ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

НАУЧНО-КОНСУЛЬТАТИВНЫЙ СОВЕТ ПРИ СОВЕТЕ МИНИСТРОВ ВНУТРЕННИХ ДЕЛ
ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

БЮРО ПО КООРДИНАЦИИ БОРЬБЫ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ
И ИНЫМИ ОПАСНЫМИ ВИДАМИ ПРЕСТУПЛЕНИЙ НА ТЕРРИТОРИИ
ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ НА ПРОСТРАНСТВЕ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Аналитический обзор с предложениями

МОСКВА 2023

УДК 343.79

А в т о р с к и й к о л л е к т и в:

Н. Н. Дьяченко, ведущий научный сотрудник 3 отдела НИЦ № 3,
кандидат юридических наук;
О. А. Надейкина, старший научный сотрудник 2 отдела НИЦ № 3;
Д. В. Кирган, старший научный сотрудник ученого совета;
И. А. Грозан, заместитель начальника ОНИПНКиОДНС ЦООНД;
В. А. Казакова, главный научный сотрудник 3 отдела НИЦ № 3,
доктор юридических наук, профессор
(ВНИИ МВД России);
О. И. Новосельцев, начальник Управления организационно-правового
и информационно-аналитического обеспечения;
О. В. Демковец, старший инспектор по особым поручениям,
кандидат юридических наук, доцент
(БКБОП)

Современное состояние и тенденции развития киберпреступности на пространстве Содружества Независимых Государств : аналитический обзор с предложениями / Н. Н. Дьяченко, О. А. Надейкина, Д. В. Кирган, И. А. Грозан, В. А. Казакова, О. И. Новосельцев, О. В. Демковец. – Москва : ВНИИ МВД России, 2023. – 72 с.

Проанализированы способы предупреждения и борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий и их эффективность.

Для сотрудников правоохранительных органов, курсантов и слушателей образовательных организаций, а также представителей государственных органов стран Содружества, уставных и отраслевых органов СНГ, занимающихся вопросами борьбы с преступностью в сфере информационных технологий.

УДК 343.79

ВВЕДЕНИЕ

Актуальность рассматриваемой темы обусловлена существованием юридических и социально значимых проблем, не позволяющих в полной мере эффективно предупреждать и бороться с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий[1], отдельным несовершенством механизмов международного сотрудничества между правоохранительными органами в данной сфере, необходимостью решения теоретических и практических задач противодействия современной компьютерной преступности, разработки эффективной системы мер борьбы и предупреждения компьютерных преступлений, совершенствования уголовного, гражданского и информационного законодательства.

Согласно статистическим данным на территориях государств – участников Содружества Независимых Государств[2] наблюдается ежегодный рост преступлений, совершаемых с использованием ИКТ, что порождает необходимость в адекватном ответе со стороны правоохранительных органов. Так, например, актуальные проблемы сотрудничества органов внутренних дел стран Содружества в борьбе с киберпреступностью неоднократно рассматривались на заседаниях Совета министров внутренних дел государств – участников Содружества Независимых Государств[3], в результате которых были приняты решения, направленные на выработку соответствующих мер противодействия им.

Во исполнение Межгосударственной программы совместных мер борьбы с преступностью на 2019–2023 годы, Решения СМВД от 31 мая 2019 г. (г. Ташкент, Республика Узбекистан) и протокольных поручений Совета от 8 сентября 2022 г. (г. Чолпон-Ата, Кыргызская Республика) и 24 мая 2023 г. (г. Алматы, Республика Казахстан) состоялась Международная научно-практическая конференция под эгидой СМВД на тему «Киберпреступность на пространстве Содружества Независимых Государств: современные тенденции и направления противодействия». Целью конференции является ана-

[1] Далее – ИКТ.
[2] Далее также – государства – участники СНГ, страны Содружества.
[3] Далее – СМВД.

лиз состояния, актуальных проблем и перспектив развития сотрудничества органов внутренних дел государств – участников СНГ в борьбе с ИКТ в современных условиях. Предложения участников конференции могут лечь в основу дальнейшего совершенствования сотрудничества министерств внутренних дел государств – участников СНГ в указанной сфере.

При проведении настоящего научного исследования была проанализирована деятельность органов внутренних дел государств – участников СНГ в части борьбы с киберпреступностью[4], исследованы нормативные правовые акты, обобщены статистические данные, изучена научная литература по рассматриваемой проблематике. Обзор основан на материалах, поступивших из министерств внутренних дел стран Содружества, где была охарактеризована практика борьбы с преступлениями, совершаемыми с использованием ИКТ.

Результаты научного исследования рекомендуются для использования в деятельности сотрудников правоохранительных органов и иных государственных органов стран Содружества.

[4] Определение киберпреступности и другие связанные с ней термины, используемые в настоящей работе, содержатся в Приложении 2.

1. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ НА ТЕРРИТОРИЯХ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Информационно-коммуникационные технологии в настоящее время стали одной из наиболее распространенных, глобальных форм человеческой деятельности, определяющих динамику развития мировой экономики и зависимых от нее ниш и сегментов. Глобальная тенденция цифровизации сокращает временные, материальные, административные и иные издержки в любых видах процессов и сделок. Однако помимо несомненной пользы обществу, она породила ряд проблем, одной из которых выступает использование ИКТ в преступных целях.

Сегодня киберпреступность активно выходит на лидирующие позиции наравне с торговлей оружием, наркоторговлей и проституцией, о чем все громче заявляют правоохранители.

В рамках СНГ сформирована нормативная правовая база межгосударственного (многосторонние и двусторонние соглашения), межведомственного, а также национального уровня, регламентирующая вопросы борьбы с преступлениями, совершаемыми с использованием ИКТ.

Преступления против информационной безопасности описаны соответствующим разделом 12 главы 30 модельного Уголовного кодекса (постановление Межпарламентской Ассамблеи государств участников СНГ от 17 февраля 1996 г., г. Санкт-Петербург). Кроме того, в иных разделах Кодекса содержится ряд статей, предусматривающих ответственность за совершение преступлений, связанных с незаконным использованием компьютеров или компьютерной информации.

В целях координации действий по созданию правового механизма противодействия киберпреступности, а также для унификации правовых норм 14 апреля 2023 г. МПА СНГ одобрен модельный закон «О противодействии киберпреступности». В данном Законе предложена терминология в области обеспечения кибербезопасности, представлены меры профилактики киберпреступлений, которые направлены на устранение основных причин совершения таких преступлений, перечислены виды киберпреступлений, в том числе включены отдельные виды, которые уже предусмотрены в уголовных кодексах Республик Казахстан и Молдова. Также в модельный закон включены положения

об основных направлениях повышения эффективности деятельности государственных органов в области противодействия киберпреступности, таких как обеспечение безопасности и киберустойчивости функционирования информационной инфраструктуры государства, в том числе критической информационной инфраструктуры, совершенствование правоохранительной деятельности, обеспечение кибербезопасности в кредитно-финансовой сфере, защита персональных данных, развитие государственно-частного партнерства. Отдельно оговорена рекомендация по созданию национального координационного органа по обеспечению кибербезопасности.

Взаимодействие органов внутренних дел государств – участников СНГ в сфере борьбы с киберпреступлениями определяется следующими документами:

Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (СГГ СНГ от 22 января 1993 г., г. Минск);

Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (СГГ СНГ от 7 октября 2002 г., г. Кишинев);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступностью (СГГ СНГ от 25 ноября 1998 г., г. Москва);

Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (СГГ СНГ от 1 июня 2001 г., г. Минск);

Соглашение об обмене информацией в сфере борьбы с преступностью (СГГ СНГ от 22 мая 2009 г., г. Астана);

Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий (СГГ СНГ от 25 октября 2013 г., г. Минск);

Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности (СГГ СНГ от 20 ноября 2013 г., г. Санкт-Петербург);

Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества в период до 2025 года (СГП 16 октября 2016 г., г. Минск);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (СГГ СНГ от 28 сентября 2018 г., г. Душанбе)[5];

[5] Документ вступил в силу для следующих государств: Республика Беларусь (12 марта 2020 г.), Кыргызская Республика (12 марта 2020 г.), Республика Узбекистан (12 марта

Стратегия обеспечения информационной безопасности государств – участников Содружества Независимых Государств (СГГ СНГ от 25 октября 2019 г., г. Москва);

Стратегия экономического развития Содружества Независимых Государств на период до 2030 года (СГП СНГ от 29 мая 2020 г.);

Межгосударственная программа совместных мер борьбы с преступностью на 2019–2023 годы (СГГ СНГ от 28 сентября 2018 г., г. Душанбе).

На межведомственном уровне действуют следующие нормативные правовые документы:

Соглашение о взаимодействии министерств внутренних дел независимых государств в сфере борьбы с преступностью (СМВД от 24 апреля 1992 г., г. Алма-Ата);

Соглашение о взаимодействии министерств внутренних дел в сфере обмена информацией (СМВД от 3 августа 1992 г., г. Чолпон-Ата).

Регламент согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран СНГ в сфере современных информационных технологий (СМВД от 20 июля 2018 г., г. Баку).

В целях понимания особенностей механизмов противодействия киберпреступности в странах Содружества рассмотрим сведения о состоянии борьбы с этим негативным явлением в государствах – участниках Содружества Независимых Государств.

Азербайджанская Республика

Азербайджанская Республика присоединилась к Конвенции о преступности в сфере компьютерной информации (23 ноября 2001 г., г. Будапешт)[6]. Взаимодействие с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ, по информации Министерства осуществляется на основе двусторонних соглашений по борьбе с преступностью.

2020 г.), Республика Казахстан (06.06.2020), Республика Армения (22 января 2022 г.), Российская Федерация (17 июля 2022 г.) // СПС КосультантПлюс (дата обращения: 14.02.2023). Далее также – Соглашение.

[6] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). Конвенция вступила в силу 1 июля 2004 г..

В Уголовном кодексе Азербайджанской Республики[7] закреплен ряд статей, устанавливающих ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ[8].

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ в МВД Азербайджанской Республики, входят в компетенцию Главного управления по борьбе с организованной преступностью.

Республика Армения

В 2022 г. вступил в силу новый Уголовный Кодекс Республики Армения[9], 38 глава которого посвящена преступлениям, направленным против компьютерной системы и безопасности компьютерных данных. УК Армении также предусматриваются преступления, где компьютер является орудием или средством преступления[10].

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ, входят в функциональные обязанности следующих структурных подразделений главного управления по противодействию киберпреступности[11] Полиции МВД Республики Армения.

1. Имущественные преступления – отдел по борьбе с преступлениями, совершаемыми в сфере высоких технологий Управления оперативно-розыскной информации и по борьбе с компьютерными преступлениями ГУКП Полиции МВД Республики Армения.

2. Незаконный оборот наркотиков – отдел по борьбе с незаконным оборотом наркотиков по Интернет сети Управления по борьбе с незаконным оборотом наркотиков ГУКП Полиции МВД Республики Армения.

3. Терроризм и экстремизм – отдел по борьбе с терроризмом и экстремизмом Управления розыска, по борьбе с незаконной миграцией и терроризмом ГУКП Полиции МВД Республики Армения.

4. Экономические преступления – отдел по борьбе с преступлениями в финансово-кредитной сфере Управления по борьбе с преступлениями против человека и собственности ГУКП Полиции МВД Республики Армения.

---

[7] Далее – УК Азербайджана.
[8] См.: Приложение 1.
[9] Далее – УК Армении.
[10] См.: Приложение 1.
[11] Далее – ГУКП.

Республика Беларусь

Международное сотрудничество по оперативному обмену информацией в рамках противодействия преступлениям в сфере информационных технологий осуществляется на основании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.[12], соглашений о сотрудничестве между МВД Республики Беларусь и МВД рядом зарубежных государств, в том числе с МВД Российской Федерации[13] от 30 сентября 1997 г., а также посредством международной сети национальных контактных пунктов «24/7», функционирующей под эгидой Римско-Лионской подгруппы «Группы Восьми».

В Уголовном кодексе Республики Беларусь[14] установлена уголовная ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ, также использование ИКТ в некоторых случаях установлено в качестве квалифицирующего признака. Вместе с тем практика показывает, что с использованием ИКТ совершаются и иные преступления (наиболее часто встречаются клевета и оскорбление, менее распространены доведение до самоубийства и склонение к самоубийству) [15].

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ, входят в функциональные обязанности представителей криминальной милиции МВД Республики Беларусь в Главном управлении по противодействию киберперступности, в Главном управлении по наркоконтролю и противодействию торговле людьми.

Республика Казахстан

Для взаимодействия с правоохранительными органами зарубежных государств и обмена информацией в Центре по борьбе с киберпреступностью Департамента криминальной полиции МВД Республики Казахстан функционирует Национальный контактный пункт

---

[12] Утверждено Указом Президента Республики Беларусь от 7 сентября 2001 г. № 475 «Об утверждении Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

[13] Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством внутренних дел Республики Беларусь (заключено в г. Москве 30 сентября 1997 г.).

[14] Далее – УК Беларуси.

[15] См.: Приложение 1.

«24/7», который ранее образован под эгидой «Группы восьми» (G8) для обмена оперативной информацией в сфере борьбы с киберпреступлениями.

Взаимодействие с правоохранительными органами стран Содружества осуществляется в рамках Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (СГГ СНГ от 28 сентября 2018 г., г. Душанбе)[16].

По фактам совершения уголовных правонарушений в сфере ИКТ, ответственность за которые предусмотрена в статьях главы 7 Уголовного Кодекса Республики Казахстан[17], проводится достаточно эффективная работа по предупреждению и профилактике, результатами которых является высокий процент раскрываемости уголовных правонарушений и сокращение фактов их совершения[18].

Кыргызская Республика

Кыргызская Республика осуществляет собственное движение к цифровой трансформации национальной экономики и обеспечению доступа граждан к современным цифровым сервисам. Построение цифровой экономики рассматривается как необходимое условие и национальный приоритет развития Кыргызской Республики на краткосрочную и среднесрочную перспективы. Контуры стратегии цифровой трансформации кыргызской экономики формируются в рамках Концепции цифровой трансформации «Цифровой Кыргызстан 2019–2023», одобренной решением Совета безопасности Кыргызской Республики от 14 декабря 2018 г. № 2.

Республикой заключены следующие соглашения, направленные на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ:

Соглашение о сотрудничестве между Министерством внутренних дел Республики Кыргызстан и Министерством внутренних дел Республики Узбекистан (13 мая 1992 г., г. Ош);

[16] Ратифицировано Законом Республики Казахстан от 9 декабря 2019 г. № 277-VI ЗРК.
[17] Далее – УК Казахстана.
[18] См.: Приложение 1.

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и МВД Российской Федерации (16 июня 2007 г., г. Санкт-Петербург);

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и Министерством внутренних дел Республики Казахстан (4 сентября 2014 г., г. Чолпон-Ата);

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и Министерством внутренних дел Республики Таджикистан (4 сентября 2014 г., г. Чолпон-Ата).

К законодательству Кыргызской Республики в сфере кибербезопасности могут быть отнесены:

1. Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы (утверждена постановлением Правительства Кыргызской Республики от 24 июля 2019 г. № 369 «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы»).

2. Национальная стратегия развития Кыргызской Республики на 2018–2040 годы (утверждена указом Президента Кыргызской Республики от 31 октября 2018 г. УП № 221 «О Национальной стратегии развития Кыргызской Республики на 2018–2040 годы»).

3. Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы (утверждена постановлением Правительства Кыргызской Республики от 3 мая 2019 г. № 209 «О Концепции информационной безопасности Кыргызской Республики на 2019–2023 годы»).

4. Концепция цифровой трансформации «Цифровой Кыргызстан 2019–2023» (утверждена Решением Совета безопасности Кыргызской Республики от 14 декабря 2018 г. № 2 у).

