Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

ДИПЛОМНАЯ РАБОТА

на тему «Выявление и предупреждение оперативными подразделениями органов внутренних дел преступлений в сфере информационно-телекоммуникационных технологий»

Выполнил: Салахов Ильфат Ильдарович

(фамилия, имя, отчество)

40.05.02 – «Правоохранительная деятельность,
2019 года набора, 092 учебная группа
(специальность, год набора, № группы)

Руководитель:

Доктор экономических наук, доцент,
профессор кафедры криминологии и уголовно-
исполнительного права, майор полиции
Жуковская Ирина Викторовна

Рецензент:

Начальник ОМВД России
по Лаишевскому району
подполковник полиции
Камалиев Ирек Камилевич

Дата защиты: «___» _____2024 г. Оценка_____

Казань 2024

СОДЕРЖАНИЕ:

ВВЕДЕНИЕ

Актуальность темы исследования. В современном мире цифровой трансформации оказались подвержены не только социально-экономические, производственные, управленческие процессы, но и преступность. Внешним проявлением этого процесса являются изменения ее качественных и количественных характеристик, экспоненциальный рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

На сегодняшнем этапе развития общества жизнь почти каждого человека неразрывно связана с современными технологиями. Согласно глобальному статистическому отчету по данным на апрель 2022 года более 2/3 населения планеты используют мобильные телефоны, число уникальных пользователей составляет 5,31 миллиарда человек, а пользователей сети «Интернет» — 4,95 миллиарда, то есть 62,5 % населения.[1] При этом компьютерная (цифровая) информация все чаще используется в качестве инструмента обмана и злоупотребления доверием для хищения денежных средств. Так, только в 2022 году с использованием информационно-телекоммуникационных технологий (далее ИТТ) на территории России было зарегистрировано 522065 преступлений, из которых 272233 фактов являются тяжкими или особо тяжкими.[2]

Изложенное позволяет говорить о безусловной актуальности выбранной темы дипломной работы.

Целью дипломной работы являлось изучение деятельности органов внутренних дел (ОВД) по предупреждению преступлений в сфере информационно-телекоммуникационных технологий и определение наиболее

---

[1] Global Digital 2022: вышел ежегодный отчёт об Интернете [Электронный ресурс]. URL: https://www.sostav.ru/ (дата обращения: 22.09.2023).

[2] Форма 280 раздел 1 ЦСИ ГИАЦ МВД России [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 - ЦСИ ГИАЦ МВД России (дата обращения 21.09.2023 г.).

эффективных мер в рассматриваемой сфере.

Для достижения указанной цели были поставлены следующие задачи:

1. Рассмотреть криминологическая характеристика преступлений в сфере информационно-телекоммуникационных технологий.

2. Изучить общие положения противодействия преступлениям в сфере информационно-телекоммуникационных технологий.

3. Исследовать правовую основу противодействия преступлениям в сфере информационно-телекоммуникационных технологий.

4. Проанализировать особенности предупреждения отдельных наиболее актуальных преступлений в сфере информационно-телекоммуникационных технологий.

Объектом исследования явились общественные отношения, складывающиеся в связи с предупреждением преступлений в сфере информационно-телекоммуникационных технологий.

Предметом изучения в дипломной работе выступили деятельность сотрудников органов внутренних дел по предупреждению данных преступлений.

Методологическую основу исследования составляли общенаучные и частные методы познания (системно-структурный анализ, моделирование, сравнительный, формально-логический, статистический, социологический методы).

Теоретической основой дипломной работы послужили труды таких исследователей как: А.В. Андреев, В.В. Гончар, А.И. Гайдин, А.В. Головчанский, Н.Н. Горач, И.А. Гумаров, О.В. Журкина, И.А. Калиниченко, Н. В. Летѐлкин, Е.А. Пидусов, О.Г. Урденко, Е.О. Филиппова и др.

В качестве эмпирической основы работы выступили интервьюирование руководителей оперативных и следственных подразделений, изучение судебной практики и уголовных дел.

Информационной основой выступили справочно-правовые системы «Консультант плюс», «Гарант», «ГИАЦ МВД России», нормативные правовые акты, учебники, в том числе электронные в общей библиотеке и специальная литература в спецбиблиотеке, а также электронные интернет ресурсы.

ГЛАВА 1 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, ОБЩИЕ ПОЛОЖЕНИЯ И ПРАВОВАЯ ОСНОВА ПРОТИВОДЕЙСТВИЯ ДАННЫМ ПРОТИВОПРАВНЫМ ЯВЛЕНИЯМ

§ 1. Криминологическая характеристика преступлений в сфере информационно-телекоммуникационных технологий.

Информационно-телекоммуникационные сети (далее ИТС) позволяют оптимизировать деятельность по получению, хранению и обработки различных сведений, облегчая жизнь человека. Оперативно полученные сведения становятся основополагающим фактором развития общественного прогресса.

Увеличение экономических показателей функционирования современных информационных сетей показывает занчительные результаты. Только с 2013 года рынок онлайн-торговли вырос в 2 раза с 415 до 800 млрд рублей (для сравнения, в 2009 году оборот составлял всего 90 млрд рублей).[1]

Социальная активность в интернет-пространстве, интеграция делопроизводства в электронную среду, возрастание применения цифровых процессов в деятельности муниципальных и государственных учреждений, переход на электронные платежи являются причинами правой неурегулированности различных общественных отношений.[2] Такие возможности используются в противоправной деятельности.

Согласно нормативным правовым актам[3] к преступлениям, совершенным с использованием (применением) ИТТ или в сфере компьютерной информации относятся следующие: кража с банковского счета,

---

[1] Летѐлкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография, 2019. С. 5.

[2] Журкина О.В., Филиппова Е.О. Проблемы предупреждения мошенничества в сфере компьютерной информации // Российский судья. 2022. № 12. С. 6.

[3] Указание Генпрокуратуры России № 401/11, МВД России № 2 от 19 июня 2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» (Перечень № 20) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 31.08.2023 г.)

а равно в отношении электронны. денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса) (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронны. средств платежа (ст. 159.3 УК РФ), а также преступления, предусмотренные статьями 159.6; п. «в», ч. 3 и п. «в», ч. 5 ст. 222, 222.1; п. «в» ч. 5 ст. 222.2; п. «д» ч. 2 ст. 230; п. «г» ч. 2 ст. 242.2; 272; 273; 274; 274.1 и 274.2 УК РФ.

К рассматриваемым преступлениям могут быть отнесены и другие преступления, если дополнительно имеется квалифицирующий признак, предполагающий использование ИТС, включая сеть «Интернет», при наличии соответствующей отметки, либо отметки о соответствующих способах совершения преступления (с использованием ресурсов глобальной сети, Дракнет, вредоносных компьютерных программ и др.).

Преступления, связанные с информационно-телекоммуникационных технологий могут совершаться как против жизни и здоровья человека, свободы, чести и человеческого достоинства, так и в экономической сфере. Последние доминируют в рассматриваемых преступлениях.

В 2022 году в производстве находилось 630156 уголовных дела, возбужденных по фактам преступлений, связанных с компьютерной информацией, из которых 522065 было зарегистрированы в текущем году. Из них 272233 – тяжких и особо тяжких, 21046 – экономической направленности (4516 – в крупном или особо крупном размерах), 82661 - связаны с незаконным оборотом наркотических средств и психотропных веществ, 984 - развратные действия (ст. 135 УК РФ), 862 – нарушение неприкосновенности частной жизни (ст. 137 УК РФ), 353 – нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ).

Самыми же распространенными преступлениями из указанных зарегистрированных преступлений в 2022 году являлись преступления против собственности (гл. 21 УК РФ), их было зарегистрировано 381550

фактов. Среди них 113530 – кражи (п. «г» ч.3, ч.4 ст. 158 УК РФ), мошенничество (ст. 159 УК РФ) – 249929, мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) – 7288, мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) – 334, вымогательство (ст. 163 УК РФ) – 5721.

Значимую долю преступлений в рассматриваемой сфере в 2022 году занимают: изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ) – 6598, неправомерный оборот средств платежей (ст. 187 УК РФ) – 2647, заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ) – 21424, незаконные приобретение, хранение, перевозка, изготовление, переработка нарк. средств, психотропных веществ или их аналогов.....(ст. 228 УК РФ) – 19643, незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов.... (п. «б» ч.2, чч. 3 - 5 ст. 228.1 УК РФ) - 62209, неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 9308, подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков (ст. 327 УК РФ) – 6661.[1]

Динамика рассматриваемых преступлений за последние три года приведена на графике 1.

[1] Форма 280 раздел 1 ЦСИ ГИАЦ МВД России [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 - ЦСИ ГИАЦ МВД России (дата обращения 22.09.2023 г.).

График 1.

Как видно из приведенного графика рассматриваемые преступления имеют тенденцию на увеличение.

Данные правонарушения причиняют вред не только порядку правомерного использования сетевого пространства, но и правам, законным интересам отдельных граждан, нарушают деятельность государственных органов, подрывают общественную безопасность и могут привести к чрезвычайным ситуациям.

За рассматриваемый период потерпевшими в преступлениях были признаны 369429 граждан, из них 67766 – пенсионеры по старости, 5327 – несовершеннолетние.[1]

По отдельным видам преступлений в сфере информационно-телекоммуникационных технологий наблюдается снижение количества зарегистрированных фактов. Это касается, прежде всего краж, совершаемых с использованием ИТТ. Динамика таких преступлений за последние три года приведена на графике 2.[2]

---

[1] См. там же.

[2] На данном и последующем графике указаны данные ФКУ «Главный информационно-аналитический центр МВД России» за последние три года из соответствующих сборников за 2020 – 2022 годы [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 ЦСИ ГИАЦ МВД России (дата обращения 22.09.2023 г.)

График 2.

С 2020 г. также произошло сокращение преступлений, за которые предусмотрена ответственность за хищения с использованием ИТТ.

Данная тенденция связана прежде всего со следующими обстоятельствами:

1. Значительное влияние оказало действие программного комплекса «Антифрод», который производит анализ всех банковских транзакций. В его структуру входят три системы: обнаружения, предотвращения и анализа фактов мошенничества.[1]

2. Немаловажным фактором снижения числа преступлений послужила эффективная работа платформы для оперативного выявления сетевого и мобильного мошенничества в режиме реального времени RSA Transaction Monitoring and Adaptive Authentication.

[1] В соответствии со ст. 27 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» органы внутренних дел также могут выступать субъектом специального предупреждения преступлений данной категории в случаях, когда система «Антифрод» финансово-кредитных организаций осуществила приостановление подозрительной операции по счетам злоумышленника, однако для возврата похищенных денежных средств клиенту необходимо обратиться в ОВД с целью вынесения сотрудниками органов предварительного следствия постановления о наложении ареста и обращении взыскания на денежные средства, находящиеся в финансово-кредитной организации.

3. Проявилась интенсификация деятельности операторов сотовой связи в блокировке звонков с подменой номера.

4. Произошло увеличение уровня цифровой грамотности населения.

5. Отмечается тенденция конкуренции среди мошеннических групп.[1]

Как показывает рассмотренная статистика, основная нагрузка по данным преступлениям ложится на сотрудников ОВД, в частности на подразделения уголовного розыска территориальных органов внутренних дел.

Нельзя не признать повышение эффективности их работы по раскрытию краж, совершенных с использованием ИТТ.

Динамика раскрытых краж, совершенных с использованием ИТТ за последние три года приведена на графике 3.

График 3.

Мы это связываем с введением в практическую деятельность оперативных подразделений ОВД примерно с середины 2020 года ИБД-Ф «Дистанционное мошенничество».[2]

Данная ИБД-Ф позволяет накапливать информацию о совершаемых хищениях с использованием ИТТ на федеральном уровне и объединяет усилия различных оперативных подразделений по установлению подозреваемых в совершении рассматриваемых краж по банковским

---

[1] Противодействие преступлениям, совершаемым в сфере информационных технологий: учебник / А.В. Андреев, В.В. Гончар, Н.Н. Горач [и др.]; под ред. И.А. Калиниченко. — Москва: ИНФРА-М, 2022. С. 311 – 312.

[2] См. подробнее «О введении в действие ИБД-Ф «Дистанционное мошенничество»: приказ МВД России от 22 апреля 2020 г. № 236.

реквизитам, идентификационным параметрам «гаджетов» правонарушителя (IMEI, IP-адресу, MAC-адресу), биометрическим данным с банкоматов, способу совершения преступления.

Анализируя личность преступника, совершающего преступления, связанные с информационно-телекоммуникационных технологий, можно сказать, что в 2022 году больше всего их было совершено возрастной группой от 30 до 39 лет – 32994 фактов (на основе анализа выявленных преступлений), далее идут возрастные группы от 18 до 24 лет – 20412, от 40 до 49 лет - 16244, от 25 до 29 лет – 15605, 50 лет и старше – 7217, от 16 до 17 лет – 2867, от 14 до 15 лет – 977 соответственно.

Женщинами было совершено 20910 преступлений с применением информационно-телекоммуникационных технологий. Из привлеченных к ответственности за рассматриваемый период 62525 не имели постоянного дохода, 11006 имели высшее образование, 969 – студенты, 3602 – учащиеся, 26124 – были ранее судимы за различные преступления.[1]

В настоящее время в уголовном законодательстве нашей страны отсутствует должное определение ИТС. В то же время, в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» такая категория рассматривается как технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.[2]

Похожее определение закрепляет ГОСТ Р 52653-2006.[3] Поэтому можно говорить о единстве нормативно-правового и технического определения ИТС. Закрепленные в них сущностные особенности позволяют выделить признаки, рассматриваемого понятия: рассмотрение ИТС как технологическую систему;

---

[1] Форма 280 раздел 2 ЦСИ ГИАЦ МВД России [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 - ЦСИ ГИАЦ МВД России (дата обращения 22.09.2023 г.).

[2] Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[3] ГОСТ Р 52653-2006. Национальный стандарт Российской Федерации. Информационнокоммуникационные технологии в образовании. Термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 419-ст). М.: Стандартинформ, 2007. С. 2.

2) основное предназначение – обеспечение передачи сведений по линиям связи; 3) доступ только через использование специальных устройств вычислительной техники.

