтіру, қаржылық шығындар және заңды проблемалар бар [1].

Тағы бір маңызды қауіп – арнайы мобильді платформаларға арналған зиянды бағдарламалық жасақтама. Мұндай бағдарламалық жасақтама құрылғыға фишингтік шабуылдар, сенімсіз көздерден қосымшаларды жүктеу немесе заңды қосымшалардағы осалдықтарды пайдалану арқылы енуі мүмкін. Зиянды бағдарламалық жасақтама деректерді ұрлау, пайдаланушы белсенділігін бақылау, спам жіберу немесе тіпті пайдаланушының білімінсіз құрылғыны криптовалюта майнингі үшін пайдалану сияқты әртүрлі зиянды әрекеттерді орындай алады.

Құрылғыда деректерді қауіпсіз сақтамау да айтарлықтай қауіп төндіреді. Көптеген қосымшалар құпия ақпаратты құрылғыда жергілікті сақтайды, және егер бұл деректер тиісті түрде шифрланбаса, олар құрылғыға физикалық қол жеткізу кезінде немесе зиянды бағдарламалық жасақтама арқылы қаскүнемдерге оңай қол жетімді болуы мүмкін.

Қорғалмаған желілік қосылымдар мобильді қосымшалардың қауіпсіздігіне тағы бір маңызды қауіп төндіреді. Қосымша деректерді қорғалмаған байланыс арқылы жібергенде, бұл ақпаратты «ортадағы адам» (Man-in-the-Middle) түріндегі шабуылдарды қолданатын қаскүнемдер ұстап алуы мүмкін. Бұл әсіресе жиі тиісті қорғанысы жоқ жалпыға қолжетімді Wi-Fi желілерін пайдалану кезінде қауіпті.

Қосымшалардың кодындағы осалдықтар да қауіптердің маңызды көзі болып табылады. Аутентификация және авторизация механизмдерін іске асырудағы қателер, криптографиялық кілттерді қауіпсіз сақтамау, кіріс деректерін тексерудің болмауы - мұның бәрін қаскүнемдер қосымшаны бұзу және пайдаланушы деректеріне рұқсатсыз қол жеткізу үшін пайдалана алады [2].

Осы қауіптерге қарсы тұру үшін мобильді қосымшалардың қауіпсіздігін қамтамасыз етуге кешенді көзқарас қажет. Негізгі әдістердің бірі – деректерді шифрлау. Құрылғыда сақталатын немесе желі арқылы берілетін барлық сезімтал деректер заманауи криптографиялық алгоритмдерді қолдана отырып шифрлануы керек. Бұл тыныштық күйіндегі деректерді де (құрылғыда сақталған), қозғалыстағы деректерді де (желі арқылы берілетін) қамтиды. Құрылғыдағы деректерді шифрлау үшін iOS-тегі KeyChain немесе Android-тегі KeyStore сияқты операциялық жүйелердің кіріктірілген механизмдерін пайдалануға болады, олар криптографиялық кілттерді қауіпсіз сақтауды қамтамасыз етеді.

Қауіпсіз аутентификация – мобильді қосымшаларды қорғаудың тағы бір маңызды аспектісі. Қазіргі жағдайда күрделі құпия сөздерді пайдалану жеткіліксіз. Оның орнына пайдаланушының түпнұсқалығын тексерудің бірнеше әдісін біріктіретін көп факторлы аутентификацияны енгізу ұсынылады. Бұған пайдаланушы білетін нәрсе (құпия сөз), оның қолында бар нәрсе (құрылғы немесе токен) және ол болып табылатын нәрсе (биометриялық деректер) кіруі мүмкін. Саусақ іздерін немесе бетті тану сияқты биометриялық аутентификация мобильді құрылғыларда кеңінен таралуда және қауіпсіздіктің қосымша деңгейін қамтамасыз етеді [3].

Кері инжиниринг пен қосымша кодын талдаудан қорғау да қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады. Қаскүнемдер оның ішкі құрылымын зерттеу және осалдықтарды табу үшін қосымшаны декомпиляциялауға тырысуы мүмкін. Бұған қарсы тұру үшін оның талдауын қиындататын кодты бүркемелеу әдістері қолданылады. Сонымен қатар, оның мінез-құлқын талдау үшін қосымшаны бақыланатын ортада іске қосуды болдырмау үшін күйін келтіру мен эмуляциядан қорғау техникасын қолдану маңызды [4].

Тұрақты жаңартулар мен патчтар мобильді қосымшалардың қауіпсіздігін сақтаудың маңызды құрамдас бөлігі болып табылады. Жаңа осалдықтар анықталған сайын әзірлеушілер осы проблемаларды жоятын жаңартуларды жедел шығаруы керек. Өз кезегінде пайдаланушылар осы жаңартуларды уақтылы орнатудың маңыздылығы туралы хабардар болуы керек. Қосымшаларды автоматты түрде жаңарту бұған көмектесе алады, бірақ ол заңды жаңартуды зиянды кодпен алмастыруды болдырмау үшін қауіпсіздікті ескере отырып жүзеге асырылуы керек.

Мобильді құрылғыларда антивирустық бағдарламалық жасақтаманы пайдалану да қорғаныс деңгейін едәуір арттыра алады. Мобильді операциялық жүйелерде кіріктірілген

қауіпсіздік механизмдері болса да, антивирустық бағдарламалық жасақтама түріндегі қосымша қорғаныс деңгейі стандартты қорғаныс механизмдері арқылы өтуі мүмкін зиянды бағдарламаларды анықтауға және бұғаттауға көмектесе алады. Қазіргі заманғы мобильді антивирустар жиі фишингтен қорғау, құпия сөздерді қауіпсіз сақтау және VPN қызметтері сияқты қосымша қауіпсіздік функцияларын қамтиды [5].

Пайдаланушыларды оқыту – мобильді құрылғылар мен қосымшалардың жалпы қауіпсіздігін қамтамасыз етудегі маңызды аспект. Тіпті ең жетілдірілген техникалық қорғаныс шаралары, егер пайдаланушылар ықтимал тәуекелдерді түсінбесе және қауіпсіздіктің негізгі ережелерін сақтамаса, тиімсіз болуы мүмкін. Пайдаланушылар фишингтік шабуылдардың белгілерін тануға, тек ресми қосымшалар дүкендерін пайдаланудың маңыздылығын түсінуге, қосымшалар сұрайтын рұқсаттарға абай болуға және өз құрылғылары мен қосымшаларын үнемі жаңартып отыруға үйретілуі керек.

Корпоративтік пайдаланушылар үшін мобильді құрылғылардан корпоративтік ресурстарға қол жеткізуді бақылау қауіпсіздіктің маңызды аспектісі болып табылады. Виртуалды жеке желілерді (VPN) пайдалану мобильді құрылғы мен корпоративтік желі арасындағы қауіпсіз байланысты қамтамасыз етеді, берілетін деректерді ұстап алудан қорғайды. Мобильді құрылғыларды басқару жүйелері (MDM) ұйымдарға корпоративтік мобильді құрылғылардың қауіпсіздігін орталықтан басқаруға мүмкіндік береді, оның ішінде құрылғыны жоғалтқан немесе ұрлаған жағдайда деректерді қашықтан бұғаттау немесе өшіру мүмкіндігі бар.

Мобильді қосымша мен серверлік бөлік арасында деректерді беру кезінде деректердің қауіпсіздігі де ерекше назар аударуды қажет етеді. Дұрыс конфигурацияланған SSL/TLS сертификаттары бар HTTPS хаттамасын пайдалану міндетті минимум болып табылады. Сонымен қатар, жалған сертификаттарды пайдалана отырып шабуылдардың алдын алу үшін сертификаттарды бекіту сияқты қосымша шараларды пайдалану ұсынылады [6].

Мобильді қосымшалардың қауіпсіздігінің маңызды аспектісі – пайдаланушы енгізуін дұрыс өңдеу. Пайдаланушыдан немесе сыртқы көздерден алынған барлық деректер әлеуетті қауіпті ретінде қарастырылуы керек.

Пайдаланушыдан немесе сыртқы көздерден алынған барлық деректер әлеуетті қауіпті ретінде қарастырылуы керек және пайдаланар алдында мұқият тексерілуі керек. Бұл код инъекциясына немесе SQL инъекциясына негізделген шабуылдардың алдын алуға көмектеседі [7].

Қауіпсіздікті тестілеу мобильді қосымшаларды әзірлеу процесінің ажырамас бөлігі болуы керек. Бұл белгілі осалдықтарды анықтау үшін кодты автоматты түрде сканерлеуді де, ақпараттық қауіпсіздік мамандары жүргізетін қауіпсіздікті қолмен тестілеуді де қамтиды. Жүйелі түрде өткізілетін пентесттер (ену сынақтары) әзірлеу процесінде жіберіліп алынуы мүмкін осалдықтарды анықтауға көмектеседі.

Ең аз артықшылық принципін сақтау да мобильді қосымшалардың қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Қосымша тек оның жұмыс істеуі үшін қажетті рұқсаттарды ғана сұрауы керек. Артық рұқсаттар теріс пайдалану қаупін арттырып қана қоймай, пайдаланушыларда күдік тудыруы мүмкін, бұл қосымшаның беделіне теріс әсер етуі мүмкін [8].

Деректерді қауіпсіз жою, әсіресе құпия ақпаратпен жұмыс істейтін қосымшалар үшін маңызды аспект болып табылады. Пайдаланушы өзінің аккаунтын немесе қосымшадан деректерді жойған кезде, бұл ақпаратты құрылғыдан да, серверлерден де толық және қайтымсыз жоюды қамтамасыз ету қажет.

Қорытындылай келе, мобильді қосымшалардың қауіпсіздігі – бұл үнемі назар аударуды және жаңа қауіптерге бейімделуді қажет ететін үздіксіз процесс екенін атап өткен жөн. Технологиялардың дамуына және шабуылдардың жаңа түрлерінің пайда болуына қарай қорғаныс әдістері де дамуы керек. Әзірлеушілер, қауіпсіздік мамандары және пайдаланушылар бірлесіп жұмыс істеп, мобильді қосымшалар пайдаланушылардың деректерінің құпиялылығы

мен тұтастығын қорғай отырып, қауіпсіз және тиімді жұмыс істей алатын экожүйе құруы керек.

Әдебиет

1. Әлізар А. (2022). Мобильді қосымшалардың қауіпсіздігі. – Мәскеу: IT-Баспа.

2. Смирнов С.В. (2023). Мобильді жүйелердегі қауіптерге қарсы тұру. – Санкт-Петербург: Питер.

3. Johnson N. (2021). Mobile Application Security. O'Reilly Media.

4. Zhang L., & Choo K.R. (2022). Mobile Security and Privacy: Advances, Challenges and Future Research Directions. Academic Press.

5. OWASP Mobile Security Project. (2023). OWASP Mobile Security Testing Guide. Retrieved from https://owasp.org/www-project-mobile-security-testing-guide/

6. Федоров А.В. (2023). Мобильді қосымшалардағы криптография. – Мәскеу: Техносфера.

7. Williams, M. (2022). Android Security: Attacks and Defenses. CRC Press.

8. Бирюков А.А. (2023). Ақпараттық қауіпсіздік: қорғаныс және шабуыл. БХВ-Петербург.

КУРБАНОВ
Ролан Диасович
старший преподаватель кафедры оперативно-розыскной деятельности
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова майор полиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ТЕХНОЛОГИЯ В ОБЕСПЕЧЕНИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Развитие цифровой экономики и компьютерных систем привело не только к увеличению числа угроз в интернет сети, но и к их усложнению. Увеличение скорости обработки данных и увеличение потока информации усложнили правила систем безопасности, которые обнаруживают события касающиеся кибербезопасности, а широкое внедрение облачных технологий сделало вычислительную инфраструктуру более динамичной. Это ставит новые задачи перед всей сферой информационной безопасности. В результате может возникнуть пропуск атак или ложная активация защитных систем, которые могут парализовать бизнес.

Искусственный интеллект используется во многих сферах человеческой деятельности. Машинный разум – более удобный, быстрый и часто более эффективный инструмент, чем человеческий разум. Он также использовался в области кибербезопасности. Таким образом, с помощью искусственного интеллекта многие компании обеспечивают надежную защиту своих баз данных, освобождая аналитические отделы за счет автоматизации повседневных задач.

Существует спрос на технологии искусственного интеллекта в области кибербезопасности. В недавно опубликованном отчете консалтинговой компании Capgemini представлена интересная статистика. В ней приводится следующая информация, 61% компаний считают, что без использования технологий искусственного интеллекта невозможно обнаружить все попытки несанкционированного проникновения в систему с целью кражи конфиденциальной информации. А 48% сообщили, что бюджеты на использование искусственного интеллекта в области кибербезопасности увеличатся примерно на 29% с начала 2020 года [1].

Усугубляет картину заявление компании Cisco, которая подтвердила, что за 2018 год ей удалось отразить 7 трлн. попыток компрометации данных своих клиентов. То есть в среднем азиатско-тихоокеанские компании каждую минуту получают 6 кибератак. Невероятная цифра.

Не стоит думать, что проблема актуальна только для Соединенных Штатов, и такая атака не затронет страны евразийского континента. В ходе отчета сотрудники Capgemini опросили 850 менеджеров из семи отраслей, включая потребительские товары, розничную торговлю, банковское дело, страхование, автомобилестроение, коммунальные услуги и телекоммуникации. 20% респондентов – IT-директор, 10% – CISO, то есть IT – руководители отдела безопасности [2].

Среди опрошенных компаний были те, чьи штаб-квартиры расположены во Франции, Германии, Соединенном Королевстве, Соединенных Штатах, Австралии, Нидерландах, Индии, Италии, Испании и Швеции. Все это подтвердило увеличение числа кибератак и увеличение потребности в новых оборонных технологиях. В том числе – с помощью искусственного интеллекта. То есть проблема есть, и у нее нет четкой географии.

Статистика показала, что по мере роста цифрового бизнеса риск кибератак экспоненциально возрастает. Большинство опрошенных заявляют, что каждый год их организации сталкиваются с нарушением кибербезопасности, что приводит к несанкционированному доступу.

Предприятия платят высокую цену за нарушения кибербезопасности: 20% сообщают о потерях средств, превышающих 50 миллионов долларов. Недавнее исследование Centrify показало, что 74% всех нарушений связаны с доступом к привилегированной учетной записи. То есть злоумышленники целенаправленно ищут учетные записи с максимальными правами, чтобы отфильтровать ценную информацию из корпоративной системы и выгодно продать ее [2].

Конечно, большой бизнес – это самый лакомый кусок. Но IT-служба там обычно посильнее, а большинство уязвимостей закрыты и достичь чего-то ценного шансов мало. Совершенно иная история со средними и малыми компаниями. Компетентность штатных специалистов часто оставляет желать лучшего. В результате получаются не только пустые пространства, но и естественные открытые двери для нападающих всех мастей.

Так происходит по следующей причине. 56% руководителей высшего звена признают, что эксперты по кибербезопасности перегружены, а четверть из них (23%) не в состоянии успешно расследовать все выявленные инциденты. Capgemini обнаружила, что хакерские организации по-прежнему успешно используют алгоритмы для отправки «фишинговых» сообщений целевым пользователям с целью получения конфиденциальной информации.

То есть масштабная работа службы IT-безопасности часто идёт насмарку из-за отсутствия интереса и безразличия человека, а также чрезмерной нагрузки на самом отдел безопасности. Следует сказать, что социальная инженерия достаточно эффективна и должна предотвратить получение таких сообщений конечному пользователю, чтобы предотвратить кибератаки. Тут соответственно искусственный интеллект может выступать в качестве фильтра.

Преимущество искусственного интеллекта в том, что он работает быстрее, чем человек, и постоянно развивается. С введением GDPR и других нормативных правовых актов, требующих защиты различных типов данных, потребность в надежных системах защиты стала еще более важной.

В настоящее время 80% телекоммуникационных компаний заявляют, что верят в искусственный интеллект, способный обнаруживать угрозы и предотвращать кибератаки.

73% компаний тестируют варианты использования искусственного интеллекта в области кибербезопасности, уделяя особое внимание вопросу безопасности конечных точек. Это важный момент, особенно если учесть, что по прогнозам количество конечных устройств (в том числе поддерживающих IT) к 2021 году достигло 24 миллиардов.

51% менеджеров используют или работают с искусственным интеллектом для обнаружения киберугроз на ранней стадии. Машинный интеллект значительно опережает традиционные системы прогнозирования и реагирования. Поэтому качество прогнозирования и скорость реагирования повысятся за счет того, что компании, активно изучают внедрение и использование искусственного интеллекта в рамках комплекса мер по обеспечению кибербезопасности [1].

Многие руководители считают, что искусственный интеллект снижает затраты на выявление угроз и своевременное реагирование на них (экономит от 1% до 15%, в среднем 12%). Благодаря искусственному интеллекту общее время, затрачиваемое на выявление угроз и нарушений, сократится до 12%. А время задержки (количество времени, которое злоумышленник может игнорировать) сокращается на 11%. Сокращение времени достигается за счёт постоянного сканирования известных или неизвестных аномалий, которые показывают паттерны угроз.

Этому есть реальные подтверждения. PetSmart, популярный магазин товаров для домашних животных в США, сэкономил $12 млн, используя искусственный интеллект для обнаружения мошенничества. В партнерстве с Kount PetSmart внедрил технологию AI/Deep Learning, которая изучает миллионы транзакций и их результаты. Умная система определяет легитимность каждой транзакции, сравнивая ее со всеми другими полученными транзакциями. Выявляемые мошеннические заказы отменяются, что позволяет экономить деньги компании, не нанося ущерба бренду [1].

Искусственный интеллект следует называть будущим кибербезопасности по следующим причинам.

С помощью искусственного интеллекта возможно более быстрое обнаружение мошенничества, обнаружение вредоносных программ, обнаружение вторжений, оценка риска в сети и анализ поведения пользователя машины - это пятёрка самых актуальных способов применения искусственного интеллекта для улучшения кибербезопасности.

Искусственный интеллект реально меняет привычные аспекты кибербезопасности. Он улучшает способности компаний предвидеть и предотвращать киберпреступления, защищает устройства с нулевым уровнем доверия, может контролировать даже устаревание паролей! То есть искусственный интеллект действительно необходим для обеспечения безопасности периметров любого бизнеса.

Поиск взаимосвязей между угрозами и анализ вредоносных файлов, подозрительных IP-адресов или необычную деятельность сотрудника длится считанные секунды или минуты, то есть уже сейчас искусственный интеллект помогает человеку обеспечивать кибербезопасность. А в дальнейшем его возможности будут только расширяться, делая участие человека в процессе защиты чисто номинально.

Взять те же банки – благодаря искусственному интеллекту антифрод-системы станут работать надёжнее и быстрее, что позволит сэкономить нервы и деньги как клиентов финансовых учреждений, так и самих банкиров. А по мнению компании Dell, занимающейся разработкой в том числе и подобных продуктов, искусственный интеллект способен защитить, контролировать и отслеживать данные в гибридных средах, а также предотвращать 99% атак вредоносного ПО [2].

Что интересно, искусственный интеллект вполне можно сделать облачным. Это позволит ему автоматически масштабироваться при резком повышении нагрузки (например, если хакеры пытаются «положить» сервер или замаскировать свою активность под лавиной типовых действий в другом направлении). Кроме того, «облако» позволит расширить безопасный периметр компании, если носимая электроника будет подключена к контролируемой искусственным интеллектом среде.

Следует отразить и преступную деятельность, использующую искусственный интеллект в преступных целях.

Киберпреступники используют и злоупотребляют возможностями искусственного интеллекта и машинного обучения. Следует описать текущие сценарии использования искусственного интеллекта в преступных целях, возможные варианты развития инструментов киберпреступности в будущем, а также методы борьбы с ними, которые будут полезны представителям правоохранительных органов, правительственных и других организаций.

«Искусственный интеллект способен помочь миру повысить эффективность процессов в самых различных областях, уровень их автоматизации и общей автономности. Сейчас общественность все больше беспокоят сценарии неправомерного использования искусственного интеллекта, поэтому мы должны, открыто говорить о возможных угрозах, но и не забывать при этом о потенциальных преимуществах технологий искусственного интеллекта, – отметил Эдвардас Шилерис (Edvardas Šileris) [3], глава Центра по борьбе с киберпреступностью, входящего в состав Европола.

Этот доклад дает возможность предвидеть возможные злоупотребления искусственным интеллектом и методы его применения в противозаконных целях, а также своевременно

предотвращать эти угрозы. Только так мы сможем полностью раскрыть потенциал технологии и извлечь выгоду из её внедрения в мире».

В отчете говорится о том, что киберпреступники будут использовать искусственный интеллект и как вектор, и как поверхность атаки. В настоящее время дипфейки (Deep Fakes) остаются наиболее известным сценарием применения искусственного интеллекта в качестве вектора атаки. Однако, по мнению авторов доклада, в будущем потребуются новые технологии проверки данных, которые помогут бороться с кампаниями дезинформации и попытками вымогательства, а также угрозами, нацеленными непосредственно на массивы данных искусственного интеллекта [4].

Вот всего несколько примеров использования искусственного интеллекта в преступных целях:

– крупномасштабные и правдоподобные атаки с использованием социальной инженерии;

– вредоносное ПО для уничтожения документов, которое повышает эффективность атак киберпреступников;

– обман систем распознавания изображений и голоса;

– помощь в поиске целей и уклонении от систем защиты при атаках с применением программ-вымогателей;

– «загрязнение» массивов данных за счёт выявления слепых зон в правилах обнаружения.

Применение искусственного интеллекта начинает оказывать вполне реальное влияние на наш мир, и становится ясно, что эта технология станет одной из фундаментальных в будущем человечества, – отметил Ираклий Беридзе (Irakli Beridze), руководитель Центра искусственного интеллекта и робототехники ЮНИКРИ. – Однако угроза злонамеренного использования искусственного интеллекта не менее реальна для общества, чем польза от его применения. Для нас большая честь работать с Европолом и компанией Trend Micro и совместно пролить свет на «темную сторону» технологий искусственного интеллекта, чтобы стимулировать дальнейшее обсуждение этой важной темы [5].

В докладе также говорится о том, что уже сейчас разрабатываются системы на базе искусственного интеллекта, которые должны повысить эффективность вредоносного программного обеспечения и препятствовать работе антивирусов и технологий распознавания лиц.

Киберпреступники всегда первыми внедряли новейшие технологии, и искусственный интеллект не исключение. В докладе говорится, что искусственный интеллект уже используется для подбора паролей, взлома CAPTCHA и клонирования голоса, а в разработке находится еще немало инновационных инструментов, – отметил Мартин Рёслер (Martin Roesler), руководитель подразделения Trend Micro по исследованию перспектив развития угроз. – Мы гордимся тем, что объединили усилия с Европолом и ЮНИКРИ, чтобы повысить осведомленность об этих угрозах и помочь в создании безопасного цифрового будущего для человечества [5].

В завершение доклада авторы дают несколько рекомендаций:

– Потенциал технологий искусственного интеллекта необходимо использовать в качестве инструмента борьбы с киберпреступностью, чтобы защитить индустрию ИТ-безопасности и правоохранительные органы в будущем.

– Необходимо продолжать исследования, которые помогут развивать технологии кибербезопасности.

– Также необходимо популяризировать и разрабатывать безопасные среды проектирования искусственного интеллекта.

– Политическую риторику об использовании искусственного интеллекта в целях кибербезопасности стоит минимизировать.

– Рекомендуется активно использовать государственно-частное партнёрство и создавать мультидисциплинарные экспертные группы.

Применение искусственного интеллекта в системе правоохранительных органов.

В странах СНГ применение искусственного интеллекта в правоохранительной системе развито явно недостаточно. Основным фактором, сдерживающим проникновение искусственного интеллекта, является

финансовая ситуация. Однако первичная проблема – недостаточное правовое регулирование. Правительство должно задать направление регулирования сферы искусственного интеллекта, что оно и делает сейчас, разработав Концепцию развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года [6].

Конечно, одной лишь концепции недостаточно. Необходим прежде всего апробационный период, в ходе которого будут выявлены сферы нормативного регулирования, которые требуют наибольшего внимания, а также устранены законодательные пробелы. Если говорить про сферы права, на которые необходимо обратить наибольшее внимание, – это гражданское законодательство (естественно, как основа интеллектуальной собственности), а также административное право, уголовное право. Именно регулирование на уровне отраслей права заложит основу для регулирования искусственного интеллекта без привязки к конкретной сфере экономики или общества.

Из-за этих основных проблем мы пока в основном можем лишь наблюдать, как применяют искусственный интеллект правоохранители в других странах. Опыт скопился достаточно приличный, чтобы для нашей страны наметить те узкие сферы, где можно начинать применять искусственный интеллект относительно безопасно.

1. Первая область, где точно стоит применять искусственный интеллект, – расследование киберпреступлений. Пока в этом направлении искусственный интеллект применяется лишь бизнесом для раннего предотвращения возможных угроз.

2. Распознавание лиц. Городская система распознавания лиц работает во многих странах уже достаточно давно и показывает отличные результаты. Старт технологии дан, далее вопрос упирается лишь в финансовый фактор.

3. Оценка рисков для тюрем и коррекционных учреждений. Система определения рисков изучает и сравнивает профили и поведение заключенных до приговора и после заключения, их взаимоотношения, их предыдущую активность в интернете, после чего дает рекомендации по размещению в определенных учреждениях и камерах, которое исключало бы возникновение конфликтов. Такие исследования проводились в США, показав успешные результаты. На данный момент система не вводится ввиду возможного общественного и политического резонанса [6].

4. Оценка рисков при условно-досрочном освобождении. Это именно та область, в которой за рубежом искусственный интеллект применяется довольно активно. Риски обычно определяются такими факторами, как криминальная история, возраст, этническая принадлежность, пол и т.д. Для расчета вероятности рецидива используется алгоритм, который классифицирует риски по уровням: низкий, средний, средне-высокий или высокий. Учитываются также отношение к социуму, преступные связи, образование, занятость, досуг и т.д.

5. Автоматическая идентификация измененных отпечатков пальцев. Люди, связанные с криминальным миром, периодически целенаправленно наносят повреждения кончикам пальцев: стирают поверхность кожи, наносят кислоту, режут, делают небольшие операции. Иногда это происходит непреднамеренно: виноваты условия работы, заболевания или медицинские процедуры. На данный момент используется лишь искусственный интеллект, который определяет наличие и возможные причины таких изменений отпечатков.

6. Искусственный интеллект в работе американских судов помогает госслужащим структурировать данные из множества документов, а гражданам – разобраться в судебной системе, заполнять формы документов и правильно проходить этапы судебных разбирательств.

7. Анализ ДНК. За границей давно используют искусственный интеллект для анализа ДНК.

8. Исследование выстрелов. Ученые работают над разработкой алгоритмов обнаружения выстрелов, их характеристик, направления, времени, определения количества присутствующего огнестрельного оружия, соответствия конкретных выстрелов конкретному огнестрельному оружию, оценки вероятностей класса и калибра. Это перспективное направление разработок искусственного интеллекта, которое не имеет точных сроков внедрения.

9. Предсказание преступлений. Это очень широкая сфера применения искусственного интеллекта, поскольку уголовные кодексы содержат большое количество видов преступлений.

При этом выявляются не только возможные нарушители, места будущих преступлений, но и возможные жертвы. Это позволяет полиции расставлять приоритеты в управлении ресурсами, чаще направлять патрули в места возможных преступлений [6].

Ясно, что искусственный интеллект будет и дальше внедряться в практику правоохранительной деятельности с развитием и расширением доступности технологий умного города, датчиков, интернета вещей.

Литература

1. https://www.securitylab.ru/contest/500573.php.
2. https://www.securitylab.ru/contest/504222.php.
3. https://www.itweek.ru/security/news-company/detail.php?ID=215884.
4. https://www.osp.ru/news/2020/1128/13039197.
5. https://cwr.osp.ru/news/Kiberprestupniki-ispolzuyut-II-instrumenty-v-svoih-interesah.
6. https://www.if24.ru/iskusstvennyj-intellekt-ustroilsya-v-pravoohranitelnye-organy/.

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

ИСТОРИЧЕСКИЕ АСПЕКТЫ РАЗВИТИЯ, ТЕНДЕНЦИИ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Первые упоминания о мошенничестве относятся еще к Римскому праву, откуда посредством рецепции и в российском праве, и в праве государств ближнего и дальнего зарубежья, образующих одну из мировых правовых систем современности – Романо-германское право, – сформировалось понимание необходимости уголовной ответственности за такой вид завладения чужим имуществом, как мошенничество.

Данный тезис подтверждает сравнение определений мошенничества, предусмотренных законодателями: Германии («причинение кому-либо имущественного ущерба путем введения его в заблуждение или поддержания в нем заблуждения с намерением доставить себе или третьему лицу противоправную имущественную выгоду» (§ 263 УК Германии); Франции («Тот, кто, используя ложное имя или звание, либо прибегнув к обманным уловкам с целью убедить в существовании мнимых предприятий, мнимой власти или кредита или с целью породить надежду или опасение в отношении какого-либо успеха, происшествия или любого другого вымышленного события, понудит к передаче или выдаче денежных ценностей, движимого имущества или облигаций, распоряжений, векселей и одним из этих способов выманит все или часть имущества другого» (ст. 405 УК Франции); Латвийской Республики («получение чужого имущества или прав на такое имущество путем злоупотребления доверием или обмана» (ст. 177 УЗ Латвии) и др.

Проблема уголовно-правовой охраны отношений собственности стала возникать ещё в ранней Руси, она изменялась вместе со сменой общественных отношений и политического строя.

Впервые об ответственности за посягательства на собственность в уголовном праве упоминается в ст. 5 Двинской уставной грамоты 1397г. Статья 11 Судебника 1497г. рассматривает повторную кражу, понятием которой охватывалось «мошенничество», как квалифицированную. При отсутствии у виновного имущества он не выдавался истцу для возмещения убытков, а подвергался смертной казни. Судебник 1550г., не изменив общих признаков рецидива, а также наказания за него, закрепил в ст. 56 новый подход к ответственности за повторные кражи.