5. Концепция национальной безопасности Кыргызской Республики (утверждена Указом Президента Кыргызской Республики от 20 декабря 2021 г. № 570 «О Концепции национальной безопасности Кыргызской Республики»).

6. Законы Кыргызской Республики от 19 июля 2017 № 127 «Об электронном управлении», от 14 апреля 2008 г. № 58 «Об информации персонального характера», от 15 декабря 2017 г. № 210 (15) «О защите государственных секретов Кыргызской Республики».

Постановлением Правительства Кыргызской Республики от 21 мая 2020 г. № 266 «О некоторых вопросах в сфере обеспечения кибербезопасности Кыргызской Республики» было утверждено «Положение о Координационном центре по обеспечению кибербезопасности Госу-

дарственного комитета национальной безопасности Кыргызской Республики», также утвержден главный уполномоченный орган в сфере обеспечения кибербезопасности, реагирования на компьютерные инциденты, а также по выявлению, предупреждению и пресечению причин и условий, способствующих подготовке и реализации компьютерных атак – Государственный комитет национальной безопасности.

Уголовным Кодексом Кыргызской Республики[19] с квалифицирующим признаком использования ИКТ предусмотрен ряд статей в сфере имущественных преступлений, в экономической сфере, а также иные составы преступлений, где в качестве квалифицирующего признака предусмотрено использование ИКТ.

В то же время в статьях, устанавливающих уголовную ответственность за преступления в сфере незаконного оборота наркотиков и преступлениях против несовершеннолетних, в качестве квалифицирующего признака использование ИКТ не предусмотрено. Также не предусмотрены санкции за преступления, где объектом посягательства, предметом или орудием, используемым при совершении преступлений выступают цифровые финансовые активы, в том числе токены и криптовалюта[20].

Республика Молдова

Двусторонние соглашения, направленные на организацию взаимодействия правоохранительных органов других стран в целях предупреждения выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ в Республике отсутствуют.

Ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ, установлена Уголовным кодексом Республики Молдова[21] за имущественные преступления, преступления в сфере незаконного оборота наркотических средств и психотропных веществ, преступления в экономической сфере, преступления экстремисткой направленности, преступления, совершаемые против несовершеннолетних. Также внесены предложения в УК Молдовы по регулированию «Незаконных операций с безналичными средствами платежа» [22].

[19] Далее – УК Кыргызстана.
[20] См.: Приложение 1.
[21] Далее – УК Молдовы.
[22] См.: Приложение 1.

Российская Федерация

В декабре 2020 г. принято решение о создании в МВД России киберполиции, в Следственном департаменте МВД России и территориальных органах предварительного следствия сформированы специализированные подразделения по расследованию преступлений, совершенных с использованием ИКТ. В 2022 г. в МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий[23].

С 2013 г. в Российской Федерации образована и действует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, которой обеспечение информационной безопасности по сервисной модели осуществляется в соответствии с требованиями и методическими рекомендациями ФСБ России и ФСТЭК России.

Уголовный кодекс Российской Федерации[24] в главе 28 «Преступления в сфере компьютерной информации» содержит четыре вида преступления, однако круг совершаемых с использованием информационных технологий деяний более широк[25].

Республика Таджикистан

Заключаемые республикой двусторонние соглашения, направленные на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ, опираются на «Конвенцию о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам» (22 января 1993 г., г. Минск).

В настоящее время на основе протокола, подписанного в рамках переговоров между Департаментом общественной безопасности города Нанкина КНР и Управлением МВД по городу Душанбе, осуществляется совместная реализация договоренностей и сотрудничество, направленное на поощрение и внедрение устойчивых передовых методов предупреждения и пресечения преступлений, фактов присоединения граждан республики к международным террористическим группировкам, незаконного оборота наркотиков, оружия и регио-

[23] См.: URL: мвд.рф/news/item/32844180/ (дата обращения: 19.04.2023).
[24] Далее – УК РФ.
[25] См. Приложение 1.

нальной безопасности. Периодически изучается передовой опыт Департамента общественной безопасности указанного города по обеспечению общественного порядка, борьбе с преступностью и другим приоритетным направлениям, которые непосредственно используются в практической оперативно-служебной деятельности УМВД.

В Уголовном кодексе Республики Таджикистан[26] определена отдельная глава 28 (Преступления против информационной безопасности), где квалифицирующим признаком являются деяния, связанные с информацией, хранящейся в компьютерной системе, сети или на машинных носителях. В 15 статьях УК Таджикистана в качестве квалифицирующего признака предусмотрена ответственность за использование ИКТ. Также установлены иные составы преступлений, совершаемые с использованием ИКТ[27].

Республика Узбекистан

В Республике планируется создать систему предотвращения киберпреступности и разработать Стратегию кибербезопасности Республики Узбекистан на 2023–2026 годы. Определен комплекс задач и основные направления по кибербезопасности интернет-пространства в доменной зоне «UZ», а также по защите электронного правительства, энергетики, цифровой экономики и других сфер, связанных с важной информационной инфраструктурой. Одновременно планируется пересмотреть уголовную ответственность за киберпреступность.

Система мониторинга кибератак и угроз в информационном пространстве будет и дальше совершенствоваться. Это включает в себя расширение технической инфраструктуры Единой сети кибербезопасности, дальнейшее ускорение деятельности «IT-парка инноваций в кибернетике», а также проведение на базе центров обучения цифровым технологиям в регионах обучения по кибербезопасности для молодежи, ежегодное проведение республиканских конкурсов среди учащихся и студентов по выявлению кибератак.

Статья 3 Закона Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О киберпреступности» гласит, что киберпреступность – совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов.

[26] Далее – УК Таджикистана.
[27] См.: Приложение 1.

В национальном понимании под преступлениями в сфере информационных технологий понимаются такие уголовно-запрещенные под угрозой наказания общественно-опасные деяния, которые непосредственно совершены с использованием информационных технологий и информационно-телекоммуникационных сетей, в виртуальном мире. В Узбекистане термин «киберпреступность» употребляется в тесной связи с преступлениями, совершенными с использованием информационных технологий. Но учитывая, что преступления с использованием информационных технологий является более широким понятием, нежели киберпреступность, употребления термина «киберпреступность» для обозначения широкого спектра правонарушений, включая традиционные компьютерные и сетевые преступления, не является критической ошибкой в толковании.

На данный момент двусторонних соглашений, направленных на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ в Республике Узбекистан не имеется.

Глава XXI Уголовного кодекса Республики Узбекистан[28] очерчивает спектр преступлений в сфере информационных технологий[29]. Также в уголовном законодательстве имеются преступления, где в качестве квалифицирующего признака или диспозиции предусмотрено использования информационных технологий. В связи с ростом экономических преступлений в 2022 г. было ужесточено наказание краж и мошенничеств, так как данные виды преступлений начали совершаться с использованием высоких технологий. В настоящее время ведется работа по внесению дополнений и изменений в УК Узбекистана в сфере оборота наркотических средств с использованием информационных технологий и сети Интернет, а также прорабатывается нормы упорядочивающие взаимоотношения, где объектом выступают цифровые финансовые активы, криптовалюты, а также токены.

Таким образом, анализ национальных законодательств свидетельствует различных подходах в странах Содружества к пониманию «киберпреступность», «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», а также в вопросах криминализации деяний, совершаемых в киберпространстве.

[28] Далее – УК Узбекистана.
[29] См.: Приложение 1.

2. АНАЛИЗ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИКТ НА ТЕРРИТОРИЯХ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Рассмотрим более подробно преступления, совершенные с использованием ИКТ за последние три года, на территориях государств – участников Содружества Независимых Государств.

Азербайджанская Республика

Официальный представитель «Лаборатории Касперского» в Азербайджанской Республике сообщил, что пирамида киберпреступности в 2022 г. существенно не изменилась: в ее основании разместились мошенничество, в том числе с применением средств мобильной связи, фишинг, в середине находятся атаки при помощи вирусов-шифровальщиков, требующие от злоумышленников соответствующей квалификации и навыков программирования. На вершине пирамиды находятся таргетированные кибератаки, направленные на конкретные коммерческие организации или государственные ведомства. При этом в нынешнем году эти атаки начнут усложняться, появятся новые техники и уязвимости «нулевого дня»[30].

Основная масса киберинцидентов, выявленных за 2022 г. в Азербайджанской Республике – это фишинг-атаки, социальная инженерия, создание сайтов-клонов средств массовой информации, госструктур, банков и других организаций, а также попытки взлома почтовых и иных ресурсов корпоративного сектора.

По словам начальника управления Государственной службы специальной связи и информационной безопасности в Азербайджанской Республике за 2022 г. были заблокированы 1 192 специальных индикатора безопасности, что позволило защитить госучреждения от целенаправленных кибератак[31]. Проблема кибербезопасности более чем серьезна, если принять во внимание, что в 2022 г. кибератакам под-

[30] См.: URL: https://az.sputniknews.ru/20230205/kakie-kiberugrozy-budut-aktualny-dlya-polzovateley-azerbaydzhana-v-2023-godu-451421171.html (дата обращения: 14.04.2023).

[31] См.: URL: https://caliber.az/print/143843/ (дата обращения: 14.04.2023).

верглись 97 информационных ресурсов, зарегистрированных в доменной зоне Азербайджанской Республики «Az». Расследование случившихся инцидентов выявило ряд нарушений в сфере обеспечения сетевой безопасности инфоресурсов республики. Так, 34 % веб-ресурсов были закодированы некорректно и небезопасно, а у 66 % были неверно выполнены настройки сервера, в результате чего они и подверглись хакерской атаке. При этом, несмотря на повторные нападения, в восьми из этих веб-ресурсов, меры по устранению недочетов так и не были приняты.

За последние три года в Азербайджанской Республике зарегистрировано 1 625 преступлений, совершенных с использованием ИКТ, 157 (9,7 %) из которых составляют тяжкие. Динамика рассматриваемого вида преступности характеризуется тенденцией к росту с резким скачком в 2022 г.: + 196,3 % к аналогичному показателю прошлого года.

Преобладающее большинство совершенных противоправных деяний – 1 380 (или 84,9 %) составили преступления против собственности: кража, мошенничество, вымогательство, а 233 (15,1 %) приходятся на преступления против общественной безопасности и общественного порядка, среди них: организация незаконных международных телекоммуникационных услуг с подключением к телекоммуникационной сети, незаконный оборот наркотических средств и психотропных веществ, организация и проведение азартных игр, киберпреступления.

Среди зарегистрированных преступлений против общественной безопасности и общественного порядка самое значительное число – 200 (85,9 %) приходится на долю незаконного оборота наркотических средств и психотропных веществ, на долю киберпреступлений приходится 28 (12 %) от числа совершенных.

Число зарегистрированных за последние три года преступлений против личности невелико – 12 (0,7 %) от общего числа деяний, совершенных с использованием ИКТ.

Минимальные показатели зарегистрированы по составам «Организация незаконных международных телекоммуникационных услуг с подключением к телекоммуникационной сети» – 1 преступление и «Организация и проведение азартных игр» – 4 (см. рис. 1)[32].

[32] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Азербайджанской Республики, представлена в Приложении 3.

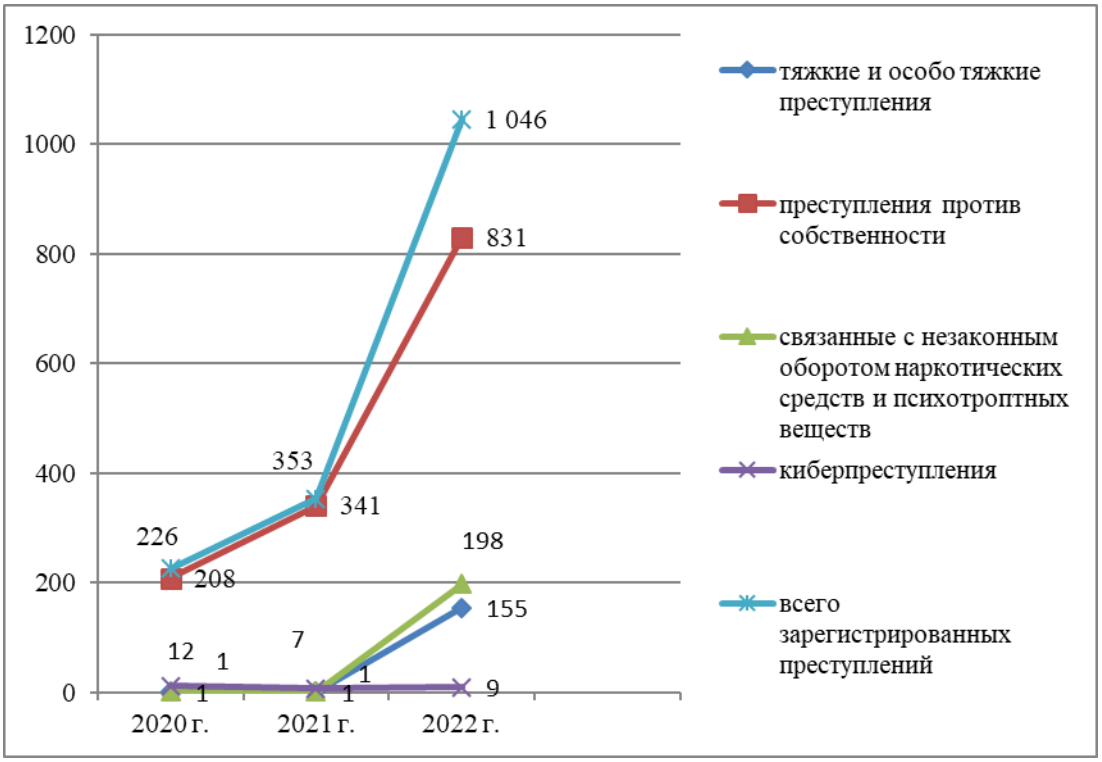

Рис. 1. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Азербайджанской Республики

Республика Армения

В Республике Армения с 2020 по 2022 г. всего возбуждено 1 997 уголовных дел, совершенных с использованием ИКТ. Прирост противоправных деяний довольно плавный (+165,4 % в 2021 г. и +92,4 % в 2020 г.).

Наибольшее значение имеют показатели по статьям «Компьютерное хищение» – количество таких преступлений за три года составило 691 (34,6 %) от всех возбужденных уголовных дел и «Электронное мошенничество» – 838 (42,0 %) от всех возбужденных уголовных дел. Значительные показатели имеет также «Незаконный оборот наркотиков» – 137 (7 %) и «Неправомерное завладение компьютерной информацией» – 169 (8,5 %) соответственно.

Минимальное число возбужденных уголовных дел приходится на экономические преступления, совершенные с использованием ИКТ, а также на составы «Разглашение врачебной тайны», «Применение насилия против представителя власти», «Публичные призывы к терроризму, финансированию терроризма и международному терроризму, публичное оправдание или пропаганда совершения указанных преступлений» – суммарно таких преступлений за 2020 и 2021 гг. совершено 8 (по одному в каждый год по конкретному составу),

в 2022 г. уголовные дела по рассматриваемым составам не возбуждались (см. рис. 2)[33].