Верховный суд РФ в постановлении поддержал данную точку зрения и разъяснил, что под вмешательством в функционирование средств хранения и передачи компьютерной информации следует понимать воздействие на средства вычислительной техники (компьютеры), в том числе и портативные (смартфоны, ноутбуки и т. д.), снабженные соответствующим программным обеспечением.[1]

Таким образом, главное функциональное предназначение телекоммуникационной сети – дистанционный обмен информацией. Фактически, ИТС – это технологическая система, являющееся средством получения, хранения и передачи сведений по линиям связи путем использования вычислительных устройств (различных гаджетов, в том числе компьютеров).

Особенностью механизма совершения преступлений в рассматриваемой сфере является специфическая следовая картина, для которой характерно наличие большого количества виртуальных следов. Выявление таких следов, их фиксация и исследование требуют применения современных технических тактических и организационных средств, внедрение которых в практику деятельности правоохранительных органов осуществляется со значительным опозданием. Об этом свидетельствует низкий уровень раскрываемости преступлений, совершаемых в сети Интернет.

Современные сетевые преступники активно применяют способы сокрытия следов своей причастности к совершению преступных деяний путем применения программных и аппаратных способов затрудняющих их идентификацию. Наиболее эффективными средствами анонимизации в сети Интернет на сегодняшний день выступают программные технологии «VPN»,

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Бюллетень Верховного Суда РФ. 2018. № 2. С. 7–13.

«TOR», «SSL», позволяющие менять IP-адреса, создавать динамические или нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров.[1]

Способы совершения преступлений рассматриваемой категории правонарушений постоянно совершенствуются. Приведем наиболее актуальные из них:

1. Хищение денежных средств с банковских счетов граждан путем направления в банки распоряжений о перечислении денежных средств на счета, подконтрольные преступникам.

Распоряжение о переводе создается от имени клиента с применением аутентификаторов и электронных средств платежа, полученных различными способами, наиболее актуальным из которых является использование методов социальной инженерии (психологических знаний, умений, приёмов) при совершении преступлений. В результате таких противоправных деяний владельцы денег сами предоставляют реквизиты своих банковских карт, конфиденциальную информацию, а также паспортные данные, позволяющие провести идентификацию и совершить хищение денег. При развитии атаки по указанному сценарию в зависимости от конкретной ситуации преступники могут инициировать от имени клиента на сервисе переводов платеж с карты на карту, или входят в приложение дистанционного банковского обслуживания под учетной записью клиента и оттуда осуществляют платежи. Данный способ представляет наибольшее распространение и социальную опасность, имеет тенденцию к значительному увеличению.

2. Совершение преступлений в качестве услуги или cybercrime-as-aservice, включающей в себя предоставление в аренду БОТНЕТов (значительное количество компьютеров «зараженных» вредоносными компьютерными программами, используемыми для обеспечения удалённого доступа и управления ими), активно используемыми при совершении

---

[1] Особенности расследования преступлений, совершаемых в сети интернет с использованием средств анонимизации: методические рекомендации / А.И. Гайдин, Е.А. Пидусов, А.В. Головчанский. – Воронеж: Воронежский институт МВД России, 2021. С. 4.

различных преступлений, в том числе организации и проведении DoS и DDoSатак, массовой sms или email рассылки вредоносных программ и фишинговых писем.

Совершение фишинговых рассылок, заключающихся в том, чтобы убедить лицо перейти по электронной ссылке. Другой проблемой является создание преступниками фишинговых сайтов, визуально копирующих сайты известных торговых площадок, финансово кредитных учреждений, транспортных компаний, платежных систем и др. Основной задачей создания фишинговых сайтов является получение от жертвы реквизитов банковской карты, необходимых для дальнейшей оплаты товаров и услуг без согласия держателя карты.

3. Мошенничества на сайтах бесплатных объявлений (Авито, Юла, Drom и др.), которые заключаются в предложении сообщить данные банковской карты для перевода на неё средств в счет оплаты товара, либо в просьбе осуществить предоплату за товар или оплаты каких-либо услуг по фиктивной доставке товара. Данные преступления получили значительное распространение ввиду простоты исполнения и отсутствия необходимости использования сложных технических средств преступниками.

В январе 2019 г. СО ОП № 3 УМВД России по г. Тамбову окончено производством уголовное дело № 11801680034000539 по обвинению Заболотских и Ясулевичуса в совершении мошеннических действий в отношении граждан, проживающих в различных субъектах Российской Федерации, совершенных под предлогом сдачи в аренду жилья в Краснодарском крае и республика Крым на летний период отдыха по объявлениям размещенными ими в сети «Интернет».

4. Кражи с банковского счета, а равно в отношении электронных денежных средств (кражи из электр. кошельков, со счетов физических и юридических лиц) и хищения из банковских устройств самообслуживания с использованием вредоносного программного обеспечения (Black Box атаки).

СУ УВМД России по г. Владимиру в январе 2019 г. окончено производством с направлением в суд уголовного дела № 11701170001008705, в отношении Леонтьева возбужденное по факту хищения денежных средств из банкомата ПАО «МИнБанк» в размере более 4.5 млн руб. Установлено, что Леонтьев сделал в корпусе банкомата отверстия, через которые осуществил подключение флеш-накопителя с вредоносным программным обеспечением Cutlet Maker к его системному блоку, после чего модифицируя компьютерную информацию банкомата, нейтрализовал средства защиты и инициировал автоматическую выгрузку денежных средств. В апреле 2019 г. Леонтьев признан виновным в совершении указанного преступления и ему назначено наказание в виде реального лишения свободы сроком на 3,5 года.

5. Атаки на облачные хранилища данных пользователей, в целях получения доступа к их конфиденциальной информации. Продолжают совершаться взломы электронных почтовых ящиков, учётных записей социальных сетей, в результате чего появляется возможность совершить «кражу цифровой личности» и совершать под её видом различные противоправные действия. Кроме того, всё чаще фиксируются преступления, связанные со взломом различных компьютерных систем в сфере торговли и услуг, с целью получения персональных данных, коммерческой и банковской информации (целевые атаки). В этих же целях работают специализированные Колл-центры, под разными предлогами обзванивающие потенциальных жертв, собирающие информацию о их интересах с целью выработки наиболее реализуемых сценариев хищения у конкретного лица.

В качестве положительного примера расследования подобного преступления можно привести работу СУ УМВД России по Приморскому краю окончившего производством в январе 2019 г. с направлением в суд уголовного дела № 11801050010002354 по обвинению Пугоева в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ.

В ходе предварительного расследования установлено, что Пугоев, через интернет форму wwh-club.net, приобрел в 2017 г. базу данных

реквизиты доступа к электронным почтовым ящикам неопределенного круга лиц, а также вредоносное программное обеспечение. Используя вредоносное программное обеспечение «UBC Universal Brute Checker v2.0.3», «Private Keeper 7.8.1.30», «Money and Shop SoftWare by HIDRA | 3.0.0», «Costco.ca Software v1.0 by Coco», «Checker Sears Inc. Software v1.4 by Coco», «ESP Brute by Coco v1.0», «Amazon Brute\Checker MasterSILVA v7.1» и др. преступник получал доступ к личным кабинетам и данным граждан (ФИО, телефон, банковские карты), зарегистрированным на официальных сайтах различных интернет магазинов, после чего осуществлял от их имени приобретение различных товаров, которые затем перепродавал на указанном форуме за 60 – 70 % от их стоимости, используя для приема оплаты Bitcoin и Qiwi кошельки.

6. Организация незаконного оборота наркотических средств, психотропных веществ, их прекурсоров, оружия, боеприпасов и иных запрещенных к свободному обороту предметов, совершаемых с использованием сети Интернет.

В основном, преступники активно используют программные продукты – анонимайзеры, позволяющие продавцам и покупателям не знать информацию друг о друге и лично не встречаться, ведя зашифрованную переписку. Технологии анонимного обмена информацией посредством анонимайзеров основаны на том, что сообщения неоднократно шифруются и затем отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами, что не позволяет установить местонахождение преступников и их серверного оборудования. Предметы распространятся путём закладок в общедоступных местах.

7. Совершение мошенничеств, связанных с использованием электронной подписи при оказании государственных услуг, регистрации сделок и имущества.

Подводя итог криминологической характеристике преступлений, совершаемых в сфере компьютерной информации, можно отметить, что организаторы и исполнители таких преступлений нередко обладают высокой

квалификацией и глубокими знаниями в области информационных технологий, психологии, банковского обслуживания клиентов и др. Поэтому органам внутренних дел особенно важно противопоставить их действиям своевременные и квалифицированные меры по выявлению, пресечению и предупреждению преступных посягательств в этой сфере, их разоблачению и привлечению виновных к уголовной ответственности.

§ 2. Общие положения противодействия преступлениям в сфере информационно-телекоммуникационных технологий

За последние пару лет количество мобильных транзакций увеличилось в четыре раза и теперь киберпреступники нацеливаются на мобильных пользователей, для того чтобы добывать данные и деньги. Мобильные приложения широко используются не только для развлечения, но и для простоты и удобства выполнения повседневных задач, таких как оплата счетов, управление банковскими счетами, предоставление услуг и т.д. В результате эти приложения более подвержены кибератакам.[1]

В нашем случае в качестве ключевого элемента преступлений выступает ИТС как средство совершения преступления. Информационно-телекоммуникационные сети представляют собой технологические системы, предназначенные для хранения и передачи по линиям связи информации, доступ к которым осуществляется с использованием средств вычислительной техники (компьютеров).

Средство совершения преступления согласно российского уголовного права рассматривается отдельным признаком, который влияет на квалификацию и на назначение наказания.

---

[1] Профилактика преступлений: отечественный и зарубежный опыт: учебное пособие / под общей редакцией Ф.К. Зиннурова. - Казань: КЮИ МВД России, 2023. С. 165.

ИТС, как и любое другое средство совершения преступления, имеют важное значение в современном отечественном уголовном законодательстве, поскольку:

1) являются обязательным признаком объективной стороны основного состава преступления (ч. 3 ст. 137, ч.1 ст. 1712 , ч. 1 ст. 1853 , ч. 1 ст. 282 УК РФ);

2) учитываются при технико-юридическом конструировании квалифицированных составов преступлений, предусмотренных п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 1101 , ч. 2 ст. 1102 , п. «в» ч. 2 ст. 1512 , ч. 2 ст. 2052 , п. «б» ч. 2 ст. 2281 , п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 2421 , п. «г» ч. 2 ст. 2422 , п. «г» ч. 2 ст. 245, п. «б» ч. 2 ст. 2581 , ч. 2 ст. 280, ч. 2 ст. 2801 УК РФ;

3) могут учитываться при назначении наказания в случаях, когда фактически не являются конструктивным признаком, но объективно повышают степень общественной опасности.

Указанные сети являются важным элементом состава преступлений в рассматриваемой сфере, используются ворами, мошенниками. Все начинается с увлечения компьютерными играми в подростковом возрасте. Безконтрольность со стороны взрослых приводит к совершению правонарушений уже в зрелом возрасте.

На степень общественной опасности кроме остального, влияет и содержание объективной стороны преступления. Применение ИТС в качестве средства совершения преступления изменяет содержание самого деяния. То есть, меняется степень общественной опасности.

Сведения о преступлениях, совершаемых с применением ИТТ в статистической отчетности появились сравнительно недавно. Они подтверждают существенный рост преступности в сфере компьютерной информации и ее негативное воздействие на общественные отношения. Список преступлений с использованием ИТТ, как видно из предыдущего параграфа дипломной работы очень велик. В то же время основными способами совершения таких преступлений остаются «социальная

инженерия» и «фишинг». Правонарушители используют беспечность граждан для получения доступа к их «личному пространству» («мобильный банк», страницы в социальных сетях, данные банковских карт и др.). Возможности ИТС позволяют преступникам обеспечивать себе анонимность и избегать наказания. Поэтому можно говорить о повышенной общественной опасности применения таких сетей как средства совершения преступления.

Согласно позиции Верховного суда РФ, закрепленную в Постановлении Пленума от 22.12.2015 № 58 «О практике назначения судами Российской Федерации уголовного наказания» (п. 1) характер общественной опасности посягательства определяется из совокупности признаков конкретного состава преступления, установленного Уголовным кодексом. Судам следует в первую очередь учитывать направленность деяния на охраняемые законом социальные ценности и причиненный им вред. То есть Пленум Верховного Суда РФ, как и уголовно-правовая доктрина, во главу угла при определении качественного содержания посягательства ставит характеристики объекта преступления. Степень же общественной опасности в целом зависит от обстоятельств.[1]

Применение ИТС (включая сеть «Интернет») позволяет совершать преступления, имеющие международную окраску, правонарушитель может совершать противоправные действия, находясь за тысячи километров от потерпевшего. Документирование таких действий в свою очередь требует значительных затрат в связи с необходимостью установления и задержания правонарушителя.

Деятельность законодателя по учету совершения преступления с применением ИТТ, безусловно, востребована. Но постепенное включение такого признака в структуру уголовного закона не способно в полной мере противостоять всей массе подобных посягательств в сфере информационно-телекоммуникационных технологий.

---

[1] «О практике назначения судами Российской Федерации уголовного наказания»: постановление Пленума Верховного Суда РФ от 22.12.2015 № 58 // Бюллетень Верховного Суда Российской Федерации. 2016. № 2. С. 17–29.

Для противодействия преступлениям в сфере информационно-телекоммуникационных технологий важно систематизировать всю информацию в этой сфере. Первоочередное значение имеют следующие сведения, содержащие:

- изготовление и распространение в преступных целях информационных, когнитивных, коммуникационных, компьютерных, робототехнических, космических и иных высоких технологий;

- деятельность преступных групп, использующих высокие технологии для возможного совершения преступлений в банковской, научно-технической, оборонно-промышленной, космической и иной подобных сферах;

- противоправная деятельность разведывательных и специальных служб, использующих компьютерную информацию;

- деятельность террористических и экстремистских организаций, применяющие компьютерную информацию;

- посягательства на функционирование объектов критической информационной инфраструктуры нашего государства;

- продвижение идеологии киберпреступников и их криминальной субкультуры в молодежной среде;

- деятельность международных преступных групп, совершающих рассматриваемые преступления на территориях нашей страны.

Данная информация должна являться объектом предупредительной работы. Каждый из них должен попадать под юрисдикцию отдельных правоохранительных органов. Приведенный перечень объектов не является исчерпывающим, он может быть расширен за счет новых факторов, влияющих на развитие преступности в рассматриваемой сфере.