В последующем ответственность лиц, виновных в нескольких кражах, была снижена, и ст. 11 Медынского губного наказа 1550г. (в отличие от Судебника 1550г., который за вторую кражу устанавливал смертную казнь) предусматривала за первую кражу битье кнутом и тюремное заключение, за вторую – битье кнутом и отсечение руки, а третья и последующие кражи влекли за собой смертную казнь. В дальнейшем эта норма нашла свое отражение в ст. 187 главы 10, ст.ст. 10, 16, 17 главы 21 Соборного уложения 1649г., арт. 189, 191 Артикула воинского 1715г., изданного в период реформ, проводимых Петром I.

Следующим крупным законодательным актом в области уголовного права, завершившим систематизацию российского законодательства, проведенную при Николае 1, стало Уложение о наказаниях уголовных и исполнительных 1845г., в котором термин «собственность» употреблялся в уголовно-правовом значении в качестве синонима «имущество» для обозначения всей массы имущественных прав и интересов в их многообразии. Впоследствии Уголовное уложение 1903г. объединило преступления «против имущества и доходов казны», «против собственности частных лиц» в рамках единых составов преступлений.

После свершения Октябрьской революции 1917г., по УК РСФСР 1922г. простое мошенничество, то есть «получение с корыстной целью имущества или права на имущество посредством злоупотребления доверием или обмана», наказывалось принудительными работами на срок до 6 месяцев или лишением свободы на аналогичный срок. В примечании в указанной статье содержалось принципиальное уточнение в отношении обмана, который законодатель понимал «как сообщение ложных сведений, так и заведомое сокрытие обстоятельств, сообщение о которых было обязательно». Квалифицированное мошенничество, «имевшее своим последствием убыток, причиненный государственному или общественному учреждению» было закреплено иной статьей 188, и предусматривало наказание в виде лишения свободы на срок до 1 года [1, с. 218-243].

В дальнейшем «усиливалась ответственность за хищения государственного и общественного имущества, в июне 1947г. за эти виды преступлений были увеличены сроки наказания (до 10-25 лет), к лишению свободы приговаривались также лица, виновные в недоносительстве по этим преступлениям. Были отменены статьи, предусматривавшие дифференцированные виды хищения общественной собственности и соответствующие им виды наказания, произошла унификация составов преступлений, что привело к возникновению трудностей в судебной практике и большему произволу в судебных решениях».

УК РСФСР 1960г. содержал сразу несколько норм о мошенничестве, дифференцированных в зависимости от объекта посягательства – формы собственности, и содержащих достаточно жесткие основные и дополнительные виды наказания. Так, ст. 93 УК РСФСР 1960г. предусматривала уголовную ответственность за «хищение государственного или общественного имущества, совершенное путем мошенничества», то есть «завладение государственным или общественным имуществом путем обмана или злоупотребления доверием». В данном случае виновным грозило наказание в виде лишения свободы на срок до 3 лет или исправительных работ на срок до 2 лет или штрафа от ста до пятисот рублей.

Аналогичное деяние, «совершенное повторно или по предварительному сговору группой лиц» наказывалось лишением свободы на срок до 6 лет с конфискацией имущества или без таковых или исправительных работ на срок от 1 года до 2 лет с конфискацией имущества или без таковой. Виновных в мошенничестве, причинившем крупный ущерб государству или общественной организации или совершенном особо опасным рецидивистом, карали лишением свободы на срок от 5 до 15 лет с конфискацией имущества [2, с. 16-37].

Общественная опасность мошенничества. Вопросы борьбы с экономической преступностью в т.ч. с различного рода мошенническими действиями становятся все более актуальными. Мошенничество приобретает все большие масштабы и проявляется во всех новых формах.

С переходом к рыночным отношениям, многообразию форм собственности и свободе предпринимательства значительно повышается активность людей не только в дозволяемых формах, но и в рамках криминальных способов бизнеса и обогащения. В условиях галопирую-

щей инфляции, экономической и правовой нестабильности ущерб от экономических преступлений исчисляется миллионами. Экономические преступления видоизменяются, приобретают новые, порой еще неизведанные, качественные формы.

При осуществлении мошенничества, связанного с не целевым использованием денежных средств усилия преступников направлены на фальсификацию подлинных документов и придание своим действиям видимости мнимой законности. Не менее важным представляется рассмотрение способа мошеннических действий при осуществлении мошенничества в сфере банковской деятельности. В процессе дальнейшего развития рыночных отношений и частного сектора хозяйствования, увеличения числа предприятий и организации, в том числе в сфере мелкого и среднего предпринимательства, финансово-имущественных отношений, числа занятых в этих структурах работников, обострение конкуренции, возрастание опасности банкротства также неминуемо ведут к росту мошенничества. К числу наиболее характерных особенностей современного мошенничества можно отнести:

– высокий уровень групповых посягательств, совершенных в крупных и особо крупных размерах;

– межрегиональный характер действия мошенников, совершающих обманные действия в одних регионах, присвоение чужой собственности -–в других, а ее сбыт – за чистую в-третьих;

– активное использование подложных или фальсифицированных документов, печатей, штампов, а также создание лжефирм;

– использование различных легальных правовых средств (типовые контракты, гарантии, поручительства, векселя), хозяйственных институтов (биржи, коммерческие банки, страховые фирмы) и их возможностей (безналичные расчеты) для последующего достижения преступных целей;

– быстрое появление новых способов обмана и их адаптация к меняющимся социально-экономическим условиям.

В этой связи мошенничество можно рассматривать в качестве одного из индикаторов реального состояния экономической преступности [3, с. 37-42].

В современных условиях экономической нестабильности преступность в сфере информационно-телекоммуникационных технологий приобретает новые направления, а Интернет выступает не только инструментом, но и благоприятной средой для противоправной деятельности.

Процесс глобальной информатизации общества создает предпосылки для возникновения новых видов мошенничества. Официальная статистика подтверждает тот факт, что количество информационно-телекоммуникационных мошенников с каждым месяцем увеличивается: «По итогам второго полугодия 2021 года случился рекордный за последние три года всплеск различных сетевых мошенничеств – сразу на 12 % по сравнению с аналогичным периодом 2020 года» [4].

В связи с этим Интернет-мошенничество, на сегодняшний день, является одной из самых актуальных проблем современности, т.к. носит дистанционный характер, имеет цифровую форму записи информации и обладает повышенной степенью латентности.

Привлечения к уголовной ответственности за совершенные Интернет-мошенничества (по сравнению с другими преступлениями) все еще относительно редки, но это не дает оснований предполагать исключительность криминального явления.

Разделяя данную позицию, Рассел Джон Смит утверждает, что онлайн-мошенничество состоит из совокупности необнаруженных, незарегистрированных, нераскрытых преступлений по причинам латентности, сложности определения цифровых следов и нежелания жертв сообщать о случившемся [5, с.25-29]. Опросы жертв преступлений только за последние несколько лет начали включать вопросы об интернет-преступлениях, а СМИ – публиковать статистические данные об инцидентах, связанных с компьютерной безопасностью: вирусах, шпионском ПО, фишинге и других вредоносных программах.

Р.И. Дремлюга справедливо отмечает общественную опасность и отличие показателей причиняемого ущерба киберпреступностью: «Особенности развития интернет-мошенничества

связаны с запоздалостью на 15-20 лет появления Интернета в странах СНГ, а также с высоким техническим уровнем отечественных интернет-мошенников». Это позволило преступности в некоторых аспектах деятельности обогнать зарубежную [6, с.39-49].

На официальном сайте «Лаборатория Касперского» размещена географическая специфика киберпреступлений. Согласно представленным данным, в разных частях мира отличаются вредоносные программы, приоритетные направления компьютерных атак и способы обогащения, которые активно используют злоумышленники. Связано это не только с тем, где физически находятся киберпреступники, но и с особенностью стран, в которых проживают потенциальные жертвы. В данном случае ключевым фактором выступают уровень проникновения Интернета в стране, количество пользователей информационно-телекоммуникационной сетью и общий уровень экономического развития.

По итогам 2021 года в число наиболее пострадавших от Интернет-мошенничества стран вошли: США – 65 %, Россия – 84 %, Африка – 71 %; Китай – 76 % [7].

В связи с этим была изучена и проанализирована эволюция интернет-преступности в США, России, Гане, Нигерии и Китае (на основании официальных данных Лаборатории Касперского, работы Г.О. Крылова «Международный опыт правового регулирования информационной безопасности и его применение в странах СНГ», научных трудов Скотта Хендерсона «Новое лицо киберпреступности» и Дэниела Джордан Смита «Повседневный обман и народное недовольство в Нигерии»).

Этапы развития Интернет-мошенничества:

1 этап (1972-1991гг.). Данный период характеризуется становлением интернет-преступности. Преступления совершаются узким кругом лиц, зарождается специализация компьютерных преступников, принимаются попытки разработки правовых и организационных средств борьбы с мошенничеством в сфере высоких технологий.

Одно из первых преступлений, совершенных с использованием информационно-телекоммуникационных технологий, было зарегистрировано в 1980г. в г. Вильнюсе, который на тот момент времени входил в состав СССР. Этот факт занесен в международный реестр правонарушений и стал отправной точкой развития интернет-преступности. Наряду с совершением преступления, начался активный поиск путей криминологического и уголовно-правового регулирования вопросов, касающихся предупреждения, профилактики, пресечения и привлечения виновных к уголовной ответственности.

2 этап (1991-2001гг.). Интернет становится средой совершения традиционных преступлений. Период характеризуется созданием и внедрением «хакеров», стремительным развитием преступности. В конце периода количество интернет-пользователей исчисляется миллионами. Интернет посредством информационных сетей связывает различные учреждения всей планеты. Продолжается реформирование нормативно-правовых актов в части ответственности за информационно-телекоммуникационные мошенничества.

3 этап (2001г. – по настоящее время). Интернет-преступность приобретает межнациональный характер. Период характеризуется появлением международных хакерских организаций во всех сферах IT-преступности, а также использованием Интернета в политических сферах. Интернет-мошенничество становится все более общественно опасным, появляются новые схемы и способы противоправной деятельности. Интернет предоставляет мошенникам особые возможности при совершении противоправной деятельности [8].

Анализ информационных ресурсов позволил выявить актуальные способы совершения сетевых противоправных деяний на территории СНГ.

1. Кибersквоттинг – захват чего-либо с использованием доменных имен в киберпространстве. Лиц, осуществляющих указанную деятельность, называют хапперами. Злоумышленники приобретают в личное пользование домены; регистрируют их, присваивая брендовые наименования (имеющие громкие названия и узнаваемые людьми); продают их заинтересованным лицам, зарабатывая на этом в десятки раз больше вложенных средств.

2. Тайпсквоттинг – разновидность кибersквоттинга. Домены, имеющие схожесть с имеющимися брендами, но с умышленными опечатками: «Ростнефть. ру; Лугойл.com; rembler.ru» и т.д. Обычно хапперы не продают такие домены, а оставляют в личном пользовании для построения прибыльного бизнеса (используют сайты в качестве рекламы, на которых можно отслеживать несколько тысяч просмотров), распространения вирусов. Как правило, опечатка влечет за собой угрозу утери идентификационных данных.

3. Ноах-программы. Цель их заключается в навязывании пользователю персонального компьютера или смартфона (планшета) ложной истины о легко доступной возможности материального обогащения.

4. Коммерческие утилиты. Разработаны и внедрены в процесс виртуальной реальности с целью вскрытия онлайн-систем безналичной оплаты и программ, основанных на случайном выигрыше (казино, ставки на спорт, черное и белое). Подобные программы запускаются только в пробной версии на небезопасных сайтах, путем перехода по сомнительной ссылке.

5. Создание искусственного вирусного и антивирусного программного обеспечения. Суть процесса заключается в моделировании процесса заражения операционной системы вирусами-маскировщиками и выводом на экран в режиме онлайн последовательных рекомендаций: перейти по ссылке, скачать, установить, выполнить сканирование предложенным антивирусным обеспечением. Скачиваемое оборудование, как правило, содержит рекламного бота, который в процессе деятельности рассекречивает и пересылает конфиденциальные данные, включая логины и пароли.

6. Интернет-магазины. Товар продается либо с большой скидкой, либо уцененный. Как правило, мошенники требуют стопроцентную предоплату, после чего направляют в адрес жертвы пустую посылку.

7. Мошенничество с использованием телекоммуникационных технологий. Жертву убеждают отправить СМС на указанный номер в целях разблокировки учетной записи, после чего автоматически на телефоне подключается платная ежедневная подписка и др. [9, с.36-39].

Отцом-основателем американских исследований и освоений мира компьютерной преступности принято считать ученого Донна Б. Паркера, который начал деятельность с 1971г., работая в должности исследователя компьютерной преступности и информационной безопасности в SRI International (Стэнфордский исследовательский институт), а позже выступил основным автором первого базового федерального руководства для правоохранительных органов США: «Компьютерные преступления – Справочное руководство по уголовному правосудию» [10, с. 201].

С 1979г. граждане Америки начали активно использовать в повседневной деятельности интернет-коммуникации. Этот год был ознаменован запуском первых веббраузеров, появлением повсеместных поисковых систем, зарождением онлайн торговли и распространением электронной почты как средства коммуникации.

Наряду с прогрессом в данной области, расширялись возможности преступников. Интернет предлагал кибермошенникам легкий доступ к персональным данным многих пользователей при относительно низких затратах и рисках.

Признавая необходимость сбора и оценки информации о Интернет-мошенничестве, ФБР в мае 1995г. создало Центр жалоб на совершаемые информационно-телекоммуникационные мошенничества. В настоящее время этот Центр переименован в IC3 [11].

За первый год работы IC3 зарегистрировало 49 811 жалоб, направленных в большей степени на аукционное мошенничество и фиктивную доставку товаров. В марте 2020г. IC3 зарегистрировал свою 5-миллионную жалобу. Преступления, внесенные в каталог IC3, отражают эволюцию Интернета практически за три десятилетия: «Масштабы и скорость влияния киберугроз с течением времени имеют тенденцию видоизменяться. Преступники обладают навыком мгновенной адаптации в киберсреде, создавая при этом сложные мошеннические схемы» [12].

В настоящее время тип киберпреступников изменился, а изощренность современных преступлений вызывает наибольшее беспокойство, становится сложнее фиксировать поддельные

вебсайты и документы. Очень важным видом деятельности киберпреступников на территории США является кража персональных данных пользователей. На хакерских форумах можно найти массу объявлений о продаже баз данных клиентов различных магазинов и сервисов. Необходимо отметить, что частая причина утечки информации – уязвимости и ошибки в настройке серверов данных.

Наиболее распространенными уязвимостями являются SQL-injection (ошибки систем аутенфикации). Помимо уязвимостей, преступники зачастую используют ошибки в конфигурации веб-приложений, такие как не удалённые аккаунты, открытый доступ к частным данным, хранение паролей в незашифрованном виде и др.

В Западной Африке Интернет-мошенничество зародилось в период с 1999-2000гг. До этого времени информационные преступления были связаны с мошенничеством, совершаемым с использованием кредитных карт. Однако с 2004г. начали формироваться новые формы IT-преступности.

Аппарат Национальной безопасности Ганы выделил три основных вида Интернет-мошенничества в стране:

1. Подделка личных данных в результате взаимодействия с жертвой через социальные сети, такие как Facebook и eHarmony. Граждане Ганы предпочитают вести общение под вымышленными именами. Цель противоправной деятельности – установление контакта с жертвой и получение необходимой персональной информации.

2. Ложная идентификация. Как известно, в Гане находятся крупнейшие в мире запасы золотоносной руды. В настоящее время ганскими преступниками в киберпространстве создана масса веб-сайтов с фиктивными предложениями инвестиций в золото.

3. Мошенничество с недвижимостью. Злоумышленники создают поддельные веб-сайты известных строительных фирм, специализирующихся на строительстве домов. Создание сайтов сопровождается многочисленными рекламами и неоригинальными фотографиями [13].

Необходимо отметить тот факт, что до 2007 г. в Гане не существовало нормативно-правовых актов, регулирующих киберпреступность, однако, в 2008 году был принят Закон об электронных операциях (Закон 772) [14], который закрепил понятие «Интернет-мошенничество» и повысил эффективность преследования киберпреступников.

К. Джайшанкар точно оценивает, что «люди имеют склонность совершать преступления в киберпространстве, которые в физическом пространстве не совершили бы никогда», а также тот факт, что «гибкость личности, диссоциативная анонимность и отсутствие фактора сдерживания в киберпространстве предоставляют правонарушителям выбор для совершения киберпреступлений» [15, с. 283-301].

Кроме того, киберпреступность в Гане в значительной степени совпадает с возникновением и распространением исследуемого явления в других странах. Скотт Хендерсон подтверждает, что банковское мошенничество является одним из самых распространенных видов Интернет-мошенничества: «Злоумышленники посредством технических манипуляций с банковскими сайтами преобразовывают или подменяют законные сайты учреждений, фальсифицируют данные об операциях клиентов. Большинство ганских киберпреступников применяют простейшие мошеннические приемы для реализации противоправного умысла: телефонные звонки будущим жертвам от имени официального представителя банка с просьбой назвать секретное слово или пароль от персональной карты, смс-сообщения, массовые рассылки электронных писем, создание фишинговых сайтов, использование вирусного программного обеспечения и т. д.» [16, с. 101-104].

По итогам 1980-1990 гг. в стране использовалось 419 схем информационно-телекоммуникационного мошенничества. Изначально преступления совершались с использованием кредитных карт. Дэниел Джордан Смит отмечает, что первые Интернет-мошеннические схемы в Нигерии на заре XXI века были «кибер» только по своей телекоммуникационной природе: «В Интернет-кафе с двадцатью пятью терминалами не менее четырех терминалов использовались для отправки мошеннических писем» [17].

При возникновении дискуссионных споров между рассматриваемыми странами представители Ганы утверждают, что ведущей проблемой возникновения киберпреступности выступает ЭКОВАС (Экономическое сообщество западноафриканских государств), благодаря которому граждане могут свободно перемещаться между двух стран. В течение последнего десятилетия нигерийские кибермошенники массово приезжали в Гану с целью совершения противоправных действий.

Местные жители утверждают, что, оказавшись в стране, нигерийские мигранты собираются в тесные группы вокруг крупных городов, таких как Ахиомота и Нима, где, получив конфиденциальный доступ к Интернету, реализуют свой преступный умысел.

Объектами ганских злоумышленников обычно выступают пожилые, разведенные, овдовевшие женщины, чаще всего родом из Великобритании, США и Германии.

Мишенями нигерийских кибермошенников, как правило, являются мужчины среднего возраста, занимающие руководящие должности на Среднем Западе США, в частности Техасе. В основе последней тенденции лежат две причины. Во-первых, в Техасе, в таких городах, как Хьюстон и Даллас, преобладает нигерийская популяция. Во-вторых, нигерийцы зачастую приезжают в Техас, так как он является добывающим нефтяным центром США. Сотрудничество между нигерийскими и техасскими нефтедобывающими компаниями провоцируют нигерийских правонарушителей на следующие мошеннические действия.

В Китае первая мощная волна киберпреступности была зафиксирована в конце 80-х гг., когда в электронные почтовые ящики пользователей внедрялись вредоносные программы с целью обеспечения кибепреступникам доступа к персональным данным.

Вторая волна поднялась в 90-х гг. и совпала с развитием веб-браузеров, большинство из которых были уязвимы для вирусов. Вирусы распространялись через Интернет-соединения при посещении пользователями сомнительных сайтов. Мощный взлет киберпреступности в 2005г. был вызван появлением и развитием социальных сетей. Неограниченный доступ к личной информации пользователей позволил преступникам совершать разнообразные финансовые махинации.

Сегодня Интернет-мошенничество Китая превратилось в глобальную криминальную отрасль с оборотом около двух миллиардов долларов ежегодно. Преступники объединяются в группировки, используют новейшие способы и технологии для достижения максимального преступного эффекта:

1. Ботнеты и зомби. Незаконные групповые рассылки веб-писем в мгновенных социальных сетях или электронной почте.

2. Профили пользователей чатов и социальных сетей («ВК», «ОК» и т.д.). Мошенники, взломав аккаунты друзей жертвы, отправляют приватные сообщения с просьбами оказать помощь и перевести срочно определенную денежную сумму, проголосовать.

3. Система мгновенных сообщений (ICQ). Используются фишерами для обращения к пользователям данных программ в форме предложения неких товаров, услуг за небольшое количество денег. Зачастую мошенники преодолевают социальную дистанцию жертвы за счет притворства дальним родственником или бывшим коллегой.

4. Онлайн-чаты. Публичные обращения, мошенничества с платежными системами, фишинг с рекламой, Ноах-программы.

5. Индивидуальный персональный компьютер, ноутбук, планшет, смартфон юзера. Взломы ПК в виде вирусных атак, установки баннеров и т.д.

6. Веб-сайты. Например, сайты знакомств, которые выступают основным пространством деятельности скамеров. На веб-страницах другого контента мошенники осуществляют незаконные действия с платежными системами посредством ссылок и аудиосообщений.

7. Osint. Поиск, сбор и анализ информации по открытым источникам в Интернете и др.

Проанализированные этапы развития интернет-преступности позволяет обобщить данные, определить основные признаки, характеризующие Интенет-мошенничество, конкретизирующие его и отграничивающие от других видов мошенничества:

1. Дистанционное взаимодействие с жертвами посредством использования информационно-телекоммуникационных технологий (персональный компьютер, планшет, ноутбук, смартфон, умные часы и т.д.). Интенет-мошенничество включает в себя «анонимные, сетевые отношения между преступниками и жертвами».

2. Манипулирование данными и программным обеспечением (в процессе совершения преступления мошенники могут копировать без потери качества и изменять данные без видимых следов).

3. Программное обеспечение, запущенное в Интернете, может атаковать миллионы компьютеров как кратковременно, так и в течение длительного периода времени с использованием базового программного обеспечения.

4. Интернет позволяет увеличивать масштаб преступления – от незначительного неудобства до серьезного ущерба.

5. Интернет позволяет агрегировать большое количество несуществующих выгод, что подтверждает значительное число жертв и небольшой причиненный ущерб.

6. Интернет способствует развитию информационной экономики, в которой информация стала ценным активом как на легальном рынке (музыка, фильмы, программное обеспечение, книги), так и на теневом (продажа кредитных карт, личной информации, персональных данных и паролей с целью облегчения Интернет-мошенничества).

7. Имеет быстрые инновационные циклы, что позволяет использовать новые методы и инструменты для совершения преступлений в максимально короткие сроки.

8. Преступники используют психологию лжи и различные методы обмана.

На основании предложенных признаков нами сформулировано собственное понятие Интернет-мошенничества, исключающее возможность его пересечения и смешения с другими видами мошенничества, – хищение чужого имущества или приобретение права на чужое имущество, совершенное с использованием информационно-телекоммуникационных технологий, которое включает в себя совокупность противоправных дистанционных средств, методов обмана жертвы и злоупотребления доверием, а также имеет глобальный охват для поиска наиболее уязвимых мест с целью достижения корыстных целей.

Считаем, что указанные признаки и сформулированное понятие могут послужить теоретической базой при составлении учебных пособий, а также разработке практического комплекса борьбы с киберпреступностью на международном уровне.

Литература

1. Баранов И.Р. Виды телекоммуникационного мошенничества / Баранов И.Р. // Вестник Владимирского юридического института. – 2015. – С. 218-243.

2. История развития мошенничества, современные виды мошенничества и способы борьбы с ними – Алпатов А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / Алпатов А.С. // Трибуна молодого ученого. – 2016. – №2. – С. 16-37.

3. Колескин Д.В. История развития мошенничества, современные виды мошенничества и способы борьбы с ними // Социально-гуманитарные проблемы современности: сборник научных трудов по материалам Международной научно-практической конференции 24 апреля 2020г.: Белгород: ООО Агентство перспективных научных исследований (АПНИ), 2020. – С. 37-42.

4. Официальный сайт Интерпола. URL: https://www.interpol. int

5. Рассел Джон Смит. Борьба с преступностью в эпоху цифровых технологий: исследование последствий для прав человека // Международный журнал кибер-криминологии. 2004. №3. – С. 25-29.

6. Дремлюга Р.И. Виртуальная реальность: проблемы правового регулирования. Т. 15. 2020. №9. – С. 39-49.

7. Официальный сайт «Лаборатория Касперского». URL: https://securelist.ru/geografiya-kiberprestuplenij-zapadn/147/ .

8. Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации: автореф. дис. …канд. юрид. наук / Г. О. Крылов. – М., 2007.

9. Старостенко О.А. Новые способы мошеннических действий в период пандемии COVID 19 и их классификация. Юридическое образование и наука. 2021. №2. – С. 36-39.

10. Донн Б. Паркер. Справочник по компьютерным преступлениям уголовного правосудия. США, 1989. – С. 201.

11. Официальный сайт ФБР. URL: https://www.fbi.gov.

12. Центр жалоб на Интернет-преступления [Электронный ресурс]. URL: https://www.ic3.gov.

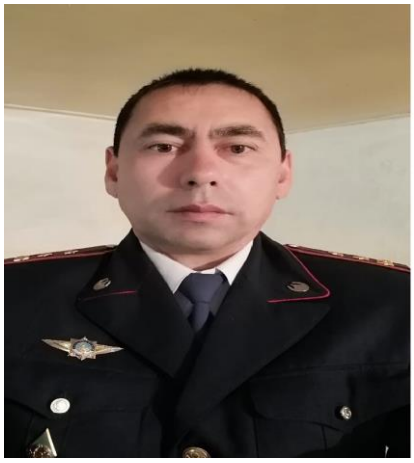
13. Официальный сайт Национального центра кибербезопасности Ганы. URL: https://cybersecurity.gov.gh.

14. Закон 772 «Об электронных операциях», 2008. URL: https:// www.researchictafrica.net/countries/ghana.

15. Джайшанкар К. Создание теории киберпреступлений [Электронный ресурс] // Международный журнал кибер- криминологии. Т. 1. 2007. №7. – С. 283-301. URL: http://www. cybercrimejournal.com.

16. Хендерсон Скотт. Новое лицо киберпреступности [Электронный ресурс]. Великобритания, 2007. – С. 101-104. URL: https://www.crn.com/news/security/21080078 .

17. Смит Дэниел Джордан. Повседневный обман и народное недовольство в Нигерии [Электронный ресурс]. Нью-Джерси, 2010. URL: https://scholar.google.com/citations.



ТАСБУЛАТОВ
Руслан Ермекович
магистрант 2 курса научно-педагогической магистратуры
факультета послевузовского образования
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова капитан полиции

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ

Развитие цифровой экономики не только открывает новые возможности для общества и государства, но и вооружает преступников новыми методами совершения уголовных правонарушений, а также создает дополнительные криминальные угрозы для многочисленных сфер общественной жизни. Вынужденный переход на дистанционный режим работы во время пандемии спровоцировал увеличение числа уголовных правонарушений, совершенных с использованием информационных технологий. Вместе с развитием информационных технологий и стремлением государства к полной цифровой трансформации всех сфер общественной жизни, цифровой прогресс совершенствует также инструменты для совершения преступлений, увеличивая их количество. На сегодняшний день цифровые преступления являются одной из актуальных проблем не только для нашего государства, но и для всего мира.

Наука уголовного права рассматривает общественно опасные деяния не как абстрактную категорию, неизменную, раз и навсегда данную, ни от чего не зависимую, а как реальную социальную категорию, тесно связанную с другими, обуславливающими ее появление и существование социальными явлениями. Наука уголовного права устанавливает, что уголовное правонарушение является исторически изменчивой категорией, которая существовала не всегда, а возникла на определенном этапе развития человеческого общества: с общественным разделением труда, образованием частной собственности, делением общества на классы, с появлением государства и права.

В нашем обществе уголовное правонарушение представляет собой посягательство на охраняемые уголовным законодательством общественные отношения, интересы и блага. Не является исключением и такая модель уголовного правонарушения – как цифровое преступление.

Цифровые преступления – это совершенные виновно общественно опасные деяния (действия или бездействия), запрещенные уголовным кодексом Республики Казахстан, под угрозой наказания. Цифровому преступлению, как и любому другому присущи такие признаки – как общественная опасность, противоправность, виновность и наказуемость.

Общественная опасность – материальный признак преступления, это объективное свойство деяния (действия или бездействия) который реально причиняет существенный вред охраняемым уголовным законом общественным отношениям или создает угрозу причинения такого вреда. Именно общественная опасность (вредоносность) действия или бездействия берется во

внимание законодателем при решении вопроса о таких процессах уголовной политики: как криминализация или декриминализация деяния. Это является конструктивным основанием для процессов уголовной политики, как криминализация или декриминализация общественно опасного деяния. По этому же основанию, были криминализированы цифровые преступления. Только в том случае целесообразно устанавливать уголовную ответственность за те или иные деяния, если они объективно общественно опасны. Но даже если законодатель сочтет необходимым установить в уголовном законе запрет на то или иное поведение, это еще не значит, что конкретное действие или бездействие, подпадающее под признаки деяния, указанного в законе, всегда является преступным. Общественная опасность как материальный признак имеет качественную и количественную характеристику [1, с. 35]. Важно установить, что инкриминируемое виновное деяние имеет общественную опасность. Общеизвестно, что согласно части второй статьи 10 Уголовного Кодекса «не является преступлением действие или бездействие, хотя формально и содержащее признаки какого-либо деяния, предусмотренного Особенной частью настоящего Кодекса, но в силу малозначительности не представляющее общественной опасности, то есть не причинившее вреда и не создавшее угрозы причинения вреда личности, обществу или государству» [2].