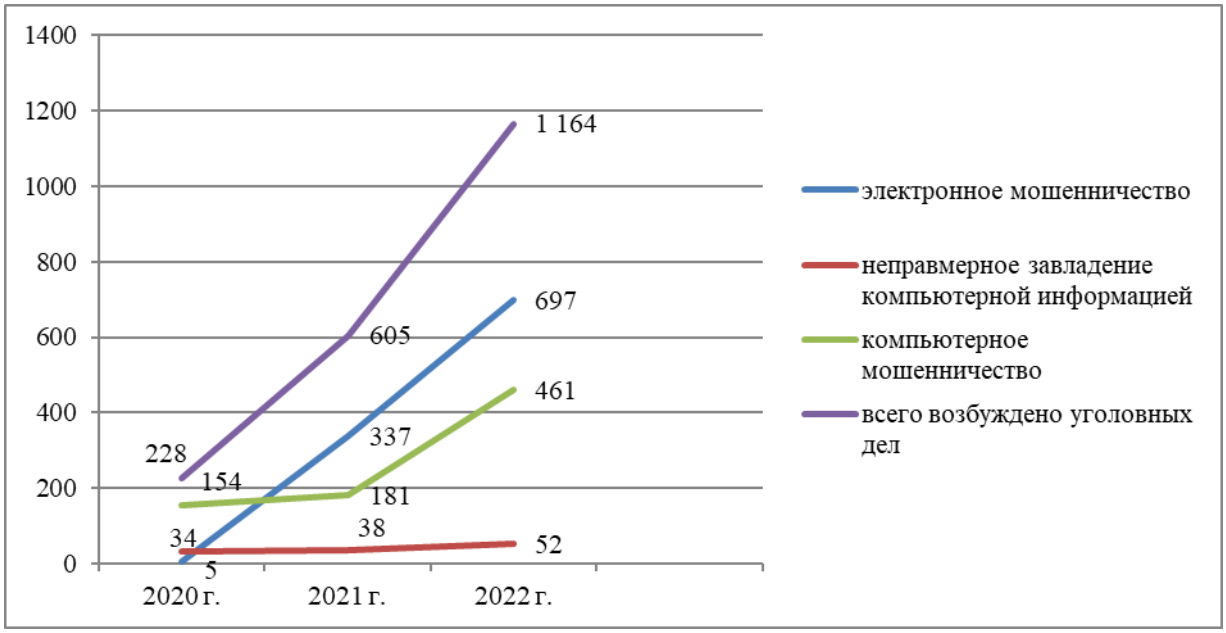

Рис. 2. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Армения

Республика Беларусь

По информации МВД Республики Беларусь, каждое второе преступление из числа зарегистрированных в 2022 г. совершено с использованием сети Интернет[34]. Генеральный прокурор Республики Беларусь, выступая на совместном заседании палат Национального собрания, отметил, что, несмотря на снижение в 2022 г. числа совершенных киберпреступлений, остаются актуальными вопросы их профилактики и пресечения. По его словам, удельный вес таких деяний в структуре преступности остается значительным – больше 16 %.

В Республике Беларусь с 2020 по 2022 г. возбуждено 54 811 уголовных дел по преступлениям, совершенным с использованием ИКТ.

На протяжении последних трех лет максимальное количество противоправных деяний приходится на составы: «Хищение путем модификации компьютерной информации» – 50 194 (91,6 %) и «Несанкционированный доступ к компьютерной информации» – 3 943

[33] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Армения, представлена в Приложении 3.

[34] См.: URL: https://www.sb.by/articles/v-mvd-rasskazali-kak-chasto-belorusy-povtorno-stanovyatsya-zhertvami-kiberprestupnikov.html (дата обращения: 14.04.2023).

(7,2 %) от всех зарегистрированных деяний соответственно. Эти два состава образуют большую часть преступлений, совершенных с использованием ИКТ, в Республике. Характерной тенденцией является снижение противоправных деяний по данным составам – на 47,7 % за три года.

Минимальное значение имеет состав «Изготовление (сбыт) средств для получения неправомерного доступа к компьютерной системе (сети)» – за три года возбуждено всего одно уголовное дело (рис. 3)[35].

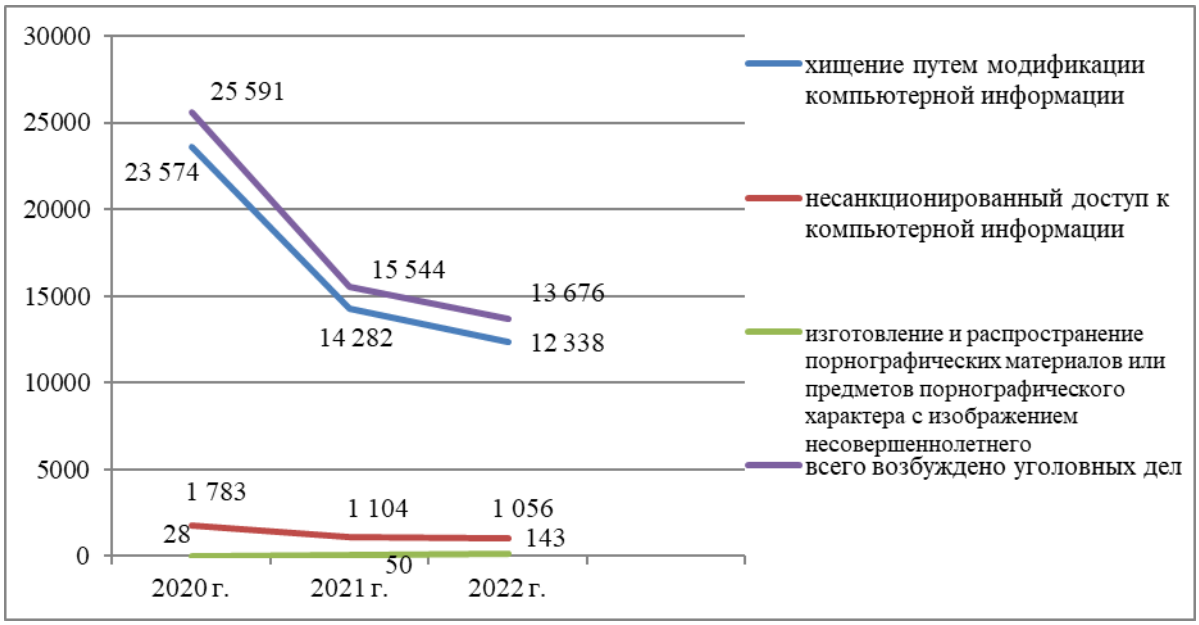

Рис. 3. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Беларусь

Республика Казахстан

По данным МВД Республики Казахстан в 2022 г., в стране было зарегистрировано 20 444 факта интернет-мошенничества, что на 4 % меньше, чем в 2021 г., также в 2022 г. было зарегистрировано более 3 тысяч фактов интернет-мошенничеств по оформлению онлайн-кредитов с применением методов социальной инженерии[36]. Больше всего интернет-мошенничеств в 2022 г. отмечено в столице – 4 397 (22 %).

[35] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Беларусь, представлена в Приложении 3.

[36] См.: URL: https://kapital.kz/gosudarstvo/113106/v-astane-bylo-zafiksirovano-22-vsekh-kibermoshennichestv-v-rk-mvd.html (дата обращения: 14.04.2023).

По данным Генеральной прокуратуры Республики Казахстан, в 2022 г. количество интернет-мошенничеств, связанных с выдачей кредитов, снизилось на 28 %[37]. В ведомстве отмечают, что Агентство по регулированию и развитию финансового рынка внесло изменения в правила предоставления микрокредитов электронным способом и ввело дополнительные способы аутентификации заемщиков.

В МВД Республики Казахстан также сообщают, что по инициативе ведомства ужесточены процедуры оформления онлайн-кредитов с помощью биометрии и электронной цифровой подписи. Операторами связи проведены технические работы по интеграции антифрод-систем[38], которые позволяют определять и блокировать подменные номера на этапе поступления звонка казахстанскому абоненту.

В 2022 г. компаниями сотовых связей было заблокировано 5,5 млн звонков с «подменных» номеров. Министерство внутренних дел Республики Казахстан ликвидировало 6 организованных преступных группировок и пресекло работу 165 сайтов с признаками мошенничества.

Согласно статистике по уголовным правонарушениям, связанным с интернет-мошенничествами, наивысший процент раскрываемости наблюдался в 2018 г. На протяжении последующих трех лет (2019–2021 гг.) процент раскрываемости не превышает отметки в 25 %, наименьший процент раскрываемости приходится на 2020 г. (24 %)[39].

В Республике Казахстан с 2020 по 2022 г. суммарно зарегистрировано 60 323 уголовных преступлений, совершенных с использованием ИКТ. Существенный рост зарегистрированных деяний (+51,3 %) по сравнению с аналогичным показателем прошлого года наблюдался в 2021 г., а в 2022 г. число зарегистрированных деяний несколько снизилось (–3,8 %), хотя и продолжает оставаться значительным.

На протяжении последних трех лет максимальное количество противоправных деяний формируется преступлениями против собственности, а именно мошенничеством – за истекшие три года зарегистрировано 55 829 таких деяний, что составляет 92,6 % всех преступлений, совершенных с использованием ИКТ, и кражей – 3 325 (5,5 %). Минимальное значение имеет состав «сепаратистская

[37] См.: URL: https://www.gov.kz/memleket/entities/prokuror/press/news/4?lang=ru (дата обращения: 14.04.2023).

[38] Anti-fraud – борьба с мошенничеством с англ.

[39] См.: Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения // Российско-азиатский правовой журнал. № 2. 2022. С. 49–55.

деятельность» – таких фактов за истекшие три года зарегистрировано всего 3 (рис. 4)[40].

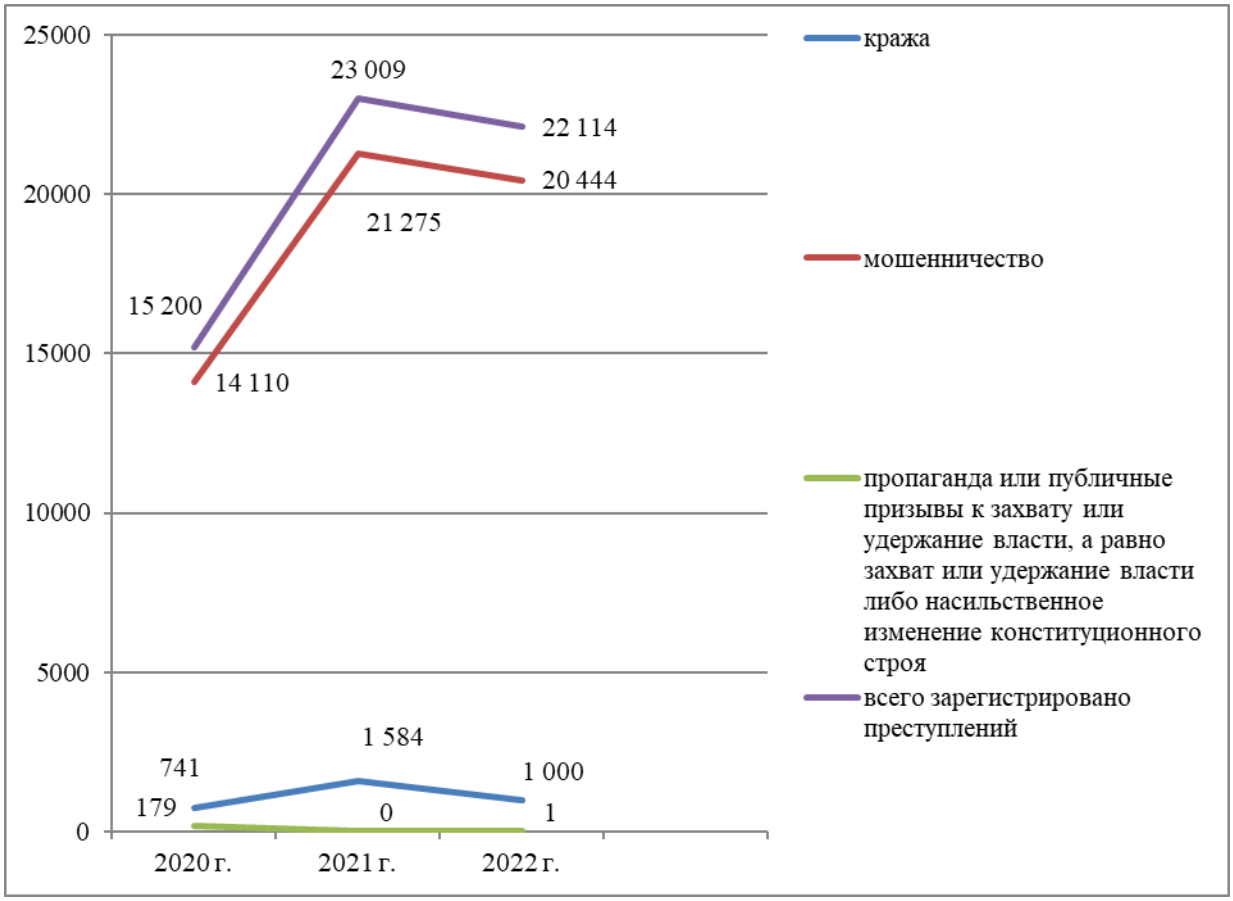

Рис. 4. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Казахстан

Кыргызская Республика

В Кыргызской Республике за 2020–2022 гг. с использованием ИКТ совершено 803 преступления, их количество год от года увеличивается.

Наибольшее значение приходится на долю мошенничества – 365 (45,5 %) всех совершенных деяний; изготовления, распространения экстремистских материалов – 218 (27,2 %); незаконного изготовления наркотических средств с целью сбыта – 119 (14,8 %).

Минимальное число совершенных преступлений приходится на содействие террористической деятельности, создание преступного

[40] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Казахстан, представлена в Приложении 3.

сообщества, подделку документа, создание опасности для потребителей – по 1 ежегодно (рис. 5)[41].

С учетом имеющихся угроз, связанных с распространением идеологии экстремизма в интернет-пространстве, принимаются меры по выявлению и блокированию сайтов религиозно-экстремистских и террористических организаций. За период с 2012 по 2021 г. во взаимодействии с Генеральной прокуратурой Кыргызской Республики и Государственным комитетом информационных технологий и связи Кыргызской Республики в судебном порядке заблокированы более 240 сайтов, распространяющих идеологию экстремистских и террористических организаций.

Так за 2022 г. выявлено и направлено в Судебно-экспертную службу при Министерстве юстиции Кыргызской Республики 28 сайтов и 10 аккаунтов. На основании решения суда 28 сайтов заблокированы.

Из социальных сетей удалено 142 фото-, видео- и аудиоматериалов, пропагандирующих разжигание экстремистской, террористической и межнациональной вражды, загружено 33 видеоматериала пользователям социальных сетей для профилактики экстремизма и терроризма.

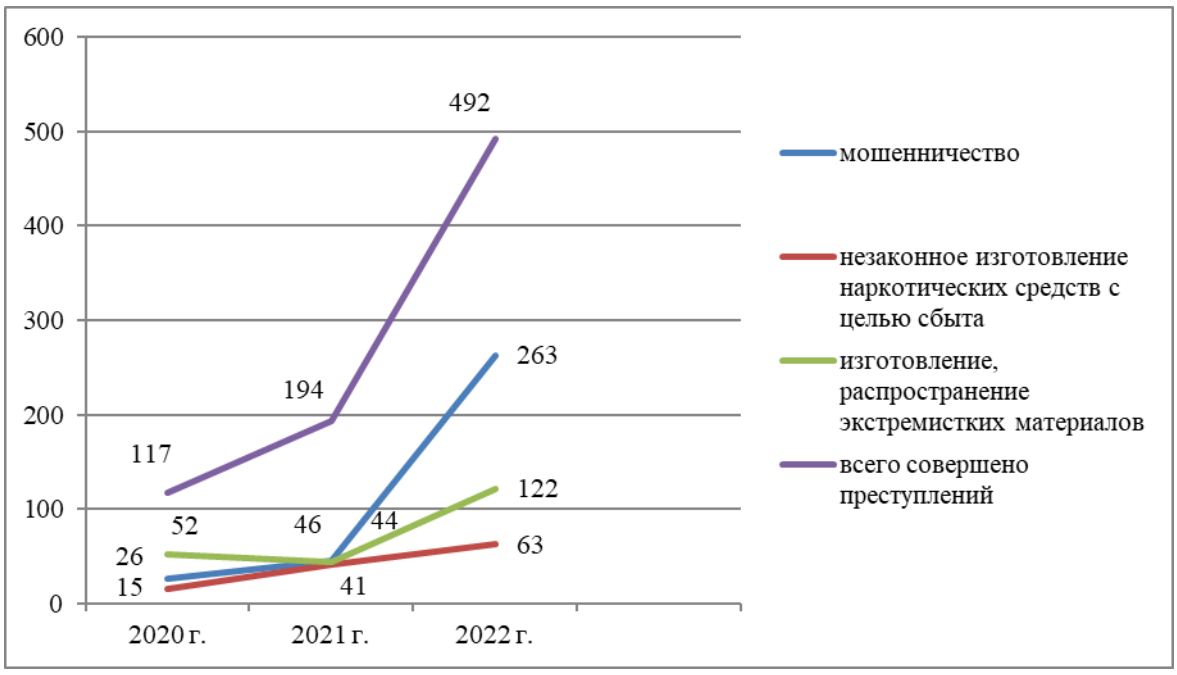

Рис. 5. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Кыргызской Республики

[41] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Кыргызской Республике, представлена в Приложении 3.