К числу общих субъектов предупредительной работы в рассматриваемом направлении следует отнести: федеральные органы государственной власти, органы государственной власти субъектов

Российской Федерации, органы местного самоуправления, институты гражданского общества, организации и физические лица.

К числу специальных субъектов относятся различные правоохранительные органы, специальные частные гражданские организации.

С вступлением в силу Федерального закона от 27 июня2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» и запуском автоматизированных систем «ФинЦЕРТ» и «Фид-Антифрод» кредитно-финансовые организации наделены полномочиями своевременно блокировать незаконные транзакции.

Разработан проект федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации», наделяющий Банк России правом досудебной либо внесудебной блокировки фишинговых сайтов и мошеннических колл-центров, что в сочетании с выполнением кредитно-финансовыми организациями требований действующего законодательства в области обеспечения информационной безопасности призвано обеспечить комплексную защиту средств клиентов.

МВД России приняло участие в подготовке проекта федерального закона «О внесении изменений в Федеральный закон «О банках и банковской деятельности», в соответствии с которым предлагается сократить сроки предоставления правоохранительным органам запрашиваемой информации до 5 суток[1].

Однако, проанализировав результат деятельности ОВД по противодействию всем видам рассматриваемых мошенничеств, приходим к выводу, что принимаемые меры недостаточно разработаны и необходимо дальнейшее совершенствование данного направления деятельности.

---

[1] Решение Коллегии МВД России от 1 ноября 2019 г.№ 3КМ.

Росту данных преступлений способствует широкое распространение и использование банковских карт, а также операций, совершаемых в сети «Интернет» и с помощью мобильных средств связи. Даная ситуация обусловлена отсутствием единообразной практики применения норм уголовного закона об ответственности за мошенничества, возникающими проблемами квалификации отдельных их видов.

С множеством проблем сталкиваются сотрудники ОВД, одним из них является определение места совершения преступления. В связи с этим в территориальные органы МВД России на окружном, межрегиональном и региональном уровнях направлено указание МВД России от 13 июля 2015 г. №1/5562 «Об организации работы по противодействию отдельным видам мошенничества»[1]. В нем указано, что проверка по заявлению о мошенничестве с использованием средств мобильной связи должна проводиться органом, принявшим заявление, с последующим принятием процессуального решения. Тем не менее, не во всех органах внутренних дел организовано надлежащее исполнение данного указания.

Разрешению вышеназванных вопросов, обеспечению законности принимаемых процессуальных решений, повышению качества расследования дел указанной категории будут способствовать разъяснения в новой редакции постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[2], подготовка которого осуществляется при участии МВД России, а также разработка ведомственного нормативно-правового акта, регламентирующего порядок рассмотрения заявлений о дистанционных мошенничествах. Дистанционное мошенничество в настоящее время наиболее распространенный вид мошенничества, когда происходит опосредованный контакт злоумышленника с потерпевшим с помощью средств связи или сети Интернет.

---

[1] Письмо МВД РФ от 13.07.2015 № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества».

[2] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда от 30.11.2017 г. №48 // Российская газета. - №208. – 2017.

Изучение аналитических справок в рамках преддипломной практики в оперативных подразделениях свидетельствует о том, что Основную массу мошенничеств с использованием средств связи и сети Интернет, дистанционно совершают лица цыганской национальности, находящиеся (постоянно или временно) в момент совершения преступления в других регионах России: Калужской области (г. Малоярославец), Пензенской область (г. Пенза), Челябинской области (г. Челябинск), Пермской области (г. Пермь – челябинские цыгане), Ростовской области (г. Батайск), Владимирской области (пос. Савница, Петушки, Городище), Республике Башкортостан (г. Уфа), Свердловской области, Чувашской области (г. Ново-Чебоксарск), а также Тульской области, Краснодарского и Ставропольского краев.

Идентификация данных граждан, установление их точного местонахождения и задержание являются не просто трудными, но и достаточно затратными мероприятиями по временным и иным задействуемым ресурсам. Учитывая, что основная масса преступлений совершается лицами, которые находятся за пределами региона, приходится направлять личный состав ОВД в другие субъекты РФ, затрачивая значительные суммы на командировочные расходы. Кроме этого по каждому факту мошенничества, связанного с использованием средств связи и сети «Интернет» требуется исполнение десятков запросов по установлению конкретного абонента. При этом средний срок исполнения фоноскопических экспертиз (с момента поступления материала в ЭКЦ МВД по РТ и до окончания экспертизы) составляет 80 суток, срок компьютерных экспертиз – 100 суток соответственно.

Поэтому нами предлагается повсеместно осуществлять работу по запросам через электронные системы документооборота, проработать вопрос об установлении такого документооборота с организациями, представляющими услуги связи непосредственно оперативными сотрудниками УР, у которых находятся зарегистрированные первичные

материалы по преступлениям. Подразделения ЭКЦ ОВД нужно доукомплектовать соответствующими специалистами для сокращения сроков проведения экспертиз по рассматриваемой линии работы.

Обратим внимание на тот факт, что мошенничество общеуголовной направленности относится к категории латентных преступлений, поэтому граждане редко обращаются в правоохранительные органы с заявлением. Связано с тем, что психоэмоциональное состояние человека не позволяет ему признаться в своей правовой или технической безграмотности, неправоте, ошибочности.

Специальные частные гражданские организации не наделены властными полномочиями в сфере противодействия преступности, но могут оказывать содействие физическим и юридическим лицам по выявлению и предупреждению рассматриваемых нами преступлений (операторы связи, Университет «Иннополис», Dr.Web, Group-IB и др.).

Любой гражданин может использовать свое конституционное право на обращение в государственные органы и органы местного самоуправления, предусмотренное ст. 33 Конституции Российской Федерации, и сообщить в правоохранительные органы информацию о планируемых, готовящихся и совершаемых киберпреступлениях, тем самым участвуя в системе противодействия такой преступности. В связи с этим первоочередной задачей сотрудников правоохранительных органов является должная организация взаимодействия не только с другими организациями, но и отдельными лицами. Для сбора и поступления подобной информации можно создавать специальные ресурсы в интернет-пространстве. При этом сведения могут поступать и обезличенно (анонимно).

Современная система предупреждения преступлений в информационно-телекоммуникационных технологий должна основываться на принципах: законности, соблюдения прав и свобод человека и гражданина, свободы экономической деятельности, гласности, неотвратимости наказания за

совершенное преступление; использования в деятельности современных достижений науки и техники, технологий и информационных систем и др.

Социально-правовое предупреждение преступлений в сфере компьютерной информации имеет некоторые показатели эффективности. Среди них особую значимость приобретают: быстрота реагирования на значимую информацию, межведомственное взаимодействие, обмен сведениями, техническое обеспечение. Современные тенденции диктуют необходимость создания следующих условий для эффективной профилактики преступлений в сфере информационно-телекоммуникационных технологий:

1) своевременная передача сведений о попытке неправомерного использования компьютерной информации, чтобы организации обеспечили оперативное устранение проблемы;

2) развитие государственных операционных систем на национальном и межгосударственном уровнях для работы с информационными потоками;

3) ведение специальных курсов кибербезопасности в образовательных организациях. Оно должно стать обязательной частью обучения каждого гражданина;

4) постоянное совершенствование технологической платформы по недопущению кибератак.

Для осуществления предупредительных действий необходимо знать источники информации о возможном совершении преступлений в сфере информационно-телекоммуникационных технологий. Исходя из изучения практического опыта в рамках преддипломной практики, можно назвать следующие из них:

- техническое средство потерпевшего (заявителя);

- от операторов IP-телефонии (сведения об IP-адресе, MAC-адресе, времени и продолжительности связи, точке доступа к сети «Интернет);

- от операторов сотовой связи;

- от операторов платежных систем, банков и иных кредитных

учреждений;

- техническое средство подозреваемого (обвиняемого);

- информационные ресурсы сети «Интернет».

Резюмируя, отметим, что деятельность сотрудников органов внутренних дел по предупреждению рассматриваемых правонарушений заключается в знании причин и условий совершения отдельных видов киберпреступлений.

§ 3. Правовая основа противодействия преступлениям в сфере информационно-телекоммуникационных технологий

Право человека на пользование информацией независимо от государственных границ закреплено в ст. 19 Всеобщей декларации прав человека[1] и ст. 19 Международного пакта о государственных правах[2]. В 2011 году «Интернет» в Организации Объединенных Наций такое положение признано ключевым средством реализации права и является одним из важнейших инструментов коммуникации. Таким образом, доступ к ИТС (в частности сети «Интернет») признана неотъемлемым правом человека.

Основным нормативным правовым актом в нашем государстве является Конституция РФ[3]. В Конституции закреплены основные предписания по вопросам безопасности, обеспечения прав и свобод граждан, охраны собственности и общественного порядка. В этом нормативном правовом акте нашло отражение фактических обстоятельств, которые указывают, что сбор, хранение, а также распространение и использование информации о частной жизни лица возможно только при наличии согласия такого лица. Кроме того, отмечается, что должностные лица

---

[1] «Всеобщая декларация прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948) [Электронный ресурс] // Доступ из справочной правовой системы «Консультантплюс» (дата обращения 24.09.2023)

[2] Международный пакт о гражданских и политических правах (Нью-Йорк. 16.02.1996) [Электронный ресурс] // Доступ из справочной правовой системы «Консультантплюс» (дата обращения 24.09.2023)

[3] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (Дата обращения: 13.08.2023).

государственных и муниципальных органов обязаны обеспечивать возможность ознакомления с документацией и материалами, которые затрагивают права и свободы граждан

На основе Конституции формулируются принципы правоохранительной деятельности, в частности и те, которые перечислены в ст. 3 комментируемого Закона: законность, уважение и соблюдение прав и свобод человека и гражданина и др.

Она содержит основные предписания по вопросам безопасности, обеспечения прав и свобод граждан, охраны собственности и общественного порядка. В ст. 45 Конституции Российской Федерации говорится, что «Государственная защита прав и свобод человека и гражданина в Российской Федерации гарантируется». Органы внутренних дел и другие субъекты оперативно-розыскной деятельности призваны обеспечивать выполнение этих предписаний во всех направлениях своей деятельности, включая осуществление оперативно-розыскных мер.

Федеральный закон «Об ОРД» является специальным источником законодательного уровня, непосредственно регулирующим отношения в области оперативно-розыскной деятельности (далее ОРД), в том числе в сфере борьбы с преступлениями в сфере компьютерной информации. В рассматриваемом законе оперативно-розыскная деятельность (ОРД) признается как социально полезная, государственно-властная функция и вид юридической практики, объективно необходимой и правомерно применяемой в борьбе с преступностью.

Защита собственности от преступных посягательств, равно как и защита жизни, здоровья, прав и свобод человека и гражданина, обеспечение безопасности общества и государства, составляет одну из главных установленных указанным федеральным законом целей, на достижение которых направлена ОРД специально уполномоченных на то оперативных подразделений соответствующих государственных органов (ст. 1). Одна из основных задач ОРД заключается в добывании информации о событиях или

действиях (бездействии), создающих угрозу экономической безопасности РФ (ст. 2).

В Федеральном законе об ОРД получили правовую регламентацию положения, имеющие особое значение для организации и тактики оперативно-розыскной деятельности по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий (далее ИТТ). К ним следует отнести нормативное закрепление в ч. 1 ст. 6 ФЗ об ОРД таких оперативно-розыскных мероприятий, как: сбор образцов для сравнительного исследования; исследование предметов и документов; наблюдение; обследование помещений, зданий, сооружений, участков местности и транспортных средств; снятие информации с технических каналов связи, получение компьютерной информации. Их применение позволяет повысить эффективность борьбы с рассматриваемыми преступлениями.

Федеральный закон об ОРД является в настоящее время основным правовым актом прямого действия. В предмет его регулирования входят наиболее важные общие вопросы оперативно-розыскной деятельности. Другие нормативные правовые акты лишь дополняют и развивают его отдельные предложения.

Направления деятельности сотрудников оперативных подразделений ОВД закреплены в Федеральном законе от 7 февраля 2011 г. № 3-ФЗ «О полиции»[1]. Он относит к их числу защиту личности, общества, государства от противоправных посягательств; выявление, предупреждение и раскрытие преступлений, производство дознания по уголовным делам, розыск лиц (ст. 1 - 2), определяет место ОВД в системе государственных органов исполнительной власти, их задачи, принципы и правовую основу деятельности, взаимоотношения с гражданами, организацию, обязанности и права. Так, в соответствии со ст. 12 этого закона на сотрудников полиции

[1]Федеральный закон «О полиции» от 07.02.2011 г. № 3-ФЗ // СЗ РФ от 14.02.2011 г. № 7. Ст. 900.

возлагаются обязанности по осуществлению оперативно-розыскной деятельности в целях выявления, предупреждения, пресечения и раскрытия преступлений, обеспечения собственной безопасности, а также в иных целях, предусмотренных федеральным законом (п. 10). Эти положения непосредственно указывают на необходимость принятия сотрудниками полиции мер по борьбе с рассматриваемыми преступлениями.

К основополагающим законодательным актам, создающим правовые предпосылки для применения конкретных мер сотруднкиами оргвнов внутренних дел, относится Уголовный кодекс РФ (УК РФ). Подробнее положения УК РФ в рассматриваемой сфере были рассмотрены в предыдущих параграфах. К правовой основе предупреждения и раскрытия рассматриваемых преступлений относится ряд законов, включающих правовые нормы, содержащие предписания о необходимости применения оперативно-розыскных, уголовно-процессуальных, административно-правовых и иных мер, или регулирующих отдельные общие вопросы правоохранительной деятельности.

Основополагающее значение для организации сотрудниками органов внутренних дел и их подразделений деятельности по противодействию преступлениям в сфере компьютерной информации имеют конкретные нормы уголовно-процессуального законодательства. УПК Российский Федерации устанавливает такие понятия, как обстоятельства, подлежащие доказыванию, доказательства и недопустимые доказательства, перечень преступлений, по которым проводится предварительное следствие и их подследственность и др. Они являются основой для организации и осуществления противодействия лицам, обосновано подозреваемым в подготовке или совершении преступлений (ст.ст. 38, 41, 73-84, 85-90, 140-145, 146-149, 150, 151, 163 и др.).