Вторым обязательным признаком цифрового преступления является противоправность, то есть его запрещенность уголовным законом. Противоправность – это формальный признак цифрового преступления. Уголовная противоправность преступного поведения напрямую связана с процессами криминализации и декриминализации [3, с. 71]. При криминализации происходит законодательное признание тех или иных общественно опасных деяний преступными и наказуемыми, что не обошло стороной исследуемые преступления. А при декриминализации происходит исключение из категории уголовного правонарушения, то есть отмена за их совершение уголовной ответственности. На наш взгляд, в новых условиях, когда принцип законности становится краеугольным камнем в фундаменте возводимого здания правового государства, формальный признак преступления по своей важности нисколько не уступает материальному. Оба эти признака довольно тесно – взаимосвязаны и –взаимообусловлены. Законодатель обычно устанавливает уголовно-правовой запрет на деяние, которое общественно опасно и, как правило, когда общественная опасность утрачивается, отменяется и его уголовно-правовой запрет (деяние декриминализируется). Между тем, встречаются и несовпадения. Это не только рассмотренные выше случаи, когда предусмотренное уголовным законом действие или бездействие в силу малозначительности не представляет общественной опасности, но и эксцессы, объективно причиняющие вред довольно существенный, тем или иным общественным отношениям, но эти общественные отношения не защищены уголовным законом, то есть не установлен запрет на причинение им вреда. В обоих случаях деяние не может быть признано преступным. Надо иметь в виду, что о цифровом преступлении может идти речь только в том случае, если запрет установлен именно уголовным законом. Противоречие деяния нормам других отраслей права не дает оснований для признания его преступным.

Неразрывно с противоправностью связаны следующие два признака цифрового преступления: виновность и наказуемость. В теории уголовного права есть специальный принцип, принцип виновной ответственности, который очень связан с этим признаком. Выделение законодателем виновности, то есть факта наличия в действиях лица вины, в самостоятельный признак преступления свидетельствует о значении, которое придается этому институту. Общеизвестно, что согласно второй особенной части статьи 19 Уголовного Кодекса Республики Казахстан объективное вменение, то есть уголовная ответственность за невиновное причинение вреда, не допускается [2]. Виновным же в преступлении признается лишь лицо, совершившее деяние умышленно или по неосторожности. Поскольку виновность является одним из обязательных условий противоправности (уголовным законом запрещены исключительно виновные действия или бездействие), то отсутствие в действиях субъекта вины означает отсутствие в его деянии и признака уголовной противоправности. Цифровые преступления характеризуются только умышленной формой вины.

Немаловажным по своей сути, является следующий признак цифрового преступления – наказуемость. Наличие уголовно-правового запрета, не подкрепленного угрозой применения наказания, не дает оснований утверждать, что запрещаемое деяние является преступным. Так, в общей теории уголовного законодательства установлен ряд запретов (на придание закону, устанавливающему преступность или наказуемость деяния, усиливающему ответственность или наказание или иным образом ухудшающему положение лица, совершившего это деяние, обратной силы и др.). Следует иметь в виду, что признаком преступления является именно наказуемость, то есть наличие в законе угрозы применения наказания, а не реальная несказанность деяния. Лицо, виновное в совершении конкретного общественно опасного, запрещенного уголовным законом под угрозой наказания деяния, может и не подвергнуться наказанию (вследствие истечения срока давности привлечения к уголовной ответственности, амнистии и пр.), но от этого совершенное деяние не перестает быть преступным. Таким образом, наказуемость – это предусмотренная законом возможность назначения наказания [1, с. 39]. Такая возможность реализуется не во всех случаях совершения уголовного правонарушения. Это может быть связано со следующими обстоятельствами: не каждое уголовное правонарушение регистрируется правоохранительными органами; не каждое зафиксированное раскрывается; в некоторых случаях, по различным законным основаниям, лицо, виновное в совершении уголовного правонарушения, может быть освобождено от применения в отношении него мер уголовно-правового воздействия.

Все перечисленные признаки цифрового преступления тесно взаимосвязаны и дополняют друг друга, отсутствие одного из признаков будет свидетельствовать об отсутствии основания уголовной ответственности.

Хотелось бы отметить, что такие процессы уголовной политики: как криминализация и декриминализация тесно взаимосвязаны с такими признаками как общественная опасность и противоправность не только цифрового преступления, но и всех уголовных правонарушений без исключения, независимо от их вида.

К сожалению, технологии, которые появляются в результате его стремительного развития, становятся инструментом для причинения вреда общественным отношениям, вследствие чего и появились цифровые преступления. При этом появление новых угроз не является единственным его негативным следствием. Не менее опасным становится использование современных технологий при совершении «традиционных» для уголовного закона преступлений, уголовная ответственность за которые уже в нем закреплена [4, с. 78].

Литература

1. Уголовное право. Общая часть: Учебник под редакцией профессора А.И. Рарога. – М.: Институт международного права и экономики. Издательство «Триада, Лтд», 1997. – С 320.

2. Уголовный кодекс Республики Казахстан от 03 июля 2014 года №226 – V ЗРК (с изменениями и дополнениями по состоянию на 09.09.2024 года) http: // online.zakon.kz.

3. Учебник уголовного права. Общая часть. – М.:Издательство «Спарк», 1996, – С 412.

4. Козаев Н.Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты. – Москва: Юрлитинформ, 2016. – С 192.

БАТЫРХАН
Темірлан Мейірханұлы
магистрант научно-педагогической магистратуры
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова капитан полиции

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКНЫХ И СЛЕДСТВЕННЫХ МЕРОПРИЯТИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ РАСПРОСТРАНЕННЫХ ВИДОВ И СПОСОБОВ СОВЕРШЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Интернет представляет собой глобальную компьютерную сеть, основанную на принципе саморегуляции, автономности, самодостаточности.

Если оценивать возможности которые глобальные информационные технологии предоставляют мошеннику для реализации его преступных замыслов, то можно выделить следующие обстоятельства, по которым мошенничество в Интернете развивается такими темпами:

Анонимность, во многом определяет специфику общения пользователей в глобальной сети. При этом не происходит личностно-визуального контакта, что снимает психологические барьеры и приводит к раскрепощенности [1, с. 29].

Практически невозможно установить личность человека, который хочет остаться незамеченным в виртуальном пространстве, пока существуют программы, маскирующие реальный IP – адрес, например, такие как (HideMyIP, SafeIP, HideALLIP, HideMy.nameVPN, Freegate) и многие другие по которым можно идентифицировать местонахождение персонального компьютера преступника.

Технологии мобильного Интернета усугубляют ситуацию, поскольку преступник может свободно перемещаться в пространстве, используя различные точки доступа. Практический каждый человек имеет возможность воспользоваться доступом в Интернет за сравнительно небольшие деньги.

Еще одна специфическая особенность, оперативность действий производимых в Интернете, «в режиме реального времени». Оперативность любых операций распространяется на всё пространство в Интернете, охватывающее страны и континенты [2, с. 7-8]. С помощью Интернета стало возможным общение людей из различных уголков планеты.

Применение новых технологий значительно облегчило задачу. При тиражировании и рассылки писем с помощью обычной почты, понадобилось бы затратить на почтовые расходы крупную сумму денег. Современные сетевые технологий не только упрощают, но и удешевляет совершение мошенничества.

Отсутствие социально-правового контроля со стороны общества за процессами информатизации. В начале рыночных реформ мы утратили остатки той системы социально-нравственного контроля за обществом, что прежде существовала в Советском Союзе [2, с. 14].

Являясь глобальной формой организации общественных отношений, Интернет обществом не контролируется: особенности современных сетевых технологий, предоставляющих возможности для успешного ведения преступной деятельности; отсутствие социально-правового контроля со стороны общества за процессами информатизации; недостатки в сфере правового регулирования; недостатки правоохранительной деятельности.

В особенности следует отметить, что в связи с тенденцией современности, когда все онлайн-платформы и информационные системы перешли на мобильный формат, в последние годы для совершения интернет-мошенничества, преступники используют в основном мобильные телефоны, а не компьютеры, как раньше.

В результате изучения оперативно-следственной практики и материалов уголовных дел по фактам Интернет-мошенничества выявлены следующие случаи, наиболее часто формирующиеся на начальных этапах раскрытия и расследования по способу хищения денежных средств:

– денежные средства снимаются со счета потерпевшего после того, как потерпевший по требованию мошенника представил ему свои персональные данные;

– денежные средства переводятся по требованию мошенника на банковский счет, зарегистрированный на имя конкретного физического лица, или на определенный мобильный номер телефона через другие системы онлайн-платежей (QIWI, Каспи, Халык или Криптовалюту);

– денежные средства выдаются потерпевшим курьером или другим лицом;

– денежные средства потерпевшие передают через курьеров или другим лицом;

– мошенник оформляет микрокредит в микрофинансовых организациях с использованием персональных данных потерпевшего;

– мошенник звонит или отправляет SMS на мобильный телефон потерпевшего по мобильному телефону, после чего знакомится с ним как с сотрудником банка, коммерческой организации или рекламной компании, сообщает потерпевшему, что на его имя вышел крупный «розыгрыш» (автомобиль, бытовая техника, туристическая путевка и т.д.) и передает потерпевшему денежные средства в определенном объеме для получения или доставки подарка (как налог, аванс, оплата доставки и т.д.) предлагает перевести на указанный им счет;

– мошенник, позвонив или отправив SMS на мобильный телефон потерпевшего по своему мобильному телефону, сообщает потерпевшему о том, что его банковский счет или счет мобильного номера телефона заблокирован, и представившись сотрудником банка или оператора сотовой связи, предлагает свою помощь, говоря что для решения необходимо набрать определенную комбинацию в банкомате или платежном терминале либо в мобильном приложении (Kaspi, Homebank и др.) после чего переводит средства на свои счета.

В результате таких простых действий деньги переводятся на счет мошенника или его знакомых.

Также можно отметить несколько видов интернет-мошенничеств, в основном по описанию субъектов преступления:

1) совершенные преступниками, находящимися на свободе - чаще всего мошенники звонят клиентам банков с целью выманить персональные данные и конфиденциальные банковские сведения: фамилию, имя и отчество, паспортные данные, имена и фамилии родственников, кодовое слово клиента банка, данные платёжных карт, коды подтверждения банковских операций (например, содержимое SMS с кодом). Также часто мошенники звонят с целью стимулировать жертву совершить нужные им действия с платёжной картой или банковским счётом жертвы. При этом звонящий может подменить номер, который показывает аппарат жертвы (АОН), чтобы жертва восприняла входящий звонок, как будто он - с публичного телефонного номера банка [3];

2) совершенные преступниками, отбывающими наказание в местах лишения свободы.

В организации «телефонного мошенничества» участвуют несколько преступников, в такие группы входят лица, отбывающие наказание в учреждениях Комитета уголовно-исполнительной системы (далее – КУИС). В основном они звонят или отправляют короткое текстовое сообщение (SMS), чтобы связаться со своими жертвами, используя незаконно полученные SIM-карты, при этом преступники связываются из разных регионов и даже из-за рубежа.

На начальном этапе очень сложно определить данные о преступнике этой категории. Как правило, мошенников можно узнать по способу общения и интересу к личным данным, данным платежных карт. Все зависит от способа обмана.

В результате бездействия должностных лиц учреждений КУИС в этих учреждениях действуют преступные группы, систематически осуществляющие интернет и телефонное мошенничество, состоящие из лиц, отбывающих уголовные наказания. Учреждения КУИС бессильны, не заинтересованы в полной блокировке. Несмотря на то, что КУИС вновь включен в состав МВД с 2012 года, вопрос не решается полностью. Несмотря на то, что были предприняты некоторые меры по недопущению передачи мобильных телефонов, вопрос до конца не решен

В целом, в большинстве случаев основное внимание уделяется двум группам вредителей:

– лица, потерявшие долгосрочную работу и место жительства, неоднократно осужденные за мошенничество или иные правонарушения против имущества;

– мошенники-рецидивисты, совершающие мелкие мошенничества, в основном их жертвами становятся знакомые люди.

Существует несколько способов классификации личности интернет-мошенника в зависимости от мотива совершения уголовного правонарушения. В классификации, предложенной В.Б. Веховым, личность интернет-мошенника распределяется следующим образом:

1) субъекты, отличающиеся профессионализмом и компетентностью, сочетающие в себе хорошие знания и навыки в области информационных технологий и программирования, а также проявляющие лояльность к профессии и склонность к изобретению новых схем. У них нет четкого проявления антисоциальных намерений, которые часто могут быть использованы злоумышленниками на начальном этапе;

2) лица с интернет зависимостью;

3) хакеры, целенаправленно занимающиеся интернет-мошенничеством, имеющие явную корыстную подлость. Они отличаются повторным совершением уголовных правонарушений, обладают существенными навыками убеждения и убеждения, а также сокрытия следов преступлений;

4) простые люди, не имеющие существенной профессиональной квалификации в области технологий, освоившие потребительский характер только в социальных сетях и интернете [4].

Денежные средства, украденные мошенническим путем, выводятся различными способами.

Способы совершения интернет-мошенничества многочисленны и разнообразны. Это связано, в первую очередь, с быстрым ростом количества и постоянным развитием качества услуг в сфере информационных технологий.

Наиболее распространенные популярные способы совершения преступлений, связанных с интернет-мошенничеством, включают фишинг, вишинг, кибersквоттинг, тайпсквоттинг.

При этом, в основном предметом преступления в сети Интернет являются не наличные денежные средства, а виртуальные, то есть переводы денежных средств через данные банковских карт, счетов, платежных систем. В случае перечисления денежных средств вероятность обнаружения преступника минимальна из-за того, что получатели денег не вступают в прямой контакт с потерпевшим.

Существующие методики раскрытия и расследования интернет-мошенничества раньше позволяли разоблачать преступников. Однако в настоящее время они становятся неэффективными, так как существенно изменились уголовно-правовые, оперативно-розыскные, криминалистические и криминологические характеристики данных видов преступлений.

Первые оперативно-розыскные мероприятия и следственные действия, порядок их проведения рассматриваются в зависимости от того, раскрывается ли преступление по горячим следам, выявляется ли мошенник и задерживается ли он. В большинстве случаев о случае интернет-мошенничеств сообщается в орган уголовного преследования через некоторое время, и при поступлении заявления об этом инцеденте большей информации совершенно неизвестно, кто совершил интернет – мошенничество.

Для повышения качества раскрытия и расследования данного вида преступлений необходимо совместное планирование оперативно-розыскных мероприятий, процессуальных и непроцессуальных действий.

1. При поступлении заявления или сообщения об Интернет-мошенничестве, при получении подробного ответа от заявителя, допроса преступник в какое время, с какого абонентского номера он звонил, сколько раз звонил, кем он себя представлял, что говорил, какие действия предлагал совершить, на какую сумму денежные средства и за какие услуги он просил перечислить, определить способ направления денежных средств (блиц-перевод, наличный перевод, перевод на мобильный номер телефона и т.д.), узнать преступника по голосу или нет, описать его голос. В случае, если денежные средства выданы нарочно через посредника, предложить описать его внешний вид, а затем с его помощью составить фотопортрет;

2. Мобилизация всех внешних служб экстренного органа внутренних дел (патрульную полицию);

3. В случае поступления сообщения о «телефонном мошенничестве» оперативный сотрудник или следователь незамедлительно определяют, к какому оператору сотовой связи зарегистрирован абонентский номер, его владелец, где он находится;

4. Составление биллинга исходящих и входящих звонков с данного абонентского номера, определение сведений об именах и личности владельцев соответствующих абонентов, их доставка и получение ответа;

5. В целях получения дополнительных данных об интересующем абоненте по уголовному делу выносится постановление об абоненте, а при необходимости о получении информации, о телефонных разговорах или проведении контроля и записи телефонных разговоров. Анализ информации, полученной от оператора сотовой связи, позволяет выявить лиц, потерпевших и свидетелей, причастных к расследованию неизвестного преступления. Это допрос людей.

6. Если деньги переведены через банки второго уровня Республики Казахстан:

– определить, при каких обстоятельствах был произведен перевод, какие персональные данные сообщил потерпевший преступнику. Запрос, получение и рассмотрение документов, касающихся перевода с потерпевшего, регистрация в материалах дела, признав их доказательствами;

– получение от банков информации о денежных переводах, поступивших фигуранту по уголовному делу, их дальнейшем движении, наименовании и адресе отделения банка или банкомата, если наличные изъяты, а также снятие записей с камер видеонаблюдения;

– в случае выявления лица, получающего денежные средства, проверка сведений о его подсудности, сбор описательных материалов, допрос по обстоятельствам получения денежных средств путем проведения видеосъемки, получение образцов голосов и представление их потерпевшему для признания, при необходимости назначение экспертизы; выявление родственников и других близких лиц, состоящих на рассмотрении, в том числе подсудность за аналогичные преступления проверка наличия лиц, имеющих или отбывающих наказание; проверка причастности выявленных лиц к другим ранее совершенным преступлениям;

7. После получения информации от оператора сотовой связи:

– выявление и допрос лица, на котором зарегистрирован мобильный номер, по которому был произведен звонок потерпевшему, проведение осмотра его телефона, при необходимости проведение выемки, получение образцов голоса и представление его потерпевшему для признания, при необходимости назначение психофизиологического исследования;

– если лицо, у которого зарегистрирован мобильный номер, указывает, что он не оформил номер на свое имя, получить соответствующие документы у оператора сотовой связи и назначить экспертизу подписи;

– выявление родственников и других близких в отношениях лиц, в том числе имеющих судимость или отбывающих наказание за аналогичные преступления; проверка причастности выявленных лиц к другим ранее совершенным преступлениям;

8. Если денежные средства направлены на мобильный номер или электронный кошелек (Каспи, Web Money, Яндекс деньги, QIWI):

– направление в организацию, осуществляющую администрирование электронного кошелька, письма-запроса о предоставлении регистрационных данных владельца, выписок из журналов входа в систему и транзакций, данных по IP-адресу, по которому осуществлен вход в систему;

– выявить и допросить лицо, к которому прикреплен электронный кошелек, получить образцы голоса и представить его потерпевшему для опознания, при необходимости назначить психофизиологическое исследование;

– выявление родственников и других близких в отношениях лиц, в том числе имеющих судимость или отбывающих наказание за аналогичные преступления; проверка причастности выявленных лиц к другим ранее совершенным преступлениям;

9. В случае если денежные средства выданы наличными:

– составление субъективного портрета лица, которому выданы деньги в присутствии заявителя;

– наличие камер внешнего наблюдения в месте выдачи денег, просмотр и снятие видеозаписей, если таковые имеются, при необходимости признание в качестве прецедента и регистрация материалов дела;

10. Регистрация в материалах дела всех документов и предметов, полученных в ходе досудебного расследования, с соблюдением требований УПК.

Литература

1. Журавлева Е.Ю. Основные категории пользователей среды сети Интернет // «Социология и Интернет: 2014-2015. – С. 29.

2. Залесский П. Интернет: российская аудитория в анфас и в профиль // Медиа - альманах. 2015. №7-8. – С. 17.

3. Интернет ресурс – https://ru.wikipedia.org/wiki/Телеф-е_мошенничество.

4. Вехов В.Б. «Компьютерные преступления. Способы совершения и методика расследования». [Электрондық деректер] // – Режим доступа: https://www.studmed.ru/view/vehov-vb-kompyuternye-prestupleniya-sposoby- soversheniya-i-metodika-rassledovaniya_781a155ddb1.html? page=3 (жүгінген күн: 02.03.2023ж.).

АЛМАЗҚЫЗЫ
Карлыгаш
Қазақстан Республикасы ІІМ М. Есболатов
атындағы Алматы академиясы
киберқылмысқа қарсы іс-қимыл бойынша
мамандарды даярлау орталығының
аға оқытушы-әдіскері полиция подполковнигі

ҚҰЛМАН
Ернұр Ерланұлы
Қазақстан Республикасы ІІМ М. Есболатов
атындағы Алматы академиясы
киберқылмысқа қарсы іс-қимыл бойынша
мамандарды даярлау орталығының
аға оқытушы-әдіскері полиция подполковнигі

ҚАЗІРГІ ЖАҒДАЙДАҒЫ КИБЕРҚЫЛМЫСТЫ БОЛДЫРМАУДЫҢ КЕЙБІР МӘСЕЛЕЛЕРІ ТУРАЛЫ

Бүгінде киберқауіпсіздікті қамтамасыз ету мәселелері бүкіл әлемдік қауымдастыққа әсер етуде. Аталған мақалада автормен қазіргі уақыттағы киберқылмыстылықтың жағдайы, оларға қарсы ісқимыл және алдын алу проблемалары қарастырылған. Осыған байланысты автормен шетелдік тәжірибеге, халықаралық сарапшылардың тәжірибесіне талдау жасала отырып, киберқылмыстылық түрлері және ақпараттық технологияларға байланысты қылмыстылық проблемалары жан-жақты зерделенген. Киберкеңістіктегі заңсыз әрекеттердің түрлерінің ерекшеліктері ашылған. Киберқылмыспен күресуде халықаралық ынтымақтастықтың тиімді тетіктерін әзірлеу қажеттілігі негізделген.

Киберқылмыстылық жаһандық халықаралық проблема болып танылды. Құқық қорғау органдары мен арнайы органдардың алдында тұрған ең үлкен қиындық олардың әрекеттерін мемлекеттік шекараларда, түрлі юрисдикциялар мен заңнамалық жүйелер шеңберіндегі тиімді үйлестірудің мүмкін еместігі. Киберқылмысқа қарсы іс-қимыл өзіне қылмысты, олардың жасалу механизмдерін туғызатын субъективті себептер мен объективті жағдайларды қосатын, анықтау, жолын кесу, тергеу тәсілдері; сот қарауының тәжірибесі сияқты барлық ісшаралар жүйесін білдіреді. Қылмыстық және криминологиялық зерттеулердің нәтижелерін заңнамалық және нормативтік қызметке енгізудің тиімді механизмдерін құру, сондай-ақ құқық қорғау органдарының және киберқылмыспен күрес жөніндегі арнайы органдарды даярлаудың жаңа әдістерін әзірлеу қажеттілігі туындап отыр. Қазіргі заманғы ақпараттық – коммуникациялық технологиялардың мүмкіндіктері ұйымдасқан қылмыстық қоғамдастық пен жеке қылмыскерлермен белсенді түрде қолданылады.

Бұл қылмыстық әрекеттердің қазіргі заманғы киберқылмыс түрлерінің пайда болуына алып келеді. Қылмыскерлердің өкілдері компьютерлік жүйелер мен компьютерлік желілердің жұмысына заңсыз араласуды жүзеге асырады, ұрлық, заңсыз иелену, компьютерлік ақпаратты

қорқытып алу, ақпараттық ресурстарға қашықт ағы шабуылдарды ұйымдастыру, компьютерлік вирустарды дамыту және тарату және т.с.с. Киберқылмыстылық өзінің механизімі, олардың жасалу және жасырылуын қамтамасыз ету тетігі бойынша белгілі бір ерекшеліктерге ие. Олар латенттіліктің жоғары деңгейімен және мұндай қылмыстардың төмен ашылуымен ерекшеленеді. Бұл тұрғыда ерекше орынды Интернет алады, оның құқықтық мәртебесі анық көрсетілмеген, сот практикасы үшін осы «жаңа құбылыстың» мемлекеттік реттелуінің негізделген тетіктері әзірге жоқ. Тиісінше, бұл жағдай қылмыстық әлемге қолайлы болады және Интернеттің жедел қылмыстық сипатқа ие болуына ықпал етеді. Мысалы, наркодилермен олардың клиенттері жиі «жабық» сұхбат арналарында мәміле жасайды, олар арнайы бағдарламалық жасақтама мен аппараттық құралдармен сырттан келгендердің назарынан тыс қалады. Атап айтқанда, киберқылмыстың алдын алу және тергеу саласында мамандандырылған Group-IB халықаралық компаниясының сарапшылары әлемдік киберкеңістіктегі қазіргі кезеңде киберқылмыс жасайтын негізгі қылмыстық әрекеттер болып:

1) интернет-банкинг жүйелеріндегі алаяқтық;

2) интернет-алаяқтықтың түріне жататын фишинг, оның мақсаты – құпия пайдаланушының деректеріне кіру және парольдерге қол жеткізу. Бұған танымал брендтердің атынан электрондық поштаға жаппай хат тарату арқылы, сондай-ақ түрлі қызметтердегі жеке хабарламалар, мысалы, банктер атынан хабарламалар жіберу арқылы қол жеткізуге болады.

3) электрондық ақшаны ұрлау;

4) басқа да заңсыз кірістерді қолма-қолға айналдыру қызметтері;

5) спам – коммерциялық және басқа жарнамаларды немесе басқа да хабарламаларды қаламаған тұлғаларға жіберу. Мысалы, дәрі-дәрмектер және әртүрлі контрафактілік өнімдер, жасанды бағдарламалық қамтамасыз ету, қызметтер, білім, туризм туралы ақпарат және т.б.;

6) трафикті сату;

7) эксплойттарды сату;

8) жүктеулерді сату;

9) анонимизация – әрекет етуші тұлғаның ақпарат көзін мақсатында деректерді (құжаттардан, дерекқордан және т.б.) жою процесі және т.б.

10) DDoS шабуылдары – компьютерлік жүйеге тосқауыл қою немесе пайдаланушыларға берілген жүйелік ресурстарға (серверлерге) қол жеткізуді қиындату мақсатында оған шабыл жасау. DDoSшабуыл – қорғалған компьютерлік жүйелерді (мысалы, мемлекеттік билік органдарының, банктердің, ірі компаниялардың, электронды БАҚ және т.б.) блоктауы үшін көптеген компьютерлерден жасалынған DoS шабуылының түрі [1].

Өз кезегінде, жыл сайын Қазақстандағы, жақын және алыс шетелдегі киберқылмыстылық жағдайын талдауды жүзеге асыратын Касперский Зертханасының (GReAT) Ғаламдық зерттеулер мен тәуекелдерді талдау орталығының мамандары киберқылмыстылыққа (кәсіби сленгте «компьютерлік қатерлер») төмендегілерді жатқызады:

1) мақсатты кибершабуылдар;

2) кибершпионаж;

3) хактивизм;

4) дербес деректерлерді ұрлау;

5) киберқорқытып алу;

6) жалдауға арналған кибершабуылдар (кибер-жалшылық);

7) мобильдік құрылғыларға арналған зиянды бағдарламаларды пайдалану;

8) мақсатты фишинг;

9) жеке өмірге қолсұғылмаушылықты бұзу;

10) бағдарламалық жасақтаманың осалдығы үшін эксплоиттерді пайдалану;

11) ботнеттер құру және пайдалану [2].

Антивирустық бағдарламалық жасақтама өндіретін Panda халықаралық компаниясының PandaLabs зертханасының сарапшылары киберкеңістікте келесідей негізгі қылмыстық әрекеттер жасалды:

1. Кибер бопсалау (мысалы, Crypto Locker сияқты зиянды бағдарлама, компьютерге еніп, пайдаланушыға құнды болуы мүмкін барлық құжаттарды (электрондық кестелер, құжаттар,

дерекқорлар, фотосуреттер және т.б.) шифрлайды. Содан кейін жәбірленуші файлдарды қалпына келтіру мүмкіндігі үшін ақша төлеуді талап етіп бопсалайды).

2. Компаниялардың, ұйымдардың, мекемелердің және т.б. ақпараттық ресурстарға бағытталған кибер-шабуылдар.

3. Клиенттердің банк карталарын ұрлау үшін төлем терминалдары бойынша кибершабуылдар жасауы.

4. APT-шабуылдар (Advanced Persistent Threats) – ірі компанияларға немесе стратегиялық маңызы бар мемлекеттік және қоғамдық институттарға бағытталған мақсатты шабуылдардың түрі болып табылатын, «күрделі тұрақты қауіп» деп аталатын шабуылдар.

5. Интернетке қосылған құрылғыларды («Интернет-заттарды») бұзу. Бұл құрылғылар IPкамералардан принтерлерге дейін, Интернеттің бір бөлігі бола тұра, киберқылмыскерлердің бұзып кіруі мен пайдаланушыға зиян келтіру үшін әлсіз болып келетін бағдарламалық жасақтамадан тұрады.

6. Құпия сөздерді және пайдаланушы деректерін ұрлау үшін смартфондарға, сондай-ақ басқа мобильді құрылғыларға шабуылдар [3].

Киберқылмыстың құрылымдық сипаттамаларын әртүрлі сараптамалық бағалау тұрғысынан талдай отырып, олар бірінші кезекте ақпараттық-коммуникациялық (бағдарламалық-техникалық) критерийлерге негізделген деп қорытынды жасауға болады. Бұл көзқарас арнайы және құқық қорғау органдарының нормативтік көзқарасынан біршама ерекшеленеді, бірақ ол оларға қайшы келмейді, себебі іс жүзінде киберқауіптердің бәрі отандық Қылмыстық кодекске бағынады. Басқа сарапшылар киберқауіптерді дамытудың негізгі үрдістерінің қатарына келесілерді жатқызады:кибер-шабуылдардың санының тез өсуі, олардың көпшілігі үлкен шығындарға әкеледі;

– тшабуылдардың күрделілігін арттырады, олар бірнеше кезеңнен тұрады. Сонымен қатар, олардың бейтараптандырудан қорғаудың арнайы әдістерін қолданады; барлық электронды (цифрлық) құрылғыларға, атап айтқанда, рұқсат етілмеген қол жеткізуге жиі ұшырайтын мобильді құрылғыларға әсер ету;

– ірі корпорациялардың, маңызды өнеркәсіптік нысандардың, мемлекеттік құрылымдардың ақпараттық инфрақұрылымына жасалған шабуылдардың қарқынды өсуі;

– компьютерлік технологиялар саласында дамыған елдердің, басқа мемлекеттерге кибершабуылдың құралдары мен әдістерін пайдалануы [4].

Әлемдік киберкеңістікте бізді күтіп отырған аталған қауіптер киберқылмыс істері жөніндегі барлық жаңа фактілер мен киберқылмыспен күресудің жаңа түрлерін баяндайтын көптеген жаңалықтармен расталады.