Республика Молдова

В центре внимания властей – идентифицирующие данные владельцев SIM-карт, доступ к которым, по мнению учреждений правопорядка, позволит существенно снизить риски для национальной безопасности и повысить эффективность борьбы с киберпреступлениями. Правоохранительные органы отмечают, что преступные группировки часто пользуются телефонными картами без регистрации. Стражи порядка недовольны большим числом лиц, использующих деперсонализованные электронные услуги в Молдове. По их мнению, это препятствует выявлению злоумышленников в ходе проведения специальных следственных и уголовных мероприятий. Речь, как правило, идет о компьютерных преступлениях, преступлениях в области телекоммуникаций, а также деяниях террористического, экстремистского характера и связанных с ними[42].

Служба информационных технологий и кибербезопасности Молдовы (STISC) сообщила о том, что 5 января 2023 г. государственные учреждения страны подверглись массированным мошенническим и фишинговым атакам. На адреса электронной почты, принадлежащие различным государственным ведомствам, злоумышленниками уже отправлено более 1 330 сообщений. В рамках одной из киберкампаний электронные письма содержали уведомление о предполагаемом истечении срока действия государственного домена .md. При этом получателям предлагалось перейти по ссылке для оформления продления подписки. Фактически эта ссылка вела на фальшивую платежную страницу, через которую киберпреступники крали деньги[43].

В Республике Молдова с 2020 по 2022 г. зарегистрировано 872 преступления, совершенных с использованием ИКТ. Как и практически во всех рассмотренных государствах – участниках СНГ в Республике Молдова наблюдается тенденция к увеличению числа рассматриваемых деяний.

Немногим меньше половины из числа зарегистрированных преступлений приходится на долю мошенничеств 401 (46 %) и краж – 200 (23 %). Значительные показатели имеет также «Нарушение неприкосновенности частной жизни» – 51 (5,9 %) и «Подлог инфор-

[42] См.: URL: https://noi.md/ru/analitika/novye-pravila-budut-li-v-moldove-prodavati-sim-karty-toliko-po-pasportu (дата обращения: 14.04.2023).

[43] См.: URL: https://md.sputniknews.ru/20230105/v-moldove-rastet-kolichestvo-kiberatak-na-sayty-gosuchrezhdeniy-54937532.html (дата обращения: 14.04.2023).

мационных данных» – 62 (7,1 %) (данный состав демонстрирует резкий рост в 2022 г.) соответственно.

Минимальное число зарегистрированных деяний приходится на долю следующих составов: «Умышленное причинение телесного повреждения средней тяжести или иного средней тяжести вреда здоровью»; «Умышленное воспрепятствование деятельности средств массовой информации или запугивание за критику»; «Присвоение чужого имущества», «Присвоение, незаконное отчуждение, сокрытие заложенного замороженного имущества, имущества, взятого в лизинг, арестованного или конфискованного имущества», «Неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов», «Хулиганство», «Ложное показание, заключение или неправильный перевод», «Злоупотребление властью или служебным положением», «Злоупотребление служебным положением», «Умышленные действия, направленные на разжигание национальной, этнической, расовой или религиозной вражды, дифференциации или розни» – по 1 за последние три года (рис. 6)[44].

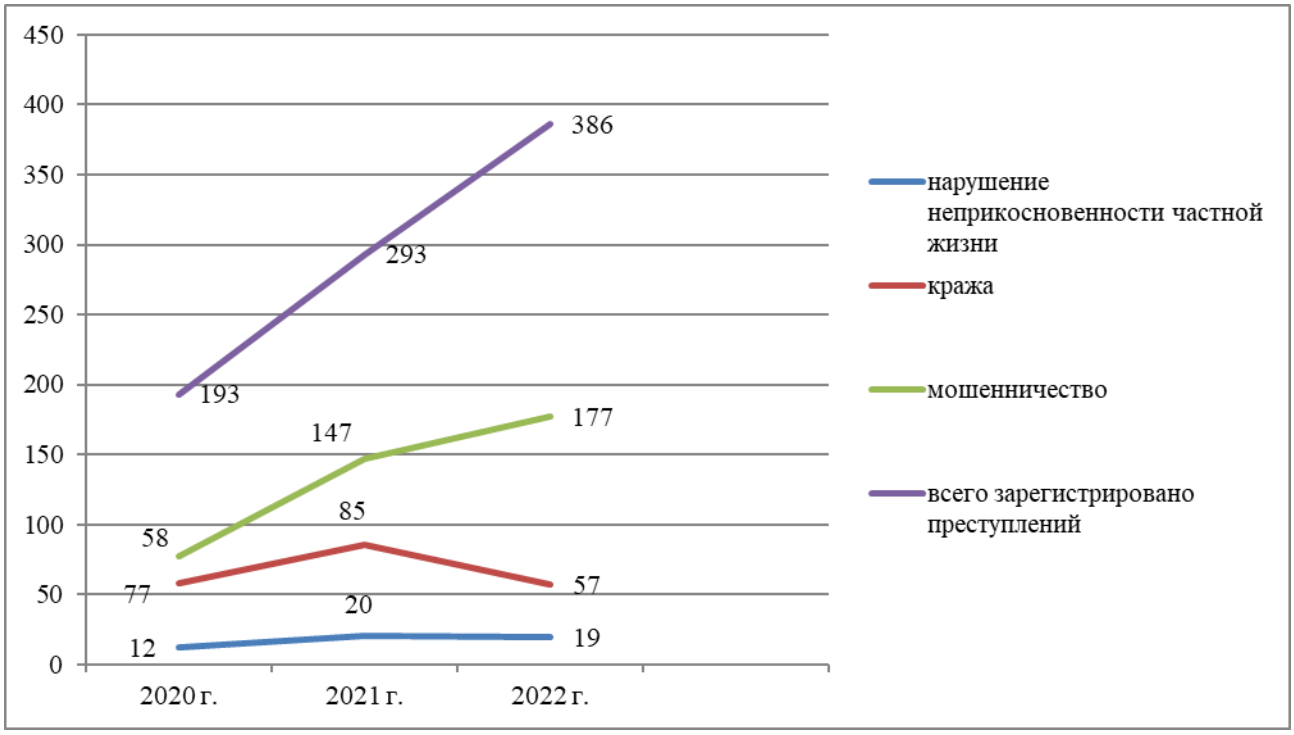

Рис. 6. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Молдова

[44] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Молдова, представлена в Приложении 3.

Российская Федерация

В 2022 г. сотрудники экспертного центра безопасности Positive Technologies провели более 50 расследований по фактам совершенных кибератак. Пик по количеству инцидентов пришелся на апрель 2022 г. Причин этому несколько: рост числа уязвимостей и их неустранение, нехватка кадров более чем у 90 % компаний, уход иностранных вендоров информационной безопасности. В некоторых атаках злоумышленникам удалось реализовать недопустимые для компаний события, например, остановить бизнес-процессы. Уровень сложности зафиксированных атак ранжируется от школьников до проправительственных APT-группировок[45], больше половины инцидентов было совершено квалифицированными злоумышленниками. При этом злоумышленники не изобретают новые способы атак, но, тем не менее, число инцидентов с применением уже известных методов продолжает расти[46].

За большинством атак в 2022 г. стояли политически мотивированные хакеры. Для атаки им достаточно иметь ноутбук с подключением к Интернету (таким образом, например, проводятся DDoS-атаки). Организаторы подобных сообществ координируют участников и направляют их активность на заранее выбранные цели[47]. Чаще всего в 2022 г. целями подобных атак становились государственные учреждения и СМИ: так, в I квартале 2022 г. количество атак, направленных на госучреждения, увеличилось практически в два раза по сравнению с последним кварталом 2021 г., а затем продолжало расти в течение всего года. Таким способом преступники пытались вызвать общественный резонанс и панические настроения среди населения.

В современном социально-политическом контексте уместно ожидать, что в ближайшее время хакерство вряд ли пойдет на спад. Более вероятным является усложнение таких атак, поскольку многие российские компании осознали важность кибербезопасности и начали укреплять защиту своего периметра.

---

[45] Advanced persistent threat (APT) – термин кибербезопасности, означающий противника, обладающего современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать угрозу опасных кибератак.

[46] См.: URL: https://habr.com/ru/news/711498/ (дата обращения: 14.04.2023).

[47] См.: URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (дата обращения: 14.04.2023).

На новый уровень вышла проблема клонированных и поддельных приложений. Мобильные приложения многих компаний были удалены из официальных магазинов, из-за чего пользователям пришлось искать их на других площадках. Злоумышленники не преминули этим воспользоваться и стали активно размещать фальшивые приложения известных компаний.

Теневой рынок преступных киберуслуг стал наращивать присутствие в мессенджерах. Теневые площадки все чаще создают каналы и группы в Telegram, в середине 2022 г. было зафиксировано рекордное количество сообщений подобного рода в мессенджере. В основном это торговля данными, вредоносным программным обеспечением, также продвигаются разного рода услуги киберпреступников: взлом ресурсов (в том числе сайтов, почтовых аккаунтов и аккаунтов в социальных сетях), обналичивание средств, распространение вредоносного программного обеспечения, спам-рассылки, услуги DDoS.

На долю преступлений, совершенных с использованием ИКТ в Российской Федерации за последние три года, приходится четверть всех регистрируемых деяний. Суммарно с 2020 по 2022 г. зарегистрировано 1 550 тыс. таких деяний. Более половины из них относятся к категориям тяжких и особо тяжких. Более чем три четверти рассматриваемых деяний совершается путем кражи – 443,6 тыс. или мошенничества – 706,5 тыс. деяний, при этом прослеживается тенденция смещения от первых к последним.

Почти каждое десятое преступление совершается с целью незаконного производства, сбыта или пересылки наркотических средств – общее их число за последние три года составило 160,7 тыс.

Для совершения двух третей преступлений с применением ИКТ преступники используют сеть Интернет, а почти половина совершается с использованием средств мобильной связи (рис. 7)[48].

[48] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Российской Федерации, представлена в Приложении 3.

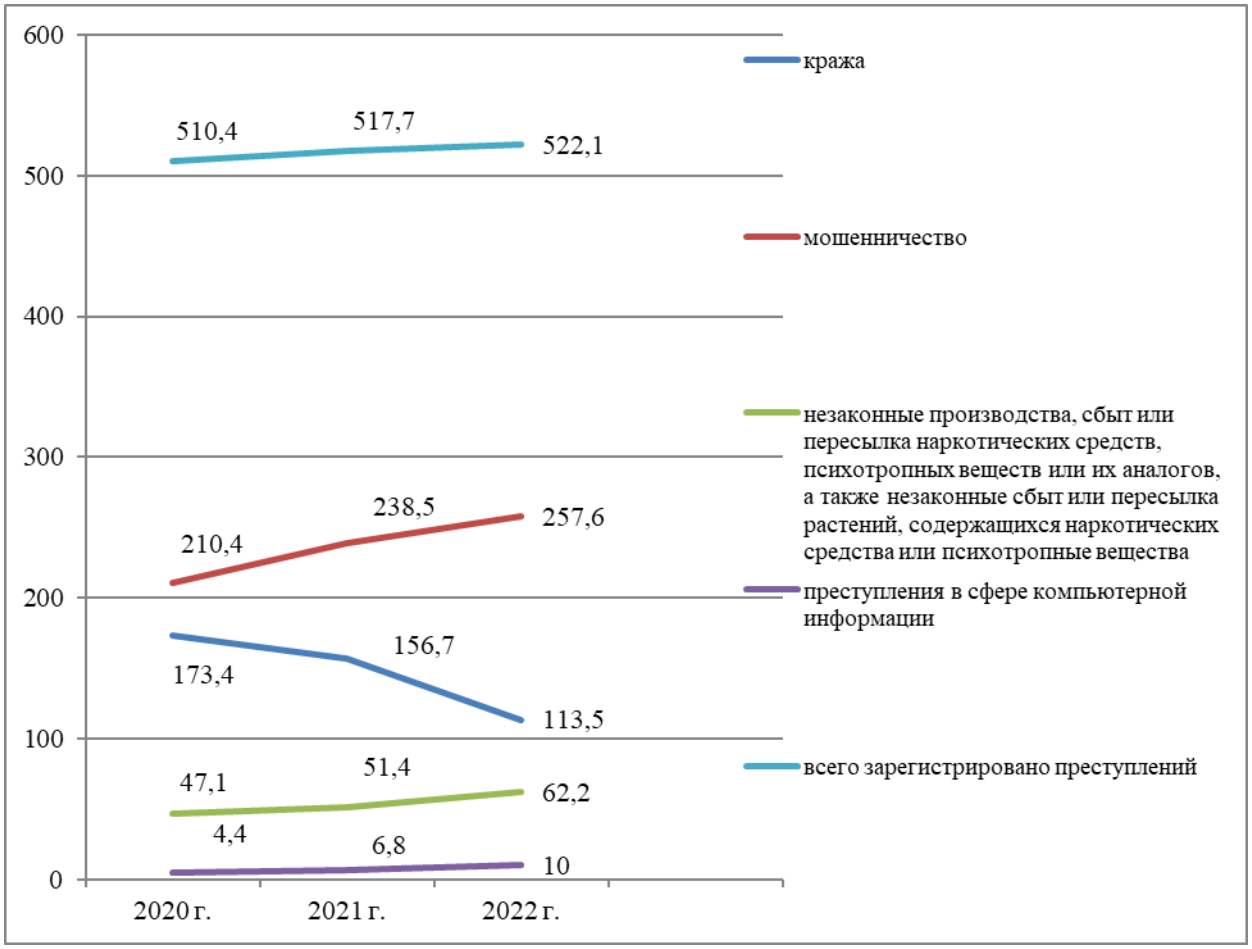

Рис. 7. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Российской Федерации

Республика Таджикистан

Анализ практических материалов показывает, что в Республике Таджикистан большинство преступлений, совершенных посредством использования ИКТ имеют экстремистский, террористический характер.

В Таджикистане за истекшие три года с использованием ИКТ совершено 3 001 преступление, которые демонстрируют тенденцию к росту с некоторым снижением в 2021 г.

Наибольшие показатели в числе зарегистрированных преступных деяний приходится на долю организации экстремистского сообщества – 1 665 (55,5 %) и возбуждения национальной, расовой, межэтнической или религиозной вражды – 1 008 (33,6 %) (с резким ростом в 2022 г.). Велика доля фактов организации сообщества и иной преступной организации – 261 (8,7 %). Это позволяет сделать вывод, что ИКТ в республике активно применяются при осуществлении террористической и экстремистской преступной деятельности различного рода сообществами и организациями, а также преступным сообществам.

Показатели по составам «Неправомерный доступ к компьютерной информации» и «Незаконное завладение компьютерной информацией» (по 1 преступлению за истекшие три года) можно охарактеризовать как незначительные (рис. 8)[49].