Строгий учет требований уголовно-процессуальных норм при выявлении, предупреждении и раскрытии преступлений, особенно на этапах документирования преступной деятельности подозреваемых лиц и

реализации оперативно-розыскных данных, во многом определяет следственную и судебную перспективу материалов оперативно-розыскной деятельности органов внутренних дел.

Важное значение для профилактики рассматриваемых преступлений имеет Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации», который устанавливает правовую и организационную основу системы профилактики правонарушений, общие правила ее функционирования, основные принципы, направления, виды профилактики правонарушений и формы профилактического воздействия, полномочия, права и обязанности субъектов профилактики правонарушений и лиц, участвующих в профилактике правонарушений. В ст. 17 данного закона раскрыты формы профилактического воздействия (правовое просвещение и правовое информирование; профилактическая беседа; профилактический учет и др.).[1]

При этом конкретные права граждан по участию в предупреждении преступлений закреплены в Федеральном законе от 02.04.2014 № 44-ФЗ «Об участии граждан в охране общественного порядка»[2]. В соответствии с этим нормативным правовым актом граждане могут объединяться в «народные дружины и общественные объединения правоохранительной направленности», оказывать внештатное сотрудничество (ст.10). К гражданам, желающим участвовать в такой деятельности, предъявляются определенные требования (не могут участвовать в организациях правоохранительной направленности лица, имеющие неснятую или непогашенную судимость; страдающие психическими расстройствами, больные наркоманией или алкоголизмом; в отношении которых осуществляется уголовное преследование; ранее осужденные за умышленные преступления и др.).

---

[1] Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

[2] Федеральный закон от 02.04.2014 № 44-ФЗ «Об участии граждан в охране общественного порядка» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

К числу вторых относятся следующие законы:

1) Федеральный закон «О прокуратуре Российской Федерации».[1] В соответствии с частью второй статьи первой этого закона прокуратура осуществляет «надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие».

2) Федеральный закон от 7 июля 2003 г. «О связи»[2] определяет вопросы взаимодействия предприятий связи с органами, осуществляющими правоохранительную деятельность (ст. 14). Они в соответствии с законодательством Российской Федерации обязаны оказывать содействие и предоставлять органам, осуществляющим оперативно-розыскную деятельность, возможность проведения оперативно-розыскных мероприятий на сетях связи.

4) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».[3] В статье 10.1 содержатся предписания об обязанностях организатора распространения информации в сети «Интернет».

5) Уголовно-исполнительный кодекс Российской Федерации от 8 января 1997 года.[4] В статье 84 данного кодекса нормативно регламентированы важнейшие положения, касающиеся осуществления оперативно-розыскной деятельности в исправительных учреждениях (задачи, субъекты и т.д.).

Основные направления обеспечения информационной безопасности закреплены в Доктрине информационной безопасности Российской

---

[1] Федеральный закон от 17.01.1992 № 2202-1 (ред. от 10.07.2023) «О прокуратуре Российской Федерации» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

[2] Федеральный закон от 7 июля 2003 г. «О связи» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

[3] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

[4] Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ (ред. от 24.06.2023) (с изм. и доп., вступ. в силу с 05.07.2023) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

Федерации. В ней, в числе национальных интересов Российской Федерации в информационной сфере указаны защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности не только уже развернутых, но и создаваемых на территории страны информационных и телекоммуникационных систем.[1]

Утвержденная в 2017 г. Президентом РФ Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы к числу приоритетных задач также относит обеспечение комплексной защиты информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры.[2]

Указом Президента РФ от 12 декабря 2014 г. № К 1274 была утверждена Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в которой представлена государственная Система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА).[3]

Наряду с этим необходимо назвать еще целый ряд нормативных правовых актов ведомственного и межведомственного уровня, в определенной мере затрагивающих различные элементы организации и тактики оперативно-розыскной деятельности ОВД по рассматриваемому направлению деятельности.

---

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_208191/ (дата обращения: 15.09.2023).

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_216363/ (дата обращения: 15.09.2023).

[3] Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: утв. Президентом РФ 12.12.2014 № К 1274. URL: http://www.consultant.ru/ document/cons_doc_LAW_181661/ (дата обращения: 17.09.2023).

Непосредственно регламентируют деятельность органов внутренних дел по предупреждению и раскрытию краж, совершаемых с использованием ИТТ, следующие нормативные правовые акты:

- Инструкция о деятельности органов внутренних дел по предупреждению преступлений, утвержденная приказом МВД России от 17 января 2006 г. № 19;

- Инструкция по организации совместной оперативно-служебной деятельности подразделений ОВД РФ при раскрытии преступлений и расследование уголовных дел, утвержденная приказом МВД России от 29 апреля 2015 г. № 495дсп;

Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд от 27 сентября 2013 г.[1] и др.

Подводя итоги рассмотрению правовой основы противодействия преступлениям в сфере информационно-телекоммуникационных технологий нужно сказать, что решению проблем совершенствования правовой основы предупреждения и раскрытия преступлений в сфере компьютерной информации будет являться криминализация использования сетей телекоммуникации при совершении преступлений в рамках отдельной статьи Особенной части Уголовного кодекса РФ. Об этом говорят и ученые в сфере уголовного права.[2]

---

[1] Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утверждена приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 [Электронный ресурс] // Доступ из справ.- правовой системы СТРАС «Юрист» (дата обращения 29.07.2023 г.).

[2] См., например: Летелкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография, г. Нижний Новгород. 2021. С. 145.

ГЛАВА 2 ПРЕДУПРЕЖДЕНИЕ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Предупреждение мошенничества в сфере информационно-телекоммуникационных технологий.

В предупреждении преступлений принимают участие многие государственные органы и общественные формирования. Значительную роль в решении этой задачи призваны играть территориальные органы МВД России на районном уровне с использованием присущих им сил, средств и методов.[1]

Понятие «предупреждение преступлений органами внутренних дел» сформулировано в Инструкции о деятельности органов внутренних дел по предупреждению преступлений, утвержденной приказом МВД России от 17 января 2006г. №19.

В разделе «Общие положения» данной Инструкции оно определяется как: «…деятельность служб, подразделений и сотрудников органов внутренних дел, осуществляемая в пределах их компетенции, направленная на недопущение преступлений путем выявления, устранения или нейтрализации причин, условий и обстоятельств, способствующих их совершению, оказание профилактического воздействия на лиц с противоправным поведением»[2].

Предупредительная деятельность относительно мошенничества в сфере информационно-телекоммуникационных технологий, как отмечают некоторые исследователи, предусматривает следующие меры: своевременное обнаружение и пресечение совершаемых преступлений, совершенствование современных технических средств, информационное обеспечение работы правоохранительных органов, своевременную разработку новых методов,

---

[1] Гумаров И.А. Основы предупреждения преступлений оперативными подразделениями полиции на районном уровне: учебное пособие – Казань: Казанский юридический институт МВД России, 2020. С. 6.

[2] п. 1 Приложения №1 к Инструкции о деятельности органов внутренних дел по предупреждению преступлений, утвержденной приказом МВД России от 17 января 2006 г. № 19.

средств и приемов расследования и раскрытия преступлений, необходимость создания спецподразделений в ведомственных учреждениях. Что касается виктимологической предупредительной деятельности, то здесь следует проводить профилактические мероприятия, осведомлять о новых методах кибермошенничества, развивать информационную образованность населения в целом и налаживать взаимодействие с правоохранительными органами.[1]

В современном мире, как правило, каждый пользователь имеет гаджет, благодаря которому он может оплачивать и покупать вещи, не выходя из дома, общаться с дальними родственниками, путешествовать и развиваться. Однако нередко возможна и такая ситуация, что лицо для упрощения своей жизни подключает на телефон дополнительную услугу, например оплату онлайн. Такую ситуацию использует обычно злоумышленник для совершения противоправных действий.

Основные проблемы возникают при отслеживании правонарушителя, когда последний использует незарегистрированную SIM-карту. В настоящее время требуется пресекать использование таких SIM-карт через операторов связи. Для предупреждения подозрительных транзакций банки и пользователи должны отслеживать услуги, подключенные к телефону.

Кроме того, в целях оперативной блокировки сайтов, мошеннических колл-центров, номеров телефонов, с использованием которых осуществляются мошеннические действия, требуется разработать и внедрить механизмы взаимодействия органов внутренних дел с другими правоохранительными органами, органами государственной власти и коммерческими организациями; проанализировать актуальность использования рассылки писем гражданам с официального почтового ящика МВД России. В ней должны демонстрировать материалы о современных видах, способах хищений, совершаемых злоумышленниками. Подобного рода информацию необходимо также размещать в самостоятельном разделе

---

[1] Знобищева, А. С. Криминологическая характеристика и предупреждение мошенничества в сфере компьютерной информации (ст. 159.6УК РФ) / А. С. Знобищева // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сборник материалов, Воронеж, 21 мая 2020 года. Том Часть 1. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2020. – С. 83.

официального сайта МВД России, в том числе на официальных сайтах ведомства в субъектах Российской Федерации.

Во взаимодействии со средствами массовой информации органам внутренних дел следует продолжать информировать население о способах совершения преступлений в сфере компьютерной информации и преступлений, в том числе посредством электронных средств платежа.

Основной задачей здесь выступает формирование культуры личной информационной безопасности (правила хранения данных, периодичность и случаи смены паролей, программы родительского контроля за виртуальной деятельностью несовершеннолетних и т. п.).

Нами предлагается обратить внимание на идею введения неких интернет-паспортов при размещении товаров и услуг в интернет пространстве. При этом такая инициатива должна пройти жесткую проверку с точки зрения концепции неприкосновенности частной жизни лица.

Одной из первостепенных организационно-технических мер предупреждения мошенничества в сфере компьютерной информации, на наш взгляд, является создание на основе взаимодействия государственных органов, отраслевых структур и общественных организаций системы мониторинга информационных ресурсов на предмет обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества в целях дальнейшего блокирования данных ресурсов.

Вместе с тем, сотрудникам органов внутренних дел следует усилить работу по выявлению преступлений, которые предшествуют совершению мошенничеств с использованием компьютерной информации. В уголовном законе России есть круг уголовно-правовых норм, предусматривающих ответственность за преступления, создающие условия для совершения именно компьютерного мошенничества. Прежде всего к числу таких норм следует отнести нормы об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и

распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационнотеле-коммуникационных сетей (ст. 274 УК РФ). Изучение статистических данных показывает, что данные нормы применяются крайне избирательно (показатели по количеству лиц, привлеченных по указанным статьям с 2003 по 2017 год из года в год разнятся от 152 до 347, а общее количество преступлений в сфере компьютерной информации исчисляются несколькими тысяч в год)[1].

Таким образом, в целях эффективного предупреждения мошенничества в сфере информационно-телекоммуникационных технологий мы считаем необходимым:

1. продолжить взаимодействие с средствами массовой информации по разъяснению населению новых способов мошенничества с применением ИТТ;

2. актуальную информацию по рассматриваемым преступлениям размещать на официальных сайтах органов внутренних дел;

3. создать на основе взаимодействия государственных органов, отраслевых структур и общественных организаций системы мониторинга информационных ресурсов на предмет обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества;

4. усилить работу по выявлению преступлений, которые предшествуют совершению мошенничеств с использованием компьютерной информации (ст. 272 – 274 УК РФ)

[1] См. там же. С.92.

§ 2. Особенности предупреждения краж, совершенных с банковского счета, а равно в отношении электронных денежных средств

Общими предпосылками к распространению преступлений в сфере информационно-телекоммуникационных технологий, в том числе краж являются такие факторы, как:

рост количества финансовых операций и сделок, осуществляемых опосредованно (интернет-торговля);

повышение доступности и конфиденциальности персональной информации;

снижение возраста пользователей, участвующих в финансовых сделках;

процесс глобализации и технологизации, который стирает границы перемещения денежных средств, товаров и услуг;

разнообразие форм финансовых ресурсов.

Одной из специфичных тенденций рассматриваемых краж является то обстоятельство, что все чаще преступники, в том числе рецидивисты, отбывшие наказание, связанное с лишением свободы, получают от сокамерников знания о более легком и безопасном заработке путем совершения хищений в IT-сфере, в связи с чем происходит распространение указанных преступлений.

При огромной популярности глобальных информационных и социальных сетей, стремительной скорости распространения информации невозможно установить эффективную систему контроля, в том числе социального, за ее содержанием, достоверностью и источниками поступления. Кроме того, существуют риски внесения злоумышленниками намеренных искажений в содержание информации в процессе ее хранения и передачи по незащищенным каналам. Сегодня одновременно используются сети 2G, 3G, 4G и 5G, что делает невозможной выработку единых требований

по их безопасности и значительно усложняет процесс защиты каждого типа сети.

Учитывая, что используется глобальная сеть Интернет рассматриваемое направление необходимо развивать в рамках Международных организаций.

В настоящее время имеются специальные международные организации, деятельность которых направлена на обеспечение безопасности компьютерной информации. Так, например, международное многостороннее партнерство против киберугроз (IMPACT) является исполнительным органом в рассматриваемой сфере — Международного союза электросвязи (МСЭ).

В качестве первого в мире всестороннего альянса против киберугроз, поддерживаемого ООН, IMPACT объединяет правительства, академические организации и экспертов отрасли в целях повышения способности глобального сообщества решать проблемы, связанные с информационной безопасностью. Партнерство IMPACT, штаб-квартира которого расположена в Сайберджае (Малайзия), является оперативной базой для реализации Глобальной программы кибербезопасности МСЭ.

Все кражи, совершаемые в сфере компьютерной информации можно разделить на две группы: 1) дистанционные хищения безналичных денежных средств граждан с использованием средств мобильной телефонной связи (так называемые телефонные кражи); 2) дистанционные хищения безналичных денежных средств граждан с использованием сети Интернет (так называемые интернет-кражи).

В соответствии с разъяснениями Верховного Суда РФ, «когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного

квалифицируются как кража» (п. 17 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Несмотря на это, анализ способов совершения преступлений данного вида показывает, что часто преступники не ограничиваются выяснением только лишь реквизитов банковской платежной карты (БПК) или персональных данных потерпевшего. Например, используя преступную схему с удаленной перерегистрацией Интернет-банка потерпевшего, злоумышленники до окончания преступления (т.е. вплоть до перевода денежных средств с вкладов и счетов потерпевшего) находятся с ним на связи. В ряде случаев они прямо сообщают потерпевшему о намерении перевода денег с его БПК, он это осознает, но по разным причинам продолжает доверять преступникам. В связи с тем что обман в указанных случаях направлен непосредственно на завладение чужим имуществом, полагаем, что действия преступников по-прежнему будут образовывать состав мошенничества (п. 2 указанного Постановления).