Жыл сайын жаһандық желіде миллиардтаған зиянды нысандар анықталып, жыл сайын олардың саны шамамен 40% артады. Ақпараттық кеңістіктегі зиянды шабуылдардан келтірілген залал 100 миллиард АҚШ долларына бағаланады. Сарапшылардың айтуынша, жер бетіндегі шамамен 12 адам киберқылмыскерлердің әр секунд сайын құрбандары болып табылады. Әдетте, хакерлердің ең табысты шабуылдары жаһандық желіге қосылған соңғы пайдаланушылардың серверлеріне және компьютерлеріне бағытталған. Әдетте кибершабуылдарға зиянды бағдарламалар, трояндық жылқылар, ботнеттер, фишинг, қызметтік шабуылдардан бас тарту және «ортасында адам» сияқты құралдар қолданылады. Қазіргі кезде ақпараттық қауіпсіздіктің, оның ішінде киберқауіпсіздіктердің ең осалының бірі болып мобильді құрылғылар табылады. Нарықтық үлесі шамамен 80% болатын Android мобильдік құрылғыларға арналған барлық бағдарламалық жасақтама АҚШ арнайы қызметтері бақылайтын «ашық» кодқа негізделген. Бұл құбылыс оны шетелдік арнайы қызметтердің бақылауына тапсыра отырып, еліміздің ұлттық қауіпсіздігіне қатер төндіреді. Сонымен бірге, Android-құрылғыларына бағытталған Android операциялық жүйесі үшін әзірленген зиянды бағдарламалардың үлесі қарқынды дамып келеді. Мәселен, 2012 жылдың соңына дейін Android ОЖ-іне негізделген цифрлы құрылғыларға арналған вирустар үлесі басқа ұялы байланыс операторларына арналған вирустардың жалпы санының 94%-ын құрады. Содан кейін, зиянды бағдарламалық қамтамасыз ету адамдарға заманауи байланыс құралдарын пайдаланып бақылау мақсатында мобильді құрылғыларға құпия түрде орнатылады. Бұл жағдайда, Wall Street Journal-тің жариялауына сәйкес, ФТБ-да смартфондарға және Android операциялық жүйесімен

жұмыс істейтін планшеттерге микрофонды қашықтан қосуға мүмкіндік беретін технологиялар бар. Яғни, шын мәнінде, ұялы телефон күнделікті пайдаланушылардың өздерімен бірге алып жүретін жазу құрылғысына (жучок) айналады. Android платформасынан ұлттық қауіпті көрген ҚХР-ның билігі осы мәселеден қауіп көріп отыр [4].

Осы бағыттағы киберқауіпсіздікті қамтамасыз ету, біздің ойымызша, ел ішінде ақпараттықкоммуникациялық өнімдер үшін электронды өнімдер мен тарату арналарын құру мен дамытудан тұруы мүмкін. Мәселені кешенді түрде шешу үшін құзыретті құрылымдар мен кәсіпорындар арасында әлемдік деңгейдегі сұранысқа ие өнімдерді нарыққа шығаруды қамтамасыз ету үшін бірқатар ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды ұйымдастыру қажет. Бұл біздің елімізге киберқауіпсіздіктің қауіпсіз инфрақұрылымын қалыптастыруға және отандық ақпараттық-коммуникациялық шешімдерді өндіруге негізделген экономиканың дамуын қамтамасыз етуге мүмкіндік береді. Киберқылмыстың құрылымы әртүрлі елдерде, ақпараттық-коммуникациялық технологиялардың даму дәрежесі мен сипатына, интернет желісінде таратуға, электрондық қызметтерді және электронды коммерцияны пайдалануға және т.б. байланысты өзгереді. Қазақстандық Ақпараттық Қауіпсіздік Қауымдастығының төрағасы В.В. Покусовтың айтуынша, «боттардың көмегімен жасалған, яғни өздері шабуыл жасайтын, таратылатын автоматтандырылған жүйелер арқылы шабуылдар бірінші орында болады. Екінші орында – зиянды бағдарламалық қамтамасыз етуді енгізумен байланысты шабуылдар екен. Осы шабуылдың екі түрі мұндай шабуылдардың жалпы санының ішінде 60% құрайды. Бұған қоса, маңызды ақпараттың шығып кетуіне байланысты жағдайлар бар, бұл көбінесе қызметкерлердің қауіпсіздік ережелерін бұзған жағдайда орын алады». Маманның айтуы бойынша, Қазақстандағы киберқауіптердің арасында екінші орында компьютерге қашықтан қол жеткізу жүйелерін енгізу болса, үшінші орында – рұқсатсыз кіру деп ескерілген. Интернетте жиі кездесетін қорлау оқиғалары да бар 100-ден астам осындай жағдай тіркелді. Жиі әйгілі адамдардың атынан жалған аккаунттар жасалып, фотосуреттерін таратады және бұл олардың беделін төмендету үшін жасалады. Бұл ақпараттық шабуылдарға жатады [5].

Трансұлттық лаңкестік және экстремистік ұйымдардың ақпараттық-коммуникациялық технологиялар мен компьютерлік желілерді дамыту фактілерінің көбейіп келе жатқанын атап өткен жөн, бұл киберқылмыстың ең қауіпті нысанын – кибертерроризмнің пайда болуына әкелді. Сарапшылардың пікірінше, қазіргі уақытта салдары өзін-өзі өлтіретін адамдарды, жарылғыш заттарды және т.б. қолдану арқылы жасалатын дәстүрлі лаңкестік актілерінен кем болмайтын мемлекеттік ақпараттық жүйелер бойынша кибершабуылдардың саны айтарлықтай өсті. Мұндай қылмыстық әрекеттер кез келген мемлекеттің маңызды өмірлік жүйелерін: ядролық және басқа да маңызды объектілерді, мұнай және газ құбырларын, электр станцияларын, теміржолдарды, әуежайларды, сумен жабдықтау нысандарын және т.б. басқаруды және олардың жұмыс істеуін тоқтатады. Кейбір сарапшылардың айтуынша, дүниежүзі күткен жаңа киберқауіптер пайда болды.

Мұндай қауіптердің ішіне киберқаруды қолданумен жасалатын кибершабуылдар кіреді. Маманның пікірінше «...бұл қарапайым трояндар емес, бұл өте күрделі жүйелер. Оларға, өз кезегінде қорғаныстық киберқарумен қарсы тұру қажет. Біздің өміріміздегі киберқарудың пайда болуымен бүкіл координат жүйесі өзгерді, себебі шын мәнінде белсенді қорлаушы арсенал ғана емес, сонымен қатар, әлдеқайда қауіпті, жасырынбарлау жасайтын киберқылмыс бар» [5]. Демек, киберқауіпсіздікті қамтамасыз етудегі маңызды құрамдас бөлік болып соңғы уақытта шабуылға ұшыраған маңызды мемлекеттік және өндірістік объектілерді қорғау болып табылады. Көптеген өнеркәсіптік бақылау жүйелеріне еніп, шабуыл жасаушы олардың кодтарын оператордың келісімінсіз ұстап қала алатын Stuxnet, Duqu және Flame құрттары біраз шулатты. Осылайша, заводттардың және атом электростанцияларының жарамсыздығына алып келуге болады. Мысалы, Stuxnet бағдарламасы уранды байыту үшін Иран центрифугаларының 80% -ын істен сәтті ажыратты. Бұған қоса, американдық арнайы мамандардың осы күрделі зиянды бағдарламаларды құруға қатысқаны туралы, сондай-ақ кибер-кеңістіктегі шабуылдарды қаржыландыру АҚШ мемлекеттік құрылымдарымен жүргізілетіндігі мәлім болды [4].

Жаңа ақпараттық және коммуникациялық технологиялармен байланысты қылмыс ауқымын нақты түсіну, киберкеңістіктегі жаңа қылмыстық қауіп-қатерлерге тек әлемнің

барлық мемлекеттерінің бірлескен күш-жігері арқылы ғана қол жеткізуге болатынын түсіндіреді. Бұл факт қазіргі уақытта заңнаманы біріздендіру және жаһандық деңгейде құқық қорғау қызметін үйлестірудің саналы үрдісі болып табылатындығымен расталады. Киберқылмыспен күресудің негізгі бағыттарының бірі киберқауіпсіздікті қамтамасыз ету және тұтастай алғанда ақпараттық қауіпсіздікті қамтамасыз ету үшін халықаралық ынтымақтастық болып табылады. Бұл осы саладағы халықаралық өзара әрекеттесудің жалпы логикасын көрсетеді. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы халықаралық ынтымақтастық үшін мемлекетаралық және мемлекеттік емес факторлардың қатысуымен ынтымақтастықтың жаңа модельдері сипатталады, көп жақты серіктестік немесе көп деңгейлі ынтымақтастық деп аталады.

Мұндай әрекеттесудің рөлі ақпараттық қауіпсіздікті қамтамасыз ету кезінде өсіп отырады. Сонымен бірге мемлекеттер осы саладағы үйлестіруші рөлге ие. Киберқауіпсіздікті қамтамасыз етудің халықаралық режимін қалыптастырудың логикасы және тұтастай алғанда ақпараттық қауіпсіздік халықаралық таратпау режимін қалыптастырудың логикасына жақын [6]. Біздің көзқарасымыз бойынша, мемлекетіміздің ақпараттық қауіпсіздік режимін аймақтандыру үрдісін сақтап қалу қажет. Мысалы, АҚШ базасында және ШЫҰ шеңберінде еуразиялық кеңістікте Еуразиялық экономикалық одақ шеңберінде посткеңестік кеңістіктегі ақпараттық қауіпсіздік режимін қалыптастыру шеңберінде.

Ақпараттық қауіпсіздік режимін аймақтандырудағы бұл қадам біздің елімізге киберқауіпсіздікті қамтамасыз ету саласындағы дамып жатқан жағдайды тиімді бақылауға мүмкіндік береді. Осы саладағы маңызды қадамдардың бірі Қазақстан Республикасының Президенті Н. Назарбаевтың «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастығы туралы келісімді ратификациялау туралы» Қазақстан Республикасының Заңына қол қоюы болды [7].

Халықаралық ынтымақтастық ақпараттық-коммуникациялық технологияларды дамыту мен қолданыстағы заңнамаға әсер ету арасындағы құқықтық вакуумды жоюдың кілті екендігін сенімділікпен айтуға болады. Киберқауіпсіздікті және ақпараттық қауіпсіздікті тұтастай алғанда халықаралық деңгейде қамтамасыз ету жөніндегі шараларды әзірлеу және қабылдау күрделі мәселе, бірақ бұл киберқылмыспен қылмыстық қол сұғушылықтан және киберқылмыскерлерді тиімді алдын-алудан қазіргі заманғы жағдайлардағы маңызды жол болып табылады.

Әдебиет

1. Информация международной компании Group-IB по киберпреступлениям // http://report2016. group-ib.ru).
2. Бюллетень Центра глобальных исследований и анализа угроз «Лаборатории Касперского» (GReAT) // http://securelist.ru/files/2016/ 12/Kaspersky-Security-Bulletin-2016-RU.pdf
3. Информация лаборатории PandaLabs по киберпреступлениям // http://www.viruslab.ru/upload/ files/ download/wp/wp_reports_2016.pdf
4. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях //Теория и практика общественного развития. – Краснодар. – 2015. – №13. – С. 96-99.
5. Казахстанская ассоциация информационной безопасности предоставила статистику киберугроз в нашей стране // https://informburo.kz/novosti/specialisty-nazvali-lidiruyushchie -vidy-kiberprestupnosti 140 ҒЫЛЫМ, 2019, N 1 – v-kazahstane.html
6. Зиновьева Е.И. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // .Зиновьева Е.С. // Вестник МГИМО-Университета. – 2016. – №4 (49). – С. 235-247. – С. 235-247.
7. Назарбаев ратифицировал соглашение в сфере информбезопасности стран СНГ // https:// www.nur.kz/1730046-nazarbaev-ratificiroval-soglasenie-v-sfere-informbezopasnosti-stran-sng.html.

БЕЙСЕНБАЙ
Әлия Бейсенбайқызы
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы киберқылмысқа қарсы іс-қимыл бойынша мамандарды даярлау орталығының аға оқытушы-әдіскері
полиция майоры

ОНГАРБАЕВ
Габит Сабитулы
Қазақстан Республикасы ІІМ
М. Есболатов атындағы
Алматы академиясының
магистранты полиция капитаны

ИНТЕРНЕТ ЖЕЛІСІНДЕГІ АЛАЯҚТЫҚ ЖӘНЕ ОДАН ҚОРҒАНУ ТӘСІЛДЕРІ, АЛДЫН АЛУ ЖОЛДАРЫ

Қазіргі таңда техникалық прогресс бір орында тұрмай күннен күнге даму үстінде. Алайда, бұл – интернеттегі алаяқтықтың көбеюіне әкеп соқтыруда. Бұл мақаланың мақсаты қазіргі виртуалды әлемдегі интернет-алаяқтықтың негізгі мәселелерін анықтау болып табылады. Интернет-алаяқтық әлеуметтік құбылыс ретінде қоғамға теріс әсер етуде. Бұл мақалада ғаламдық Интернет желісіндегі алаяқтықтың жіктелуі қарастырылып, соның негізінде талдау жүргізіледі, пайдаланушылардың ақпаратын қорғау шаралары, сондай-ақ әлеуметтік желілер сайттарында компьютерлік қылмыстың алдын алу шаралары жасалады.

Кілтті сөздер: интернет, алаяқтық, коммуникациялар, әлеуметтік желілер, фишинг, қылмыскерлер, қорғау.

Қазіргі әлем компьютерлік технологиялармен және ақпараттық процестердің жаһандануымен тығыз байланысты. Халықаралық интернет желісінің пайда болуы, сондай-ақ оны әлеуметтік қоғамның барлық салаларында пайдаланудың ауқымы кеңеюде.

Интернет жаңа әлеуметтік қатынастар орнатты. Адамдар күн сайын интернет арқылы тауарлар мен қызметтерді көбірек сатып алады. Сондықтан интернет халыққа үйден шықпай-ақ әртүрлі операцияларды ыңғайлы жүзеге асыруға мүмкіндік береді. Бұл процестің дамуы мен жаһандануы виртуалды әлемде алаяқтық сияқты әлеуметтік құбылысқа әкеп соқтырды. Интернеттің ақпараттық және коммуникативті мүмкіндіктері қарқынды дамып келе жатқандықтан, интернет әртүрлі әлеуметтік процестер мен құбылыстар орын алатын коммуникативті алаң ретінде әрекет етеді. Ең көп тарағандардың бірі-әртүрлі нысандардағы алаяқтық [1].

Қылмыстық заңға сәйкес, мүлікті немесе ақшаны теріс мақсатта пайдалану және алдау арқылы ұсақ немесе ірі көлемдегі ұрлау алаяқтығы деп танылады. Бұдан басқа, алаяқтық қолма-қол ақшасыз ақша аударымдары мен операцияларды қоса алғанда, электрондық төлем құралдарын пайдалану арқылы орын алуы мүмкін [2].

Соңғы уақытта халық жүлделерді жеңіп алу туралы, сондай-ақ пайызсыз несиелер, қарыздар және т. б. алу мүмкіндігі туралы хабарламалар немесе электрондық хаттарды жиі алады. Жүлделер немесе жеңілдетілген несиелер алу үшін алаяқтар әдетте белгілі бір ақша сомасын электронды шоттарға аударуды немесе несие алған кезде ақша сомасын салуды сұрайды, осылайша адамдарды ынталандырады. Аванстық ақшаны алғаннан кейін олар байланыстан кете бастайды немесе қосымша сома ұтысын ресімдеуді аударуды сұрайды. Осындай «трюктерден» қорғану үшін: «Мен қандай да бір ұтыс ойындарына қатыстым ба» деген сұрақ туралы ойлану керек, сонымен қатар кез-келген жеңіс салық түріндегі міндеттемелерді тудыратынын есте сақтау керек. Ақша аудару мәселесіне қатысты кез-келген өтініш әр адамды алаңдатуы тиіс.

Сондықтан бүгінгі таңда интернетте алаяқтықтың көптеген түрлері бар. Олардың арасында әртүрлі акциялар, лотереялар, виртуалды қызметтер, қайырымдылық қорлар, фишинг, фрилансинг, әлеуметтік инженерия, Интернет-банкингке шабуылдар жиі кездеседі. Операциялардың барлық түрлерін алаяқтар интернетті қолдана отырып жүргізеді. Интернетте орын алған қылмыстарды толығырақ қарастырайық:

– Интернет-қайырымдалық – бұл интернеттегі алаяқтықтың ең танымал түрі, ол белгілі бір ақшаны сыйға тарту туралы өтініш түрінде көрінеді. Қайыр сұраудың ең оңай жолы-веб-сайтыңызды құру және пайдаланушылардан ақша сұрау. Алаяқтықтың бұл түрі әлеуметтік желілерде қолданылады, әсіресе Facebook, Instagram,Telegram, Viber, WhatsApp, Вконтакте және Одноклассники-де танымал;

– Интернет-дүкендермен байланысты алаяқтық. Мысал ретінде, біз осы жағдайды қарастырамыз: сатып алушы тауарды сатып алу туралы шешім қабылдады, шешім қабылдағаннан кейін ол тауарды төлейді, содан кейін оны алады немесе алмайды, бірақ аз мөлшерде немесе нашар сапада;

– Құпия деректерге қол жеткізуге негізделген Фишинг көбінесе қаржылық сипатта болады. Фишинг негізінен алаңдаушылық тудыратын ақпаратты қамтиды (мысалы, банктік картаны бұғаттау). Фишерлер, хакерлерден айырмашылығы, азаматтардың сенімін алдауды пайдаланады. Фишинг әлеуметтік желілерде, пошта жүйелерінде, интернет-банкингте және басқа да төлем жүйелерінде кеңінен таралған. Фишинг әлеуметтік даму әдістерін қолдана отырып, шабуылдар кезінде де орын алуы мүмкін. Фишерлер әртүрлі маңызды себептерді ойластырып, Клиентті өзінің жеке деректерін хабарлау үшін қорқыта алады. Кейде фишинг ұйым бөліміне де бағытталуы мүмкін [3].

Интернет виртуалды кеңістік болғанына қарамастан, ол нақты әлеуметтік салдары бар нақты әлеуметтік процестерді жүзеге асырады. Мысалы, интернеттегі алаяқтықтың қаржылық шығындары әлеуметтік-психологиялық салдары бар, олар көңілсіздік сезімін, стрессті және т. б. қамтуы мүмкін.

Бүгінгі күні қылмыскерлер жеке деректерге қол жеткізу үшін ұйымдастырушылық және техникалық шараларды жүргізудің қажеті жоқ. Адамдар оларды өздері бөліседі. Әлеуметтік желілерде өздері туралы аналитикалық ақпаратты егжей-тегжейлі жариялай отырып, пайдаланушылар оларды көптеген адамдарға сеніп тапсырады. Бірақ, дегенмен, бәрі де сенімді емес. Сондай-ақ, бүгінгі таңда алаяқтық компьютерлік саладағы қылмыс болуы мүмкін екенін атап өткен жөн, өйткені ақпараттық технологиялардың қарқынды дамуы интернет арқылы толыққанды экономикалық қызметті жүзеге асыру үшін көптеген мүмкіндіктер жасайды.

Цифрландыру саласындағы алаяқтық – бұл компьютерлік ақпаратты енгізу, пайдалану, жою, блоктау, түрлендіру не компьютерлік ақпаратты немесе ақпараттық-телекоммуникациялық желілерді сақтаудың, өңдеудің немесе берудің жұмыс істеп тұрған құралдарына өзге де араласу арқылы бөтеннің мүлкін ұрлау немесе мүлік құқықтарын емдену [4].

Соңғы жылдары интернет алаяқтық фактілерінің саны артып келеді. Олардың көпшілігі тергеудің күрделілігіне байланысты ашылмаған күйінде қалады. Соңғы бірнеше жылда интернетті пайдалану қылмыстарының саны артты. 2018 жылы 4 мыңға жуық интернет-алаяқтық тіркелген, олардың 3500-ге жуығы ашылмаған. 2019 жылы олардың саны екі есеге артып, 7 739 қылмысты құрады, 6000-нан астам қылмыс ашылған жоқ. Бұл туралы Қазақстанның ішкі істер министрлігі хабарлады.

Статистикаға сәйкес, осы жылдың басынан бастап еліміздің ішкі істер органдары ақпараттық жүйелерді пайдаланушыларға қатысты жасалған алаяқтық туралы 8 337 істі тіркеді. Аталған саннан 1709 іс ашылды, 5000-ға жуығы ашылмаған күйінде қалып отыр. Ведомстволық хабарлауынша, сайттар мен әлеуметтік желілердегі жарнамалар алаяқтықтың ең көп таралған түрі болып табылады.

Қылмысқа, атап айтқанда алаяқтыққа қарсы күрестің тиімділігі жөніндегі шараларды әзірлеу үшін оның объективті заңдылықтарын, жай-күйін, динамикасын, сипаты мен құрылымын, яғни сандық және сапалық белгілерін, алаяқтық жасау тетігін көрсету қажет.

Виртуалды кеңістікте назардан тыс қалғысы келетін адамның жеке басын анықтау мүмкін емес нақты IP мекенжайын жасыратын бағдарламалар болған кезде, сіз дербес компьютердің орналасқан жерін оңай анықтай аласыз. Сондықтан барлық ақшаны жоғалтқаннан гөрі, барлық жағдайға сенімсіз қарап, сақ болған жақсы [6]. Интернеттегі алаяқтықтың құрбаны болмау үшін сіз келесі ұсыныстарды орындауыңыз керек:

– сатушы туралы барлық қажетті ақпаратты тексеріңіз;

– тауарды алғанға дейін төлемеу;

– карта мен телефонды бір уақытта енгізбеңіз;

– жеке деректерді хабарламау және Интернеттен тыс бейтаныс адамға фото немесе видео жібермеу;

– ақша аудару туралы өтініштерге жауап бермеу;

– жаңа операциялық бағдарламалардың пайда болу динамикасын бақылау және анықталған қателерді жоятын жаңартуларды уақтылы орнату;

– сенімсіз көздерден алынған файлдарды ешқашан жүктемеңіз немесе сақтамаңыз;

– операциялық жүйені Интернетте және әлеуметтік желілерде жұмыс істеу кезінде қауіпсіздіктің негізгі ережелері қамтамасыз етілетіндей етіп конфигурациялау керек, сондай-ақ, мүмкін болса, операциялық бағдарламалардың ескі параметрлерін пайдаланудан бас тарту керек;

– лицензияланған антивирусты орнату және оны дұрыс пайдалану қажет [7].

Осылайша, Интернеттегі алаяқтық-бұл нақты әлемнен виртуалды әлемге енген құбылыс. Интернеттегі алаяқтық бүгінде экономикалық қауіпсіздіктің негізгі қауіптерінің бірі болып табылады. Көптеген адамдар бірнеше есептік жазбалар арасында ақпарат алмасу үшін әртүрлі бағдарламалар мен сайттарды пайдаланады. Көптеген адамдар үшін Интернеттегі виртуалды байланыс күнделікті өмірде таныс болды, бұл тірі тікелей қарым-қатынасты толығымен алмастырды.

Желідегі байланыс негізінен иесіздендірілген және кез-келген адам профиль фотосуретінің артында жасыра алады. Сондықтан, ешқандай жағдайда бейтаныс адамға жеке өмірінің егжей-тегжейін ашпау керек өйткені зиян келтіруі мүмкін. Бейне және онлайн трансляциялы хат жазысуларды алаяқтар сақтауы мүмкін және кейіннен құқыққа қарсы мақсаттарда пайдалануы мүмкін екенін есте сақтау қажет.

Интернеттегі алаяқтықтан қорғаудың көптеген жолдары бар:

1) Сенімді логин мен пароль. Үлкен және кіші әріптерді, символдар мен сандарды, бас әріптерді және т. б. қамтитын күрделі логиндер мен парольдерді ойлап табу қажет;

2) Телефонды тіркеу. Көптеген бағдарламалар мен қосымшаларда ұялы телефон нөмірін тіркеу мүмкіндігі бар. Оны СМС-хабарлама арқылы дербес деректерді растау мақсатында бекіту қажет;

3) Бағдарламалық жасақтама мен антивирусты жаңарту. Жаңа жаңартулар пайда болған жағдайда жүйені немесе антивирусты жаңарту қажет. Бұл электрондық қауіптерді қорғайды. Сондай-ақ, антивирустың лицензиялық толық нұсқасын алып, компьютерді үнемі тексеріп, жаңартып отырған жөн;

4) Ұқыптылық пен сенімсіздік. Күдікті сілтемелер мен хаттарға өте мұқият және қырағы болу керек, оларды ашпай-ақ дереу жойған дұрыс. Сондай-ақ, белгісіз сайттарда әлеуметтік желілерден логин мен парольді ешқашан енгізудің қажеті жоқ екенін есте сақтаңыз және біліңіз [8].

Әдебиет

1. Белоножко Е.С., Чеджемов Г.А. Мошенничество в сети Интернет // Наука XXI века: актуальные направления развития. Самара. СГЭУ. – 2017. – №1-1. – С. 86.

2. Гладкий А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. – М.: АВТОР, 2018. – С. 899.

3. Фишинг. – [Электронный ресурс]. – Режим доступа: http://www.saferunet.ru.

4. Осипенко А.Л. Сетевая компьютерная преступность теория и практика борьбы: монография. Омск: Омская академия МВД России, 2018 .

5. Официальный сайт компании «Лаборатория Касперского». – [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru.

6. Кибермошенники атакуют руководителей компании. – [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru.

7. Романов С.А. Мошенничество в России. 1000 способов как уберечься от аферистов. – М.: Конец века, 2018. – С. 320.

8. Шейнов, В. П. Как защититься от обмана и мошенничества: моногр. / В.П. Шейнов. – М.: Харвест, 2019. – С. 464.

БЕЙСЕНБІ
Арна
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
жоғары оқу орнынан кейінгі білім беру факультетінің ғылыми-педагогикалық
магистратурасының 2 курс магистранты полиция аға лейтенанты

ҚОҒАМДАҒЫ ОРЫН АЛЫП ЖАТҚАН КИБЕРБУЛЛИНГТІҢ ЗАРДАПТАРЫ

Мақалада буллинг ұғымы агрессивті мінез-құлықтың бір түрі ретінде қарастырылған. Бұл ұғымға қатысты ғалымдардың бірнеше ғылыми тұжырымдары берілген. Авторлар жалпы білім беретін орта мектепте буллингтің алдын алу жұмыстарының практикалық аспектілерін өздері жүргізген диагностикалық жұмыстарының нәтижелері арқылы көрсете білген. Сонымен қатар, буллингке де және оның құрбандарына қатысты болатыны ғылыми идея тұрғысында жазылған.

Кілтті сөздер: интернет, кибербуллинг, коммуникациялар, әлеуметтік желілер, фишинг, қылмыскерлер, қорғау.

Кибербуллинг – бұл цифрлық технологияны қолдану арқылы қорқыту және қорлау. Ол әлеуметтік желілерде, хабар алмасу қосымшаларында, ойын платформаларында және ұялы телефондарда болуы мүмкін. Мысалы

– жалған ақпарат тарату немесе әлеуметтік желілерде біреудің ұятсыз фотосуреттерін орналастыру;

– хабар алмасу платформалары арқылы қорлайтын хабарламалар немесе қауіптер жіберу;

– өзін басқа адам ретінде көрсету және оның атынан ұятсыз хабарламалар жіберу.

Кибербуллингтің салдары айтарлықтай зиянды болуы мүмкін. Зардап шеккен адамдарда мазасыздық, депрессия, өзін-өзі бағалаудың төмендеуі және суицидтік ойлар белгілері болуы мүмкін. Қазақстаннан келген балалардың 75%-ы интернетте түрлі қауіп-қатерлерге тап болды.

Кибербуллинг дегеніміз – біреуді цифрлық технологиялардың көмегімен қудалау. Кибербуллинг әлеуметтік желілерде, мессенджерлерде, ойын платформалары мен ұялы телефондарда орын ала алады. Бұл – қудалау нысанына айналған адамды қорқыту, ашуландыру немесе масқаралауды көздейтін мақсатты мінез-құлық үлгісі.

Қудалау (буллинг) – қорлау, қудалау және (немесе) қорқыту сипатындағы жүйелі әрекеттер, соның ішінде жария түрде немесе бұқаралық ақпарат құралдарын және (немесе) телекоммуникация желілерін, және (немесе) онлайн платформаларды (кибербуллинг) пайдалана отырып, қандай да бір әрекетті жасауға итермелейтін не оны жасаудан бас тартуға мәжбүрлейтін әрекеттер.

Кибербуллингке келесілер жатады:

– әлеуметтік желілерде біреу туралы жалған ақпарат тарату немесе біреудің келіссіз фотосуреттерін орналастыру;

– хабар алмасу платформалары арқылы тіл тигізетін хабарламалар немесе бопса жіберу;

– өзін басқа адам ретінде таныстырып, оның атынан келіссіз хабарламалар жіберу.

Шынайы өмірде қудалау және кибербуллинг көбінесе бір уақытта қатар орын ала алады. Бірақ интернеттегі қудалау цифрлық із қалдырады – бұл пайдалы болуы мүмкін және қорқытуды тоқтату үшін қажет дәлел бола алады. Буллинг пен кибербуллинг баланы өз-өзіне қол жұмсауға дейін жеткізеді. Қазіргі таңда еліміздегі жасөспірімдердің 12 пайыздайы осы кибербуллингтен зардап шегеді екен. Осы мәселе турасында Мемлекет басшысы Қасым-Жомарт Тоқаев былтырғы «Жаңа жағдайдағы Қазақстан: іс-қимыл кезеңі» атты Қазақстан халқына Жолдауында «Балаларды кибербуллингтен қорғау жөніндегі заңнамалық шараларды қабылдайтын кез-келді. Балалар құқын қорғау жөніндегі басқа да шараларды күшейту керек», деген болатын. Бүгінде жат ағымның жетегінде кеткен жастардың басым көпшілігін де осы кибершабуылдың құрбаны деп қарауға болады.