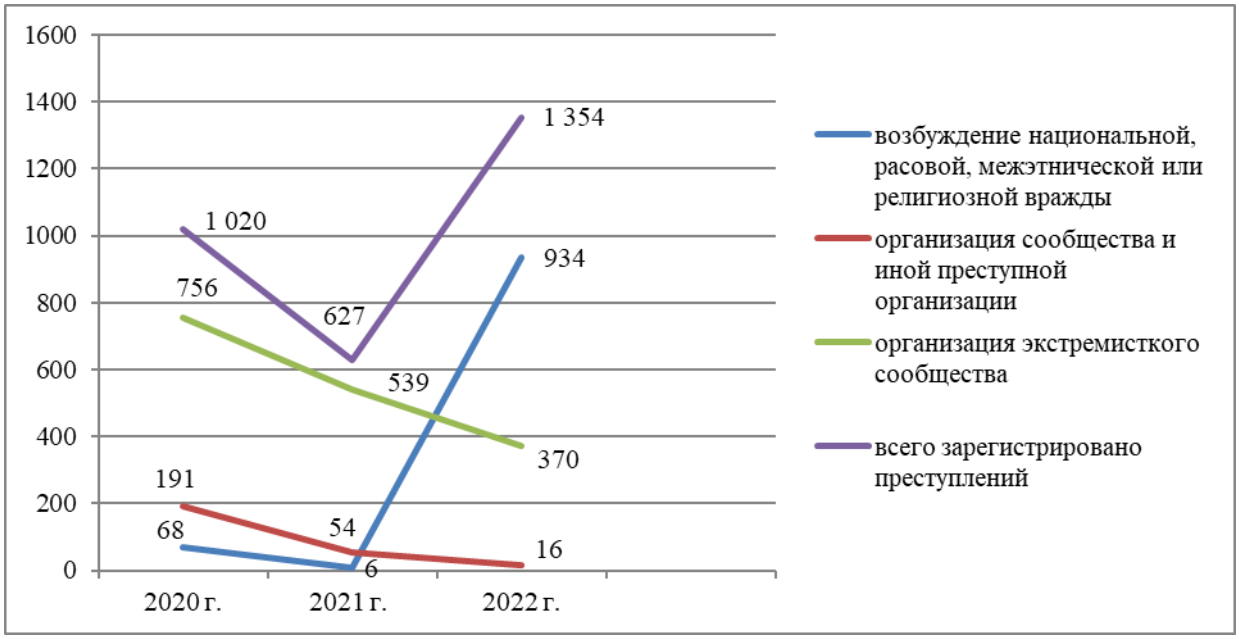

Рис. 8. Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Таджикистан

Республика Узбекистан

Должностные лица Центра кибербезопасности МВД сообщили на пресс-конференции, что в 2023 г. в Республике Узбекистан насчитывалось более 25 млн пользователей Интернета. Растет не только число пользователей, но и число совершаемых ими киберпреступлений: за последние три года этот показатель увеличился в несколько раз. При этом самым популярным видом онлайн-правонарушения является мошенничество, жертвой которого становятся владельцы пластиковых карт. Преступники используют для получения кода, приходящего в виде SMS-уведомления, такие предлоги как перевод средств или выдача выигрыша. Кроме того, многие пользователи сталкиваются с вымогательством, при котором преступники присваивают и угрожают распространить их личные данные. Участились случаи кибербуллинга – запугиваний, оскорблений в социальных сетях и доведения до суицида[50].

[49] Более подробно информация о количестве зарегистрированных преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Таджикистан, представлена в Приложении 3.

[50] См.: URL: https://nuz.uz/obschestvo/1246386-v-uzbekistane-vyroslo-kolichestvo-kiberprestuplenij.html (дата обращения: 14.04.2023).

За 2021 г. в Республике учтено 785 преступлений, совершенных с использованием информационной сети, что составляет 0,7 % по отношению к общей преступности. Максимальная доля названных деяний – 532 (67,8 %) приходится на подготовку, хранение, распространение или демонстрацию материалов, угрожающих общественной безопасности. Значительную долю составляют факты клеветы – 87 (11,1 %) и оскорбления – 111 (14,1 %), минимальное число приходится на организацию и проведение азартных и иных игр, основанных на риске, – 1 (0,1 %).

В 2022 г. число учтенных деяний возросло почти вдвое (+55,5 %) и составило 1 221 деяний (1,2 % в массе общей преступности) с максимальной долей подготовки, хранение, распространения или демонстрации материалов, угрожающих общественной безопасности, – 791 преступление (64,8 %). Возросло количество фактов оскорбления – 245 (20,1 %) и клеветы – 117 (9,6 %), на прежнем уровне держатся факты организации и проведение азартных и иных игр, основанных на риске, – 1 (0,1 %) (рис. 9).

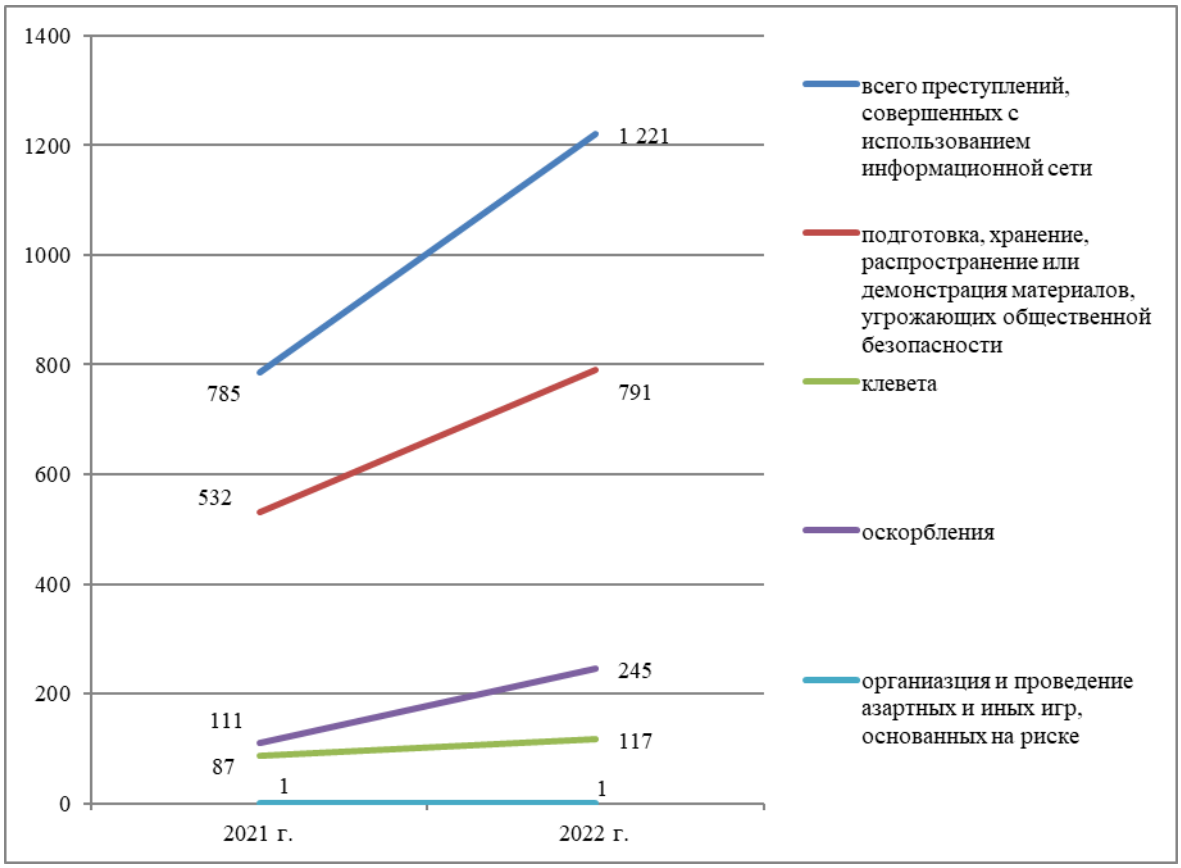

Рис. 9. Динамика количества преступлений, совершенных с использованием ИКТ за 2021 гг. на территории Республики Узбекистан

Проведенный анализ преступлений, совершенных с использованием ИКТ на территориях государств – участников Содружества Независимых Государств, позволяет отметить следующие тенденции.

1. Практически во всех странах Содружества на протяжении последних трех лет общее число преступлений, совершаемых с использованием ИКТ, характеризуется тенденцией к росту. Исключение составляет Республика Беларусь, где прослеживается обратная тенденция, а также Республика Казахстан, где в 2022 г. наблюдается незначительное снижение общего числа рассматриваемых деяний.

2. Значительные показатели в числе рассматриваемых деяний приходятся на долю преступлений против собственности: мошенничества, кражи и прочие формы хищений. Вместе с тем следует иметь в виду, что преступность, связанная с посягательствами на собственность, самая представительная в структуре преступности любого государства, поэтому отмеченная тенденция позволяет утверждать лишь то, что преступниками активно совершенствуется противоправная деятельность по незаконному изъятию чужого имущества путем применения ИКТ.

3. В государствах – участниках СНГ, уголовное законодательство которых предусматривает ответственность за преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, совершаемые с использованием ИКТ, число выявляемых преступлений является значительным (Азербайджанская Республика, Республики Армения и Казахстан, Российская Федерация). Это позволяет сделать вывод о том, что наркопреступность активно применяет ИКТ, что подразумевает отражение в законодательстве и в деятельности правоохранительных органов стран Содружества.

4. Значительная доля деяний, совершаемых с использованием ИКТ, приходится на распространение экстремизма и терроризма в интернет-пространстве. Это предполагает ответную реакцию законодателя и внесение корректив в деятельность правоохранительных органов.

3. ПРОБЛЕМНЫЕ АСПЕКТЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В ГОСУДАРСТВАХ – УЧАСТНИКАХ СНГ

В сложившихся реалиях цифровая безопасность (кибербезопасность) становится предметом пристального внимания со стороны государств – участников СНГ, а ее обеспечение нуждается в комплексном регулировании.

Несмотря на принимаемые меры по борьбе с киберпреступностью в странах Содружества, все же продолжают оставаться проблемы, препятствующие эффективному осуществлению данной борьбы.

1. Одной из первых стоит выделить длительность законодательного ответа на появление новых видов киберпреступности.

Механизмы борьбы с киберпреступностью разрабатываются и применяются исходя из практики применения национального законодательства, с учетом необходимости соблюдения обязательств по международным договорам. Чтобы согласовать и учесть все требования требуются значительные временные затраты, в то время как преступники, необремененные необходимостью соблюдения закона, действуют на опережение и находятся на несколько шагов впереди тех, кто им противодействует.

2. Ряд сложностей создает недостаточная оперативность взаимодействия между правоохранительными органами государств – участников СНГ.

Преступления, совершаемые с использованием ИКТ, с точки зрения фиксации цифровых следов имеют ряд особенностей, поэтому временной период, затрачиваемый на направление запроса, его доставление, получение ответа имеет большое значение. Поэтому отправка запросов в другие страны Содружества на бумажных носителях приводит к затягиванию сроков, а также утрате следов.

3. Затруднения создает и разнонаправленность действий взаимодействующих субъектов и необходимость соблюдать баланс государственных и межгосударственных интересов.

4. Различия в национальных законодательствах стран Содружества, затрудняющие международное сотрудничество в борьбе с пре-

ступлениями, совершаемыми с использованием ИКТ (сети Интернет), также препятствуют эффективной борьбе с рассматриваемыми деяниями.

Так, например, несмотря на наличие перечня деяний, относимых к категории совершенных в сфере информационных технологий, отсутствует терминологическая определенность в характеристике киберпреступлений, а отдельные деяния, такие, как наркопреступность с использованием информационно-телекоммуникационных сетей в качестве элемента состава либо в качестве квалифицирующего признака, находят свое отражение в УК не всех стран Содружества.

5. Анализ киберпреступлений показал, что они обладают рядом характерных признаков, существенно затрудняющих их раскрытие «по горячим следам», а именно трансграничный характер совершения, использование динамических IP-адресов и проч.

Ряд проблем обусловлен использованием преступниками сервисов-анонимайзеров, IP-адресов, принадлежащих преимущественно зарубежным сегментам сети Интернет.

Проблемы создает и нахождение серверов электронной почты на территории иного государства, чем то, где находится правонарушитель.

Также отсутствие оперативного обмена информацией в отношении социальных сетей и почтовых сервисов, не зарегистрированных на территории стран Содружества, существенно затрудняет идентификацию личности и, соответственно, привлечение к установленной законом ответственности преступников, которые при совершении преступлений пользуются приложениями для обмена мгновенными сообщениями, либо социальными сетями и проч.

Как следствие, для повышения уровня раскрываемости таких деяний необходимо оперативное взаимодействие с правоохранительными органами иностранных государств.

6. Самостоятельным фактором выступает недостаточная подготовка сотрудников правоохранительных органов в области компьютерных технологий. В настоящее время для выявления и раскрытия киберпреступлений необходимы специальные познания. В связи с отмеченным, на первый план выдвигается необходимость подготовки сотрудников правоохранительных органов стран Содружества.

7. Помимо специальной подготовки сотрудников, занимающихся борьбой с киберпреступлениями, высокие требования предъявляются к техническому оснащению: имеется необходимость в высокоскоростных компьютерах, установке дорогостоящего программного обеспечения. Этому препятствует недостаточная материально-

техническая обеспеченность, отсутствие специализированных компьютерных программных средств.

8. Также в числе проблем отмечаются сложности с обменом передовым опытом и информацией, в том числе методической литературой.

4. ПРЕДЛОЖЕНИЯ ПО РЕШЕНИЮ ПРОБЛЕМНЫХ ВОПРОСОВ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ НА ТЕРРИТОРИЯХ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Для решения отмеченных проблем, а также повышения эффективности борьбы с киберпреступностью на территориях государств – участников СНГ целесообразно предпринять ряд мер, направленных на достижение согласованности и оперативности действий по ряду вопросов.

1. Видится необходимым совершенствование национальных уголовных правовых систем, в части установления ответственности за совершение киберпреступлений. Одним из инструментов может стать разработка общего перечня преступлений, совершаемых с использованием ИКТ, что в свою очередь позволит в дальнейшем более продуктивно решать вопросы оказания правовой помощи и экстрадиции лиц, их совершивших.

2. Учитывая, что развитие кибертехнологий происходит максимально быстро, требуется адекватное реагирование со стороны законодательной базы. Повышению эффективности противодействия киберпреступлениям будут способствовать актуализация Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.

3. Анализ информации, поступившей из МВД стран Содружества, выявил проблему отсутствия единого понимания терминов, используемых при организации взаимодействия правоохранительных органов стран Содружества. В этой связи возможна разработка глоссария терминов, связанных с противодействием преступлениям, совершаемым с использованием ИКТ[51].

4. Имеется необходимость усиления взаимодействия правоохранительных органов, в частности:

повышение оперативности взаимодействия в сфере борьбы с преступлениями, совершаемыми с использованием ИКТ – налаживание каналов межгосударственного сотрудничества, позволяющего обмениваться информацией в режиме онлайн;

[51] См.: Приложение 2.

установление рабочих контактов между профильными подразделениями МВД стран Содружества;

необходимо накопление сведений о цифровых следах киберпреступлений;

важна активизация обмена информацией о новых способах совершения киберпреступлений и опыте работы МВД государств – участников СНГ по противодействию угрозам.

5. С учетом того, что киберпреступность носит трансграничный характер, борьба с ней должна координироваться и осуществляться с привлечением механизмов государственно-частного партнерства, объединяющего телекоммуникационные компании, банки, компании по информационной безопасности, регуляторов.

Это требует активизации взаимодействия всех участников процесса противодействия киберпреступности, начиная с правоохранительных органов государств – участников СНГ и заканчивая их исследовательскими и академическими структурами.