Для совершения дистанционных хищений безналичных денежных средств у граждан с использованием средств мобильной телефонной связи преступники используют сотовую или проводную стационарную связь, контактируя с потерпевшими посредством живого разговора по телефону или посредством SMS-сообщений.

Внутри нашего государства борьба с рассматриваемыми преступлениями предполагает развитие государственно-частного партнерства. В связи с этим, в Российской Федерации в 2015 г. Центральным банком РФ по поручению Совета Безопасности РФ был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), в задачи которого входит сбор сведений о кибератаках на банки и их клиентов, о потенциальных киберугрозах, а также передача этой информации финансовым учреждениям и правоохранительным органам.

Современная система предупреждения краж, совершаемых с использованием ИТТ, должна основываться на принципах: законности, соблюдении прав и свобод человека и гражданина, гласности, свободы экономической деятельности, неотвратимости наказания за совершенное преступление; взаимодействия органов власти с институтами гражданского общества, международного сотрудничества и др.

Социально-правовая профилактика указанных преступлений имеет ряд критериев эффективности: скорость реагирования, межведомственное взаимодействие, информирование, развитие технологической платформы. Современные тенденции диктуют необходимость создания следующих условий для профилактики хищений с применением ИТТ:

1) Развитая система взаимодействия органов и организаций на национальном и международном уровне для создания новых хранилищ знаний и данных, развития операционных систем.

2) Обмен информацией с максимальной скоростью при учете интернет трафика для того, чтобы организации сразу после обнаружения угрозы могли обмениваться данными для быстрой ликвидации проблемы.

3) Развитие технологической платформы в связи с тем, что для осуществления эффективного противодействия киберпреступности требуются вычислительные мощности.

4) Ведение комплексной программы кибербезопасности совместно с обучением основам кибербезопаности для того, чтобы обучение основам кибербезопасности стало частью развития образования каждого человека.

Профилактика рассматриваемых правонарушений заключается в знании причин и условий совершения отдельных видов киберпреступлений. Так, например, в качестве основных причин несанкционированных операций с использованием платежных карт являются: использование электронных систем платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности; нарушение клиентом порядка использования такого платежа; побуждение владельца электронных систем

платежа к совершению операции путем обмана и злоупотребления доверием; воздействие вредоносного кода.

Одна из главных мер в предупреждении рассматриваемых преступлений – интернет-мониторинг в целях выявления и своевременной блокировки опасного контента (интернет-пирамиды (хайп-проекты), фишинговые сайты, сайты, размещающие экстремистские, порнографические материалы, онлайн-казино и т. п.). Особое внимание следует обратить на внедрение ПАО «Сбербанк» антифрод-системы в иные финансово-кредитные организации, что обеспечивает временную блокировку счета в случае возникновения сомнений у специалиста в правомерности перевода денежных средств до момента подтверждения собственником.

Особенностью различных хищений с использованием информационно-телекоммункационных технологий является подтверждение правомерности совершения операции владельцем счета, который находится под влиянием злоумышленников. Это связано с тем, что, когда служба банка по противодействию кибермошенничеству в системе дистанционного банковского обслуживания определяет операции как подозрительные при осуществлении фрод-мониторинга такая операция, как правило, блокируется.

Кроме того для получения доступа к личным данным активно используется социальная инженерия (знания психологии, нейролингвистическое программирование). Зачастую хакерами осуществляются атаки виртуального пространства граждан с помощью вредоносного программного обеспечения, позволяя получить удаленный доступ к устройству с дальнейшим совершением противоправных действий.

Успешность противодействия преступлениям в сфере информационно-телекоммуникационных технологий во многом зависит от возможности быстро идентифицировать злоумышленника. Для этого требуются специальные технологии, в том числе использующие искусственный интеллект, которые могут оперативно обнаруживать и реагировать на такие атаки. Законопослушный потребитель информационных услуг является

самым слабым звеном в цепочке обеспечения информационной защиты. В последнее время принципиально поменялось направление атак в сфере компьютерной информции: если раньше они были нацелены на банки и коммерческие организации, то теперь – на физических лиц, если раньше в качестве жертвы выбирали пожилых людей, то с 2019 г. их фокус атак сместился на 25–30-летних.

Особое внимание следует уделить на обеспечение безопасности самих информационных сетей связи. Повышение степени защищенности сетей и устройств, информационно-телекоммуникационных технологий неизбежно приведет и к увеличению стоимости кибератак, что сделает их невыгодными для преступников. Добиться этого можно следующими способами:

1) сканировать клиентские устройства и требовать улучшения их безопасности;

2) отправлять уведомления хостингам, которые используют киберпреступники;

3) распространять доказательства атрибуции атак;

4) блокировать трафик, идущий от атакующего.

Наиболее перспективным направлением повышения защищенности информационно-телекоммуникационных устройств является использование биометрических технологий, которое получит дальнейшее распространение по следующим направлениям:

- идентификация и аутентификация при доступе к определенным системам;

- идентификация сотрудников (сбор информации, поиск инсайдеров, верификация нарушений со стороны персонала).

§ 3. Технико-криминалистические средства и методы получения и изъятия компьютерной информации

Для проведения различных операций с виртуальными следами используют два вида технических средств: общеупотребительные и специализированные. К первому виду относятся программы, которые могут быть известны даже среднестатистическому пользователю, например, для просмотра подключений к компьютеру применяется программа-анализатор трафика для компьютерных сетей Wireshark; вся информация о процессах на компьютере хранится в разделе memory damp, в swap файлах можно найти отпечатки разных программ подключения, а также ряд специализированных прикладных программ (например, «Volatility» - для поиска вирусов и скрытых процессов). Нужно понимать, что в некоторых файлах содержится информация «в миниатюре», например в файлах samp.db.

В экспертную деятельность внедряются программно-аппаратные комплексы, позволяющие комплексно решать целый ряд задач по исследованию компьютерной информации и техники (например, EnCase Forensic Edition, UFED, X-Ways Forensics, Belkasoft, Мобильный криминалист Эксперт). Так, например, «Мобильный криминалист Эксперт» способен извлечь необходимый пласт физических данных. Облачная криминалистика является важным направлением при работе с извлечением данных, так как на современных мобильных устройствах пользователь содержит необходимую информацию в облачном сервисе приложений. X-Ways Forensics - это программный комплекс, позволяющий исследовать носители информации и снимать с них необходимые для расследования уголовного дела сведения.

Кроме этого следует использовать специальные инструменты по извлечению информации, такие как «Zimmerman tools» (она позволяет отображать соответствующие криминалистические данные, включая экспорт

данных во многие широко используемые форматы); Elkomsoft, MOBILed.it; с использованием уязвимости BootROM («загрузчик» устройства) – checkm8.

Для документирования следов преступления с применением ИТТ наиболее эффективными будут являться проведение таких оперативно-розыскных мероприятий как «исследование предметов и документов», «наблюдение» и «сбор образцов для сравнительного исследования». Здесь важно грамотно зафиксировать результаты проведения таких мероприятий. В целях фиксации информации можно использовать фотоаппарат и видеокамеру, такие функции на компьютере как сочетания клавиш «PrtSc» (позволит зафиксировать снимок экрана и перенести в открытый файл), «Alt PrtSc» (для фиксации отдельного «окна» на экране), «Win Shift S» (для копирования части «окна» на экране).

Одной из серьезнейших проблем по сбору цифровых следов является отсутствие технического оснащения в органах внутренних дел.

Имеются недостатки в практическом применении криминалистической техники: чаще всего применяются только определенные средства (UFED и Мобильный криминалист Эксперт), не используют возможности IT – специалистов по сбору информации через Big data (специальные ресурсы по сбору данных), программные возможности изучения разделов memory damp, swap файлов. Это связано с несовершенством организации и правового регулирования использования криминалистической техники; научно-методического и технико-криминалистического обеспечения ее применения. Несмотря на направляемые в территориальные органы внутренних дел алгоритмы действий по работе сотрудников в рассматриваемом направлении, изменить ситуацию не получается: на практике ограничиваются привлечением к ответственности только отдельных участников преступных групп.

В настоящее время необходимо создавать свои отечественные специальные программы для выявления правонарушителей в киберпространстве по аналогии с другими государствами (например,

зарубежное специальное программное обеспечение Magnet Forensics позволило обнаружить улики на 30 электронных устройствах, принадлежащих террористам, ответственным за атаку во время Бостонского марафона (братья Царнаевы, 2013 г.); в 2018 г. Министерство внутренних дел Великобритании доложило о создании лондонской технологической компанией ASI Data Science комплексного инструмента искусственного интеллекта для обнаружения в 95% террористического контента в онлайн-видео, с вероятностью выявления в 99,9%)[1].

[1] Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities. URL: https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov (дата обращения 29.07.2023 г.).

ЗАКЛЮЧЕНИЕ

Резюмируя проведенное исследование в рамках дипломной работы необходимо отметить, что согласно Указанию Генпрокуратуры России № 401/11, МВД России № 2 от 19 июня 2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» к рассмотренным нами преступлениям относятся более 12 составов преступлений. При этом самыми распространенными преступлениями из них в последние годы являлись преступления против собственности. Основная их масса совершена возрастной группой от 30 до 39 лет.

В качестве ключевого элемента преступлений в сфере информационно-телекоммуникационных технологий выступает информационно-телекоммуникационные сети как средство совершения преступления. Используя данный термин законодатель ввел дополнительный квалифицирующий признак в Особенной части УК РФ.

Особенностью механизма преступной деятельности с использованием информационных технологий является специфическая следовая картина, для которой характерна значительная доля виртуальных следов. Обнаружение таких следов, их фиксация и исследование требуют применения современных технических тактических и организационных средств, внедрение которых в практику деятельности правоохранительных органов осуществляется со значительным опозданием.

Для эффективного предупреждения преступлений в сфере компьютерной информации сотрудниками ОВД требуется:

1) продолжить взаимодействие с средствами массовой информации по разъяснению населению новых способов мошенничества с применением ИТТ;

2) актуальную информацию по рассматриваемым преступлениям размещать на официальных сайтах органов внутренних дел;

3) создать на основе взаимодействия государственных органов, отраслевых структур и общественных организаций системы мониторинга информационных ресурсов на предмет обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества;

4) усилить работу по выявлению преступлений, которые предшествуют совершению мошенничеств с использованием компьютерной информации (ст. 272 – 274 УК РФ).

Наиболее перспективным направлением повышения защищенности информационно-телекоммуникационных устройств является использование биометрических технологий, которое, мы надеемся, получит дальнейшее распространение.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Законы, нормативные правовые акты и иные официальные документы

1. «Всеобщая декларация прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948) [Электронный ресурс] // Доступ из справочной правовой системы «Консультантплюс» (дата обращения 24.09.2023)

2. Международный пакт о гражданских и политических правах (Нью-Йорк. 16.02.1996) [Электронный ресурс] // Доступ из справочной правовой системы «Консультантплюс» (дата обращения 24.09.2023)

3. Резолюция, принятая 23 января 2002 г. Генеральной Ассамблеей [по докладу Третьего комитета (A/56/574)] 56/121. Борьба с преступным использованием информационных технологий Генеральная Ассамблея. Режим доступа: https://undocs.org/ru/A/RES/56/121 (дата обращения 13.08.2023 г.).

4. Резолюция Генеральной Ассамблеи ООН от 04.12.2000 № 55/59 (Венская декларация о преступности и правосудии: ответы на вызовы XXI века: Резолюция Генеральной Ассамблеи ООН от 04.12.2000 № 55/59// СПС «КонсультантПлюс» (дата обращения: 26.09.2023).

5. Резолюция, принятая 22 января 2001 г. Генеральной Ассамблеей [по докладу Третьего комитета (A/55/593)] 55/63. Борьба с преступным использованием информационных технологий. Режим доступа: https://undocs.org/ru/A/RES/55/63 (дата обращения: 13.08.2023).

6. Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 г. Режим доступа: https://rm.coe.int/1680081580 (дата обращения 13.08.2023).

7. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. № 1(37). С. 138–145.

8. Решение Совета глав государств Содружества Независимых Государств о Концепции сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий, от 25.10.2013 // URL: http://cis.minsk.by/reestr/ru/index.html# reestr/view/text?doc=4008 (дата обращения: 25.09.2023)

9. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (Дата обращения: 13.08.2023).

10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 15.03.2023) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 25.09.2023 г.)

11. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ (ред. от 24.06.2023) (с изм. и доп., вступ. в силу с 05.07.2023) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 25.09.2023 г.).

12. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 28.04.2023) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 03.07.2023 г.) Федеральный закон «О полиции» от 7 февраля 2011 года № 3-ФЗ (ред. от 29.12.2022) [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 25.09.2023 г.).

13. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

14. Федеральный закон от 02.04.2014 № 44-ФЗ «Об участии граждан в охране общественного порядка» [Электронный ресурс] // Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

15. Федеральный закон от 17.01.1992 № 2202-1 (ред. от 10.07.2023) «О прокуратуре Российской Федерации» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 27.09.2023 г.).

16. Федеральный закон от 7 июля 2003 г. «О связи» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

17. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Доступ из справ.- правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

18. Федеральный закон «О полиции» от 07.02.2011 г. № 3-ФЗ // СЗ РФ от 14.02.2011 г. № 7. Ст. 900.

19. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних: федеральный закон от 29.02.2012 № 14-ФЗ // СЗ РФ. 2012. № 10. Ст. 1162.

20. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» [Электронный ресурс] // Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения 12.08.2023 г.).

21. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации: федеральный закон от 30.10.2009 № 241-ФЗ // СЗ РФ. 2009. № 44. Ст. 5170

22. О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 20.07.2011 № 250-ФЗ // СЗ РФ. 2011. № 30 (ч. 1). Ст. 4598.

23. О внесении изменений в отдельные законодательные акты Российской Федерации в целях совершенствования прав потерпевших в уголовном судопроизводстве: федеральный закон от 28.12.2013 № 432-ФЗ // СЗ РФ. 2013. № 52 (ч. I). Ст. 6997.

24. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению: федеральный закон от 07.06.2017 № 120- ФЗ // СЗ РФ. 2017. № 24. Ст. 3489.

25. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_208191/ (дата обращения: 15.09.2023).

26. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_216363/ (дата обращения: 15.09.2023).

27. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: утв. Президентом РФ 12.12.2014 № К 1274. URL: http://www.consultant.ru/ document/cons_doc_LAW_181661/ (дата обращения: 17.09.2023).

28. Указание Генпрокуратуры России № 401/11, МВД России № 2 от 19 июня 2023 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» (Перечень № 20) [Электронный ресурс] // Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения 31.08.2023 г.)

29. Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд:

утверждена приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 [Электронный ресурс] // Доступ из справ.- правовой системы СТРАС «Юрист» (дата обращения 29.07.2023 г.).

30. Инструкция о деятельности органов внутренних дел по предупреждению преступлений, утвержденная приказом МВД России от 17 января 2006 г. № 19 [Электронный ресурс] // Доступ из справ.- правовой системы СТРАС «Юрист» (дата обращения 29.07.2023 г.).

31. «О введении в действие ИБД-Ф «Дистанционное мошенничество»: приказ МВД России от 22 апреля 2020 г. № 236.

32. ГОСТ Р 52653-2006. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 419-ст). М.: Стандартинформ, 2007.

33. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Бюллетень Верховного Суда РФ. 2018. № 2

34. «О практике назначения судами Российской Федерации уголовного наказания»: постановление Пленума Верховного Суда РФ от 22.12.2015 № 58 // Бюллетень Верховного Суда Российской Федерации. 2016. № 2.

2.Монографии, учебники, учебные пособия

35. Гумаров И.А. Основы предупреждения преступлений оперативными подразделениями полиции на районном уровне: учебное пособие – Казань: Казанский юридический институт МВД России, 2020.

36. Густова Э. В. Построение санкций в уголовном праве Российской Федерации: теоретический аспект: дис. ... канд. юрид. наук. 12.00.08. Воронеж: Воронежский институт МВД России, 2015.

37. Журкина О.В., Филиппова Е.О. Проблемы предупреждения мошенничества в сфере компьютерной информации // Российский судья. 2022. № 12.

38. Знобищева, А. С. Криминологическая характеристика и предупреждение мошенничества в сфере компьютерной информации (ст. 159.6УК РФ) / А. С. Знобищева // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сборник материалов, Воронеж, 21 мая 2020 года. Том Часть 1. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2020.

39. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. …канд. юрид. наук. Пятигорск, 2011

40. Летелкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография, г. Нижний Новгород. 2021.

41. Особенности расследования преступлений, совершаемых в сети интернет с использованием средств анонимизации: методические рекомендации / А.И. Гайдин, Е.А. Пидусов, А.В. Головчанский. – Воронеж: Воронежский институт МВД России, 2021.

42. Паутова Э.В. Квалифицированные виды мошенничества: практический комментарий. М.: Право доступа, 2017.

43. Противодействие преступлениям, совершаемым в сфере информационных технологий: учебник / А.В. Андреев, В.В. Гончар, Н.Н. Горач [и др.]; под ред. И.А. Калиниченко. — Москва: ИНФРА-М, 2022

44. Профилактика преступлений: отечественный и зарубежный опыт: учебное пособие / под общей редакцией Ф.К. Зиннурова. - Казань: КЮИ МВД России, 2023.

3.Статьи, научные публикации

45. Тамаев, Р.С. Предупреждение мошенничества в сфере компьютерной информации / Р.С. Тамаев, М.Д. Фролов // Ученые труды Российской академии адвокатуры и нотариата. – 2018. – № 3(50).

46. Урденко О.Г. Необходимость компьютерной криминалистики (forensics) как науки. Режим доступа: http://www.epos.ua/site/file_uploads/cfu2012_1-4_Urdenko.pdf (дата обращения: 26.09.2023).

47. Форма 280 раздел 1 - 3 ЦСИ ГИАЦ МВД России [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 - ЦСИ ГИАЦ МВД России (дата обращения 21.09.2023 г.).

48. Сборники о состоянии преступности за 2020 – 2022 годы [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 ЦСИ ГИАЦ МВД России (дата обращения 22.09.2023 г.).

49. Global Digital 2022: вышел ежегодный отчёт об Интернете [Электронный ресурс]. URL: https://www.sostav.ru/ (дата обращения: 22.09.2023).

50. Ict facts and figures 2017. Geneva, July 2017 // URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID (дата обращения: 24.09.2023).

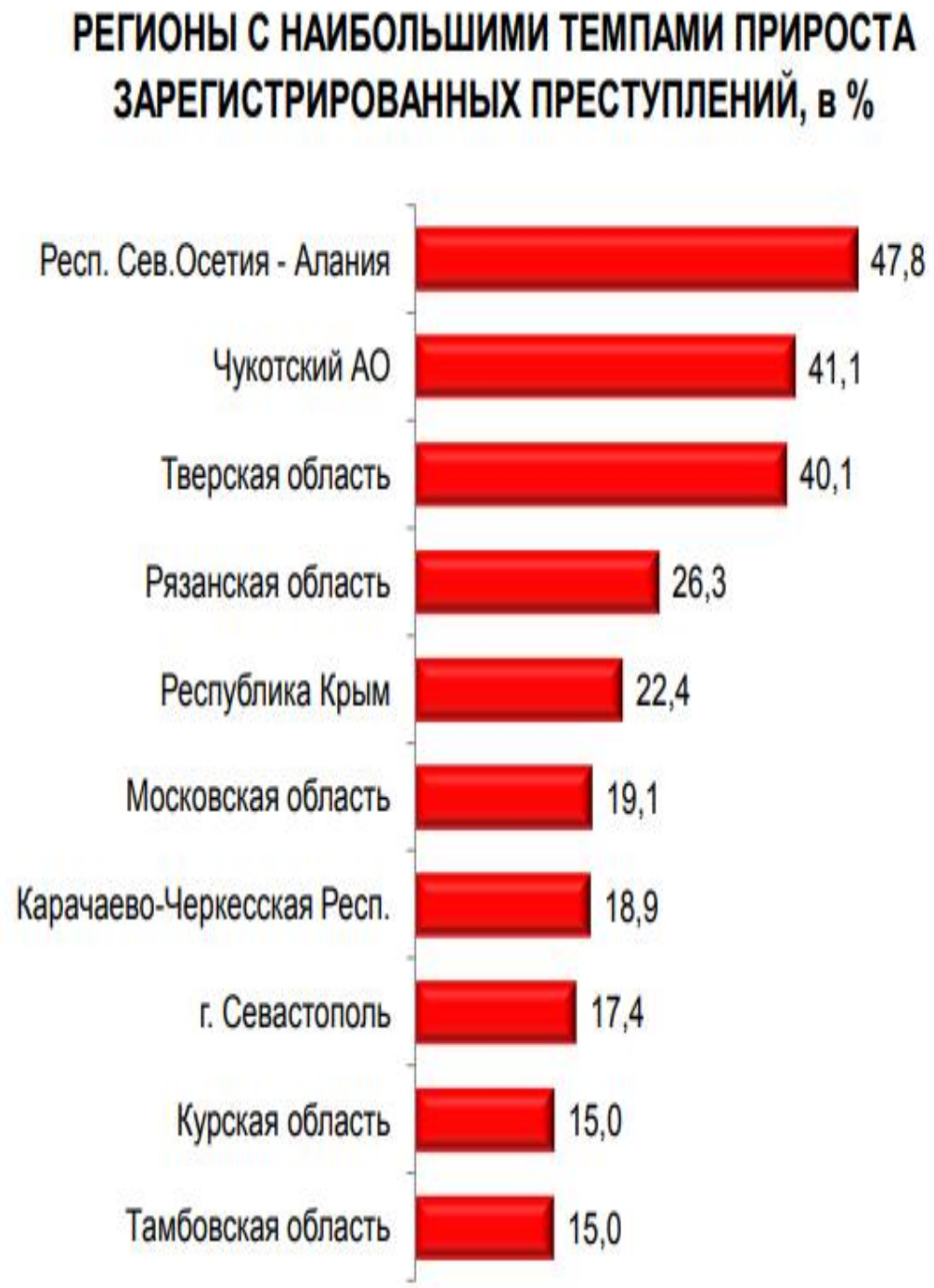
51. Доклад о работе тринадцатого Конгресса Организации Объединенных Наций по предупреждении преступности и уголовному преследованию; Доха, 12-19 апреля 2015 г. // Официальный сайт Организации Объединенных Наций. Режим доступа: http: www.un.org/ru/events/crimecongress (дата обращения 23.03.2021).

52. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: резолюция ООН A/RES/53/70 от 04.12.1998 [Электронный ресурс] // URL: https://documents-

ddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf (дата обращения: 2509.2023)

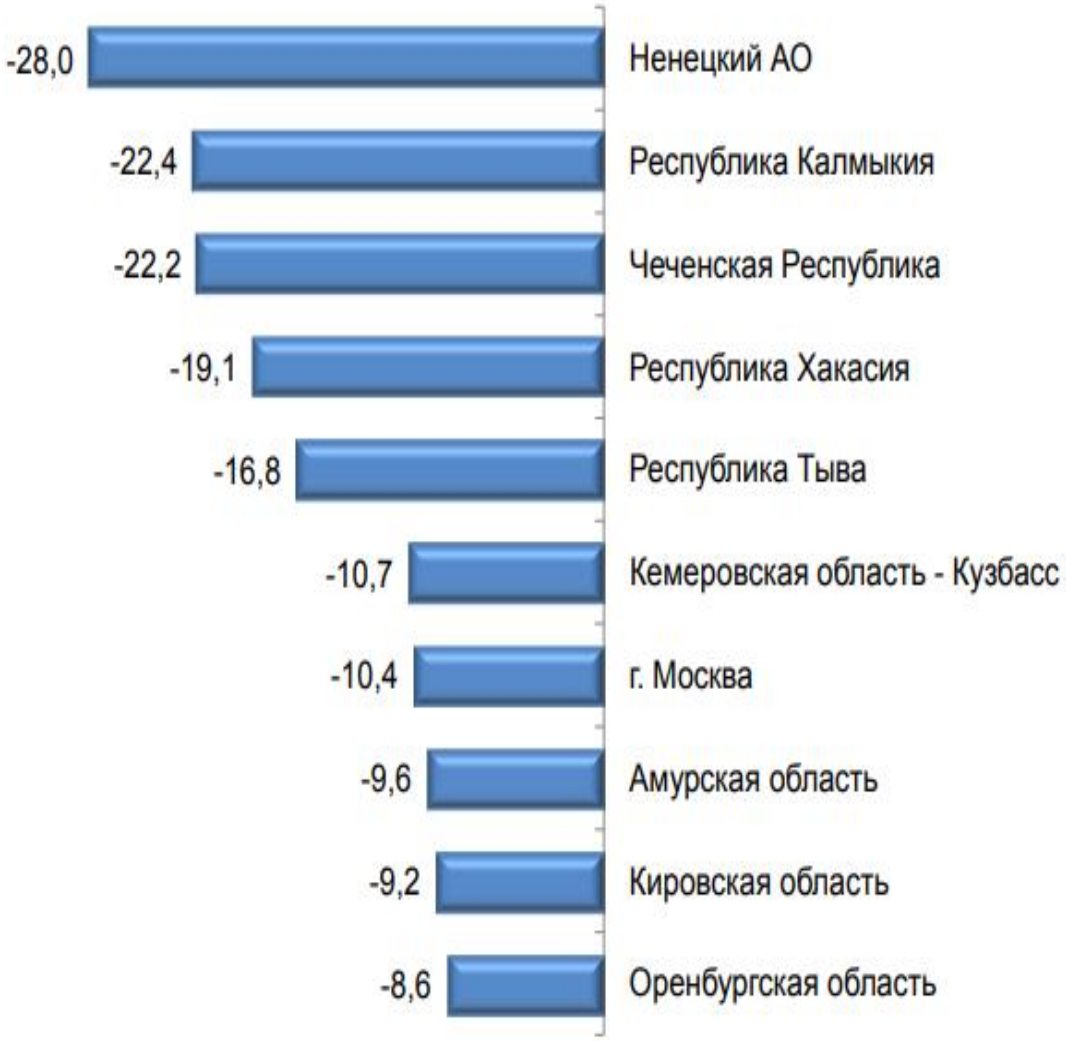
Приложение 1.

ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ЗА 2022 ГОД[1]



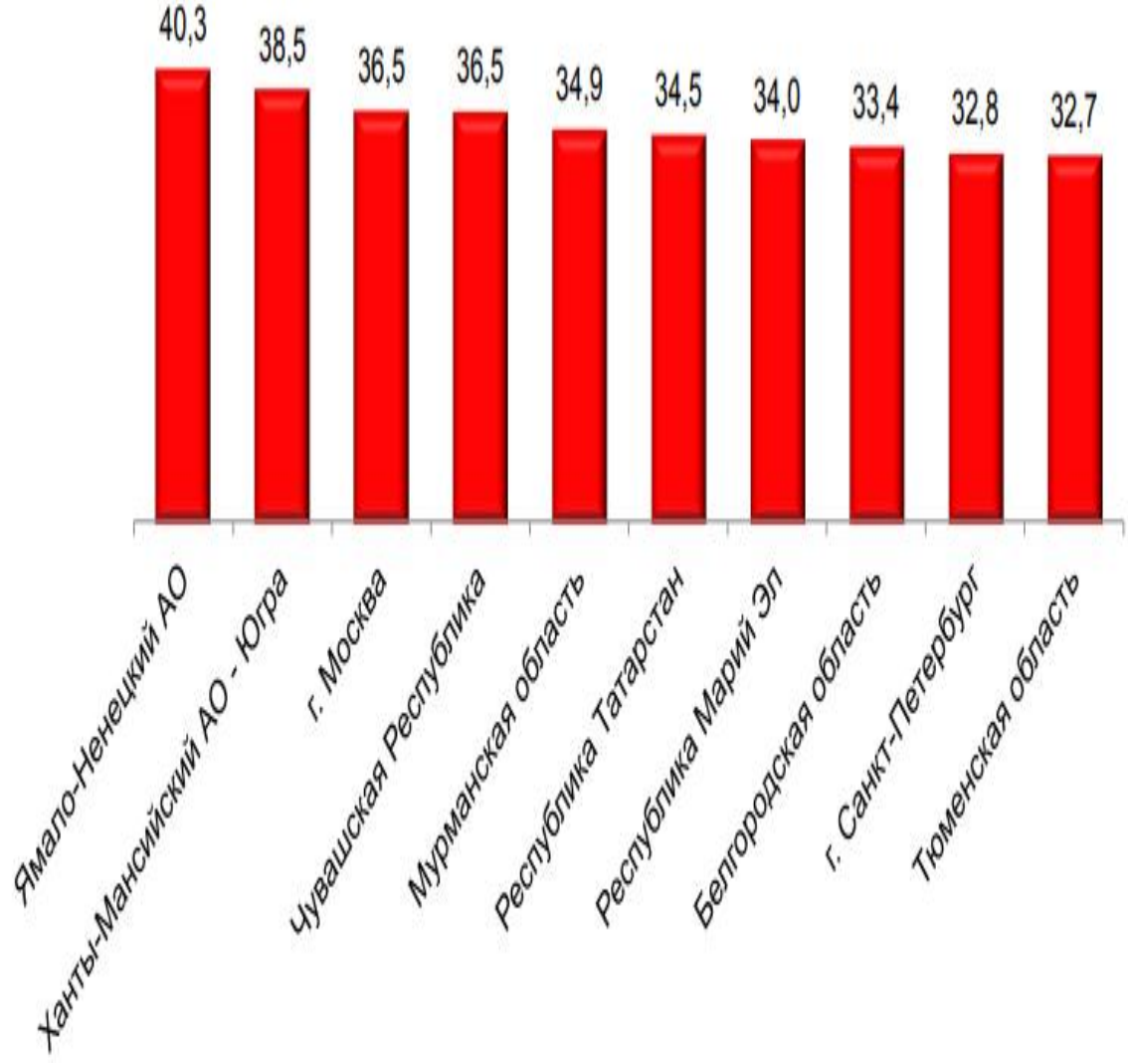
[1] Здесь и далее приводятся данные на основе изучения Формы 280 ЦСИ ГИАЦ МВД России [Электронный ресурс] // Доступ из СЭД МВД России: 10.5.0.15 - ЦСИ ГИАЦ МВД России (дата обращения 27.09.2023 г.).

РЕГИОНЫ С НАИМЕНЬШИМИ ТЕМПАМИ ПРИРОСТА ЗАРЕГИСТРИРОВАННЫХ ПРЕСТУПЛЕНИЙ, в %

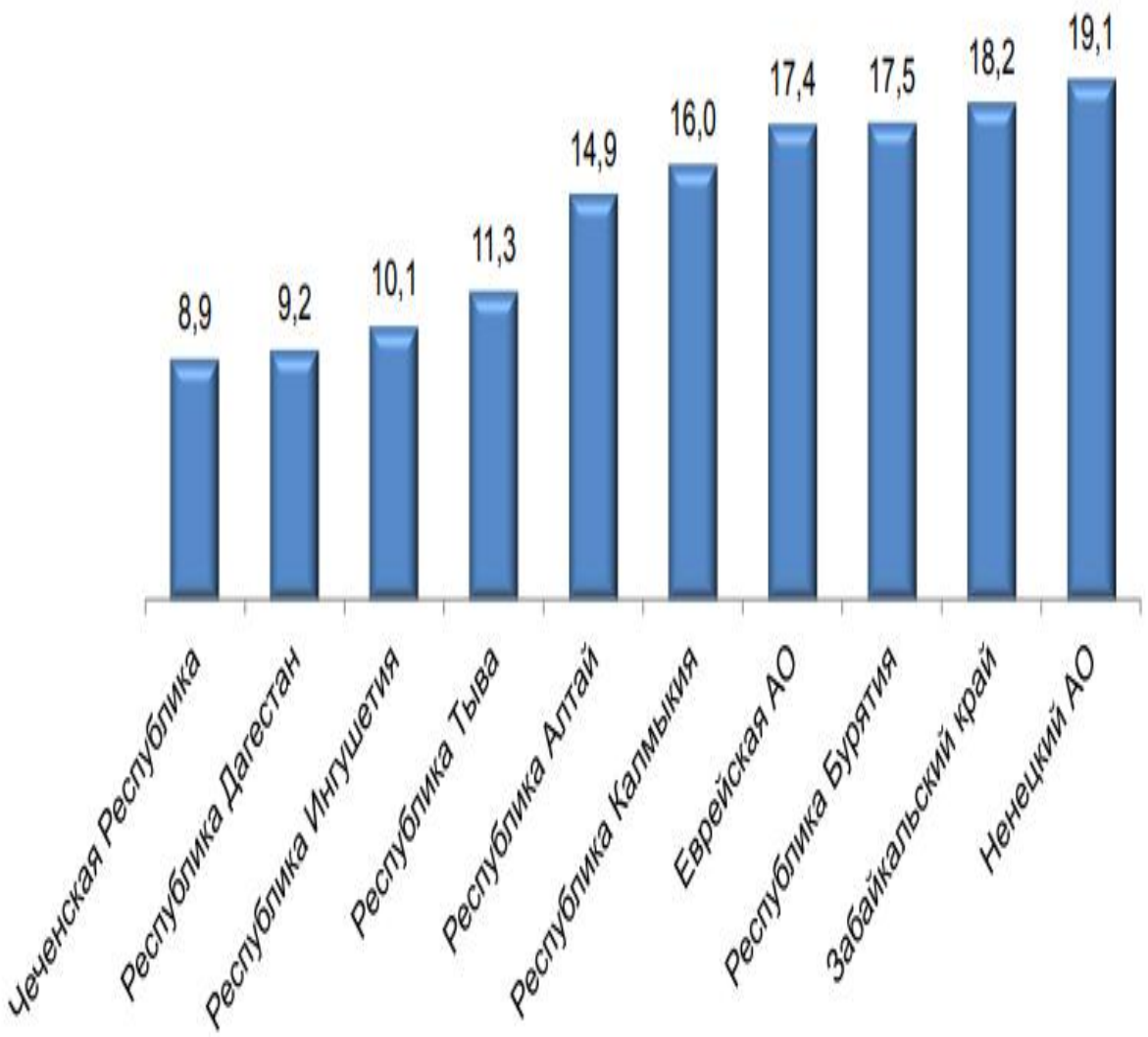


УДЕЛЬНЫЙ ВЕС ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (В ОБЩЕЙ СТРУКТУРЕ ПРЕСТУПНОСТИ)

РЕГИОНЫ С НАИБОЛЬШИМ УДЕЛЬНЫМ ВЕСОМ, в %

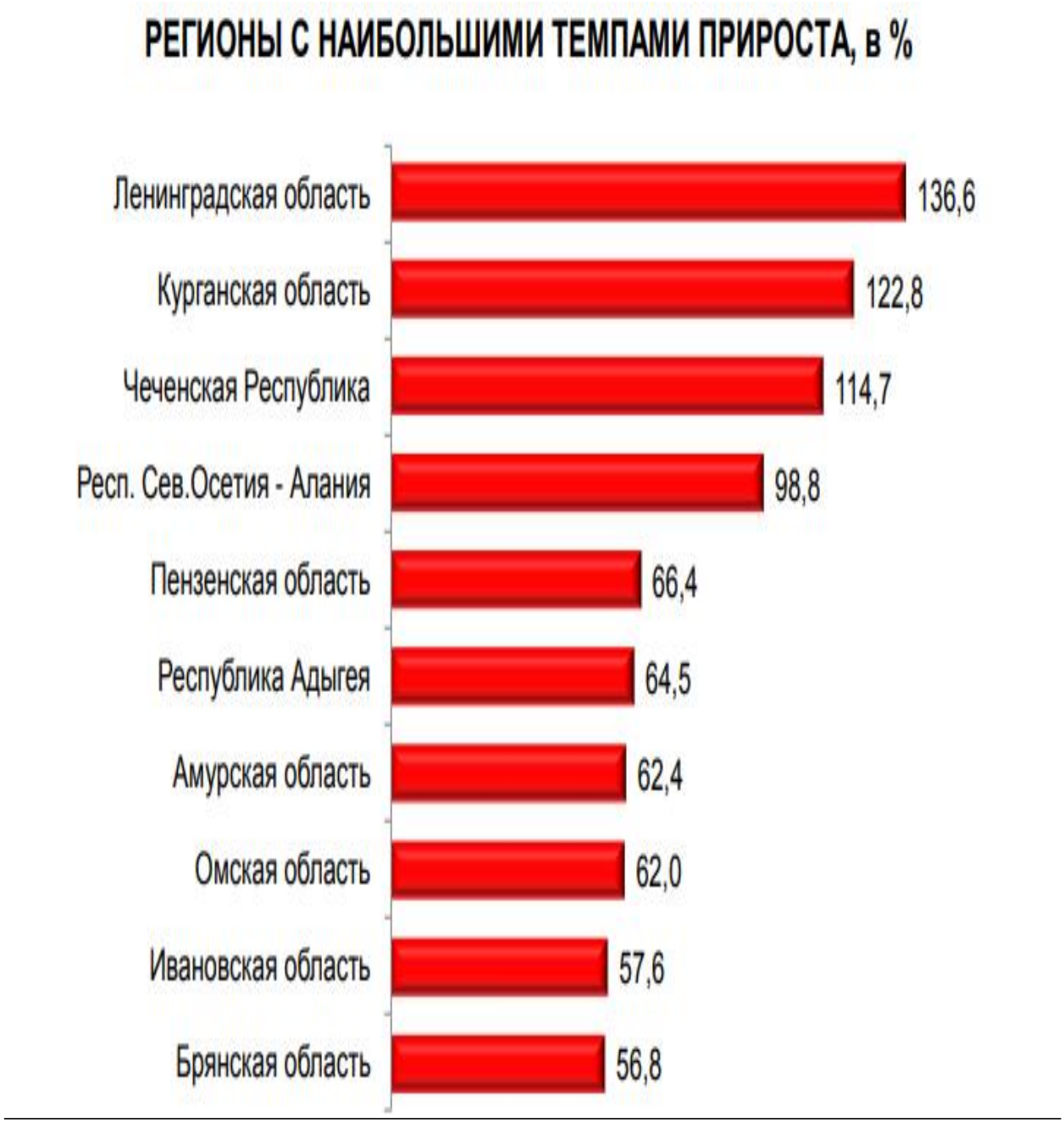


РЕГИОНЫ С НАИМЕНЬШИМ УДЕЛЬНЫМ ВЕСОМ, в %

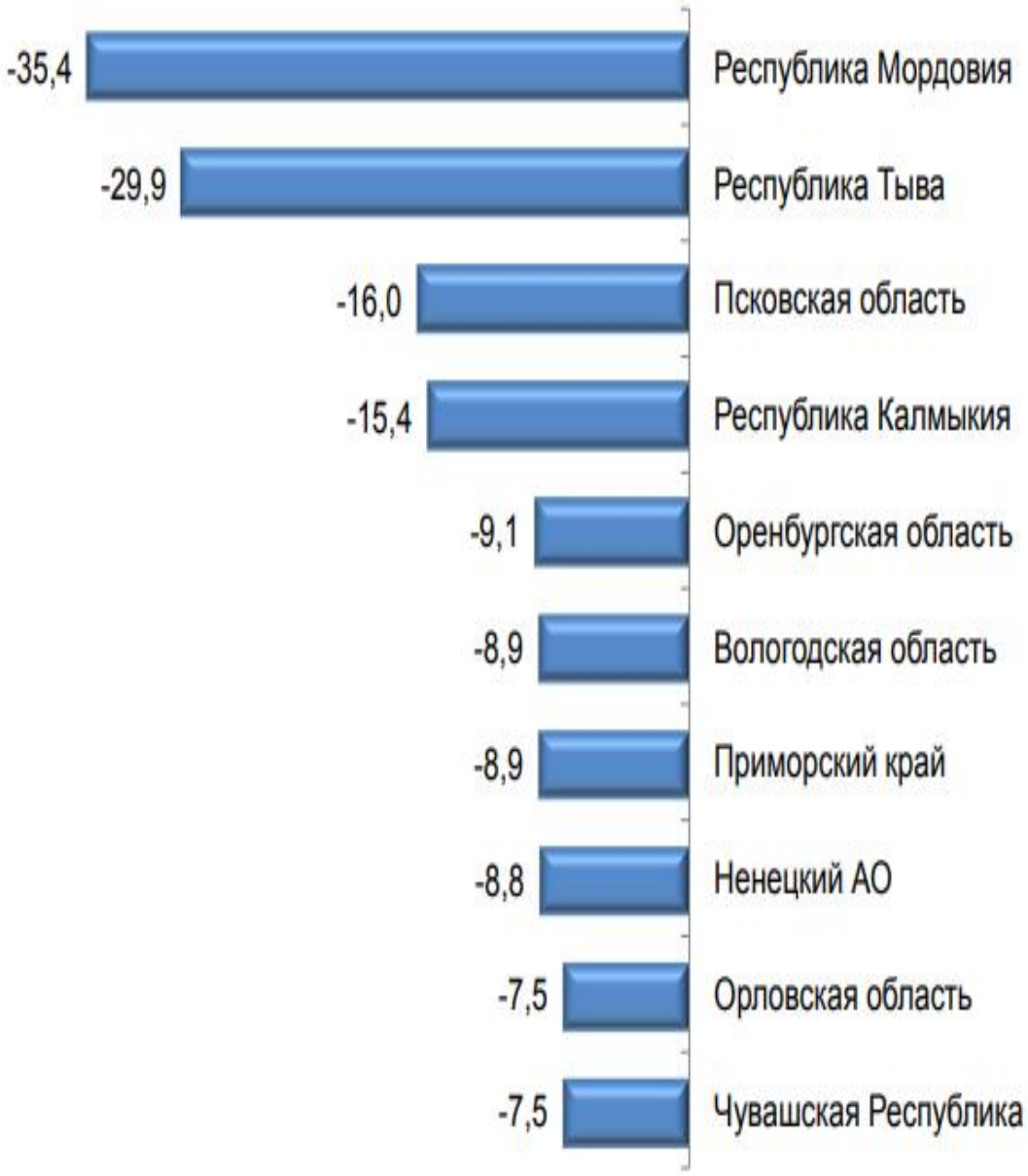


Приложение 2.