Қазақстан Республикасының кейбір заңнамалық актілеріне баланың құқықтарын қорғау, білім беру, ақпарат және ақпараттандыру мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» 2022 жылғы 3 мамырдағы Заңмен «Қазақстан Республикасындағы баланың құқықтары туралы» және «Білім туралы» Заңдарға «жәбірлеу (буллинг), кибербуллинг» ұғымдары енгізілді. 15 сәуір күні президент әйелдер құқығын қорғау туралы және балалар қауіпсіздігі туралы екі заңға қол қойды. Заңнамаға енгізілген өзгертулер 16 маусымда күшіне енді. Осы өзгертулердің нәтижесінде Әкімшілік құқық бұзушылық туралы кодекске (бұдан әрі-ӘҚБтК) 127-2-бап «Кәмелетке толмаған баланы қорлау (буллинг, кибербуллинг)» пайда болды. Бұрын Елімізде мұндай құқық бұзушылықтар үшін жауапкершілік қарастырылмаған.

Буллинг (bullying) – ағылшын тілінен аударғанда, қорлау, қудалау, мазалау дегенді білдіреді. Буллинг жасаушы мұны күшпен де, сөзбен кемсіту арқылы да жасайды әрі бұл әрекетін жиі қайталауы мүмкін. Қоғамда «буллинг мектеп оқушылары арасында ғана болады» деген түсінік қалыптасқан. Шындығында, кез келген жастағы адам үйде, көшеде, жұмыста, оқу орнында, барлық жерде буллингпен ұшырасуы мүмкін. Ал құрбанға топ болып әлімжеттік жасауды моббинг дейді. Кибербуллинг – интернет, әлеуметтік желі, түрлі сайт арқылы қоқан-лоқы көрсету. Жәбірлеуші телефонмен хабарласып немесе әлеуметтік желіде жазып, адамды қорқыта алады. Кибербуллинг жасаушы ауызша немесе белгілі бір фото, видео жариялап, қорлауы мүмкін. Осы күні ғаламторда баланың өз-өзіне, жақындарына, туыстарына қол жұмсауына итермелейтін ойындар да аз емес. Бұдан бірнеше жыл бұрын кибербуллингтердің «жемісі» саналатын «Көк кит», «Тыныш үй», «Мені сағат 04:20-да оят», «Қызыл жапалақ», «Киттер мұхиты», «Құс жолы», «NaN», «F57» сынды ойындар дүние жүзін дүрліктіргені белгілі. Енді осындай қауіпті ойындардың қазақ тілінде де пайда бола бастағаны жұртшылықты алаңдатуда. Кибербуллинг өз құрбанына тәулігіне 24 сағат бойы тыным бермейді, жасөспірімнің өзінің қорғаусыз қалғанын сезінтіп, ауыр психологиялық күйге ұшыратады. Жасөспірім өзін кім аңдып жүргенін білмейді және қауіпті ұлғайтып көрсетуге бейім келеді. Аңдушылардың аты-жөнінің жасырын болуы қорқыныш, үрейін күшейте түседі. Кибербуллинг кім-кімге де қатты әсер етеді. Тек жасөспірім ғана емес, ересектер де оның құрбанына айналуы мүмкін. Қазір Қазақстанда жасөспірімдерді интернет шабуылынан қорғайтын мемлекеттік деңгейдегі бағдарлама мен сайттар жоқ десе де болады. Тек safekaznet.kz қызметі арқылы шағымдануға болады. Ондағы мамандар посттың заңсыздығын тексеріп, қажет жағдайда парақшаны бұғаттайды.

Егер де сен интернет технологияларды біреуді әдейі ренжіту, қорлау немесе ызасын келтіру үшін пайдалансаң, онда бұл – кибербуллинг. Тіпті, сен біреу туралы ренішті постқа лайк бассаң да, немесе ренішті постты жіберсең, бұл да – кибербуллинг. Буллинге ұшыраған адам үмітсіздік пен шарасыздық күйге түседі. Кей кездері буллингтің кесірінен адамдар өзін-өзі өлтіру жайында ойлап, өзіне қол жұмсауы мүмкін. Сондықтан буллинг қашанда жақсы емес, бірақ әр уақытта көмек сұрауға болады. Кибербуллинг сөзінің мағынасына тереңнен үңілу үшін жақында қайтыс болған жазушы Аягүл Мантайдың өлімі туралы айтуымызға тура

келеді. Мәжіліс депутаты, саясаттанушы Ерлан Саиров суицид салдарынан қайтыс болған жазушы Аягүл Мантайдың өлімінен кейін әлеуметтік желіде өзін-өзі ұстаудың этикасы болуы керектігін айтып, «Әлеуметтік желі кодексін» қабылдау мәселесін көтерді. Депутат желінің жоғары деңгейдегі мәдениетін қалыптастырудың маңызын, оның басты аспектісі адамның жеке басына қол сұқпау, адамның ар-ожданын ардақтау екенін атап өтті. Әлеуметтік желіде жазушының өзіне қол жұмсауына әлдекімдердің жеке басына айтқан сөзі себеп болуы мүмкін деген ақпарат тарап жатыр.

Қазақстанда нақты кибербуллинг проблемасына қатысты заңнаманы жетілдіру мәселесі күн тәртібінде тұр. Бұған дейін Мемлекет басшысы жолдауларының бірінде кибербуллингті заңдық негізде енгізу, әсіресе балаларды қорғауға қатысты шаралар қабылдау керек екенін айтқан еді. Оның сөзінше, бүкіл әлемдегі сияқты Қазақстанның азаматтары да интернеттегі ғайбаттаулардан қорғана алмай отыр.

Буллинг – әлем бойынша көптеген мектеп оқушыларының күнделікті өмірінде кездесетін үлкен әлеуметтік мәселе. Буллингке ұшыраған оқушылар көбінесе психологиялық және физикалық тұрғыдан қиындықтарға тап болып, өмірге деген қызығушылықтарын жоғалтып жатады. Бұл құбылыс барлық елде бар болғанымен әр мемлекет буллингпен күресу үшін түрлі тәсілдерді қолданады. Буллинг терминінің шығу тарихына тоқтала отырып, шетелдік тәжірибелерді қарастырып көрейік.

Дамыған елдердің көпшілігінде кибербуллингке қарсы шаралар заңмен бекітілген. Оңтүстік Корея 2007 жылы онлайн қорқытуға қарсы арнаулы заңды қабылдады. Жаңа Зеландияда интернетте басқа адамға зиян келтіретін хабарламаларды жариялаған (қорлау, қорқыту, т.б.) авторды екі жылға бас бостандығынан айырып, 40 мың доллардай айыппұл салуы мүмкін. Ал сайт немесе платформаның иесі 160 мың долларға дейін айыппұл төлеуі мүмкін. Германияда да кибербуллинг мәселесі заңмен қарастырылған. Кейбір елдер кибербуллингпен мектептен бастап күресу керек екенін айтып, алдын алу шараларын білім

ұйымдарынан бастап жатыр. Ұлыбританияда мектеп оқушыларын одан қорғау үшін білім туралы заңға өзгерістер енгізілген. Мәселен, мұғалімдер кибербуллингтің барлық түрлерінің алдын алу үшін арнайы дайындықтан өтеді. Францияда мұғалімдер оқушылардың блогтарын бақылап, зардап шеккендерге көмек көрсетеді, ал агрессия көрсеткендер мектептен шығарылады. Канадада мектеп оқушыларына кибербуллингтің алдын алу тәсілдерін үйрету мақсатында 130 зерттеуші-ғалым мен 62 ұлттық жастар ұйымынан Қарым-қатынастарды жақсарту және зорлық-зомбылықты жою желісі (Promoting Relationships and Eliminating Violence Network) арнайы әдістеме әзірлеп жатыр. Америка Құрама Штаттарында кибер-қорқыту туралы федералды заң жоқ, бірақ кейбір штаттарда кибербуллинг пен буллингке қатысты заң бар. Мәселен, Джорджияда 1999 жылдан бері гаджеттерді қорқыту мақсатында пайдалану заңсыз. Кейіннен Невада штатында мектеп оқушыларын ауызша немесе жазбаша қорқыту үшін қылмыстық жаза қарастырылған. Бұдан бөлек The Fight Crime: Invest In Kids коммерциялық емес ұйымы балалар арасындағы кибербуллингпен күресуге көмек қолын созады. Оның құрамында бес мыңға жуық полиция қызметкері, шериф пен заңгерлер жұмыс істейді. Олар қылмыстың алдын алу стратегияларын зерттейді. Сонымен қоса мұғалімдерге, балалар мен ата-аналарға көмектесу үшін stopbullying.gov платформасы іске қосылған. Сайт мектептердегі, жалпы күнделікті өмірде балаға буллинг пен кибербуллингтің алдын алуға көмек беру мақсатында құрылған. Сонымен қатар сайтта баланың кибербуллингке ұшырағанын қалай түсінуге болады, кім кінәлі және оған не істеу керегіне қатысты бірқатар кеңес берілген. Ерекше ауыр жағдайларда авторлар полицияға хабарласуды ұсынады. Аустралияда жала жабатын ақпаратты желіде тарату мәселесі референдумға шығарылды. Заңнамалық реформаға дайындық барысында азаматтардан бірқатар мәселе бойынша, мысалы, әлеуметтік желілерді қолданушылардың жазбалары үшін жауапкершілікке тарту, өтемақы төлету, жоққа шығару секілді дүниелерге пікір білдіру ұсынылды.

Әр ел буллингке қарсы түрлі стратегияларды қолданады. Кейбір мемлекеттер бұл мәселені заңнамалық тұрғыдан шешсе, енді біреулері психологиялық және әлеуметтік бағдарламаларды дамыту арқылы күреседі.

Әдебиет

1. Интернет ресурс: https://kaz.inform.kz/news/kiberbullingpen-kures-balalardy-korgau-otandyk-zhane-alemdik-tazhiribe_a3904689/ кіру уақыты 22.10.2024 .

2. Gov.kz сайты // Интернет ресурс: https://www.gov.kz/situations/316/intro?lang=kk кіру уақыты 24.10.2024.

3. Welcome to the United Nations // Интернет ресурс: https://www.un.org/ru/ кіру уақыты 25.10.2024.

4. Новости Zakon.kz // https://www.zakon.kz кіру уақыты 27.10.2024.

ЖАНДЫҒУЛОВА
Шолпан Ерланқызы
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
жоғары оқу орнынан кейінгі білім беру факультеті ғылыми-педагогикалық
магистратурасының 1 курс магистранты полиция лейтенанты

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ НЕМЕСЕ ТЕЛЕКОММУНИКАЦИЯ ЖЕЛІЛЕРІНІҢ ҚҰРАМЫ ЖӘНЕ ҚҰРЫЛЫМЫ

«Телекоммуникация» термині грек тілінен шыққан теле – алыс, алыс және латын communico-мен ортақ, байланыстырамын. Оны қашықтықтағы байланыс ретінде түсіндіруге болады. Сондықтан, телекоммуникациялық желі деп біз екі терминал құрылғысы (абоненттер) арасында ақпарат беруді қамтамасыз ететін құралдар жиынтығын түсінеміз. Желінің құрамына мыналар кіреді:

– соңғы құрылғыларды (дербес компьютерлер, серверлер, аудио және бейне құрылғылар, желілік принтерлер, факс аппараттары, штрих-кодты оқу құралдары және т. б.) және байланыс жабдықтарын (сымды, кабельді және (немесе) сымсыз деректер ортасын, сондай-ақ желілік адаптерлер сияқты аралық құрылғыларды қамтитын желілік жабдық, модемдер, қайталағыштар, көпірлер, қосқыштар және т.б.);

– желілік жабдықты қолдау құралдары. Телекоммуникациялық желі сияқты күрделі жүйеде бағдарламалық жасақтаманың кең арсеналы, сондай-ақ желілік құрылғылардың өзара әрекеттесу ережелерін анықтайтын байланыс хаттамаларының стандартты жиынтығы болуы керек.

Телекоммуникация желісі иерархиялық құрылымға ие (сурет. 9.1) әртүрлі ғимараттарда, елді мекендерде және өңірлерде орналасқан оның жекелеген тораптары арасындағы трафиктің қарқындылығын көрсететін. Желі тораптары – байланыс желілері қосылған көп портты құрылғылар болып табылатын қосқыштар. Телекоммуникация желісінің жеке компоненттерін қарастырыңыз.

Терминал құрылғылары пайдаланушылар телекоммуникация желісінің шетінде орналасқан және оның иерархиясының ең төменгі деңгейін құрайды. Әдетте мұндай құрылғылардың түрі желінің атауын анықтайды. Компьютерлік желідегі негізгі терминалдық құрылғылар – компьютерлер, телефонда – телефон аппараттары, теледидарда – теледидар қабылдағыштары, хабар тарату желісінде – радиоқабылдағыштар.

Пайдаланушылардан абоненттік арналар туралы ақпарат, көбінесе абоненттік аяқталулар деп аталады, кіру желісінің қосқыштарына түседі.

Кіру желісі телекоммуникациялық желі иерархиясының келесі деңгейін білдіреді. Мұндай үлкен желі бірнеше деңгейден тұруы мүмкін. Қол жеткізу желісінің негізгі функциялары:

– көптеген пайдаланушы құрылғыларынан келетін ақпараттық ағындарды бір жалпы ағынға біріктіру немесе мультиплекстеу және біріктірілген ағынды Магистральдық желі қосқышына беру;

– жиынтық ағынды жеке ағындарға қабылдау және бөлу немесе демультиплекстеу кезінде пайдаланушының аппараттық құралының кіріс портына тек оған бағытталған ақпарат түсетіндей етіп.

Магистральдық желі жіберушілердің қол жеткізу желісінен алушылардың қол жеткізу желісіне біріктірілген ақпараттық ағындарды транзиттеуге арналған. Онда коммутаторлар мен жоғары жылдамдықты байланыс желілері (магистральдар) бар [1].

Ақпараттық орталық немесе сервистерді басқару орталығы желіні пайдаланушыларға (абоненттерге) ақпараттық қызметтер көрсетуге арналған. Барлығы Интернеттің ақпараттық қызметтерін, сондай-ақ телефон желілерін (анықтамалық ақпарат алу, жедел жәрдем мен милицияны шақыру) және ұялы байланыс желілерін (телевизиялық дауыс беру) біледі.

Әрбір Телекоммуникациялық желінің өзіндік ерекшеліктері бар екенін ескеріңіз, мысалы: шағын телефон және компьютерлік желілерде ақпараттық орталықтар жоқ; жергілікті компьютерлік желінің қол жеткізу желісі мен магистралі кабель сегменттерімен ұсынылуы мүмкін; хабар тарату және телевизиялық желілердің қол жеткізу желісі тек тарату функцияларын орындайды, өйткені олардағы ақпарат бір бағытта (абоненттерге қарай) беріледі.

Телекоммуникация теориясы мен техникасының негізі әр түрлі хабарламаларды (ақпаратты) қашықтыққа беру болып табылады. Ақпарат дегеніміз кез-келген заттар, оқиғалар, біреудің іс-әрекетінің процестері және т.б. туралы ақпарат жиынтығы. Бұл сөйлеу немесе музыка, қолжазба немесе баспа мәтіні, сызбалар, теледидар бейнесі болуы мүмкін.

Байланыс арналары арқылы беру үшін әр хабарлама электр сигналына айналады. Сигнал-жіберілген хабарламаны көрсететін физикалық процесс (хабарламаның физикалық тасымалдаушысы). Хабарламалардың көрсетілуін қамтамасыз ететін өзгерістің физикалық шамасы ақпараттық немесе сигналды білдіретін параметр деп аталады.

Хабарламаларды кеңістіктің бір нүктесінен екінші нүктесіне тасымалдауды телекоммуникация жүйесі жүзеге асырады. Электрбайланыс жүйесі (телекоммуникациялық жүйе) – хабарламалардың көзден алушыға қашықтыққа берілуін қамтамасыз ететін техникалық құралдар кешені.

Жалпы телекоммуникация жүйесі екі мәселені шешеді:

1) хабарламаларды жеткізу-электр байланысы жүйесінің функциялары;

2) хабарламаларды қалыптастыру және тану – соңғы жабдықтың функциялары.

Тарату жолы – айдаланушылар арасында хабарламалардың берілуін қамтамасыз ететін құрылғылар мен желілер жиынтығы.

Беру (байланыс) арнасы-кез келген екі нүкте арасындағы беру жолының бөлігі. Тарату арнасына соңғы құрылғылар кірмейді.

Хабарламаларды беру трактінің кірісі мен шығысында хабарламаларды электр сигналдарына түрлендіруді және кері түрлендіруді қамтамасыз ететін соңғы құрылғылар қосылады. Бұл құрылғылар Бастапқы түрлендіргіштер деп аталады және олар жасаған сигналдар бастапқы деп те аталады.

Мысалы, сөйлеуді беру кезінде негізгі түрлендіргіш – микрофон, суретті беру кезінде-катодты сәулелік түтік, жеделхатты беру кезінде – телеграф аппаратының таратушы бөлігі.

Хабарлама көзі S(T) электр сигналына айналатын A(t) хабарламасын құрайды. Телекоммуникация жүйесінде сигналдардың қайталама түрленуі жүреді және олар түпнұсқадан басқа формада тасымалданады.

Электр байланысы желісі (телекоммуникациялық желі) – хабарламалардың берілуін және таралуын қамтамасыз ететін белгілі бір аумақтағы коммутациялық станциялардың, шеткі құрылғылардың байланыс елілерінің (арналарының) жиынтығы [2].

Байланыс желісінің кірісі мен шығысында хабарламаларды электр сигналдарына түрлендіруді және кері түрлендіруді қамтамасыз ететін соңғы құрылғылар қосылады. Соңғы құрылғылар коммутациялық станцияға абоненттік желілермен қосылады. Коммутациялық

станциялар бір-бірімен байланыс желілерімен байланысты. Коммутациялық станциялар кіріс желілерін тиісті мекен-жай бойынша шығыс желілерімен байланыстырады.

Жалпы алғанда, көзден алушыға берілетін хабарлама екі бөліктен тұрады: мекенжай және ақпарат. Мекенжай бөлігінің мазмұны бойынша коммутациялық станция байланыс бағытын анықтайды және хабарламаның нақты алушысын таңдайды. Ақпараттық бөлімде хабарламаның өзі бар.

Хабарламалардың берілуін қамтамасыз ететін процедуралар мен процестердің жиынтығы байланыс сеансы деп аталады, ал байланыс сеансы ұйымдастырылатын ережелер жиынтығы хаттама деп аталады.

Ұзақ уақыт бойы әртүрлі телекоммуникациялар бір-біріне тәуелсіз дамыды. Телекоммуникацияның әр түрі өз арналарын, тарату жүйелерін және желілерін құруға бағытталған. Желі құрылымы белгілі бір сипаттағы хабарламалар ағындарының таралу ерекшеліктеріне сәйкес таңдалды телекоммуникация түрлері.

Кейбір өнеркәсіп және көлік салалары саланың хабарлама жіберу қажеттіліктерін қанағаттандыруға арналған өз желілерін құра бастады. Техникалық құралдардың бөлінуі ел ауқымындағы желілер жиынтығының тиімділігін арттыруға мүмкіндік беріп қана қоймай, сонымен қатар оқшауланған желілердің дамуына кедергі келтірді. Сондықтан, 1960 жылдардың басында. желілерді дамытудың перспективалық бағыты желілерді біріктіру болуы керек екендігі белгілі болды. БАБЖ (бірыңғай автоматтандырылған байланыс желісі) құру туралы шешім қабылданды. БАБЖ әр түрлі және көптеген шағын желілерді Электр байланысының әр түрінің мемлекеттік желілеріне, содан кейін белгілі бір техникалық құралдарды, ең алдымен тарату жүйелері мен коммутация жүйелерін бөлісу мақсатында бірыңғай желіге біріктіруге негізделген.

БАБЖ құру кезінде белгілі бір техникалық құралдар хабарламалардың түріне қарамастан беру процесіне қатысады, яғни.жалпы болып табылады. Осыған байланысты елдің бүкіл желісі өзара байланысты екі компонентке бөліне бастады:

1) бастапқы желі – тарату арналары мен топтық трактілер желісін ұйымдастыруға мүмкіндік беретін желілік станциялардың, желілік тораптардың (қосымшада анықтама беру) және оларды қосатын беру желілерінің жиынтығы.

Бастапқы желінің құрылымы ел аумағының әкімшілік бөлінуін ескереді. Қазақстанның бүкіл аумағы, әдетте, облыстардың, аймақтардың аумақтарымен сәйкес келетін аймақтарға бөлінген. Осыған сәйкес бастапқы желі де келесі бөліктерден тұрады:

– жергілікті бастапқы желілер-қаланың немесе ауылдық ауданның аумағымен шектелген желінің бөлігі;

– зоналық бастапқы желілер – Бір аймақ ішіндегі әртүрлі жергілікті желілердің арналарын өзара байланыстыруды қамтамасыз ететін, зона аумағын (облыс, өлке, республика) қамтитын желінің бөлігі;

магистральдық бастапқы желі – бұл бүкіл елдегі әртүрлі аймақтық желілердің арналарын өзара байланыстыратын желінің бөлігі.

2) қайталама желі – белгілі бір түрдегі хабарламалардың берілуін қамтамасыз ететін техникалық құралдардың жиынтығы, оның құрамына: соңғы құрылғылар, Абоненттік және жалғау желілері, коммутациялық станциялар, сондай-ақ қайталама желіні қалыптастыру үшін бастапқы желіден бөлінген арналар кіреді. Екінші желілер келесі түрлерге бөлінеді:

– телефон;

– телеграф;

– деректерді беру;

– факс;

– телевизиялық хабар тарату;

– дыбыстық хабар тарату [3].

XX ғасырдың аяғында техникалық прогрестің даму барысы, сондай-ақ Қазақстанның саяси және экономикалық құрылымындағы тарихи өзгерістер байланыс желісін құрудың жаңа тұжырымдамасын-ҚР ӘҚҚ (ҚР өзара байланысты байланыс желісі) қалыптастыруды алдын ала айқындады.

Қазақстан Республикасының өзара байланысты байланыс желісі (ҚР ӨББЖ) – Қазақстан аумағында абоненттердің басым көпшілігіне электр байланысы қызметтерін ұсынуды қамтамасыз етеді. ҚР ӨББЖ – Жалпы орталықтандырылған басқармамен қамтамасыз етілген, ведомстволық тиесілілігіне және меншік нысанына қарамастан, Қазақстан аумағындағы жалпы пайдаланымдағы Электр байланысының технологиялық ұштасқан желілерінің, ведомстволық және басқа да Электр байланысының желілерінің жиынтығы.

Тұжырымдаманы қалыптастыру кезінде ҚР ҚК Wcn (Worldwidecommunicationnetwork) Дүниежүзілік байланыс желісінің құрамдас бөлігі болып табылатыны, сондай-ақ қазіргі заманғы телекоммуникациялық технологияларды пайдалана отырып, ұлттық желілерді құрудың жалпы әлемдік тәжірибесі ескерілді, елдің цифрлық байланыс желісі өзара байланысты екі құрамдас бөлікке бөліне бастады:

1) көлік желісі – магистральдық тораптарды, қалааралық станцияларды, сондай-ақ оларды жалғайтын арналар мен тораптарды (қалааралық, халықаралық) қамтитын байланыс желісінің бөлігі;

2) кіру желісі – абоненттік терминалдардың көлік желісіне қолжетімділігін, сондай-ақ көлік желісіне шықпай-ақ жергілікті байланысты қамтамасыз ететін абоненттік желілер мен жергілікті желі станцияларының (СМС) жиынтығы.

2004 жылғы 5 шілдеде байланыс туралы Қазақстан Республикасының жаңа Заңы қабылданды, оған сәйкес Қазақстанда телекоммуникацияларды дамытудың жаңа кезеңі басталды. Ресейлік телекоммуникациялардың дамуындағы жаңа кезең – бұл ақпараттандыру мен телекоммуникацияның конвергентті бірлестігі негізінде қазақстандық қоғамды электрондық-ақпараттық қоғамға айналдыру кезеңі [4].

Қазақстандық телекоммуникациялардың желілік негізі ретінде Электр байланысының бірыңғай желісі анықталды. Республикалық байланыстың құрамдас бөлігі болып табылады және Қазақстан аумағында орналасқан барлық электр байланыс желілерін біріктіреді. Электр байланысының бірыңғай желісі халықтың, мемлекеттік билік және басқару органдарының, қорғаныстың, қауіпсіздіктің, сондай-ақ шаруашылық жүргізуші субъектілердің қажеттіліктерін қанағаттандыруға арналған.

ҚР БЭЖ келесі санаттағы желілерден тұрады:

1. Жалпы пайдалану желісі – телевизиялық және радио хабарларын тарату бағдарламаларын таратуға арналған байланыс желілерін қоса алғанда, өзара іс-қимыл жасайтын байланыс желілерінің кешені болып табылатын Қазақстан Республикасының аумағындағы кез-келген пайдаланушыға электр байланысы қызметтерін ұсынуға арналған. Жалпы пайдалану желісі шет мемлекеттердің ортақ пайдалану желілеріне қосылуы бар:

– телефон;

– телеграф;

– деректерді беру желілері;

– дыбыстық хабар тарату желілері;

– телевизиялық хабар тарату желілері.

2. Шектеулі пайдалану желісі – контингенті корпоративтік клиенттермен шектелген желі. СОгП үш түрге бөлінеді:

– байланыстың технологиялық желілері ұйымдардың өндірістік қызметін қамтамасыз етуге және технологиялық процестерді басқаруға арналған (бос ресурстар болған кезде жалпы пайдаланылатын желілер санатына ауыстыра отырып, жалпы пайдалану желісіН қосылуы және пайдаланушыларға ақылы қызметтер көрсету үшін пайдаланылуы мүмкін);

– бөлінген байланыс желілері пайдаланушылардың шектеулі санына қызмет көрсетуге арналған (мұндай желілер өзара әрекеттесе алады, егер ол оның талаптарына сәйкес келсе, ортақ пайдаланылатын желі санатына ауыстыра отырып, жалпы пайдалану желісі қосылуы мүмкін);

– арнайы мақсаттағы байланыс желілері мемлекеттік басқаруды, қорғаныстық, қауіпсіздікті және құқықтық тәртіпті қорғауды қамтамасыз етуге арналған).

Желілерді басқаруды ретке келтіру, олардың жай-күйін мониторингілеу және олардың өзара іс-қимылын қамтамасыз ету мақсатында электр байланысы жүйесіндегі әрбір желінің ор-

нын анықтауға, жүйелік тәсіл негізінде желілердің қасиеттерін әртүрлі көзқарастардан анықтауға мүмкіндік беретін әртүрлі маңызды белгілер бойынша желілерді жіктеу қажет. 1.1-кестеде ҚР БЭЖ желілерінің жіктелуі (Б қосымшасы) келтірілген.

Жеке хабарламаларды беру желілеріне қойылатын негізгі талаптардың бірі (телефон, телеграф, факсимиль, деректерді беру) – бұл желі әр пайдаланушыға басқа пайдаланушымен байланысу мүмкіндігін қамтамасыз етуі керек. Осы талапты орындау үшін байланыс желісі жұмыс істеу жағдайларына байланысты белгілі бір принцип бойынша құрылады. Сондықтан байланыс желілері әр түрлі құрылымға ие болуы мүмкін, яғни түйіндер мен терминалдардың (станциялардың) саны мен орналасуымен, сондай-ақ олардың өзара байланысының сипатымен ерекшеленеді [5].

Құрылыстың толық байланысқан әдісімен («әрқайсысы әрқайсысымен» принципі) түйіндер арасында тікелей байланыс бар. Желідегі түйіндердің аз саны үшін қолданылады.

Желіні құрудың радиалды әдісімен түйіндер арасындағы байланыс орталық түйін арқылы жүзеге асырылады. Ол салыстырмалы түрде шағын аумақта желі құру кезінде қолданылады.

Үлкен аумақта байланыс желісі радиалды-тораптық әдіспен салынуда.

Желіні құрудың сақиналық әдісі сағат тілімен де, сағат тіліне қарсы бағытта да байланыс орнатуға мүмкіндік береді. Бұл жағдайда белгілі бір учаскеде бүлінген кезде желі өзінің жұмысын сақтайды.

Желіні құрудың біріктірілген әдісімен жоғарғы иерархиялық деңгейдегі түйіндер толық байланысқан схема бойынша байланысады . Бұл жағдайда түйіндердің біреуінің шығуы бүкіл желіні бұзбайды.

Телекоммуникациялық желілерде ақпарат алмасу белгілі, алдын ала келісілген ережелер (стандарттар) бойынша жүзеге асырылады. Бұл ережелерді бірқатар халықаралық ұйымдар әзірлейді.

Қазіргі заманғы телекоммуникациялық желілердегі өзара іс-қимыл 1980 жылы Халықаралық стандарттау ұйымы (ISO-international Organisation for Standartisation) есептеу желілері үшін ұсынған ашық жүйелердің өзара іс-қимылының эталондық моделіне сәйкес ұйымдастырылады.

Ашық өзара әрекеттесу хаттамаларын қолданатын жүйелер деп аталады. Хаттама-тәуелсіз құрылғылар немесе процестер арасында хабар алмасу үшін өзара әрекеттесуді реттейтін ережелер жиынтығы.

Ашық өзара әрекеттесу хаттамаларын қолданатын жүйелер деп аталады. Хаттама-тәуелсіз құрылғылар немесе процестер арасында хабар алмасу үшін өзара әрекеттесуді реттейтін ережелер жиынтығы.

Жалпы байланыс мәселесі екі бөліктен тұрады:

1) бірінші бөлім байланыс желісіне қатысты-желі арқылы берілетін деректер мақсаты бойынша дұрыс түрде және уақтылы түсуі тиіс;

2) екінші бөлім – одан әрі пайдалану үшін деректерді тануды қамтамасыз ету-пайдаланушының соңғы жабдықтарының функциялары. Пайдаланушылардың өзара әрекеттесуін ұйымдастыру үшін шешілетін барлық міндеттер жеті топқа бөлінеді – анықтамалық модель деңгейлері.