6. Немаловажным является формирование современной материально-технической базы и продолжение работы по подготовке кадров для подразделений, осуществляющих в борьбу с киберпреступностью.

Это предполагает, в частности, дополнительную подготовку и повышение квалификации сотрудников, задействованных в борьбе с преступлениями с использованием ИКТ, в том числе путем стажировки, проведение конференций, семинаров и учебных курсов, а также усиление оснащенности соответствующих подразделений, в том числе путем разработки специального программного обеспечения и обучения сотрудников его использованию.

7. Выработка мер противодействия преступлениям в сфере информационных технологий немыслима без оценки масштабов и тенденций IT-преступности, что обусловливает необходимость изучения не только всего массива такого рода деяний, но и прогнозирования развития отдельных видов и групп таких преступлений.

Это, в свою очередь, подразумевает усиление научно-методической базы борьбы с киберпреступностью путем проведения исследований, направленных на систематизацию информации о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в указанной сфере, об используемых программных продуктах.

8. В целях повышения эффективности противодействия киберпреступлениям видится целесообразным стремление к формирова-

нию многоуровневой институциональной системы кибербезопасности, которая включала бы в себя:

алгоритмы обсуждения вопросов обеспечения кибербезопасности как на национальном, так и на межгосударственном уровнях;

подготовку межгосударственных соглашений, предусматривающих конкретные мероприятия, направленных на противодействие киберпреступности;

повышение технической, цифровой и финансовой грамотности населения в качестве профилактической меры воздействия.

Приложение 1

Статьи в Уголовных кодексах государств – участников Содружества Независимых Государств, устанавливающие уголовную ответственность за преступления в сфере ИКТ

Азербайджанская Республика

Ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ, в Азербайджанской Республике установлена следующими статьями УК Азербайджана:

148-1. Клевета или оскорбление в информационном интернет-ресурсе с использованием поддельных имен пользователя, профилей или учетных записей.

171-1. Распространение, рекламирование, продажа, передача другим, отправление, предложение, создание условий для приобретения, либо изготовление, приобретение или хранение с целью распространения или рекламы детской порнографии.

177.2.3-1. Кража с использованием электронных носителей информации, либо информационных технологий.

233-4. Организация незаконных международных телекоммуникационных услуг с подключением к телекоммуникационной сети.

234.4.4. Незаконные приобретение или хранение в целях сбыта, изготовление, производство, переработка, перевозка, пересылка либо сбыт наркотических средств или психотропных веществ с использованием средств массовой информации, в том числе информационных интернет-ресурсов или информационно-телекоммуникационных сетей.

242. Незаконные изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов или предметов, а равно незаконная торговля печатными изданиями, кино- или видеоматериалами, изображениями или иными предметами порнографического характера.

244-1.2.2. Организация или проведение азартных игр с использованием информационных интернет-ресурсов или информационно-телекоммуникационных сетей.

Республика Армения

С июля 2022 г. вступил в силу новый УК Армении, 38 глава которого посвящена преступлениям, направленным против компьютерной системы и безопасности компьютерных данных.

УК Армении также предусматриваются преступления, где компьютер является орудием или средством преступления.

Преступления, направленные против компьютерной системы и безопасности компьютерных данных предусмотрены следующими статьями:

359. Проникновение в компьютер, компьютерную систему или компьютерную сеть.

360. Изменение компьютерных данных.

361. Компьютерный саботаж.

362. Незаконный перехват компьютерных данных или владение ими;

363. Незаконный оборот специальных программных или инструментальных средств.

364. Компьютерный подлог.

365. Нарушение правил или требований эксплуатации компьютера, компьютерной системы или компьютерной сети.

Ответственность за преступления, где компьютер является орудием или средством преступления, устанавливают пункты и части статей других глав УК Армении:

134. Прямое и публичное подстрекательство к совершению геноцида /п. 1 ч. 1/.

136. Публичное отрицание, оправдание, пропаганда или преуменьшение опасности геноцида или преступлений против человечности /п. 1 ч. 2/.

151. Прямые и публичные призывы к осуществлению агрессии /ч. 2/.

201. Совершение непристойного деяния /п. 3 ч. 2/.

202. Предложение половых отношений или других действий сексуального характера лицу младше 16 лет либо создание или производство детской порнографии (груминг).

204. Нарушение тайны личной или семейной жизни /ч. 2/.

205. Разглашение врачебной тайны /ч. 2/.

227. Нарушение авторских или смежных прав /п. 2 ч. 2/.

228. Нарушение патентного права /п. 2 ч. 2/.

238. Склонение несовершеннолетнего к совершению преступления или вовлечение в его соучастие /п. 2 ч. 2/.

239. Склонение или вовлечение ребенка в действие по изготовлению или распространению порнографических материалов или предметов /п. 2. ч. 2/.

240. Вовлечение ребенка в совершение антиобщественных действий /п. 2 ч. 2/.

257. Компьютерное хищение.

297. Хулиганство /п. 3 ч. 2/.

300. Создание, распространение или хранение порнографических материалов или предметов.

313. Оправдание, пропаганда терроризма или призывы к совершению террористической деятельности, а также распространение материалов или предметов, содержащих такие призывы /п. 3 ч. 2/.

314. Распространение ложной информации о террористическом акте. /п. 2 ч. 2/.

328. Публичные призывы к массовым беспорядкам /п. 3 ч. 3/.

329. Публичные выступления, направленные на возбуждение либо пропаганду ненависти, дискриминации, нетерпимости или вражды, а также распространение материалов или предметов в этих целях /п. 2 ч. 3/.

330. Публичные призывы к насилию, публичное оправдание или пропаганда насилия, а также распространение материалов или предметов с этой целью /п. 3 ч. 2/.

422. Публичные призывы к захвату власти, нарушению территориальной целостности либо насильственному свержению конституционного строя /ч. 2/.

445. Служебный подлог.

429. Уничтожение или повреждение документов, предметов или компьютерных данных, содержащих государственную тайну.

430. Нарушение правил обращения с документами, предметами или компьютерными данными, содержащими государственную тайну.

Отдельные нормы за незаконный оборот наркотиков с использованием ИКТ в УК Армении не предусматриваются. Диспозиции статьей 393, 394 и 396 УК Армении, устанавливающих уголовную ответственность за преступления в сфере незаконного оборота наркотических средств, охватывают также деяния, связанные с незаконным оборотом наркотических средств и их аналогов с использованием ИКТ (сети Интернет).

Республика Беларусь

Уголовная ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ в УК Беларуси установлена следующими статьями:

212. Хищение путем использования компьютерной техники.

340. Заведомо ложное сообщение об опасности.

343-1. Изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего.

349. Несанкционированный доступ к компьютерной информации.

350. Модификация компьютерной информации.

351. Компьютерный саботаж.

352. Неправомерное завладение компьютерной информацией.

353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

354. Разработка, использование либо распространение вредоносных программ.

355. Нарушение правил эксплуатации компьютерной системы или сети.

Также в некоторых случаях в качестве квалифицирующего признака является использование ИКТ в следующих статьях УК Беларуси:

208. Вымогательство.

209. Мошенничество.

216. Причинение имущественного ущерба без признаков хищения.

222. Изготовление либо сбыт поддельных платежных средств.

Вместе с тем практика показывает, что с использованием ИКТ совершаются и иные преступления. Наиболее встречающиеся: «Клевета» (ст. 188) и «Оскорбление» (ст. 189), менее распространенные: «Доведение до самоубийства» (ст. 145) и «Склонение к самоубийству» (ст. 146).

Республика Казахстан

Уголовная ответственность за правонарушения в сфере информатизации и связи установлена в главе 7 УК Казахстана, которая охватывает следующие составы:

205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций.

206. Неправомерные уничтожение или модификация информации.

207. Нарушение работы информационной системы или сетей телекоммуникаций.

208. Неправомерное завладение информацией.

209. Принуждение к передаче информации.

210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.

211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа.

212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели.

213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.

Кыргызская Республика

УК КР с квалифицирующим признаком использования ИКТ предусмотрены следующие статьи.

В сфере имущественных преступлений:

205. Кража.

Пунктами 5 и 6 части 3 предусмотрена уголовная ответственность за кражу:

5) с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков мошенничества);

6) путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

221. Организация финансовых пирамид.

Пунктом 2 части 2 предусмотрена уголовная ответственность за создание условий для деятельности финансовой пирамиды, предложение участвовать в ней или привлечение (получение) финансовых активов с помощью финансовой пирамиды, организацию и руководство деятельностью финансовой пирамиды, если это сопряжено с извлечением дохода в крупном размере: 2) совершенные путем осуществления незаконных операций с использованием компьютерных, информационных или телекоммуникационных систем либо сетей или систем электронных платежей.

В экономической сфере:

227. Незаконное получение информации, составляющей коммерческую или банковскую тайну.

Пунктом 1 предусмотрена уголовная ответственность за собирание сведений, составляющих коммерческую или банковскую тайну, путем хищения документов; подкупа либо угроз в отношении лиц, владеющих коммерческой или банковской тайной, или их близких; перехвата информации в средствах связи; незаконного проникновения в компьютерную систему или сеть; использования специальных технических средств, а равно иным незаконным способом.

Преступления экстремистской и террористической направленности:

255. Публичные призывы к осуществлению террористической деятельности.

Пунктом 2 предусмотрена уголовная ответственность за публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, совершенные с использованием средств массовой информации или сети Интернет.

332. Изготовление, распространение экстремистских материалов.

Предусмотрена уголовная ответственность за изготовление, распространение, перевозка или пересылка экстремистских материалов либо их приобретение или хранение с целью распространения, использование символики или атрибутики экстремистских организаций, а также посредством сети Интернет.

Иные составы преступлений, где в качестве квалифицирующего признака предусмотрено использование ИКТ:

128. Доведение до самоубийства.

Пунктом 2 предусмотрена ответственность за угрозу применения насилия, опасного для жизни и здоровья, жестокое обращение или унижение личного достоинства лица, что по неосторожности повлекло совершение потерпевшим самоубийства или попытку совершить самоубийство: 2) совершенные в отношении лица, находившегося в материальной либо иной зависимости от виновного, или в отношении ребенка, а равно посредством использования сетей телекоммуникации, в том числе сети Интернет.

129. Склонение к самоубийству.

За склонение к самоубийству, то есть возбуждение у другого лица решимости совершить самоубийство путем уговора, обмана или иным способом, что повлекло совершение потерпевшим самоубийства или попытку совершить самоубийство: 2) совершенное в отношении лица, находившегося в материальной либо иной зависимости

от виновного, или в отношении ребенка, а равно посредством использования сетей телекоммуникации, в том числе сети Интернет.

193. Нарушение тайны переписки.

Предусмотрена уголовная ответственность за: 1. Нарушение тайны переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных и иных сообщений, передаваемых средствами связи или с использованием компьютера. 2. То же деяние, совершенное с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации.

266. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

319. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи.

Предусмотрена уголовная ответственность за: 1. Несанкционированный доступ к чужой охраняемой компьютерной информации и электронным документам, в информационную систему или сеть электросвязи, повлекший уничтожение, блокирование, изменение информации, а равно повлекший нарушение или прекращение работы устройств обработки информации, причинивший умышленно или по неосторожности значительный вред. 2. То же деяние, совершенное: 3) в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре. 3. Деяние, предусмотренное частью 1, совершенное с целью умышленного уничтожения, изменения, блокирования, приведения в непригодное состояние компьютерной информации или электронного документа либо вывода из строя, разрушения информационных систем или сети электросвязи. 4. Деяние, предусмотренное частью 3, совершенное: 3) в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре.

320. Создание вредоносных программных продуктов.

Предусмотрена уголовная ответственность за: 1. Создание с целью использования либо распространения программного продукта или внесение изменений в существующие программные продукты, заведомо предназначенные для осуществления несанкционированного доступа и копирования, уничтожения, блокирования, изменения компьютерной информации и электронных документов или нейтра-

лизации средств защиты информации, нарушения работы информационных систем или сети электросвязи, а равно умышленное использование и распространение таких программных продуктов, повлекших причинение значительного ущерба или иного значительного вреда.

2. То же деяние, совершенное:

3) в отношении информационных систем и сетей электросвязи, относящихся к критической информационной инфраструктуре.

321. Кибер-саботаж.

Предусмотрена уголовная ответственность за кибер-саботаж, то есть умышленные изменение, уничтожение, блокирование, приведение в непригодное состояние информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций или программы без права вмешательства в работу компьютерных систем, с намерением помешать функционированию программных продуктов или телекоммуникационных систем, а также вывод из строя программных продуктов, оборудования.

322. Массовое распространение электронных сообщений.

Предусмотрена уголовная ответственность за массовое распространение электронных сообщений, осуществленное без предварительного согласия адресатов, приведшее к нарушению или прекращению работы программных продуктов, телекоммуникационных систем, оборудования и абонентских терминалов.

327. Публичные призывы к насильственному захвату власти.

Пунктом 2 предусмотрена уголовная ответственность за публичные призывы к насильственному захвату или насильственному удержанию власти, а равно к насильственному изменению конституционного строя: 1) с использованием средств массовой информации или информационно-коммуникационных сетей.

330. Возбуждение расовой, этнической, национальной, религиозной межрегиональной вражды (розни).

Предусмотрена уголовная ответственность за действия, направленные на возбуждение расовой, этнической, национальной, религиозной или межрегиональной вражды (розни), унижение национального достоинства, а равно пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, национальной или расовой принадлежности, совершенные публично или с использованием средств массовой информации, а также посредством сети Интернет.

В национальном законодательстве Кыргызской Республики в статьях, устанавливающих уголовную ответственность за преступления в сфере незаконного оборота наркотиков и преступлениях против несовершеннолетних в качестве квалифицирующего признака использование ИКТ не предусмотрено. Также не предусмотрены санкции за преступления, где объектом посягательства, предметом или орудием, используемым при совершении преступлений, выступают цифровые финансовые активы, в том числе токены и криптовалюта.

Республика Молдова

Ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ установлена УК Молдовы за следующие преступления:

имущественные:

186. Кража.

189. Шантаж.

190. Мошенничество.

преступления в сфере с незаконного оборота наркотических средств и психотропных веществ:

217. Незаконный оборот наркотиков, этноботанических средств или их аналогов не в целях отчуждения.

217.1 (Незаконный оборот наркотиков, этноботанических средств или аналогов таковых с целью отчуждения).

преступления в экономической сфере:

237. Изготовление или сбыт поддельных кредитных карт или иных платежных инструментов.

245/10. Незаконное получение и/или разглашение сведений, составляющих коммерческую или банковскую тайну.

преступления экстремисткой направленности:

278. Террористический акт.

281.Заведомо ложное сообщение о террористическом акте.

преступления, совершаемые против несовершеннолетних:

173. Сексуальное домогательство.

74. Половое сношение с лицом, не достигшим 16 лет.

175. Развратные действия.

175/1. Обольщение несовершеннолетнего в сексуальных целях.

208/1. Детская порнография.

На текущем этапе внесены предложения в УК Молдовы по регулированию «Незаконных операций с безналичными средствами платежа».

Российская Федерация

УК РФ в главе 28 «Преступления в сфере компьютерной информации» содержит четыре вида преступления, однако круг совершаемых с использованием информационных технологий деяний более широк.

Так, в уголовном законодательстве Российской Федерации ответственность устанавливается за преступления, совершенные с использованием информационных технологий и преступления против информационной безопасности.

Преступления, совершенные с использованием информационных технологий, включают:

1) преступления, в способе совершения которых используются информационные технологии и цифровая информация, которые не подвергаются несанкционированному воздействию (преступления, в которых информационные технологии используются как коммуникативно-координационное средство для общения между субъектом преступления и иными лицами (ст. 110.1, 163, 119 УК РФ и т. п.);

2) преступления, в которых используется операционная функция информационных технологий, в том числе как орудие и средство совершения преступления (ст. 158, 228 УК РФ и т. п.);

3) преступления, в которых используется функция информационных технологий – различные виды преступных деяний, в механизме которых информационные технологии используются как элемент сокрытия; преступления, в которых используется функция обеспечения криминальной деятельности; преступления, в которых используется информационная функция информационных технологий; преступления, совершаемые с использованием комбинации функциональных свойств информационных технологий.