Төменгі үш деңгей желі қызметтерін білдіреді. Осы деңгейлерді жүзеге асыратын хаттамалар желінің әр түйінінде қарастырылуы керек. Жоғарғы төрт деңгей соңғы пайдаланушыларға қызметтерді ұсынады және желіге емес, олармен байланысты. Төменгі деңгейлер деректерді бір пайдаланушыдан екіншісіне бағыттау үшін қолданылады. Жоғарғы деңгейлер пайдаланушыға деректерді тани алатын формада ұсыну мәселелерін шешеді. Жеті деңгейді таңдау келесі ойларға байланысты:

1) хаттаманы әзірлеу тұрғысынан олардың әрқайсысы тым күрделі болмауы үшін жеткілікті деңгейлерге ие болу керек;

2) олардың интеграциясы мен сипаттамалары тым күрделі болып кетпеуі үшін тым көп деңгейлердің болмауы ұсынылады;

3) байланысты функцияларды бір деңгейде жинау үшін табиғи шекараларды таңдаған жөн.

Анықтамалық модельде N деңгей модулі тек іргелес (n-1) және (N+1) деңгейлік модульдермен әрекеттеседі.

Модель деңгейлері келесі функцияларды орындайды:

1) **физикалық деңгей** арнаның өткізу қабілеттілігіне сәйкес жылдамдықпен белгілі бір физикалық сипаттағы сигналдар түрінде биттер тізбегін беруді қамтамасыз етеді.

2) **арна деңгейі деректер блоктарын** – кадрларды қалыптастырады, таратушы ортаға қол жеткізуді басқаруды жүзеге асырады, қателерді анықтайды және түзетеді.

3) **желілік деңгей маршруттау** функциясын жүзеге асырады. Желілік деңгейдегі деректер блоктары пакеттер деп аталады.

Физикалық, арналық және желілік деңгейлер желіге тәуелді, сондықтан олардың жұмысы байланыс желісінің түріне байланысты өзгереді.

4) **Көлік деңгейі деңгейлер** иерархиясында орталық орын алады, қосылатын соңғы құрылғылардағы процестердің өзара әрекеттесуін және осы процестер арасындағы пакеттік қозғалысты басқаруды қамтамасыз етеді. Бұл деңгейдің болуы пайдаланушыларды барлық коммутация, маршруттау және деректерді таңдау (таңдау) функцияларын зерттеу қажеттілігінен босатады [6].

Төменгі төрт деңгей (физикалық, арналық, желілік, Көлік) көлік желісін құрайды.

5) **Сеанс деңгейі** деректерді беруді ұйымдастыру және өзара әрекеттесу процедураларын синхрондау функцияларын орындау арқылы процестер арасындағы диалогты қамтамасыз етеді**.**

6) **Ұсыну деңгейі** деректерді түсіндіруді қамтамасыз етеді. Бұл деңгейде синтаксис жүзеге асырылады (символдардың көрінісі, бет пішімі, кодтау және т.б. талданады).

7) **Қолданбалы деңгей** алдыңғы деңгейлерге жатқызуға болмайтын функцияларды жүзеге асырады. Қолданбалы деңгей хаттамалары алмасатын ақпараттың тиісті мағынасын (семантикасын) береді. Қолданбалы деңгей барлық ақпараттық-есептеу процестерінің орындалуын қамтамасыз етеді [7].

Өзара әрекеттесуді көп деңгейлі ұйымдастыру деңгей функцияларына сәйкес әр деңгейдегі ақпаратты өзгерту қажеттілігін тудырады.

Әрбір деңгейде берілген кезде деректер блогы жоғары деңгейден қабылданады, деректерге басқару ақпараты қосылады және блок төменгі деңгейге беріледі. Қабылдау соңында әр деңгей тек тиісті тақырыпты қолданады, қабылданған деректер блогының қалған бөлігін қарап шықпайды. Демек, деңгейлер тәуелсіз және бір-бірінен оқшауланған. Бұл модельдің қалған бөлігіне әсер етпестен жеке деңгейдегі протоколдар мен бағдарламаларды жоюға және ауыстыруға мүмкіндік береді.

Көп деңгейлі ұйым деңгейдегі басқарудың төменгі және жоғарғы деңгейлердің жұмыс істеу тәртібінен тәуелсіздігін қамтамасыз етеді:

– ақпараттық арнаны басқару физикалық арнаның жұмыс істеуінің физикалық принциптеріне қарамастан жүреді;

– желіні басқару ақпараттық арнаның сенімділігін қамтамасыз ету әдістеріне байланысты емес;

– көлік деңгейі пайдаланушыларға хабарламаларды жеткізуді қамтамасыз ететін бірыңғай жүйе ретінде желімен өзара әрекеттеседі;

– қолданбалы процесс желі құрылымын, маршрутты таңдау тәсілдерін, байланыс арналарының түрін және т.б. ескерусіз деректерді өңдеудің белгілі бір функцияларын орындау үшін ғана жасалады [8].

Өзара әрекеттесуді ұйымдастыруға арналған пайдаланушылар өзара әрекеттесу қызметіне сүйенеді. Пайдаланушылар арасындағы өзара әрекеттесу сессия барысында хабарламалардың берілуін қамтамасыз ететін көлік арнасы негізінде жұмыс істейтін сеансты басқару құралдарымен (5-деңгей) ұйымдастырылады. 4-деңгейде құрылған көлік арнасы пайдаланушылар арасында ақпараттық арналарды ұйымдастыратын байланыс желісін қамтиды.

Коммутация жүйесі ақпараттық ағындарды тарату міндетін орындайды.

Коммутацияның екі негізгі қағидасы белгілі:

1) тікелей қосылу (берілетін ақпаратты есте сақтамай коммутация);

2) ақпарат жинақтаумен қосылу (есте сақтаумен коммутация).

Тікелей қосылу (арналарды ауыстыру)

Арналарды коммутациялау кезінде кіріс желілері тиісті мекен-жай бойынша Шығыс сызықтармен физикалық түрде қосылады.

Арналарды ауыстыру әдісінің артықшылықтары:

– «диалогты» ұйымдастыру мүмкіндігі, өйткені хабарламаны берудегі кідіріс уақыты аз;

– абоненттердің байланыс орнатылғаннан кейін басқа абоненттерден түсетін жүктемеге қарамастан хабарламаларды беру мүмкіндігі бар. Кемшілігі. Қажетті бағытта бос арналар болмаған жағдайда, қоңырау шалушы пайдаланушы байланыс орнатудан бас тартады, сондықтан КК жүйелері сәтсіздіктер (қоңыраулардың жоғалуы) жүйелері деп аталады [7].

Жоғалған қоңыраулар коммутациялық жүйенің кінәсінен хабарлама жіберумен аяқталмаған қоңыраулар деп аталады.

Шығындар жоғалған қоңыраулар санына келіп түскендердің жалпы санына қатысты бағаланады және қызмет көрсетудің сапалы көрсеткіші болып табылады.

Әдебиет

1. Вендров А.М. Проектирование программного обеспечения экономических информационных систем: Учебник. – М.: Финансы и статистика, 2004.

2. Козырев А.А. Информационные технологии в экономике и управлении: Учебник. – СПб.: Изд-во Михайлова В.А., 2004.

3. Корнеев И.К., Машурцев В.А. Информационные технологии в управлении. – М.: ИНФРА-М, 2001.

4. Матвеев Л.А. Компьютерная поддержка решений: Учебник. - СПб.: «Специальная литература», 2005.

5. Экономическая информатика / Под ред. П.В. Конюховского и Д.Н. Колесова. – СПб.: Питер, 2005.

6. Долженко А. Лекция: Решения Hewlett-Packard по управлению информационными системами [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/itmngt/misys/3/3.html. 2. Мильман С. Понять ITIL – значит «правильно применять» [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2008/05/5205540/. 3. Office of Government Commerce «ITIL Version 3 – Service Operation». – С. 112-114, 154.

7. Использование математических методов и ЭВМ в экспертной практике. (Сборник научных трудов) – М., 1989.

АЛТЫНБЕКОВ
Олжас Бабахович
Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясының 2 курс магистранты полиция майоры

КОМПЬЮТЕРЛІК ҚЫЛМЫСҚА ҚАРСЫ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ІС-ҚИМЫЛДЫҢ ШЕТЕЛДІК ТӘЖІРИБЕСІ

Қазақстан Республикасындағы компьютерлік қылмысқа қарсы іс-қимылдың тиімді қылмыстық-құқықтық тетігін әзірлеу үшін, қылмыстық әрекеттің осы түрін жасағаны үшін жауапкершілікті реттейтін шет мемлекеттердің қылмыстық заңнамасын зерттеу бөлігінде компьютерлік қылмыстармен күресудің шетелдік тәжірибесін талдау қажет болып көрінеді.

Қылмыстық құқық доктринасында қылмыстық заңнама ұлттық қылмыстық-құқықтық жүйенің құрылымдық элементі болып табылады, ол өз кезегінде тиісті құқықтық жүйенің жұмыс істеуімен және дамуымен, оларды құрайтын құқық көздерінің мазмұнымен және мәнімен, қалыптасқан заң практикасымен, қоғамдық құқықтық санамен және құқықтық мәдениетпен, ұлттық менталитетпен және т. б. ажырамас байланыста болады [1, 65б.].

Сондықтан компьютерлік қылмыстар жасағаны үшін жауапкершілікті көздейтін шетелдік қылмыстық заңнаманы талдауды тиісті қылмыстық-құқықтық жүйеге жататын құқықтық жүйенің ерекшелігін ескере отырып жүргізу орынды деп санаймыз.

Қылмыстық-құқықтық жүйелер типологиясының мәселелеріне кірмей, біз компьютерлік қылмысқа қарсы қылмыстық-құқықтық тәжірибені зерттеуді англо-саксондық (ағылшын-американдық) құқықтық жүйесіне қатысты АҚШ, Ұлыбритания қылмыстық заңнамасынан бастауды қарастырамыз.

Америка Құрама Штаттары компьютерлік қылмыстар үшін қылмыстық жауапкершілікке тартылған әлемдегі алғашқы елдердің бірі және компьютерлік қылмыс басқа мемлекеттерге қарағанда ертерек пайда болған ел болды. АҚШ қылмыстық заңнамасының айрықша ерекшелігі оның екі деңгейлі құрылымы болып табылады, оған мыналар кіреді: федералды және жекелеген штаттардың заңнамасы.

Федералды деңгейде 1977 жылы АҚШ-та федералды компьютерлік жүйелерді қорғау туралы заң жобасы жасалды. Ол: компьютерлік жүйеге көрінеу жалған деректерді енгізу; компьютерлік құрылғыларды заңсыз пайдалану; ақпаратты өңдеу процестеріне өзгерістер енгізу немесе осы процестерді бұзу; компьютерлік технологиялардың мүмкіндіктерін пайдалана отырып немесе компьютерлік ақпаратты пайдалана отырып жасалған ақша қаражатын, бағалы қағаздарды, мүлікті, қызметтерді, құнды ақпаратты ұрлау үшін қылмыстық жауапкершілікті көздеді. Осы заң жобасының негізінде 1984 жылдың қазан айында компьютерлік ақпаратқа заңсыз қол жеткізгені үшін қылмыстық жауапкершілікті белгілейтін негізгі нормативтік құқықтық акт – компьютерлерді пайдалану арқылы алаяқтық және теріс пайдалану туралы заң қабылданды. Кейін ол бірнеше рет (1986, 1988, 1989, 1990, 1994, 1996

және 2000 жылдары) толықтырылды. Қазіргі уақытта бұл заңнамалық акт § 1030, АҚШ заңдар жиынтығының 18 титулына ендірілген.

Айта кету керек, бұл заң қылмыстық қол сұғудың заты болатын компьютерлік ақпаратқа қол сұққаны үшін қылмыстық жауаптылықты бекітеді. Оны келесідей түсіндіреді:

1) Үкіметтің немесе қаржы ұйымының айрықша пайдалануындағы компьютер не Үкіметтің немесе қаржы ұйымының мүддесінде жұмыс істеу кезінде компьютердің жұмыс істеуін бұзу;

2) элементтері АҚШ-тың бірнеше штатында орналасқан жүйенің немесе желінің бөлігі болып табылатын компьютердің жұмыс істеуін бұзу.

Сонымен қатар, заң қылмыстық жауапкершіліктің келесі жағдайларда болатынын белгілейді:

1) рұқсатсыз қол жеткізу – компьютерге немесе компьютерлік жүйеге қатысты бөгде адам оларға сырттан басып кіріп, оларды пайдаланған кезде;

2) рұқсат берілген қолжетімділіктен асып кету – компьютердің немесе жүйенің заңды пайдаланушысы өз өкілеттіктері қолданылмайтын компьютерлік деректерге қол жеткізуді жүзеге асырған кезде.

Компьютерлік қылмысқа қарсы іс-қимыл мәселелеріне және компьютерлік қылмыстарға қарсы күресте №47 тарауға кіретін АҚШ заңдар жиынтығының 18 титулына, §1030 және §1029 мұқият назар аударған жөн.

Атап айтқанда, § 1030 «а» тармағында осы түрдегі қылмыстардың жеті құрамы үшін жауапкершілік қарастырылған:

1. Ақпаратқа рұқсатсыз қол жеткізуден немесе рұқсат шегінен асып кететін компьютерлік тыңшылық, сондай-ақ мемлекеттік қауіпсіздікке, халықаралық қатынастарға және атом энергетикасы мәселелеріне қатысты ақпарат алу.

2. АҚШ үкіметінің ведомствосынан, мемлекетаралық немесе халықаралық саудаға қатысы бар қандай да бір қорғалған компьютерден ақпаратқа рұқсатсыз қол жеткізу немесе қол жеткізудің рұқсат шегінен асып кету, сондай-ақ қаржы институтының, карта эмитентінің қаржылық жазбаларынан немесе тұтынушыларды басқару файлындағы тұтынушылар туралы ақпараттан ақпарат алу.

3. АҚШ үкіметінің ерекше пайдалануындағы компьютерге әсер ету немесе АҚШ үкіметі толық немесе ішінара пайдаланатын компьютердің дұрыс жұмыс істеуін бұзу.

4. Компьютерді пайдаланып алаяқтықтық жасау – алаяқтық ниетпен жүзеге асырылатын қол жетімділік және компьютерді алаяқтық арқылы құнды нәрсе алу үшін пайдалану, соның ішінде бір жыл ішінде құны 5 мың доллардан асатын машина уақытын заңсыз пайдалану, яғни компьютерлік желілер мен серверлерді пайдалану үшін ақы төлемеу.

5. Қорғалған компьютерлерге қасақана немесе абайсызда зақым келтіру.

6 Егер мұндай сауда мемлекетаралық сауда қатынастарына рұқсат етілмеген қол жеткізуге мүмкіндік беретін компьютерлік парольдерді немесе ұқсас ақпаратты сату арқылы алаяқтық басқа мемлекеттермен немесе АҚШ үкіметі пайдаланатын компьютерге әсер ету;

7. Компьютерлік технологияларды пайдалана отырып жасалатын қатерлер, бопсалау және басқа да құқыққа қайшы әрекеттер [2].

§1030 (а) көзделген қылмыстық әрекеттер үшін санкциялар өте қатал. Атап айтқанда, барлық аталған тармақтар бойынша 10 жылға дейін бас бостандығынан айыру және құпия ақпарат қайталанған немесе алынған (жиналған) жағдайда 20 жылға дейін бас бостандығынан айыру. Алайда, Санкциялар айыппұл немесе 1 жылға бас бостандығынан айыру түріндегі ең төменгі шекті, қылмыс алғаш рет жасалған жағдайда және кінәні жеңілдететін жағдайлар болған кезде қолданылады [3].

Өз кезегінде §1029 АҚШ заңдар жиынтығының 18 титулында жауапкершілікті белгілейді:

– жалған қол жеткізу құралдарын өндіру, пайдалану және сату;

– 1000 АҚШ долларынан астам материалдық пайда алу мақсатында рұқсатсыз қол жеткізу үшін аспаптарды пайдалану немесе алу;

– 15 және одан да көп жалған немесе рұқсат етілмеген қол жеткізу құралдарына ие болу;

– жалған қол жеткізу құралдарын жасауға арналған жабдықты өндіру, сату немесе иелену;

– басқа тұлғаға арналған қол жеткізу құралдарының көмегімен мәмілелер жасау;

– қандай да бір тұлғаға қол жеткізу құралдарын алу үшін пайдаланылуы мүмкін ақылы ақпаратқа қол жеткізу немесе сатып алу құралдарын ұсыну;

– телекоммуникациялық қызметтерді рұқсатсыз алу үшін өзгертілген немесе бейімделген телекоммуникациялық диагностикалық жабдықты пайдалану, өндіру, сату немесе иелену;

– телекоммуникациялық қызметтерді рұқсатсыз пайдалану мақсатында телекоммуникациялық аппаратураны модификациялау үшін сканерлеуші қабылдағыштарды, жабдықты немесе бағдарламалық қамтамасыз етуді пайдалану, өндіру, сату немесе иелену;

– кез-келген адамды несие жүйесінің мүшесіне немесе оның агентіне рұқсат етілмеген қол жетімділік құралдарымен жасалған транзакциялардың жазбаларын төлеу үшін ұсынуға мәжбүрлеу [4].

Осылайша, АҚШ заңнамасы компьютерлік қылмыстар үшін жауапкершілікті жеткілікті түрде егжей-тегжейлі реттейді, оның барлық кезеңдерінде (дайындалу, оқталу, аяқталған қылмыс) қылмыс жасағаны үшін қатаң санкциялар қарастырады деген қорытынды жасауға болады.

Сонымен қатар, қылмыстық заңнама баптарының диспозициялары қылмыстың тікелей объектісі – компьютерлік ақпаратпен қатар, қосымша объектілер ретінде мемлекет пен жеке тұлғаның ең маңызды салаларын қамтиды: үкіметтік және қаржы институттарының қызметі; телекоммуникациялық желілер мен қызметтер; мемлекеттік қауіпсіздік, мемлекеттік құпия, жеке өмір құпиясы, коммерциялық құпия және т. б., бұл тұлғалардың саралау процесін жеңілдетеді, кінәлі адамды жауапқа тарту және қылмыстық жаза түрі туралы мәселелерді шешу кезінде компьютерлік қылмыстарға жаза тағайындауды шешеді.

Сонымен қатар, зиянды компьютерлік бағдарламаларды жасағаны, пайдаланғаны және таратқаны үшін жазаны қарастыратын арнайы қылмыстық-құқықтық норма (Қазақстанның қылмыстық заңнамасындағыдай) АҚШ-тың федералды қылмыстық заңнамасында жоқ.

Ұлыбритания және Солтүстік Ирландия Біріккен Корольдігінде (бұдан әрі-Ұлыбритания) компьютерлік қылмыстар жасағаны үшін жауапкершілікті қылмыстық-құқықтық регламенттеуге жеткілікті көңіл бөлген.

Атап айтқанда, 1990 жылғы компьютерді теріс пайдалану туралы заң келесі қылмыс құрамдары үшін жауапкершілікті қарастырады:

– компьютерге немесе ондағы компьютерлік ақпаратқа немесе бағдарламаларға қасақана заңсыз қол жеткізу (1-бап);

– компьютерге немесе ондағы компьютерлік ақпаратқа немесе оларды кейіннен заңсыз мақсаттарда пайдалану үшін бағдарламаларға қасақана заңсыз қол жеткізу (2-бап);

– компьютерлік ақпаратқа машиналық тасығышта, компьютерде, компьютерлік жүйеде немесе желіде, мақсатпен немесе егер бұл ақпаратты жоюға, бұғаттауға, модификациялауға не көшіруге, компьютердің, компьютерлік жүйенің немесе желінің жұмысын бұзуға әкеп соқтырса, заңсыз қол жеткізу (3-бап) [5].

Компьютерлік ақпаратты қылмыстық қол сұғушылықтан қорғау мәселелері 1998 жылғы Дербес деректер туралы заңның бірнеше ережелеріне арналған, ол кейіннен 2018 жылғы деректерді қорғау туралы актімен ауыстырылды. Осы заңнамалық актіде келейдей қылмыстық жауапкершілік қарастырылған:

– деректерді қорғау тізіліміндегі тіркеу жазбасын бұза отырып, дербес деректерді әдейі жинау немесе сатып алу;

– заңсыз жиналған немесе заңсыз алынған дербес деректерді сату

Магистрат сотының шешімімен құқық бұзушы 5000 фунт стерлингке дейін айыппұл төлеуі мүмкін. Корона сотының шешімімен (неғұрлым ауыр қылмыстар үшін) қылмыскер шектеусіз айыппұл салуға немесе бас бостандығынан айыруға сотталуы мүмкін. Жеке

деректерді қорғау саласындағы бұзушылық үшін заңды тұлғаға (ұйымға) 20 миллион еуроға дейін айыппұл салынуы мүмкін (валюта бағамы бойынша фунт стерлингке аударылған) [6].

Сонымен қатар, 2000 жылғы Британдық терроризм актісі компьютерлерге, олардың жүйелеріне немесе желілеріне заңсыз ену, соның салдарынан айтарлықтай зиян келтіру немесе оларды жаппай зорлық-зомбылықты ұйымдастыру үшін алынған компьютерлік ақпаратты пайдалану террор актілеріне теңестірілуі мүмкін және сәйкесінше жауапкершіліктің жоғарылауына әкелуі мүмкін.

Сонымен қатар, скандинавиялық құқықтық отбасының шетелдік қылмыстық заңнамасын талдау компьютерлік ақпаратты қорғау және компьютерлік қылмыстар үшін жауапкершілікті енгізу жолындағы алғашқы қадамды заң шығарушы АҚШ-та емес, Швецияда жасағанын көрсетеді. Атап айтқанда, 1973 жылы 4 сәуірде Швецияда «деректер туралы» заң қабылданды, ол заңнамаға «компьютер арқылы теріс пайдалану» атты жаңа құқықтық түсінік енгізді [7].

Қазіргі уақытта Швеция Корольдігінің Қылмыстық кодексінде (бұдан әрі-швеция ҚК) компьютерлік қылмыстар үшін жауапкершілікті көздейтін арнайы бап жоқ. Алайда, ішінара, қылмыстық әрекеттің осы түрі үшін жаза Швеция ҚК 4-тарауының 9-бабында қамтылған: «8 және 9-баптарда көрсетілген өзге жағдайларда деректерді автоматты өңдеу жүйесіндегі жазбаға заңсыз қол жеткізетін немесе Тізілімге мұндай жазбаны заңсыз өзгертетін, өшіретін немесе қосатын адам үкім шығарылуы тиіс айыппұлға немесе екі жылдан аспайтын мерзімге бас бостандығынан айыруға қатысты деректердің құпиялығын бұзғаны үшін. Осы контекстегі жазба тіпті деректерді автоматты түрде өңдеуде пайдалану үшін электронды немесе ұқсас тәсілдермен өңделетін ақпаратты да қамтиды». [8].

Егер адам алдау арқылы айыпталушыға пайда әкелетін және алданған адамға немесе оның өкілі болып табылатын адамға шығын келтіретін кез-келген әрекетті жасауға немесе жасамауға біреуді көндірсе, онда ол сотталуы керек деп белгілейтін Швеция Қылмыстық кодексінің 9-тарауының 1 бабында екі жылдан аспайтын мерзімге бас бостандығынан айыру туралы алаяқтыққа жауаптылық қрастырылған.

Сондай-ақ, алаяқтық жасағаны үшін қате немесе толық емес ақпарат беру немесе бағдарламаға немесе есептілікке өзгерістер енгізу арқылы немесе басқа тәсілдермен ақпаратты автоматты түрде өңдеу нәтижесіне немесе қылмыс жасаған адамға пайда әкелетін кез-келген басқа автоматты өңдеуге заңсыз әсер ететін адам жазалануы керек.

Данияның қылмыстық заңнамасында компьютерлік қылмыстар үшін жауапкершілікке қатысты арнайы баптар, тараулар жоқ. Алайда, кінәлі адам компьютерлік қылмыстың жекелеген сараланған белгілерін қамтитын құқықтық норма негізінде қылмыстық жауапкершілікке тартылуы мүмкін.

Мысалы, Дания Қылмыстық кодексінің (бұдан әрі – Дания Қылмыстық кодексі) 193 – параграфының 5-тармағы төрт жылдан аспайтын кез келген мерзімге қамауға алу немесе түрмеге қамау түріндегі жазаны немесе жеңілдететін жағдайларда – егер адам заңсыз тәсілмен жария байланыс құралдарының, жария пошта қызметтерінің жұмысына, телеграф немесе телефон қызметтері, радио немесе теледидар қондырғылары, деректерді өңдеу жүйелеріне елеулі іркілістер туғызса, айыппұлды көздейді. Өз кезегінде, §279 Данияның Қылмыстық кодексі өзіне немесе басқа адамдарға заңсыз пайда табу мақсатында ақпаратты немесе деректерді электрондық өңдеу үшін пайдаланылатын бағдарламаларды заңсыз өзгертетін, толықтыратын немесе өшіретін немесе осындай деректерді өңдеудің нәтижелерін кез-келген басқа тәсілмен қозғауға тырысатын кез-келген адам компьютерде кінәлі деп алаяқтық ретінде танылатындығын қарастырады [9].

Роман-герман құқықтық отбасы елдерінің (Франция, Германия, Италия, Нидерланды және т. б.) қылмыстық заңнамасын талдау компьютерлік қылмыстардың құрамын және оларды жасағаны үшін жазаны реттейтін құқықтық нормалар жоғарыда аталған «минималды» және «қосымша» тізбелер негізінде анықталғанын Еуропа Кеңесінің министрлер комитетінің 1989 жылғы 13 қыркүйегіндегі отырысында қабылданған.[10].

Сондықтан 1995 жылға дейін Еуропа елдерінің көпшілігінде компьютерлік қылмыс жасағаны үшін жаза белгілейтін заңдар қабылданды. Көрсетілген әрекеттерден қылмыстық-құқықтық қорғау объектілері ретінде: қызметтер, мүлік және ақпарат белгіленді.

Мәселен, Германия Федеративтік Республикасының Қылмыстық кодексі (бұдан әрі – ГФР ҚК) адамдар үшін жауапкершілікті белгілейді:

– өздері үшін немесе өзге тұлға үшін тікелей қабылданбайтын, болуы мүмкін мәліметтерді электрондық, магниттік немесе басқа тәсілмен көшіруді немесе беруді құқыққа сыйымсыз сатып алу (§202a);

– жалған немесе жалған техникалық жазбаларды қолдана отырып, олар автоматты құрылғылармен толық немесе ішінара тіркелген деректерді қолдан жасау (§268);

– дәлелді мәні бар деректерді ұқсас қолдан жасау (§269);

– техникалық жазбаларды жою, өзгерту немесе жасыру (§274);

– деректерді заңсыз жою, жарамсыз ету немесе өзгерту (§303a);

– деректерді немесе ақпарат тасығыштарды өңдеуге арналған қондырғыларды бұзу, бүлдіру, жарамсыз ету не жарамсыз ету жолымен деректерді өңдеп бұзу (§303b);

Сондай-ақ, ГФР Қылмыстық кодексіндегі компьютерлік қылмыстарға мыналар жатады: телекоммуникациялық байланыс құпиясын бұзу (§206); телекоммуникациялық қондырғылардың қызметіне заңсыз араласу (§317).

Сонымен қатар, ГФР Қылмыстық кодексінің «алаяқтық және сенімді қылмыстық теріс пайдалану» №22 бөлімінде §263a «компьютерлік алаяқтық» қарастырылған, ол өзі немесе үшінші тұлғалар үшін басқа біреудің мүлкіне зиян келтіру ниетімен бағдарламаларды дұрыс жасамау, дұрыс емес немесе дұрыс емес пайдалану арқылы деректерді өңдеу нәтижесіне әсер ету толық емес деректер, деректерді заңсыз пайдалану немесе деректерді өңдеу нәтижесіне өзге де әсер ету қасақана әрекет деп түсініледі.

Жоғарыда аталған барлық қылмыстарды жасағаны үшін жазаның екі ықтимал түрін белгілейтін балама санкциялар қарастырылған: белгілі бір мерзімге бас бостандығынан айыру (§303a – 2 жылға дейін, §202a, 206 – 3 жылға дейін, § 263a, 268, 269, 274, 303b, 317 – 5 жылға дейін) немесе ақшалай айыппұл. [11].

Германияның қылмыстық заңнамасының ерекшеліктерінің қатарында ГФР Қылмыстық кодексінің компьютерлік қылмыстар үшін жауапкершілікті реттейтін баптары жеке бөлімге (тарауға) біріктірілмегенін, бірақ қылмыстық әрекеттердің «дәстүрлі» түрлеріне арналған қылмыстардың арнайы, сараланған құрамы болып табылатындығын және олармен бір бөлімде қамтылатындығын атауға болады, олардан тек қылмыстар құрамының элементтерімен ерекшеленеді: тақырып қылмыстық қол сұғушылық, қылмыстық іс-әрекет жасау тәсілімен, қылмыс жасау құралымен және т. б. Мысалы: §202a §202 «хат алмасу құпиясын бұзу» туралы арнайы норма ретінде әрекет етеді. Бұл баптар 15-бөлімнің бір (жалпы) бөлімінде «құпиялылық пен құпиялылықты бұзу», «жеке өмірге қол сұғылмаушылық» ортақ объектісіне ие және тек қылмыс затымен ерекшеленеді: §202 – басқа адамдардың хаттары мен құжаттары, §202a-машиналық ақпарат тасымалдаушылары немесе олардағы ақпарат.

Германияның қылмыстық кодексінің бұл құрылымы ұтымды және прагматикалық болып табылады, өйткені ол тиісті қылмыстық әрекеттерді саралауды жеңілдетеді.