Преступлений против информационной безопасности охватывают деяния, в способе совершения которых присутствуют процессы несанкционированных информационных преобразований цифровой информации или создается угроза информационной безопасности:

1) преступления против безопасности цифровой информации (ст. 137, 138, 272, 146, 183 УК РФ и т. п.);

2) преступления в сфере незаконного оборота цифровой информации (ст. 242, 242.1, 110.2, 187 УК РФ и т. п.);

3) преступления в сфере незаконного оборота программных и технических средств, используемых против информационной безопасности (ст. 138.1, 187, 273 УК РФ).

Республика Таджикистан

В Республике Таджикистан в 15 статьях УК Таджикистана в качестве квалифицирующего признака предусмотрена ответственность за использование ИКТ.

Анализ практических материалов показывает, что в Республике Таджикистан большинство преступлений, совершенных посредством использования ИКТ, имеют экстремистский и террористический характер. Вместе с тем уголовная ответственность за совершенные преступлений экстремистской направленности предусмотрено в статьях 307, 307(1), 307 (3) (Публичные призывы к насильственному изменению конституционного строя Республики Таджикистан) УК Таджикистана, в отдельных частях которых ответственность наступает за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ, в том числе сети Интернет.

Аналогичная ответственность с указанными квалифицирующими признаками предусмотрена и в частях статей 241 (Незаконные изготовление и оборот порнографических материалов или предметов), 241(2) (Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов) УК Таджикистана.

Также установлены иные составы преступлений, совершаемые с использованием ИКТ нормы в УК Таджикистана. Национальным законодательством страны в УК Таджикистана определена отдельная глава – глава 28 (Преступления против информационной безопасности), где квалифицирующим признаком являются деяния, связанные с информацией, хранящейся в компьютерной системе, сети или на машинных носителях, уголовная ответственность которых предусмотрены в отдельных частях статей 298–304 УК Таджикистана.

Также с квалифицирующими признаками использования ИКТ – сети Интернет установлены и в нижеследующих статьях УК Таджикистана:

137. Публичное оскорбление Президента Республики Таджикистан или клевета в его адрес.

137(1). Публичное оскорбление Основателя мира и национального единства – Лидера нации или клевета в его адрес.

144. Незаконное собирание и распространение информации о частной жизни.

179(1). Вовлечение в совершение преступлений террористического характера или иное содействие их совершению.

179(3). Публичные призывы к совершению преступлений террористического характера и (или) публичное оправдание террористической деятельности.

189. Разжигание социальной, расовой, национальной, региональной, религиозной (конфессиональной) вражды или розни.

330. Оскорбление представителя власти.

334(1). Незаконное осуществление религиозного обучения.

396. Публичные призывы к развязыванию агрессивной войны.

Республика Узбекистан

Согласно нормам уголовного законодательства (глава XXI УК Узбекистана) к преступлениям в сфере информационных технологий относятся:

278.1. Нарушение правил информатизации.

278.2. Незаконный (несанкционированный) доступ к компьютерной информации.

278.3. Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций.

278.4. Модификация компьютерной информации.

278.5. Компьютерный саботаж.

278.6. Создание, использование или распространение вредоносных программ.

278.7. Незаконный (несанкционированный) доступ к сети телекоммуникаций.

В Узбекистане преступления, совершенные с использованием информационных технологий, также встречаются в других составах преступления, предусмотренных уголовным законодательством. К примеру, в связи со стремительным ростом экономических преступлений возникла потребность в ужесточении наказания за кражи и мошенничества, так как при совершении данных видов преступлений начали использоваться высокие технологии. В связи с этим был

принят Закон Республики Узбекистан «О внесении дополнений в некоторые законодательные акты Республики Узбекистан» от 19 октября 2022 г. № ЗР У-794.

Согласно нововведениям, мошенничество, то есть завладение чужим имуществом или правом на чужое имущество путем обмана или злоупотребления доверием с использованием информационной системы, в том числе информационных технологий теперь наказывается штрафом от 300 до 400 базовых расчетных величин или исправительными работами от 2 до 3 лет либо лишением свободы от 5 до 8 лет с лишением определенного права. Также изменения ужесточили кражу с незаконным (несанкционированным) проникновением в информационную систему или ее использованием, которое теперь наказывается лишением свободы от 5 до 8 лет.

Стоит отметить, что согласно статье 244.1 УК Узбекистана («Изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности и общественному порядку») криминализируется деяние за изготовление или хранение с целью распространения материалов, содержащих идеи религиозного экстремизма, сепаратизма и фундаментализма, призывы к погромам или насильственному выселению граждан либо направленных на создание паники среди населения, а также изготовление, хранение с целью распространения либо демонстрации атрибутики или символики религиозных экстремистских, террористических организаций, также в качестве квалифицирующего признака в части третьей данной статьи выступает пункт с использованием средств массовой информации либо сетей телекоммуникаций, а также всемирной информационной сети Интернет.

В УК Узбекистана преступления, где в качестве квалифицирующего признака или диспозиции предусмотрено использования информационных технологий (кроме главы XXI) можно встретить в следующих статьях:

103. Доведение до самоубийства.

103.1. Склонение к самоубийству.

130. Изготовление, ввоз, распространение, рекламирование, демонстрация порнографической продукции.

130.1. Изготовление, ввоз, распространение, рекламирование, демонстрация продукции, пропагандирующей культ насилия или жестокости.

139. Клевета.

140. Оскорбление.

141.2 Нарушение законодательства о персональных данных.

158. Посягательства на Президента Республики Узбекистан.

168. Мошенничество.

169. Кража.

188.1. Незаконная деятельность по привлечению денежных средств и (или) иного имущества.

244. Массовые беспорядки.

244.1. Изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности и общественному порядку.

244. Распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций.

244.6. Распространение ложной информации.

278. Организация и проведение азартных и других основанных на риске игр.

Кроме этого, в данный момент совместно с правоохранительными органами Республики Узбекистан ведется работа по внесению дополнений и изменений в УК Узбекистана касательно оборота наркотических средств с использованием информационных технологий и сети Интернет, а также прорабатываются нормы упорядочивающие взаимоотношения, где объектом выступают цифровые финансовые активы, криптовалюты, а также токены.

Приложение 2

Глоссарий терминов, используемых органами внутренних дел государств – участников СНГ по вопросам противодействия преступлениям, совершаемым с использованием ИКТ

Агентство национальной безопасности – официальная криптологическая организация Соединенных Штатов при Министерстве юстиции. Отвечает за глобальный мониторинг, сбор и обработку информации и данных как для внешней, так и для внутренней разведки.

Активная атака – атака, которая приводит к изменению функций и параметров системы или изменению данных, к нарушению интерактивных операций и взаимодействий в сети и др.

Активная кибероборона – проводимые в реальном времени координированные комплексные мероприятия, направленные на обнаружение, идентификацию, анализ и смягчение вредоносных последствий в случае кибератак с использованием уязвимостей компьютерной системы, сети.

Антивирус, антивирусная программа – приложение, предназначенное для обнаружения и удаления компьютерных вирусов.

Атака методом перебора (грубой силы) – метод, используемый для получения частной пользовательской информации, например введение многих паролей в надежде, что они в конечном итоге будут угаданы правильно.

Аутентификатор – способ подтверждения личности пользователя.

Биометрическая идентификация, биоидентификация – совокупность биометрических способов идентификации пользователя, основанная на уникальности характеристик человеческого тела.

Биткоин – криптовалюта, форма электронных денег.

Блокчейн – децентрализованная, распределенная и часто публичная цифровая книга, состоящая из записей, называемых блоками, которая используется для записи транзакций на многих компьютерах, так что любой задействованный блок не может быть изменен задним числом, без изменения всех последующих блоков.

Блэклист, чёрный список – список ресурсов, объектов, систем, хостов, приложений, которые ранее были связаны с вредоносными атаками, операциями и считаются поэтому опасными для организации, страны.

Бот – программы, которые автоматически выполняют задачи по указанию создателя программы, которая их заразила.

Ботнет – сеть зомбированных компьютеров, зараженных вредоносным программным обеспечением, которые контролируются без ведома владельца.

Брандмауэр – фильтр интернет-трафика, предназначенный для остановки несанкционированного входящего и исходящего трафика.

Бэкдор – секретный портал, используемый для получения несанкционированного доступа к системам, альтернативный способ доступа к программному или аппаратному обеспечению, внедренный спецслужбами.

Вайлинг – разновидность мошенничества или фишинга, направленная на пользователей высокого социального уровня – крупных бизнесменов, политиков. Для выуживания персональной и/или коммерческой (финансовой) информации применяются, как правило, методы социальной инженерии.

Вирус – элемент, прикрепляющийся к файлам, приложениям или загрузкам, представляющий скрытые угрозы.

Вредоносное программное обеспечение – это любое программное обеспечение, предназначенное для повреждения компьютерных систем или обеспечения несанкционированного доступа к ним.

Груминг детей – соблазнение детей или домогательство в отношении детей с сексуальными целями.

Даркнет, темная паутина – часть Всемирной паутины, известная своими веб-сайтами с затрудненным доступом и скрытыми веб-сайтами, на которых осуществляются незаконные действия и реализуются незаконные товары и услуги и доступ, к которым возможен только с помощью специализированного программного обеспечения.

Двухфакторная аутентификация – привязка номера телефона или адреса электронной почты к учетной записи для повышения безопасности.

Догпайлинг – форма онлайн домогательств, тактика, при помощи которой пользователи в рамках одного пространства в Интернете засыпают жертв непристойными, оскорбительными и угрожающими сообщениями, чтобы заставить их замолчать, вынудить их забрать свои слова обратно и/или извиниться или заставить их покинуть платформу.

Доксинг – публикация личной информации в Интернете с целью причинения какого-либо вреда.

Доменное имя – представление IP-адреса в интернет-браузере (или веб-браузере).

Индустриальный интернет – технология подключения к информационно-телекоммуникационной сети Интернет промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами для обмена данными.

Интернет вещей – сеть взаимосвязанных и взаимодействующих друг с другом устройств с выходом в Интернет, которые позволяют отслеживать объекты, людей, животных и растения, а также осуществлять сбор, анализ, хранение и распространение информации о них.

Интернет-тролли – люди, которые намеренно публикуют грубые, агрессивные и оскорбительные высказывания в Интернете, направленные на создание раздоров и недовольства в Интернете.

Информационная война – процесс сбора, распространения, изменения, разрушения, порчи, повреждения и ухудшения качества информации с целью получения определенного преимущества над противником.

Кибератака, атака из киберпространства (в киберпространстве) – атака, проводимая с помощью специальных программных и аппаратных средств на компьютерные сети и компьютерные системы противника с целью нарушения их работоспособности или для вредоносного управления компьютерным оборудованием/инфраструктурой, либо разрушения целостности данных или завладения информацией (данными).

Кибербезопасность, интернет-безопасность – свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз, комплекс технических, технологических, инфраструктурных и законодательных мер, процессов и практик, обеспечивающих эффективное обнаружение кибератак и противодействие им, то есть защита киберпространства (компьютерных сетей, устройств, программ и данных) от подобных атак.

Кибербуллинг – травля, оскорбления или угрозы, высказываемые жертве через социальные сети или другие средства электронных коммуникаций.

Кибервойна – высшая степень киберконфликта между или среди государств, во время которой государства предпринимают кибератаки против киберинфраструктур противника как часть военной кампании.

Кибердомогательство – использование ИКТ для преднамеренных действий с целью унижения, раздражения, нападок, угроз, запугивания, нанесения обиды и/или оскорбления лица (или лиц).

Киберзависимое преступление – киберпреступление, которое было бы невозможно без Интернета и цифровых технологий.

Киберклевета – размещение или распространение иным способом в Интернете ложной информации или слухов о взрослом или ребенке, чтобы причинить ущерб его социальному положению, межличностным отношениям и/или репутации.

Кибероружие – программное, аппаратное обеспечение, или прошивки микросхем, разработанные или применяемые для нанесения ущерба в киберсфере.

Киберпреступность, киберпреступления (компьютерная преступность) – использование киберпространства в преступных целях, которые определяются в качестве таковых национальным или международным законодательством. Основным инструментом таких преступлений являются ИКТ, компьютеры и компьютерные сети.

Кибер-прокси – посредники, непосредственно или косвенно способствующие совершению киберзависимого преступления, преднамеренно нацеленного на государство.

Киберпространство – среда, доступная с помощью цифровых устройств с выходом в Интернет, в которой осуществляется онлайн деятельность.

Кибер-саботаж – умышленные изменение, уничтожение, блокирование, приведение в непригодное состояние информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций или программы без права вмешательства в работу компьютерных систем, с намерением помешать функционированию программных продуктов или телекоммуникационных систем, а также вывод из строя программных продуктов, оборудования.

Кибертерроризм – киберзависимые преступления, совершаемые против критически важных объектов инфраструктуры, чтобы причинить какой-либо вред и вызвать страх у целевой группы населения.

Кибершпионаж – кибероперация по получению неавторизованного доступа к чувствительной информации скрытыми методами.

Контурная программа – программа, входящая в состав другой программы, которую пользователь загружает в надежде, что пользователь по привычке выберет «далее» и установит.

Криптовалюта – разновидность цифровой валюты, которая защищена с использованием продвинутого стандарта шифрования.

Криптографический ключ – число или набор символов, который используется определенным образом для шифрования/дешифрования данных.

Криптоджекинг – способ, при помощи которого вычислительная мощность зараженных компьютеров используется для добычи криптовалюты для извлечения финансовой выгоды лицом (лицами), контролирующим зараженные цифровые устройства.

Криптомаркет – веб-сайт, использующий криптографию для защиты пользователей сайта.

Критически важная инфраструктура – жизненно важные отрасли, которые считаются основополагающими для надлежащего функционирования общества.

Кэтфишинг – дача ложных или вводящих в заблуждение обещаний любви и дружбы, чтобы мошенническим путем отнять у них время, деньги и/или прочие предметы.

Метаданные – обезличенные данные, например, сколько раз пользователь нажимал или обновлял страницу при посещении веб-сайта.

Морфинг – процесс, при котором лицо или голова жертвы накладывается на тела других людей с целью диффамации, создания порнографии и/или сексуального надругательства.

Мошенничество методом социальной инженерии – склонение жертвы к раскрытию или предоставлению иным образом личной информации и/или средств злоумышленнику.

Никнейм пользователя – сетевое имя, псевдоним, используемый пользователем в Интернете, обычно в местах общения (в блогах, форумах, чатах, играх) для самоуникализации.

Облачная безопасность – стратегии и политики, используемые для защиты приложений с данными и облачных системных приложений.

Персонализация в сети – процесс, при котором преступники выдают себя за жертв, создавая учетные записи со схожими именами и используя существующие фотографии жертв.

Программы-вымогатели – разновидность вредоносного программного обеспечения, используемого для угрозы жертвам путем блокирования, публикации или искажения их данных, если выкуп не выплачен.

Прокси-сервер – промежуточный сервер, который используется для соединения клиента с сервером, с которого клиент запрашивает ресурсы.

Прошивка – код, который встроен в аппаратное обеспечение компьютера.

Средства кибербезопасности – средства и решения для управления инцидентами нарушения безопасности; единая система защиты от угроз, мультифункциональные защитные устройства; управление рисками и контроль соответствия руководящим документам и система идентификации и управления доступом.

Руткит – один из самых коварных типов вредоносных программ, поскольку они чрезвычайно скрытны и их трудно обнаружить традиционными методами защиты конечных точек.