Сонымен қорыта келе айтатын болсақ шет мемлекеттердің қылмыстық заңдарында компьютерлік қылмыстармен күресуге бағытталған нормалардың бар екендігін және компьютерлік қылмыстық қол сұғудың әртүрлі екендігін және оларға қолданылатын жазалардың да әртүрлі екендігін, тіпті олардың неғұрлым қатал екендігін көруімізге болады.

Әдебиет

1. Есаков Г.А. Основы сравнительного уголовного права: монография. – Москва: ООО «Издательство «Элит», 2007.

2. Патриотический Акт 2001 года. URL: http://www.crime-research.ru/articles/PatriotAct/4.

3. Свод законодательства США Раздел 18, часть 1, глава 47, §1030 .

4. Свод законодательства США Раздел 18, часть 1, глава 47, §1029. URL: http://www.law.cornell.edu/uscode/text/18/1029 .

5. Официальное издание Computer Misuse Act 1990. – First Published 1990, Reprinted in the United Kingdom by The Stationery Office Limited. London, 1997. 14 p.

6. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: монография. – Москва: Изд-во РУДН, 1999.

7. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. 1988. №10.

8. Уголовный кодекс Швеции. URL: http://www.sweden4rus.nu/rus/info/juridisk/ugolovnyj_kodeks_shvecii.

9. Уголовный кодекс Дании. URL: http://www.law.edu.ru/norm/norm.asp?normID=1241524&subID=100096345,100096366,100096661,100097370#text .

10. Рекомендация Комитета министров Совета Европы № (89)9 от 13 сентября 1989года. .instranet. Instra Servlet? command=com.instranet. CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 .

11. Уголовный кодекс Германии. URL: http://lexetius.com/StGB/263a.

САДУАҚАС
Ибрагим Серікбайұлы
Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясының 2 курс магистранты
полиция лейтенанты

КОМПЬЮТЕРЛІК АҚПАРАТ САЛАСЫНДАҒЫ АЛАЯҚТЫҚ ҮШІН ЖАУАПКЕРШІЛІК ТУРАЛЫ ШЕТ ЕЛДЕРДІҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫН САЛЫСТЫРМАЛЫ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Компьютерлік ақпарат саласындағы алаяқтық үшін қылмыстық жауапкершілік мәселесіне жүгінсек, қылмыстық әрекеттің осы түріне қарсы іс-қимылдың шетелдік тәжірибесін назардан тыс қалдыруға болмайды. Біріншіден, бұл тікелей практикалық маңызы бар, өйткені компьютерлік алаяқтықтың трансұлттық сипаты басқа мемлекеттердің құқық қорғау органдарымен және құқықтық жүйелерімен өзара әрекеттесу қажеттілігін білдіреді. Мұндай ынтымақтастық осы қылмыс үшін жауапкершілікті белгілеу мен іске асырудың ұлттық ерекшеліктерін нақты түсінген жағдайда ғана мүмкін болады. Сонымен қатар, салыстырмалы құқықтық зерттеу әрқашан отандық заңнамаға басқаша қарауға мүмкіндік береді, оның әлсіз және күшті жақтарын анықтауға, сондай-ақ оны одан әрі жетілдіру үшін дәлелді ұсыныстар құруға ықпал етеді.

2013 жылдың ақпанында Біріккен Ұлттар Ұйымының Есірткі және қылмыс жөніндегі басқармасы (UNODC) киберқылмысты кешенді зерттеу нәтижелері бойынша баяндама дайындады. Зерттелген елдердің ішінен UNODC тұжырымдарына сәйкес компьютерлік алаяқтыққа қарсы қылмыстық-құқықтық іс-қимыл 40% меншікке қарсы қылмыстар туралы жалпы ережелерді қолдану арқылы жүзеге асырылады, тағы 40% компьютерлік ақпарат саласындағы алаяқтық туралы арнайы нормаларды қолдану арқылы және 15% адамдардың қылмыстар жиынтығы бойынша іс-әрекеттерін саралауға негізделген жалпы қылмыстық алаяқтық және компьютерлік ақпаратқа қарсы аралас тәсіл қолданылады.

Тұтастай алғанда, шетелдік заңнаманы талдау UNODC тұжырымдарымен келісуге мүмкіндік береді – қазіргі жағдайда елдер компьютерлік ақпарат саласындағы алаяқтық үшін қылмыстық жауапкершілікті белгілеу мәселесін шешуге басқаша қарайды. Осы қылмысты жасау кезінде зиян келтірілетін қоғамдық қатынастардың мазмұнын анықтау бірдей емес. Сонымен, кейбір елдерде компьютерлік ақпарат саласындағы алаяқтық меншікке қарсы қылмыс ретінде қарастырылады (Австралия, АҚШ, Польша және т. б.), ал басқаларында – ең алдымен компьютерлік деректерді, компьютерлік жабдықтар мен жүйелерді (Канада, Жаңа Зеландия, Эстония, Африка елдері) пайдаланудың белгіленген тәртібіне қол сұғатын қылмыс ретінде қарастырылады.

Шет елдердің абсолютті көпшілігінде ұрланған мүліктің мөлшері компьютерлік ақпарат саласындағы алаяқтық үшін қылмыстық жауапкершілікті саралаудың негізгі критерийі болып

табылады. Сонымен қатар, жүргізілген зерттеу өзге де заңнамалық шешімдерді анықтауға мүмкіндік берді. Бұл қылмыстың сараланған белгісі көбінесе оны жасаудың топтық сипаты ретінде танылады (алдын-ала келісілген адамдар тобының немесе ұйымдасқан топтың құрамында). Жекелеген елдерде адамның өзінің сенімгерлік (қызметтік) жағдайын немесе «Интернет» ақпараттық – телекоммуникациялық желісін, жәбірленушінің кәмелетке толмаған немесе карт жасын пайдалануы ауырлататын мән-жайлар болып табылады. Кейбір елдерде компьютерлік ақпараттың өзгеруі, жойылуы немесе бұғатталуы сындарлы емес, компьютерлік алаяқтықтың сараланған белгісі болып табылатындығын ерекше атап өткен жөн.

Көбінесе оның құқықтық жүйесінің құрылымына байланысты компьютерлік ақпарат саласындағы алаяқтық үшін қылмыстық жауапкершілік мәселесін талдауға арналған маңызды материал Америка Құрама Штаттарының қылмыстық заңнамасын қамтиды. Айта кету керек, жекелеген штаттар деңгейінде компьютерлік қылмыс жасағаны үшін жауапкершілік туралы заңнаманы дамытудың негізі 1986 жылы қабылданған компьютерлік алаяқтық және оларды пайдалану туралы компьютерлік алаяқтық және (CFAA) заңы болды. АҚШ заңдар жиынтығының §1030 компьютерді пайдалану алаяқтық ниетпен жүзеге асырылатын компьютерлік ақпаратқа қол жеткізу немесе алаяқтық арқылы құнды нәрсе алу үшін компьютерді пайдалану ретінде анықталады [1].

Арканзас заңдар жиынтығында «қылмыс әрекеттері» (қылмыстар) 5-бөлімі «Offenses against property» (мүлікке қарсы қылмыстар) 4-кіші бөлімінде «Computer-related crimes» (компьютерлерді пайдалануға байланысты қылмыстар) 41-тарауын бөлектейді. Арканзас заңдар жиынтығының §5-41-103 «computer fraud» (компьютерлік алаяқтық) мәліметтері бойынша, егер адам компьютерге, компьютерлік жүйеге немесе желіге кіруді қолдана отырып, алдау немесе жалған өкілдік ету арқылы ақшаны немесе басқа мүлікті ұрлап кетсе, компьютерлік алаяқтық жасайды. Арканзас штатының заң шығарушысы компьютерлік алаяқтықты D класындағы фелонияға жатқызады [2].

Арканзас заңдар жиынтығының §5-4-401 «Sentence» 4-тармағына сәйкес мұндай қылмыс жасағаны үшін кінәлі деп танылған адам 6 жылға дейін бас бостандығынан айыру жазасына кесіледі.

Луизиана штатының заң жиынтығында компьютерлік алаяқтық үшін қылмыстық жауапкершілікті §73.5 «computer fraud» (компьютерлік алаяқтық) [3] белгілейді. Бұл құрамның құрылымдық белгілері – адамның компьютерді, ақпараттық желіні немесе жүйені қолдануы және алдау (жалған өкілдік). Луизиана штатының заңнамасына сәйкес компьютерлік алаяқтық 10 мың АҚШ долларына дейін айыппұл салуға немесе 5 жылға дейін бас бостандығынан айыруға немесе осы екі жазаға да жазаланады.

Луизиана штатының заңнамасының айрықша ерекшелігі – «Интернет» ақпараттық-телекоммуникациялық желісін компьютерлік қылмыс жасау кезінде адамның пайдалануын ауырлататын мән-жай ретінде арнайы анықтау. Луизиана заңдар жиынтығының «а» тармағына сәйкес §73.9 адамның адамға немесе мүлікке қарсы қылмыстық қол сұғушылық кезінде интернетті пайдалануы кем дегенде 1 жылға бас бостандығынан айыру түріндегі қосымша жаза тағайындауға әкеп соғады.

Компьютерлік алаяқтық үшін жауапкершілік туралы іс жүзінде бірдей ереже Миссисипи заңдар жиынтығының 97-45-3 «компьютерлік қылмыстар және жеке деректерді ұрлау» (компьютерлік қылмыстар және жеке деректерді ұрлау) §45-тарауында қарастырылған. Сонымен бірге, Луизиана заң шығарушысынан айырмашылығы, бұл бап кінәлі адамның жауапкершілігін жәбірленушіге келтірілген залалдың мөлшеріне қарай ажыратады. Сонымен, компьютерлік алаяқтықтың негізгі құрамы 1 мың АҚШ долларына дейін айыппұлмен немесе 6 айдан аспайтын мерзімге бас бостандығынан айырумен немесе жазаның осы екі түрімен де жазаланады. Шығын 500 доллардан асатын жағдайларда кінәлі адам 10 мың АҚШ долларына дейін айыппұл немесе 5 жылға дейін бас бостандығынан айыру немесе осы екі жаза түрімен жазаланады [4].

Батыс Вирджиния қылмыстық заңнамасы бойынша компьютерлік алаяқтық 10 мың АҚШ долларына дейін айыппұлмен немесе 10 жылға дейін бас бостандығынан айырумен немесе осы екі жазамен де жазаланады (§61 – 3С-4).

Вирджиния заң жиынтығы §18.2-152.3 «computer fraud; penalty» компьютерлік алаяқтық үшін қылмыстық жауапкершілікті қарастырады. Осы бапқа сәйкес, егер ұрланған мүліктің құны 200 доллардан аспаса, қылмыс 1-ші дәрежелі теріс қылық ретінде сараланууы керек (§18.2 сәйкес, қылмыстың бұл санаты 2500 долларға дейін айыппұлмен немесе 12 айға дейін бас бостандығынан айырумен немесе осы екі жазамен де жазаланады). Егер залал 200 АҚШ долларынан асатын болса, қылмыс 5-сыныпты фелонияға жатқызылуы керек (§18.2-10 сәйкес 1 жылдан 10 жылға дейінгі мерзімге бас бостандығынан айыру қылмыстарының осы санаты 2500 АҚШ долларына дейін айыппұлмен жазаланады) [5].

Иллинойс заңдарының жиынтығына сәйкес, компьютерлік алаяқтық мүлікті заңсыз иемденуге бағытталған әрекеттерді (16D – 5-баптың 3-тармағы) және қорғалған ақпаратты алуға (көшіруге), компьютерлік деректерді бұғаттауға, бүлдіруге немесе жоюға, компьютерлік техниканың өзін қабілетсіз етуге бағытталған кез келген басқа алаяқтық әрекеттерді біріктіретін жеткілікті белгісіз мазмұнға ие, желілер немесе жүйелер. Осы бапта кінәлі ұрланған мүліктің мөлшеріне байланысты компьютерлік алаяқтық үшін жауапкершілікті саралау келтірілген: 1 мың АҚШ долларына дейін ұрлауды 4 – сыныпты фелония (1 жылдан 3 жылға дейін бас бостандығынан айыруға жазаланады); 1-ден 50 мың АҚШ долларына дейін-3-сыныпты фелония (1 мың АҚШ долларынан 3 жылға дейін бас бостандығынан айыруға жазаланады). 2 жылдан 5 жылға дейін) және 50 мың АҚШ долларынан астам – 2-сыныпты фелония (3 жылдан 7 жылға дейін бас бостандығынан айыруға жазаланады) [6].

Айта кету керек, Иллинойс штатының заңнамасы онлайн режимінде (Online property offenses) жасалған мүлікке қол сұғушылықты бөлек бөледі. Қылмыстық жолмен өндірілген мүлікті «Интернет» желісінде өткізгені үшін қылмыстық жауапкершілікті белгілеумен қатар, 16j-15-бапта жалған деректерді пайдалана отырып, «Интернет» желісінде тауарларға немесе қызметтерге ақы төлеу бойынша кінәлі әрекеттердің жасалуына байланысты мазмұны алдау (dline theft by deception) жолымен Интернет-ұрлықтың құрамы тұжырымдалған (болжануда, немесе басқа адамның деректері). Компьютерлік алаяқтық туралы баптардағыдай, бұл қылмысты жасағаны үшін жауапкершілік ұрланған мүліктің мөлшеріне байланысты сараланады: 300 АҚШ долларына дейін ұрлау 4 – сыныпты фелония, ал көрсетілген сомадан жоғары-2-сыныпты фелония деп танылады.

16D-5 және 16J-15 баптарын салыстыру «Интернет» желісінде (онлайн режимінде) қылмыс жасауды Иллинойс штатының заң шығарушысы адам жасаған ұрлықтың қоғамдық қауіптілігінің жоғарылағанын көрсететін ауырлататын жағдай ретінде қарастырады деген қорытынды жасауға мүмкіндік береді.

Джорджия штатының заңдар жинағындағы басқа Штаттардан айырмашылығы, компьютерлік алаяқтық емес (computer fraud), бірақ компьютерді ұрлау (computer theft) категориясын қолданады. §16-9-93-тегі компьютерлік қылмыстарға арналған тарауда, егер ол компьютерді немесе компьютерлік желіні осындай пайдалану заңсыз болып табылатындығын түсініп пайдаланса, кез-келген адам компьютерлік ұрлық жасағаны үшін кінәлі деп танылады: 1) басқа адамның мүлкін алу немесе иемдену; 2) мүлікке құқықты кез-келген алаяқтық жолмен алу; 3) меншікті шартты немесе өзге де заңды міндеттемені бұза отырып қайта құру.

Осы баптың «h» тармағына сәйкес бұл қылмыс 50 мың АҚШ долларына дейін айыппұл салуға не 15 жылға дейін бас бостандығынан айыруға не осы екі жаза түріне де жазаланады.

Тағы бір тәсіл Пенсильванияның қылмыстық заңнамасында жүзеге асырылды. Сонымен, Пенсильвания штатының заң жиынтығының §7613-ке сәйкес, компьютерлік ұрлық белгілі бір құрылғының, компьютерлік жүйенің немесе желінің жадында орналасқан компьютерлік ақпаратты заңсыз иемденуге бағытталған әрекеттерді білдіреді. Бұл баптың компьютерлік қылмыстарға арналған тарауда орналасуы (76-тарау «computer offenses») меншік қатынастары осы қылмыстық қол сұғушылықтың тікелей объектісінің мазмұнын құрайтындығын көрсетеді.

Пенсильвания заңнамасы бойынша «меншікке қарсы қылмыстар» бөлімінде орналасқан жеке деректерді ұрлау туралы норманы (§4120 «identity theft») қолдану арқылы жүзеге асырылады. Осы қылмысты жасағаны үшін жауапкершілік жәбірленушіге келтірілген залалдың мөлшеріне қарай сараланады: егер залал 2 мың АҚШ долларынан аспаса, жасалған іс- әрекет 1-дәрежелі теріс қылық деп танылады (5 жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады); осы сомадан асқан жағдайда – 3 дәрежелі фелония (7 жылға дейінгі мерзімге бас

бостандығынан айыруға жазаланады). Бұдан басқа, ауырлататын мән-жайлар ретінде: 1) ұйымдасқан топ құрамында қылмыс жасау (жасалған іс-әрекетті 3-дәрежелі фелония деп танылады); 2) меншікке қарсы қылмыстар туралы бөлімде көзделген қылмысты қайта жасау (жасалған іс-әрекет 2-дәрежелі фелония деп танылады және 10 жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады) деп те аталады; 3)кәмелетке толмаған адамға, сол сияқты 60 жастан асқан адамға қатысты қылмыс жасау (егер залал 2 мың АҚШ долларынан аспайтын болса, жасалған іс-әрекет 3 – дәрежелі фелония деп танылады, осы сомадан асқан жағдайда-2-дәрежелі фелония) [7].

Нью-Йорк штатының заңдар жиынтығы компьютерлік ақпарат саласындағы алаяқтық туралы ережелер «К» бөлімінде «Offenses involving fraud» (алаяқтықпен (алдаумен) байланысты қылмыстар деп аталады [8].

190.78 – 190.8-баптарға сәйкес адам басқа адамның мүлкін ұрлау мақсатында кез келген нысанда ұсынылған дербес ақпаратты (жеке сәйкестендіру ақпараты) заңсыз пайдаланғаны үшін қылмыстық жауаптылыққа жатады. Ұрлау мөлшері кінәлінің әрекетін саралауға және жауапкершілігіне де әсер етеді: егер ұрланған заттың мөлшері 500 АҚШ долларынан аспаса, бұл әрекетті «А» класындағы теріс қылық деп таниды (190.78-бап) және 1 жылға дейін бас бостандығынан айыруға жазаланады; егер ұрланған заттың мөлшері 500 АҚШ долларынан асса, бұл әрекетті «Е» класындағы фелония (190.79-бап) мойындайды және «Е» класындағы фелония (190.79-бап) 4 жылға дейінгі мерзімге бас бостандығынан айыру; егер ұрланған зат мөлшері 2 мың АҚШ долларынан асатын болса, бұл әрекетті «D» класындағы фелония мойындайды (190.80-бап) және 7 жылға дейін бас бостандығынан айыруға жазаланады.

Невада штатының заңдар жиынтығында компьютерлік ақпарат алаяқтықтары үшін жауапкершілік туралы арнайы ереже жоқ. Мұндай әрекеттер үшін қылмыстық жауапкершілік заңмен қорғалатын компьютерлік ақпаратқа заңсыз қол жеткізу туралы жалпы нормада көзделген (§205.477 «Unlawful interference with d denial of access to us use of computers; unlawful use or access of computers»). Осы баптың 2-бөлігіне сәйкес, егер мұндай әрекеттер мүлікті заңсыз иемдену мақсатында жасалған болса, бұл әрекет «С» класындағы фелония болып табылады және 10 мың АҚШ долларына дейін айыппұлмен 1 жылдан 5 жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады [9].

Компьютерлік ақпарат саласындағы алаяқтық үшін жауапкершілік туралы шет елдердің қылмыстық заңнамасын салыстырмалы-құқықтық талдау әлемдік қоғамдастықтың компьютерлік алаяқтықпен күресудің маңыздылығын көрсетеді және отандық заңшығарушыларға шет мемлекеттердің осындай құқық бұзушылықпен күресудегі тиімді тәжірибесін біздің заңнамамызға ендіруді қарастыруға мүмкіндік береді.

Әдебиет

1. Свод законов США // URL:http://law.justia.com/codes/us/2012/title-18/part-i/chapter-47/section- 1030/

2. Свод законов штата Арканзас // URL:http://law.justia.com/codes/arkansas/2010/title-5/subtitle- 4/chapter-41/subchapter-1/5-41-103/.

3. Свод законов штата Луизиана // URL: http://law.justia.com/codes/louisiana/2011/rs/title14/rs14-73-5.

4. Свод законов штата Миссисипи // URL: http://law.justia.com/codes/mississippi/2013/title-97/chapter-45/section-97-45-3/.

5. Свод законов штата Виржиния // URL: http://law.justia.com/codes/virginia/2014/title-18.2/section-18.2-152.3/.

6. Свод законов штата Иллинойс // URL: http://law.justia.com/codes/illinois/2010/chapter720/072000050HArt_16D.html.

7. Свод законов штата Пенсильвания // URL: http://law.justia.com/codes/pennsylvania/2014/title- 18/chapter-76/section-7613/ .

8. Свод законов штата Нью-Йорк // URL: http://law.justia.com/codes/new-york/2014/pen/part- 3/title-k/article-190/.

9. Свод законов штата Невада // URL: http://law.justia.com/ 205/statute-205.477.

БЕЙСЕНАЛИЕВ
Бауыржан Нуралыулы
докторант 1-го курса докторантуры факультета послевузовского образования
Алматинской академии МВД
Республики Казахстан им. М. Есбулатова
подполковник полиции

ШАУХАР
Данияр Қанатұлы
магистрант 1 курса научно-педагогической магистратуры факультета послевузовского образования Карагандинской академии МВД
Республики Казахстан им. Б. Бейсенова
старший лейтенант полиции

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РАМКАХ ВНЕДРЕНИЯ ТРЕХЗВЕННОЙ МОДЕЛИ УГОЛОВНОГО ПРОЦЕССА

В данной статье автором рассматривается вопрос противодействия киберпреступности в рамках внедрения трехзвенной модели уголовного процесса. Особое внимание уделено сущности трехзвенной модели, как гаранта соблюдения прав и свобод человека и гражданина. Автором также были рассмотрены формы киберпреступности. Изучена стратегия борьбы с киберпреступностью в свете реформирования уголовного судопроизводства. Целью написания данной статьи является выявление причин и условий совершений киберпреступлений на фоне реформы правоохранительной системы и системы правосудия Республики Казахстан, а также внесение предложений по противодействию данному виду преступности.

Ключевые слова: противодействие киберпреступности, расследование киберпреступлений, трехзвенная модель, уголовное судопроизводство.

1 сентября 2020 года в Послании народу «Казахстан в новой реальности: время действий» Глава государства поручил поэтапно внедрить в стране трехзвенную модель уголовного процесса. Такая система действует в развитых странах Организации экономического сотрудничества и предусматривает следующую организацию процесса. Орган уголовного преследования выявляет преступления, устанавливает причастных лиц и собирает улики.

Прокурор дает оценку собранным доказательствам, пресекает нарушение прав участников уголовного процесса, не допускает вовлечение добросовестных граждан в уголовный процесс и поддерживает государственное обвинение в суде.

Суд занимается санкционированием следственных действий, рассмотрением жалоб и назначением наказания. Мировая практика показывает, что разграничение полномочий уполномоченных органов позволяет максимально обеспечить защиту прав граждан на всех стадиях уголовного процесса. Разграничение создаёт правозащитный барьер, ограждая от необоснован-

ных незаконных решений. Каждая из стадий трёхзвенной модели служит фильтром, через который должно пройти уголовное дело, перед тем как будет рассмотрено судом.

Касым-Жомарт Кемелевич Токаев подчеркнул: «Такой подход укрепит систему сдержек и противовесов, создаст на каждом этапе эффективные фильтры. Еще раз подчеркиваю: законность и справедливость должны быть обеспечены по умолчанию. Нужно помнить, что от ошибок в уголовных делах зависят судьбы людей» [1].

Если разбираться в корне, то можно прийти к выводу, что на протяжении всего времени существования уголовный процесс Республики Казахстан и так был построен по трехзвенной модели. Фактически идет не перевод системы уголовного судопроизводства на трехзвенную модель, а реформа этих самых трех звеньев и системы взаимодействий каждого звена друг с другом. По нашему мнению ключевым и связующим звеном становится прокуратура. Большинство решений необходимо будет согласовывать с прокурорами.

С политикой внедрения трехзвенной модели судопроизводства с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом. Законом существенно расширены полномочия осуществляющего надзор, а также процессуального прокурора, что фактически свело на нет и без того формально закрепленную в законе процессуальную самостоятельность следователя [2].

Переход на трехзвенную модель уголовного процесса по плану состоит из двух основных этапов. В настоящее время приводится в жизнь первый этап.

С 1 января 2021 года прокурор уполномочен согласовывать следующие процессуальные решения:

– о признании в качестве подозреваемого (ст.64, 202 УПК);

– о квалификации деяния (ст. 64, 203 УПК);

– о прерывании сроков досудебного расследования (ст. 192 УПК);

– утверждение протокола об уголовном проступке (ст.65, 528 УПК);

– утверждение постановления о прекращении производства по делу, (ст. 192, 289-290 УПК);

– утверждение постановления о применении приказного производства (ст.629-2, 629-3 УПК).

Безусловно, надзор со стороны прокурора необходим. Но при этом следует избегать излишней бюрократизации и мелочной опеки, фактически снимая ответственность следователя за принятие ключевых решений, ограничивающих конституционные права лиц, вовлеченных в процесс расследования. Полагаем, что вынесение постановления о признании лица подозреваемым – прерогатива следователя, не требующая согласования с прокурором, поскольку это вероятностное решение, правильность которого еще предстоит установить путем производства его допроса и других следственных или негласных следственных действий. Другое дело – согласование прокурором постановления о квалификации деяния подозреваемого, виновность которого подтверждается всей совокупностью собранных следователем доказательств. Но при этом сама процедура, регламентированная ст. 203 УПК РК, требует внесения поправок, соответствующих общепризнанным теоретическим постулатам. В частности, согласие прокурора с квалификацией деяния фактически означает начало официального (государственного) обвинения конкретного лица, которое должно иметь статус уже обвиняемого, а не подозреваемого [3].

Мы полностью согласны с мнением профессора Ахпанова А.Н. и доцента Хана А.Л. Согласование признания лица в качестве подозреваемого требует затраты дополнительных временных ресурсов. Возникает вопрос, как происходит согласование данного решения в ночное время либо в случаях нетерпящих отлагательства. Законодатель предусмотрел право следователя выносить в неотложных случаях постановление о признании лица подозреваемым с последующим обращением к прокурору за получением согласия (п.1-1, 4 ч.1 ст.64 УПК РК). Например, когда необходимо безотлагательно допросить подозреваемого, а согласование с прокурором сразу организовать невозможно (в ночное время, ввиду отдаленности места производства неотложных следственных действий, ввиду отсутствия доступа к ИС ЕРДР – отсутствие электроэнергии, отсутствие или неполадки с интернетом, перезагрузки ИС ЕРДР и т.п.).

Что касается остальных вышеуказанных положений, то считаем их обоснованными. Данные нововведения позволят разделить ответственность за принятие данных решений между органами прокуратуры и органами предварительного расследования, что, в свою очередь положительно отразится на качестве следственной работы и прокурорского надзора.

Следует отметить и положительные стороны трехзвенной модели уголовного судопроизводства Республики Казахстан. Анализ деятельности прокуратуры города Алматы показал, что с момента внедрения трехзвенной модели значительно улучшилось качество досудебного расследования. Так, прекращаемость дел снизилась на 37,5% (с 8 до 5 тысяч), количество прерываний сократилось на 38,5% (с 13 до 8 тысяч), а выявляемость неправильной квалификации увеличилась в 15 раз (с 6 до 89) [4].

Несмотря на то, что имеется положительная правовая статистика, налицо реальный факт распространения киберпреступности. Данная категория преступлений сегодня является самой распространенной и самой латентной. Несмотря на большое количество заявителей, львиная доля пострадавших от киберпреступлений так или иначе скрывают об этом. Но даже в этом случае правоохранительным органам очень тяжело бороться с подобными преступными проявлениями.

Главной причиной укрытия подобных преступлений является стыд со стороны жертв. Зачастую они просто не хотят разглашать тайну своей личной жизни, а кто-то просто стесняется подавать заявление в связи с тем, что не хочет казаться глупым. Например, даже среди сотрудников полиции имеется большое количество пострадавших от интернет-мошенников. Их логику укрытия данных фактов можно легко объяснить. Так как они сами являются представителями правоохранительных органов, а также, нередко, сами работают именно по линии интернет-мошенничества, было бы позорно оказаться среди потерпевших.

Также среди интернет-мошенников очень много фактов обмана именно связанных с сексуальной жизнью жертв. Например, интернет-мошенница вступает в виртуальный половой акт с пострадавшим, а после вымогает деньги за нераспространение интим-ролика с его участием.

Еще очень много фактов мошенничества среди объявлений. Речь идет не о стандартных объявлениях на сайтах рекламы, таких как КОЛЕСА.КЗ, ОЛХ и т.п. Речь идет о запрещенных сайтах, с размещением анкет с интим-услугами. Сейчас мошенники проникли и в эту итак преступную сферу. Мошенниками здесь могут являться не только женщины, но и мужчины, а также несовершеннолетние.

На сайте, таком как кыздар.нет, выкладывается объявление-анкета. Дальше, когда по данному объявлению звонят, а зачастую пишут в мессенджерах потенциальные клиенты, им предлагается произвести предоплату для производства записи на определенное время. После того, как клиент проводит перевод (на неизвестную карту, без имени), его тут же блокируют в телефоне и мессенджере. Обманутый человек далее ничего не может сделать с данной ситуацией. Обращаться в правоохранительные органы глупо и стыдно. Никто не хочет компрометировать себя как пользователя интим услуг, особенно люди, состоящие в браке, либо люди с хорошей репутацией.

Несмотря на вышеуказанное информация о пользователях таких услуг просочилась в сеть. Сегодня в мессенджере WhatsApp широко распространены файлы с опубликованной клиентской базой LoveAika, которая занималась сводничеством «Элитных моделей». Также в данных списках имеется полная база самих девушек, оказывающих интим-услуги.

Указанные данные должны были использоваться в доказывании по делу о сводничестве. А граждане, чьи данные были распространены, должны привлекаться в качестве участников расследования. Сразу налицо нарушение прав граждан, как участников уголовного процесса. С 1 января 2024 года будет проведен заключительный этап внедрения трехзвенной модели уголовного процесса. Несмотря на это не соблюдается главный принцип трехзвенной модели – соблюдение прав и свобод граждан. Безусловно все виновные лица понесут наказание. Но где же был прокурорский надзор во время распространения данных расследования?