Скрипт – компьютерная программа, набор команд для выполнения определенной задачи.

Смишинг, **SMS-фишинг** – фишинг с использованием текстовых сообщений.

Социальная инженерия – тактика использования человеческого доверия для получения доступа к частной информации.

Токены – форма представления актива или ценности в блокчейне, например, виртуальная валюта, акции, ценные бумаги, произведения искусства, объекты недвижимости.

Троян, троянский конь – разновидность вредоносного программного обеспечения, которое маскируется под безвредную компьютерную программу, но предоставляет субъектам угрозы возможность выполнять любые виды атак с целью шпионажа, кражи и/или иного причинение вреда.

Управление криптографическими ключами – административные функции по генерации, распределению (распространению), сохранению, обновлению, уничтожению и адресации криптографических ключей и других данных, связанных с информационной безопасностью (например, паролей), на протяжении всего жизненного цикла ключей.

Утечка (данных, информации) – несанкционированное и/или злоумышленное чтение, копирование, искажение или уничтожение конфиденциальной информации; например, копирование данных в незащищенное приложение с более низким уровнем безопасности, чем требуется с точки зрения секретности информации, на мобильные носители (компакт-диски, дискеты, USB-накопители), печать, открытие, редактирование чужих документов и т.д.

Уэйлинг – метод, при помощи которого преступники выдают себя за высокопоставленных руководителей компании, юристов, бухгалтеров и других лиц, занимающих руководящие и ответственные должности, чтобы обманом вынудить сотрудников отправить им денежные средства.

Фишинг – метод получения пользовательской информации посредством мошеннических сообщений, направленных непосредственно на людей. Обычно это делается с помощью электронных писем, замаскированных под поступающие из законного источника.

Хакер – кибератакующий, злонамеренно взламывающими программы и проникающими в чужие компьютеры, к защищенным ресурсам, который использует программное обеспечение и методы социальной инженерии для кражи данных и информации.

Хэш – алгоритм, который превращает большой объем данных в зашифрованный вывод фиксированной длины для сравнения без преобразования его в открытый текст. Хэш является важной частью управления блокчейном в криптовалюте.

Цифровая безопасность – инструменты, используемые для защиты личности, данных, активов и устройств.

Цифровая криминалистика – отрасль криминалистики, которая применяет вопросы права к ИКТ и цифровым устройствам.

Цифровое пиратство – незаконная загрузка фильмов с веб-сайта третьей стороны без получения права на распространение произведений, охраняемых авторским правом.

Цифровые доказательства (электронные доказательства) – под ними понимается любое доказательство, полученное из данных, которые содержатся или были произведены любым устройством, функционирование которого зависит от программного обеспечения, а также программы или данные, хранящиеся или передаваемые через компьютерную систему или сеть. Доказательства могут быть собраны из любой доступной электронной системы и по своей сути в повседневной жизни быть чем-то совершенно тривиальным.

Цифровые отпечатки – данные, оставленные пользователями ИКТ, которые могут раскрыть сведения о них, включая информацию о возрасте, половой, расовой и этнической принадлежности, гражданстве, сексуальной ориентации, мыслях, предпочтениях, привычках, хобби, истории болезни и проблемах здоровья, психологических расстройствах, статусе занятости, принадлежности к какому-либо сообществу, отношениях, геолокации, распорядке дня и прочей активности.

Цифровая судебная экспертиза – поиск, извлечение, сохранение и хранение цифровых доказательств; описание, объяснение цифровых доказательств и установление их происхождения и значимости; анализ доказательств и их убедительности, достоверности и относимости к делу; и представление доказательств, имеющих отношение к делу.

Червь – автономная вредоносная программа, которая распространяется без участия пользователя.

Ядро операционной системы компьютера – место нахождения наиболее важных функций компьютера.

IP-адрес, адрес интернет-протокола – строка чисел, применяемая для идентификации каждого компьютера, использующего Интернет в сети.

Приложение 3

Таблица 1

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг., на территории Азербайджанской Республики

Наименование статьи		**2020 г.**	**2021 г.**	**2022 г.**
Количество зарегистрированных преступлений, совершенных с использованием ИКТ Из них:		226	353	1 046
Тяжкие и особо тяжкие преступления		1	1	155
Менее тяжкие преступления		210	341	865
Преступления, не представляющие большой общественной опасности		8	11	26
Преступления против личности		4	2	6
Преступления против собственности		208	341	831
В том числе:	Кража			
	Мошенничество			
	Вымогательство			
Преступления против общественной безопасности и общественного порядка				
В том числе:	Организация незаконных международных телекоммуникационных услуг с подключением к телекоммуникационной сети	1	0	0
	Связанные с незаконным оборотом наркотических средств и психотропных веществ	1	1	198
	Организация и проведение азартных игр	0	2	2
	Киберпреступления	12	7	9

Таблица 2

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Армения

Наименование статьи	2020 г.		2021 г.		2022 г.	
	Выявлено преступлений	Возбуждено уголовных дел	Выявлено преступлений	Возбуждено уголовных дел	Выявлено преступлений	Возбуждено уголовных дел
Всего из них:	251	228	692	605	1 366	1 164
Несанкционированный доступ (проникновение) к системе компьютерной информации	4	4	5	5	7	7
Изменение компьютерной информации	3	3	2	2	6	6
Компьютерный саботаж	9	9	5	5	6	6
Неправомерное завладение компьютерной информацией	34	34	83	83	52	52
Разработка, использование и распространение вредоносных программ	5	5	1	1	–	–
Компьютерное хищение	154	137	181	144	461	410
Распространение информации, наносящей политический ущерб национальным интересам	3	3	–	–	–	–
Незаконный оборот наркотиков	1	1	2	2	134	134
Электронное мошенничество	5	5	337	287	697	546
Изготовление и распространение порнографических материалов, в том числе с участием несовершеннолетних	13	13	5	5	1	1
Нарушение работы информационных систем	–	–	–	–	2	2
Экономические преступления	1	1	–	–	–	–
Угроза убийством, причинением тяжкого вреда	7	3	13	13	–	–

Наименование статьи	2020 г.		2021 г.		2022 г.	
	Выявлено преступлений	Возбуждено уголовных дел	Выявлено преступлений	Возбуждено уголовных дел	Выявлено преступлений	Возбуждено уголовных дел
здоровью или уничтожением имущества						
Вымогательство	3	2	45	45	–	–
Незаконный сбор, хранение использование или распространение сведений личной или семейной жизни	6	5	13	13	–	–
Разглашение врачебной тайны	1	1	–	–	–	–
Применение насилия против представителя власти	1	1	–	–	–	–
Публичные призывы к терроризму, финансированию терроризма и международному терроризму, публичное оправдание или пропаганда совершения указанных преступлений	1	1	–	–	–	–

Таблица 3

Количество преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Республике Беларусь

Наименование статьи	2020 г.	2021 г.	2022 г.
Всего из них:	25 591	15 544	13 676
Хищение путем модификации компьютерной информации	23 574	14 282	12 338
Несанкционированный доступ к компьютерной информации	1 783	1 104	1 056
Уничтожение, блокирование или модификация компьютерной информации	6	45	71
Компьютерный саботаж (статья исключена из УК с 19.06.2021 г. (Закон Республики Беларусь от 26.05.2021 № 112-З «Об изменении кодексов по вопросам уголовной ответственности)	110	13	
Неправомерное завладение компьютерной информацией	5	16	36
Изготовление (сбыт) средств для получения неправомерного доступа к компьютерной системе (сети)	1		
Разработка, использование, распространение либо сбыт вредоносных компьютерных программ, или аппаратных средств	82	34	32
Изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего	28	50	143

Таблица 4

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Казахстан

Наименование статьи	2020 г.	2021 г.	2022 г.
Всего из них:	15 200	23 009	22 114
Нарушение авторских и смежных прав	14	8	4
Кража (п. 4 ч. 2 ст. 188)	741	1 584	1 000
Мошенничество (п. 4 ч. 2 ст. 190)	14 110	21 275	20 444
Незаконное распространение порнографических материалов или предметов	34	20	10
Незаконные изготовление, производство, приобретение, сбыт или использование специальных технических средств негласного получения информации	12	4	13
Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни	62	70	66
Пропаганда или публичные призывы к захвату или удержании власти, а равно захват или удержание власти либо насильственное изменение конституционного строя	179		1
Организация и участие в деятельности общественного или религиозного объединения либо иной организации после решения суда и запрете их деятельности или ликвидации в связи с осуществлением ими экстремизма или терроризма	48	15	8
Сепаратистская деятельность		1	2
Пропаганда терроризма или публичные призывы к совершению акта терроризма		10	
Заведомо ложное сообщение об акте терроризма		22	135
Пропаганда или незаконная реклама наркотических средств, психотропных веществ или их аналогов, прекурсоров			128
Посредством использования электронных информационных ресурсов (п. 5 ч. 3 ст. 297)			303

Таблица 5

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Кыргызской Республики

Наименование статьи	2020 г.	2021 г.	2022г.
Всего использованием ИКТ: Из них:	117	194	492
Мошенничество	26	76	263
Незаконное изготовление наркотических средств с целью сбыта	15	41	63
Изготовление, распространение экстремистских материалов	52	44	122
Кража	4	7	15
Возбуждение расовой, этнической, национальной, религиозной межрегиональной вражды (розни)	7	3	8
Вымогательство	1	0	5
Присвоение и растрата вверенного имущества	0	0	4
Незаконное изготовление наркотических средств без цели сбыта	9	1	4
Нарушение неприкосновенности частной жизни	1	0	3
Незаконный оборот оружия	2	1	1
Создание преступного сообщества	1	0	0
Вовлечение ребенка в порнобизнес	1	5	1
Понуждение к действиям сексуального характера	2	0	1
Создание опасности для потребителей	0	0	1
Организация и содержание притона для проведения азартных игр, проведение азартных игр	1	4	0
Заведомо ложное сообщение о совершении преступления	1	1	0
Подделка документа	1	0	0
Содействие проституции и разврату	2	1	0
Содействие террористической деятельности	1		0

Таблица 6

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Молдова

Наименование статьи	2020 г.		2021 г.		2022 г.	
	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто
Всего И них:	193		293		386	
Доведение до самоубийства или содействие совершению самоубийства	0	0	0	0	2	2
Умышленное причинение телесного повреждения средней тяжести или иного средней тяжести вреда здоровью	0	0	0	0	1	1
Угроза убийством или причинением тяжких телесных	3	3	1	0	1	0
Сексуальное домогательство	2	0	1	0	0	0
Развратные действия	0	0	2	1	4	0
Нарушение неприкосновенности частной жизни	12	6	20	6	19	7
Нарушение тайны переписки	5	0	1	0	0	0
Нарушение неприкосновенности жилища	0	0	2	2	2	2
Умышленное воспрепятствование деятельности средств массовой информации или запугивание за критику	0	0	0	0	1	0
Кража	58	17	85	7	57	15
Грабеж	1	1	3	3	0	0
Шантаж	1	1	4	3	9	5
Мошенничество	77	14	147	29	177	46
Присвоение чужого имущества	0	0	1	0	0	0
Нарушение владения	1	1	0	0	0	0
Причинение имущественного ущерба путем обмана или злоупотребления доверием	1	1	0	0	0	0
Ненадлежащее выполнение родительских обязанностей	0	0	0	0	1	1
Вовлечение несовершеннолетних в преступную деятельность	0	0	0	0	2	1
Незаконный оборот наркотиков, этноботанических	1	0	1	1	0	0

Наименование статьи	2020 г.		2021 г.		2022 г.	
	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто
средств или их аналогов не в целях отчуждения						
Незаконный оборот наркотиков, этноботанических средств или аналогов таковых с целью отчуждения	0	0	0	0	3	0
Сутенерство	2	2	0	0	0	0
Отмывание денег	0	0	0	0	1	0
Манипулирование на рынке капитала	1	0	1	0	1	0
Присвоение, незаконное отчуждение, сокрытие заложенного, замороженного имущества, имущества, взятого в лизинг, арестованного или конфискованного имущества	0	0	0	0	1	0
Несанкционированный доступ к компьютерной информации	1	0	2	0	4	1
Неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов	0	0	1	0	0	0
Неправомерный перехват передачи информационных данных	0	0	0	0	3	0
Нарушение целостности информационных данных, содержащихся в информационной системе	0	0	0	0	0	0
Воздействие на функционирование информационной системы	2	0	0	0	2	0
Неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных	0	0	0	0	0	0
Подлог информационных данных	1	0	2	0	59	11
Информационное мошенничество	12	0	11	0	5	0
Нарушение правил безопасности информационных систем	0	0	2	1	2	1
Несанкционированный до-	1	0	1	0	0	0

Наименование статьи	2020 г.		2021 г.		2022 г.	
	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто	Зарегистрировано	Раскрыто
ступ к сетям и услугам электросвязи						
Заведомо ложное сообщение о террористическом акте	2	2	2	1	14	0
Хулиганство	0	0	1	1	0	0
Ложный донос или ложная жалоба	0	0	1	1	0	0
Ложное показание, заключение или неправильный перевод	0	0	1	1	0	0
Неисполнение мер защиты жертвы насилия в семье, установленных защитным предписанием	2	2	0	0	12	10
Злоупотребление властью или служебным положением	1	0	0	0	0	0
Превышение власти или служебных полномочий	2	1	0	0	0	0
Злоупотребление служебным положением	1	0	0	0	0	0
Умышленные действия, направленные на разжигание национальной, этнической, расовой или религиозной вражды, дифференциации или розни	0	0	0	0	1	0
Самоуправство	1	1	0	0	0	0
Изъятие, хищение, сокрытие, повреждение или уничтожение документов, печатей, штампов или бланков	1	0	0	0	1	1
Изготовление, владение, сбыт или использование поддельных официальных документов, печатей, штампов или бланков	1	1	0	0	1	0

Таблица 7

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. в Российской Федерации

Наименование статьи	**2020 г.**	**2021 г.**	**2022 г.**
Всего зарегистрировано преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации, тыс. Из них:	510,4	517,7	522,1
Кража	173,4	156,7	113,5
Мошенничество	210,4	238,5	257,6
Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотических средства или психотропные вещества	47,1	51,4	62,2
Преступления в сфере компьютерной информации (гл. 28 УК РФ)	4,4	6,8	10,0
Неправомерный доступ к компьютерной информации	4,1	6,3	9,3

Таблица 8

Динамика количества преступлений, совершенных с использованием ИКТ за 2020–2022 гг. на территории Республики Таджикистан

Наименование статьи	2020 г.	2021 г.	2022 г.
Всего зарегистрировано в сфере ИТК Из них:	1 020	627	1 354
Возбуждение национальной, расовой, межэтнической или религиозной вражды	68	6	934
Организация сообщества и иной преступной организации	191	54	16
Организация экстремистского сообщества	756	539	370
Неправомерный доступ к компьютерной информации	1		
Модификация компьютерной информации	3		
Незаконное завладение компьютерной информации	1		
Незаконное изготовление и оборот порнографических материалов или предметов		28	
Финансирование преступлений террористического характера			34

ОГЛАВЛЕНИЕ

Наталья Николаевна Дьяченко
Ольга Андреевна Надейкина
Дмитрий Валерьевич Кирган
Илона Анатольевна Грозан
Вера Александровна Казакова
Олег Иванович Новосельцев
Оксана Владимировна Демковец

СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ НА ПРОСТРАНСТВЕ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Аналитический обзор с предложениями

Редактор *И. П. Стоянова*
Компьютерная верстка *И. П. Стояновой*

Подписано в печать 02.08.2023 Тираж 30 экз.
Формат 60×84 $^{1}/_{16}$ Печ. л 4,5 Уч.-изд. л. 3,0 Заказ № 94

Издатель: ВНИИ МВД России
121069, Москва, ул. Поварская, д. 25, стр. 1

Группа ОП РИО ФГКУ ВНИИ МВД России