Подводя итоги данной работы, отметим, что законодатель Республики Казахстан в очередной раз показал свой реформаторский характер. В Казахстане не боятся своевременно и резко отвечать на требования времени. С другой стороны, возникает вопрос об обоснованности внесенных изменений. Учитывая вышеуказанное, считаем, что внедрение трехзвенной модели действительно необходимо. Несмотря на критику со стороны представителей науки и следственного аппарата государственных органов, положительных тенденций у данной модели больше. Единственное, мы не согласны с согласованием признания лица в качестве подозреваемого, считаем, что данное положение следует исключить либо переработать (например, признание лица в качестве подозреваемого необходимо согласовывать по уголовным делам особо тяжкой категории). Также стоит уделить особое внимание на соблюдение прав граждан в режиме реального времени. Привлекать к ответственности должностных лиц, нарушивших права и свободы граждан, не будет необходимым, если будет работать превентивный механизм. Таким механизмом должен выступать прокурор, который должен не допускать подобные проявления в их зародыше.

Литература

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014г. №231-ЗРК. Доступ из справ.-правовой системы «Әділет».

2. Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в новой реальности: время действий» (г. Нур-Султан, 1 сентября 2020 года). Доступ из справ.-правовой системы «Параграф».

3. Ахпанов А.Н., Хан А.Л. Проект Закона РК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения трехзвенной модели с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом»: взгляд со стороны. URL: https://online.zakon.kz/Document/?doc_id=33889622 (дата обращения: 29.01.2022).

4. Ахпанов А.Н., Хан А.Л. Новые подходы к институту обвинения в уголовном судопроизводстве Республики Казахстан // Вестник Барнаульского юридического института МВД России. 2021 №2 (41).

5. Трехзвенная модель уголовного процесса в Казахстане оправдывает себя. URL: https://www.zakon.kz/5074134-trehzvennaya-model-ugolovnogo-protsessa.html (дата обращения: 30.01.2022).

ОНГАРБАЕВ
Габит Сабитулы
Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясының магистранты полиция капитаны

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ХАЛЫҚАРАЛЫҚ-ҚҰҚЫҚТЫҚ НЕГІЗДЕРІ

Жаһандық ақпараттық кеңістікті қалыптастыру процестері халықаралық ақпараттық қауіпсіздікті қамтамасыз ету мәселесін өзектендіреді. Ғылыми-техникалық прогрестің жетістіктерін пайдалану тек оң мақсаттар үшін ғана емес, сонымен бірге жеке мемлекеттің немесе мемлекеттердің халықаралық аренадағы артықшылығын қамтамасыз ету үшін де мүмкін, бұл мемлекетаралық қақтығыстың жаңа саласының пайда болуына әкеледі, ол енді жеке мемлекеттің мүдделеріне ғана емес, сонымен бірге жалпы халықаралық қауіпсіздік жүйесіне де қатысты.

Қазақстан Республикасының ұлттық қауіпсіздік туралы заңына сәйкес халықаралық ақпараттық қауіпсіздік дегеніміз жеке тұлғаның, қоғамның және мемлекеттің ақпараттық саладағы құқықтарын бұзу, сондай-ақ ұлттық маңызды ақпараттық инфрақұрылым элементтеріне деструктивті және заңсыз әсер ету мүмкіндіктері алынып тасталатын жаһандық ақпараттық кеңістіктің жағдайы. Осылайша, жаһандық ақпараттық кеңістіктің қауіпсіздігі мен ұлттық деңгейдегі ақпараттық кеңістіктің қауіпсіздігін ажырату керек.

Бұл бөлу өте шартты болғанымен, ақпараттық кеңістік біртіндеп шекараларды бұлдыратады. Халықаралық ақпараттық кеңістіктің қауіпсіздігі, яғни халықаралық ақпараттық қауіпсіздік жеке мемлекеттің ақпараттық кеңістігінің қауіпсіздігіне байланысты. Сондықтан халықаралық құжаттарда ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша мемлекеттер арасында келісімге қол жеткізу өте маңызды. Егер Қазақстан Республикасында «ақпараттық қауіпсіздік» категориясы кеңінен қарастырылса, онда халықаралық-құқықтық актілердің басым көпшілігі киберқауіпсіздіктің синонимі ретінде ақпараттық қауіпсіздікті «батыстық» түсінумен сипатталады. Алайда, киберқауіпсіздік ақпараттық қауіпсіздіктің құрамдас бөлігінен басқа ештеңе емес, яғни олар бөлік пен бүтін санмен байланысты. «Киберқауіпсіздік» сөзінің өзі (ағылш. cyber security) «кибер» сын есімі мен «қауіпсіздік» зат есімінің бірігуінен пайда болады. Оксфорд сөздігінде бұл сын есімнің келесі анықтамасы берілген: «компьютерлерге, ақпараттық технологияларға, виртуалды шындыққа қатысты». Осылайша, киберқауіпсіздікті ең жалпы түрде киберкеңістіктің заңсыз шабуылдардан қорғалу жағдайы ретінде анықтауға болады. Терминнің тар мағынасында, киберқауіпсіздік деп ақпараттық-телекоммуникациялық технологияларды қолдану қаупсіздігін санау керек.

Сонымен қатар, ақпараттық қауіпсіздіктің жекелеген құрамдас бөліктері халықаралық құқықта нормативтік-құқықтық регламенттеуді алды. Ең алдымен, бұл ақпарат алу құқығына қатысты. БҰҰ Бас Ассамблеясының бірінші сессиясында A/RES/59 (I) қарарында ақпарат алу

құқығы адамның негізгі құқығы болып табылады және бостандықтың барлық түрлерінің критерийі болып табылады деген ереже бекітілді. Ақпарат еркіндігі ақпараттық мәліметтерді барлық жерде және кедергісіз жинау, беру және жариялау құқығын білдіреді.

1948 жылғы БҰҰ-ның Адам құқықтарының жалпыға бірдей декларациясының 19-бабында әр адамның сенім бостандығына және оларды еркін білдіруге құқығы бар деген ереже бекітілген. Бұл құқыққа өз сенімдерін еркін ұстану еркіндігі және ақпарат пен идеяларды кез-келген тәсілмен және мемлекеттік шекараларға қарамастан іздеу, алу және тарату еркіндігі кіреді. Ал 12-бапта ешкім оның жеке және отбасылық өміріне ерікті түрде араласуға, оның үйінің тұтастығына, хат-хабарларының құпиясына немесе оның ар-намысы мен беделіне ерікті түрде қол сұғуға болмайды делінген. Осылайша, Декларация жеке ақпаратты заңсыз қол жеткізуден қорғау құқығын жариялады.

Адам құқықтары мен негізгі бостандықтарды қорғау туралы Еуропалық конвенцияның 10-бабы [1] сонымен қатар қоғамдық билік тарапынан және мемлекеттік шекараларға қарамастан ешқандай араласусыз ақпарат пен идеяларды еркін алу және тарату құқығын бекітеді. Осы Конвенцияның 8-бабы Жеке және отбасылық өмірді, тұрғын үй мен хат-хабарларды құрметтеу құқығына кепілдік береді.

БҰҰ Бас Ассамблеясының 2011 жылғы 16 мамырдағы есебінде Интернет желісіне қол жеткізу құқығы адамның ажырамас құқықтарына жатқызылды, Интернет желісіне қол жеткізуді шектеу және ақпаратты тарату адамның негізгі құқықтарын бұзу деп танылды.

2013 жылғы 18 Желтоқсанда 68/167 «цифрлық ғасырдағы жеке өмірге қол сұғылмаушылық құқығы» [2] қарары қабылданды, онда технологиялық дамудың жылдам қарқыны әлемнің барлық аймақтарындағы адамдарға жаңа ақпараттық және коммуникациялық технологияларды пайдалануға мүмкіндік беретінін және сонымен бірге үкіметтердің, компаниялардың және жеке тұлғалардың ақпаратты бақылау, ұстау және жинау қабілетін арттыратынын атап өтті. адам құқықтарының жалпыға бірдей декларациясының 12-бабында және осы бапта бекітілген адам құқықтарын, әсіресе жеке өмірге қол сұғылмаушылық құқығын бұзуы мүмкін. Азаматтық және саяси құқықтар туралы халықаралық пактінің 17-бабында, сондықтан бұл мәселе барған сайын алаңдаушылық туғызады. Қарар адамның желіден тыс ортадағы құқықтары, соның ішінде жеке өмірге қол сұғылмаушылық құқығында қорғалуы керек екенін растады.

Ақпараттық ресурстарды реттеу проблемаларын қозғайтын халықаралық-құқықтық актілердің ішінде, ең алдымен, 05.12.1958 жылғы халықаралық басылымдармен алмасу туралы конвенцияны бөліп көрсету керек, оның мәтініне сәйкес мемлекеттер коммерциялық мақсаттарды көздемейтін үкіметтік органдар арасында да, үкіметтік емес ағартушылық ғылыми-техникалық немесе мәдени мекемелер арасында да басылымдармен алмасуды көтермелеуге және жеңілдетуге міндеттенеді.

Мемлекеттер арасындағы ресми басылымдар мен үкіметтік құжаттармен алмасу туралы 05.12.1958 жылғы Конвенция ресми басылымдар мен үкіметтік құжаттармен алмасу тәртібін айқындайды. Бұл ретте құжатта оның құпия құжаттарға, қызметтік хат-хабарларға және жариялылыққа арналмаған өзге де құжаттарға қолданылмайтыны ескертіледі.

Жоғарыда аталған барлық құжаттар ақпараттық саладағы қылмыспен күресу мәселелеріне қатысты болмаса да, олардың маңыздылығын асыра бағалау қиын. Олар ақпараттық қауіпсіздікті қамтамасыз етудің халықаралық-құқықтық негіздері құрылатын негізді құрайды.

Көптеген мемлекеттерде ақпараттық қауіпсіздік ұғымы киберкеңістіктің және ақпараттық-телекоммуникациялық технологиялардың қауіпсіздігіне дейін азаятындықтан, ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қатынастарды реттейтін халықаралық-құқықтық актілердің көпшілігі телекоммуникация саласындағы қауіпсіздікті қамтамасыз етуге дейін азаятыны қисынды.

Осы саладағы ең маңызды халықаралық актілерге БҰҰ Бас Ассамблеясының 55/63 «ақпараттық технологияларды қылмыстық пайдалануға қарсы күрес» қарары жатқызылуы

керек, онда ақпараттық технологиялар мен телекоммуникациялық құралдарды әзірлеу мен енгізуде елеулі прогресс атап өтіледі. Сонымен қатар, қарар ақпараттық технологияларды қылмыстық пайдаланудың алдын алу қажеттілігін атап көрсетеді, өйткені технологиялық прогресс қылмыстық іс-әрекетке, атап айтқанда ақпараттық технологияларды қылмыстық пайдалануға жаңа мүмкіндіктер туғызды. Ақпараттық технологияларды қылмыстық пайдаланудың алдын алу үшін қарарда мемлекеттер осы мақсатқа жету үшін ескеруі керек шаралар кешені ұсынылды. Атап айтқанда, онда мемлекеттер өздерінің заңнамасы мен практикасы ақпараттық технологияларды теріс пайдаланатындарға кез-келген жерде баспана алуға мүмкіндік бермеуін қамтамасыз етуі керек екендігі атап өтілді. Олар ақпараттық технологияларды қылмыстық қолданумен күресте кездесетін мәселелер туралы ақпарат алмасуы керек және т. б. [3].

«Жаһандық киберқауіпсіздік мәдениетін құру» 57/239 қарары жаһандық киберқауіпсіздік мәдениетін құру мәселелеріне арналған. Ол киберқауіпсіздікті тек технологиямен қамтамасыз ету мүмкін және киберқауіпсіздікті жоспарлауға және оны бүкіл қоғамда қамтамасыз етуді басқаруға басымдық берілуі керек екенін атап көрсетеді. Тиімді киберқауіпсіздік тек мемлекеттік немесе құқық қорғау органдарының әрекеттеріне ғана байланысты емес және оған алдын алу шараларымен қол жеткізу және бүкіл қоғамда қолдау көрсету қажет. Қарарға қосымшада жаһандық киберқауіпсіздік мәдениеті өз мүшелерінен талап ететіні айтылған:

– Ақпараттық жүйелер мен желілердің қауіпсіздігін сақтау қажеттілігі туралы және олардың қауіпсіздікті арттыру үшін қабылдауы мүмкін шаралар туралы қатысушыларды хабардар ету нені білдіреді;

– әркімнің өзінің ақпараттық жүйелері мен желілерінің қауіпсіздігін қамтамасыз етуді, сондай-ақ олардың нақты шарттарға сәйкестігін бағалауды көздейтін жауапкершілік;

– қауіпсіздік талаптарын бұзуға ден қою шараларын қабылдауды білдіреді;

– этика, яғни басқа қатысушылардың заңды мүдделерін сақтау;

– демократия, бұл бір жағынан ақпараттың ашықтығын және екінші жағынан оның құпиялылығын қамтамасыз етуді білдіреді;

– тәуекелді бағалау, яғни ақпарат қауіпсіздігінің жаңа сын-қатерлері мен қатерлерін мерзімді бағалау;

– қауіпсіздікті қамтамасыз ету құралдарын жобалау және енгізу;

– қауіпсіздікті қамтамасыз етуді басқару;

– жаңа қатерлер мен сын-қатерлер туындаған жағдайда қауіпсіздікті қамтамасыз ету бойынша қабылданып жатқан шараларды қайта бағалау [4].

Еуропа Кеңесінің 2000 жылғы «киберқылмыс туралы» Конвенциясы алғаш рет қатысушы елдерге ұлттық заңнамаға киберкеңістік саласындағы қылмыстар үшін қылмыстық жауаптылық туралы нормалардың бірыңғай жүйесін енгізуді ұсынды [5,467б.].

Конвенция үш негізгі мақсатты көздейді: киберқылмыстардың құрамын анықтайды, әртүрлі елдерде қолданылатын тиісті нормаларды біріздендіру бойынша ұсыныстарды қамтиды, сондай-ақ осындай қылмыстармен бірлесіп күресудің заңды рәсімдері мен құралдарын ашады.

Конвенцияның 1-бабында компьютерлік жүйе және компьютерлік деректер ұғымдары берілген. Компьютерлік жүйе дегеніміз – өзара байланысты немесе іргелес құрылғылардың кез-келген құрылғысы немесе тобы, олардың біреуі немесе одан көп бағдарламаға сәйкес әрекет ете отырып, деректерді автоматтандырылған өңдеуді жүзеге асырады. Компьютерлік деректер – бұл компьютерлік жүйеде өңдеуге жарамды формадағы фактілердің, ақпараттың немесе ұғымдардың кез-келген көрінісі, соның ішінде компьютерлік жүйені белгілі бір функцияны орындауға мәжбүр ететін бағдарламалар. Конвенция қылмыстарды 4 топқа бөледі және әрқайсысында бірнеше қылмыс құрамы қарастырылған:

1) компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы қылмыстар:

– заңсыз қол жеткізу;

– заңсыз ұстау;

– деректерге әсер ету;

– жүйенің жұмысына әсері;

– құрылғыларды заңсыз пайдалану.

2) компьютерлік құралдарды пайдалануға байланысты құқық бұзушылықтар:

– компьютерлік технологияларды қолданатын жалғандық;

– компьютерлік технологияларды қолдану арқылы алаяқтық.

3) деректердің мазмұнына байланысты құқық бұзушылықтар:

– балалар порнографиясымен байланысты қылмыстар;

4) авторлық құқықты және сабақтас құқықтарды бұзумен байланысты құқық бұзушылықтар.

Конвенцияның нормалары келесі бағыттардағы мәселелерді шешуге бағытталған:

– қылмыстық – құқықтық сипаттағы мәселелер.

Конвенция әрбір ел ұлттық қылмыстық заңнамаға тізбесі Конвенцияда келтірілген әрекеттерді енгізуі тиіс деп ұйғарады;

– процессуалдық мәселелер.

Әрбір тарап өзінің құзыретті органдарының компьютерлік жүйеде сақталатын ақпарат ағындары туралы деректерді қоса алғанда, нақты компьютерлік деректердің сақталуын жедел қамтамасыз ету мүмкіндігіне ие болуы үшін қажетті заңнамалық және өзге де шараларды қабылдайды, атап айтқанда, бұл компьютерлік деректер әсіресе жоғалту немесе өзгеру қаупіне ұшырайды деп пайымдауға негіз болған кезде (16-бап). Әрбір тарап ақпарат ағындары туралы деректердің сақталуын және ашылуын қамтамасыз етеді (17-бап).

19-бапқа сәйкес әрбір тарап өзінің құзыретті органдарына компьютерлік жүйелерге немесе олардың бөліктеріне, сондай-ақ оларда сақталатын компьютерлік деректерге тінту немесе өзге де ұқсас қол жеткізу өкілеттіктерін беру үшін талап етілуі мүмкін заңнамалық және өзге де шараларды қабылдайды.

– халықаралық ынтымақтастық мәселелері.

Тараптар компьютерлік жүйелермен және деректермен байланысты қылмыстарға қатысты тергеп-тексеру немесе сот қудалауын жүргізу немесе электрондық нысанда қылмыс бойынша дәлелдемелер жинау мақсатында бір-бірімен барынша кең ынтымақтастықты жүзеге асырады. Тараптар компьютерлік жүйелермен және деректермен байланысты қылмыстарға байланысты тергеу немесе сот талқылауын жүргізу немесе электрондық нысанда қылмыс бойынша дәлелдемелер жинау мақсатында мүмкіндігінше бір-біріне өзара негізде барынша құқықтық көмек көрсетеді. Төтенше жағдайларда тараптар факсимильді байланысты немесе электрондық поштаны қоса алғанда, жедел байланыс құралдарын пайдалана отырып, өзара көмек туралы сұрау салуларды немесе осындай сұрау салуларға байланысты хабарламаларды осындай құралдар қауіпсіздіктің тиісті деңгейлерін және түпнұсқалығын растауды (қажет болған жағдайда шифрлауды пайдалануды қоса алғанда) қамтамасыз ететіндей шамада, кейіннен ресми растаумен жібере алады, егер сұралған тарап талап етсе. Сұрау салынатын тарап осындай сұрау салуды қабылдайды және оған кез келген ұқсас жедел байланыс құралдарының көмегімен жауап береді. Кез келген тарап екінші тараптың аумағында орналасқан компьютерлік жүйеде сақталатын және оларға қатысты Сұрау салушы тарап өзара көмек шеңберінде тінту немесе қол жеткізуді қамтамасыз ететін ұқсас іс-әрекеттер туралы, осы деректерді алу туралы немесе сақтауды қамтамасыз ету немесе жария ету туралы өтініш жіберуге ниеттенетін деректердің сақталуын шұғыл қамтамасыз етуді сұрай алады (29-баптың 1-бөлігі). Әрбір тарап компьютерлік жүйелер мен деректерге қатысы бар қылмыстарды тергеу немесе сот талқылауы мақсатында немесе қылмыстар бойынша электрондық нысанда дәлелдемелер жинау мақсатында шұғыл көмек көрсетуді қамтамасыз ету үшін аптасына жеті күн (24/7) тәулігіне 24 сағат жұмыс істейтін байланыс орталығын тағайындайды. Мұндай көмек мынадай шараларға жәрдемдесуді немесе тікелей қолдануды қамтиды: техникалық

консультациялық көмек көрсету, деректердің сақталуын қамтамасыз ету, дәлелдемелерді жинау, заңды ақпарат беру және күдікті адамдардың болуын анықтау.

32-бап ерекше қызығушылық тудырады, оның ережелеріне сәйкес тарап екінші тараптың келісімінсіз жасай алады:

a) географиялық орналасуына қарамастан жалпыға қолжетімді (ашық көзге) компьютерлік деректерге қол жеткізуге;

b) өз аумағындағы компьютерлік жүйе арқылы екінші тараптың аумағында сақталатын компьютерлік деректерге қол жеткізуге немесе егер бұл тараптың осы деректерді осы тарапқа ашуға заңды өкілеттігі бар адамның заңды және ерікті келісімі болса.

А.Г. Волеводз іс жүзінде қажетті компьютерлік ақпаратты табу және алу мақсатында шетелде компьютерлік желілерде (немесе компьютерлік деректерді сақтауға арналған ортада) тінту жүргізуден басқа ештеңені реттемейтін норма екенін дұрыс айтады. Ғаламдық компьютерлік желілердің архитектурасын ескере отырып, әлемнің кез-келген елінде шетелде сақталған немесе өзі (физикалық серверлері бар) компьютерлік деректерге (телекоммуникация желілері арқылы берілетін хабарламалар туралы мәліметтерге де, хабарламалардың өздеріне де) қол жеткізудің заңды техникалық тетіктері бар нақты қызмет көрсетушіні (провайдерді) табуға болады) шетелдік пайдаланушының компьютерлік деректерін сақтайды. Мұндай жағдайларда шет мемлекеттің аумағында компьютерлік ақпаратқа қол жеткізу шет мемлекеттің егемендік құқықтарын бұза отырып, іс жүзінде бақылаусыз жүзеге асырылатын болады [6,23 б.].

Халықаралық ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған бірнеше құжаттардың бірі 2009 жылғы 16 маусымда Екатеринбургте қол қойылған Шанхай Ынтымақтастық Ұйымына мүше мемлекеттердің «халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы» үкіметаралық келісімі болды. Келісімде халықаралық ақпараттық қауіпсіздікке төнетін қауіптердің негізгі тізбесі ашылады:

1) ақпараттық қаруды әзірлеу және қолдану, ақпараттық соғысты дайындау және жүргізу;

2) ақпараттық терроризм;

3) ақпараттық қылмыс;

4) басқа мемлекеттердің мүдделері мен қауіпсіздігіне нұқсан келтіре отырып, ақпараттық кеңістікте үстем жағдайды пайдалану;

5) басқа мемлекеттердің қоғамдық-саяси және әлеуметтік-экономикалық жүйелеріне, рухани, адамгершілік және мәдени ортасына зиян келтіретін ақпаратты тарату;

6) табиғи және (немесе) техногендік сипаттағы жаһандық және Ұлттық ақпараттық инфрақұрылымдардың қауіпсіз, тұрақты жұмыс істеуіне қауіп төндіреді.

Келісімге 1-қосымшада халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі ұғымдардың тізбесі, ал 2 – қосымшада-халықаралық ақпараттық қауіпсіздік саласындағы қауіптердің негізгі түрлерінің, олардың көздері мен белгілерінің тізбесі келтіріледі. Мәселен, ақпараттық қылмыс ақпараттық ресурстарды пайдалану және (немесе) оларға ақпараттық кеңістікте құқыққа қайшы мақсаттарда әсер ету ретінде айқындалады. Бұл қауіптің көзі ақпараттық ресурстарды заңсыз пайдалануды немесе мұндай ресурстарға қылмыстық мақсатта рұқсатсыз араласуды жүзеге асыратын адамдар немесе ұйымдар болып табылады. Оның белгілері ақпараттың тұтастығын, қолжетімділігін және құпиялылығын бұзу үшін ақпараттық жүйелерге ену; компьютерлік вирустарды және басқа да зиянды бағдарламаларды қасақана дайындау және тарату; DOS-шабуылдарды (қызмет көрсетуден бас тарту) және өзге де теріс әсерлерді жүзеге асыру; ақпараттық ресурстарға зиян келтіру болып табылады; ақпараттық саладағы азаматтардың заңды құқықтары мен бостандықтарын, соның ішінде зияткерлік меншік және жеке өмірге қол сұғылмаушылық құқықтарын бұзу; алаяқтық, ұрлық, бопсалау, контрабанда, есірткінің заңсыз саудасы, балалар порнографиясын тарату және т.б. сияқты қылмыстар жасау үшін ақпараттық ресурстар мен әдістерді пайдалану.

Келісімде ұсынылған ақпараттық қылмыс ұғымын сәтті деп тану мүмкін болмаса да, оған қол қою өте маңызды деп айту керек, өйткені онда ынтымақтастықтың негізгі бағыттары,

принциптері, формалары мен тетіктері анықталған, халықаралық ақпараттық қауіпсіздіктің негізгі қауіптері талданған.

1) егер бұл әрекет ақпаратты жоюға, бұғаттауға, түрлендіруге не көшіруге, ЭЕМ жүйесі немесе олардың желісі жұмысының бұзылуына әкеп соқтырса, заңмен қорғалатын компьютерлік ақпаратқа заңсыз қол жеткізуді жүзеге асыру;

2) зиянды бағдарламаларды құру, пайдалану немесе тарату;

3) егер бұл әрекет елеулі зиян немесе ауыр зардаптар әкелсе, ЭЕМ-ге, ЭЕМ жүйесіне немесе олардың желісіне қолжетімділігі бар адамның ЭЕМ-ді, ЭЕМ жүйесін немесе олардың желісін пайдалану қағидаларын бұзуы, ЭЕМ-нің заңмен қорғалатын ақпаратының жойылуына, бұғатталуына немесе модификациялануына әкеп соққан;

4) авторлық құқық объектілері болып табылатын компьютерлер мен дерекқорларға арналған бағдарламаларды заңсыз пайдалану, сол сияқты егер бұл әрекет елеулі залал келтірсе, авторлық құқық беру.

Бұл келісім, сөзсіз, заңнаманы біріздендіру жолындағы маңызды қадам болды, ол қазіргі уақытта кем дегенде ТМД елдерінің деңгейінде, ал одан әрі жоғары деңгейде қажет.

«Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстарға қарсы күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы» 2019 жылғы 9 желтоқсанда №277-VI ҚРЗ Қазақстан Республикасының заңымен ратификацияланды [7].

Жүргізілген талдау әлемдік қоғамдастықтың ақпараттық қауіпсіздікті қамтамасыз етудің маңыздылығын бұрыннан түсінгенін көрсетеді.

Әдебиет

1. Конвенция о защите прав человека и основных свобод (заключена в Риме 04.11.1950). URL: http://www.echr.coe.int/Documents/Convention_RUS.pdf (дата обращения: 14.01.2015).

2. A/RES/68/167 21.01.2014 «Право на неприкосновенность личной жизни в цифровой век». URL: http://un.org/.

3. A/RES/55/63 22.01.2001 «Борьба с преступным использованием информационных технологий .URL: http://un.org/

4. A/RES/57/239 31.01.2003 «Создание глобальной культуры кибербезопасности». URL: http://un.org/

5. Конвенция Совета Европы о киберпреступности от 23 ноября 2001г. // Международное уголовное право в документах, в 2 т. – т. 1. – Казань: Казанский государственный университет В.И. Ульянова-Ленина, 2005. – С. 467-482.

6. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – №2. – С. 23.

7. Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы Қазақстан Республикасының Заңы 2019 жылғы 9 желтоқсан №277-VI ҚРЗ.

«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 ІІМ Мақан Есболатов атындағы Алматы академиясында (2024 жылғы 20 қыркүйек) әр елдің ғалымдарын, сарапшылары мен құқық қорғау органдарының өкілдерін жинаған «Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында қылмысқа қарсы іс-қимыл» конференциясы цифрлық қылмыстың маңызды аспектілерін және оның алдын алу мен жолын кесу бойынша тиімді шараларды әзірлеуді қарастырды.

Конференция келесі негізгі тұжырымдар мен ұсыныстарды ескерді:

Цифрлық қылмыс жеке азаматтардың да, жалпы қоғамның да қауіпсіздігіне үлкен қауіп төндіреді. Ол кибералаяқтық, кибертыңшылық, кибертерроризм және сол сияқты шабуылдардың әртүрлі түрлерін қамтиды.

Конференцияға қатысушылар соңында цифрлық қылмыс деңгейі үнемі өсіп келеді және оның алдын алу және күресу үшін әлемдік деңгейдегі күш-жігерді күшейту маңызды деген қорытындыға келді.

Жасанды интеллект және кванттық есептеу сияқты технологиялардың дамуы киберқылмыскерлер үшін жаңа мүмкіндіктер туғызады, сол себепті ақпарат пен киберқауіпсіздікті қорғаудың жаңа әдістері мен технологияларын әзірлеу қажет.

Конференция цифрлық қылмысқа қарсы күресте халықаралық ынтымақтастықтың маңыздылығын көрсетеді. Сондықтан елдер киберқауіпсіздік стандарттары мен шараларын бірлесіп әзірлеп, енгізуі керек.

Цифрлық қылмыстың қауіптілігі туралы білім беру және хабардарлықты арттыру, онымен күресудің маңызды құрамдас бөлігі болып табылады. Қоғам, кәсіпорындар мен ұйымдар үшін білім беру бағдарламаларын және киберқауіпсіздік науқандарын күшейту қажет.

Конференция құқық қорғау органдарының цифрлық қылмысқа қарсы күрестегі рөлін нығайтуға шақырады және тергеу әдістерін жетілдіру және басқа органдармен ынтымақтастық бойынша ұсыныстар береді.

Конференция сонымен қатар цифрлық қылмысқа қарсы іс-қимылды күшейту мақсатында басқа елдер мен ұйымдар арасында ақпарат алмасуға және үздік тәжірибелерді беруге жәрдемдесуге дайын екендігін білдіреді.

Қорытындылай келе, «Қоғам мен мемлекетті цифрландыру және ақпараттандыру жағдайында қылмысқа қарсы іс-қимыл» конференциясы цифрлық қылмыстың қауіп-қатерінің ауырлығын атап көрсетеді және оны болдырмау, алдын алу бойынша тиімді шараларды әзірлеп, енгізу үшін барлық мүдделі тараптарды бірлескен күш-жігерге шақырады.

РЕЗОЛЮЦИЯ
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 (22 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

Беттеу:
Калпак Ж.М.

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу
және редакциялық-баспа жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 31 желтоқсан 2024 ж. жіберілді.
Пішімі 60х84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 8.
Таралымы 100.