ПРЕДВАРИТЕЛЬНО РАССЛЕДОВАННЫЕ ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В 2022 ГОДУ

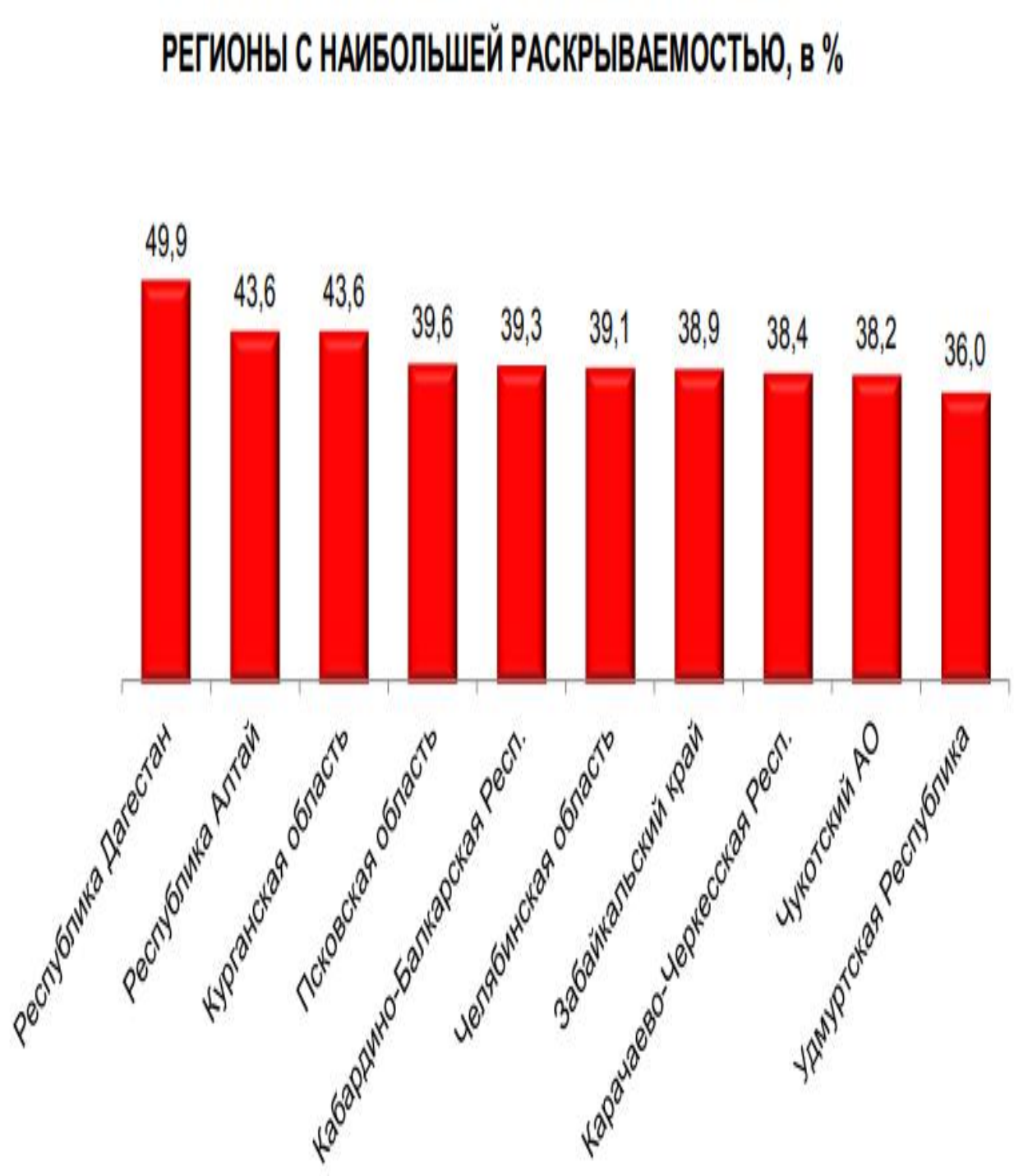


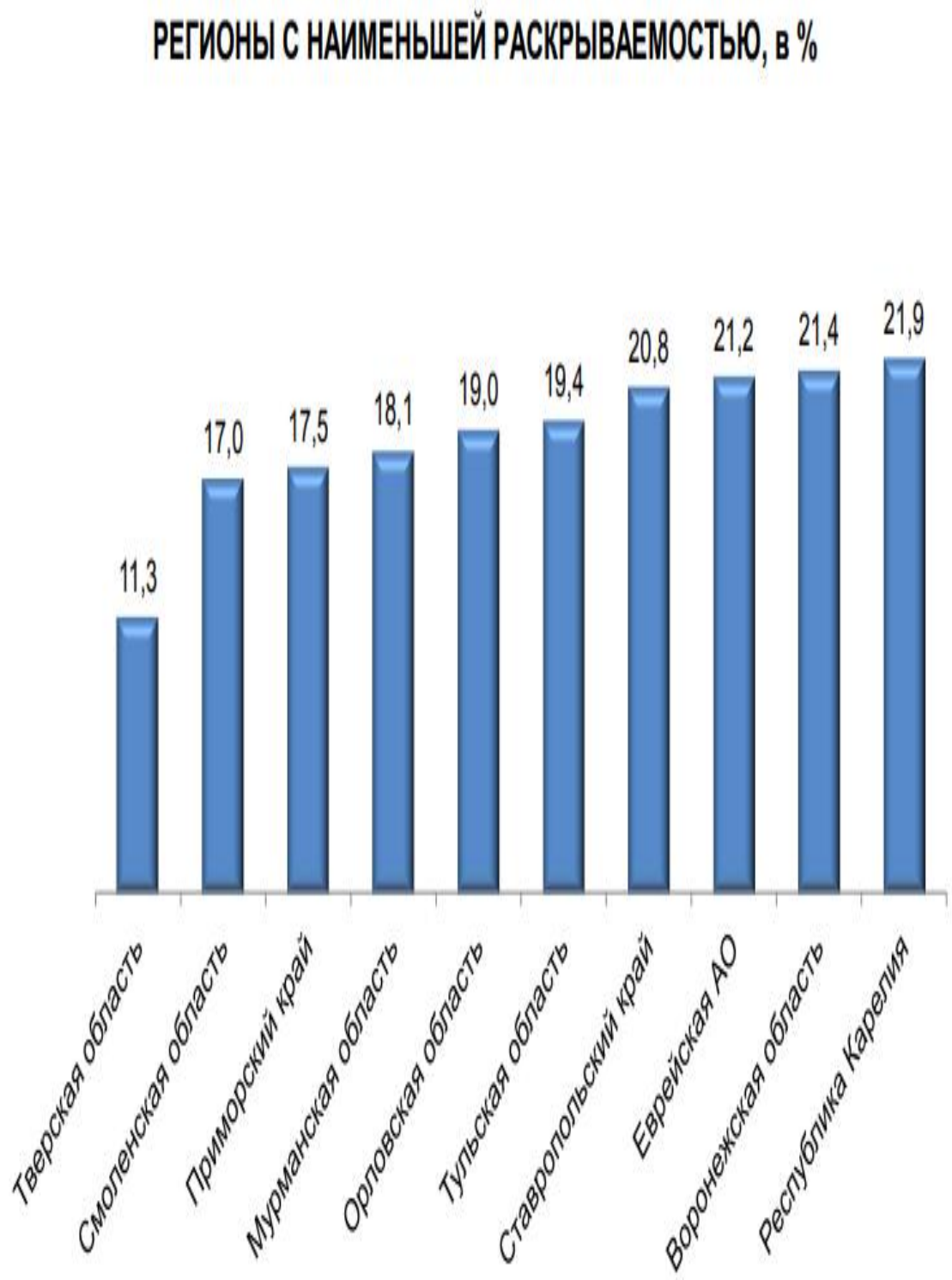
РЕГИОНЫ С НАИМЕНЬШИМИ ТЕМПАМИ ПРИРОСТА, в %



Приложение 3.

РАСКРЫВАЕМОСТЬ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ЗА 2022 ГОД




РЕГИОНЫ С НАИМЕНЬШЕЙ РАСКРЫВАЕМОСТЬЮ, в %
11,3
17,0
17,5
18,1
19,0
19,4
20,8
21,2
21,4
21,9
Тверская область
Смоленская область
Приморский край
Мурманская область
Орловская область
Тульская область
Ставропольский край
Еврейская АО
Воронежская область
Республика Карелия

Приложение 4

Сведения о размере установленного ущерба по преступлениям в сфере компьютерной информации за 2022 год

(Форма 280 раздел 4 ГИАЦ МВД России за январь-декабрь 2022 года)

	размер причиненного материального ущерба по прест.выявл.сотр.ОВД (тыс. руб.)	**размер возмещенного материального ущерба по прест.выявл.сотр.ОВД (тыс. руб.)**
кража п."г" ч.3, ч.4 ст. 158 УК РФ	8105531	589724
мошенничество ст. 159 УК РФ	81388058	4221975
мошенничество с использованием электронных средств платежа ст. 159.3 УК РФ	1410823	2927
мошенничество в сфере компьютерной информации ст. 159.6 УК РФ	49157	3946
вымогательство ст. 163 УК РФ	112890	6153
неправомерный оборот средств платежей ст. 187 УК РФ	2218	0
экстремистской направленности и террористического характера	388194	6984
заведомо ложное сообщение об акте терроризма ст. 207 УК РФ	9581	148

Приложение 5

Сведения об использовании способа совершения преступления в сфере информационно-телекоммуникационных технологий за 2022 год

(Форма 280 раздел 4 ГИАЦ МВД России за январь-декабрь 2022 года)

	Преступления, совершены с использованием или применением				
	расчетных (пластковых карт)	**компьютерной техники**	**программных средств**	**фиктивных электронных платежей**	**средств мобильной связи**
кража п."г" ч.3, ч.4 ст. 158 УК РФ	99564	1182	1075	89	31661
мошенничество ст. 159	24110	6155	2349	456	143947
мошенничество с использованием электронных средств платежа ст. 159.3 УК РФ	1558	91	21	9	3540
мошенничество в сфере компьютерной информации ст. 159.6 УК РФ	92	61	11	1	45
незаконные организация и проведения азартных игр ст. 171.2 УК РФ	6	385	115	0	8
неправомерный доступ к компьютерной информации ст. 272 УК РФ	47	3450	1167	0	1481

ОТЗЫВ

о работе обучающегося 092 учебной группы очной формы обучения, 2019 года набора, по специальности 40.05.02 Правоохранительная деятельность
Салахова Ильфата Ильдаровича
в период подготовки дипломной работы
на тему «Выявление и предупреждение оперативными подразделениями органов внутренних дел преступлений в сфере информационно-телекоммуникационных технологий»

Представленная дипломная работа посвящена исследованию вопросов, связанных с выявлением и предупреждением оперативными подразделениями органов внутренних дел преступлений в сфере информационно-телекоммуникационных технологий. Слушатель Салахов Ильфат Ильдарович при выборе темы исследования проявил самостоятельность с учетом своих научных и профессиональных интересов.

Салахов И.И. четко сформулировал цель исследования и поставил задачи, необходимые для их реализации. Логичность и корректность сформулированных задач и цели в свою очередь, сформировали четкую и последовательную структуру работы. Разработка плана исследования проводилась самостоятельно, но при этом, автор учел все предложения научного руководителя, что, несомненно сказалось на логичности и структуре плана исследования.

Актуальность темы исследования не вызывает сомнения и четко сформулирована. В работе достаточно детально и всесторонне раскрыты теоретические аспекты, касающиеся одной из актуальных проблем криминологической науки, а также практической деятельности – предупреждению преступлений в сфере информационно-телекоммуникационных технологий. Автор показал достаточно высокую степень владения методами системного анализа. Несомненным достоинством данного исследования является вдумчивый анализ действующего законодательства, чем автор продемонстрировал высокие навыки.

После каждой главы автор сформулировал выводы, которые являются решением поставленной во введении задачи. Выводы обоснованы, четко сформулированы.

В заключение своей дипломной работы автором сформулированы выводы и предложения по проведённой научно-практической значимости в рамках данного исследования.

Салахов И.И. строго соблюдал все требования и представлял все этапы выполнения работы четко и в срок, что указывает на несомненную способность рационально планировать время последовательность работ при исполнении поставленной задачи.

Все указанные научным руководителем замечания и недостатки устранялись в установленные сроки. Салахов И.И. проявлял дисциплинированность и пунктуальность, что, разумеется, сказалось положительно на результатах исследования.

В заключении своей дипломной работы автором сформулированы выводы и предложения по проведённому научно-практическому исследованию, данные предложения характеризуются продуманностью и имеют несомненную практическую значимость, что говорит о возможном их внедрении. С точки зрения практики, обоснование данных предложений и перспективы их внедрения являются главным достоинством работы.

Слушателем был проанализирован большой объем теоретического материала, для написания работы использованы научные труды отечественных и зарубежных авторов, проблема раскрыта всесторонне, с разных точек зрения. Весь собранный материал изложен четко, последовательно, с соблюдением внутренней логики повествования. Практическое исследование проведено на достаточно высоком методологическом и теоретическом уровнях. Прослеживается тщательная и глубокая проработка каждого вопроса. Таким образом, содержание данного дипломного исследования полностью соответствует первоначальному заданию и отвечает всем необходимым требованиям.

Оригинальность текста исследования 62 %, из них цитирование 13,55%. После каждой главы имеются выводы, которые подводят итог вышесказанному. В качестве недостатка данной работы можно отметить недостаточное исследование диссертационных исследований и монографий рассматриваемой темы, но указанный недостаток не является значительным.

Выбранная проблематика раскрыта полно и всесторонне, цель достигнута, задачи решены, выводы правильны и обоснованы, выработанные рекомендации и предложения имеют практическую значимость.

Исходя из вышеизложенного, представленная дипломная работа Салахова Ильфата Ильдаровича рекомендуется к защите и заслуживает высокой положительной оценки.

Научный руководитель
профессор кафедры криминологии и уголовно-исполнительного права
майор полиции _____ (подпись) И.В. Жуковская (инициалы, фамилия)

«5» 06 2024 г.

С отзывом ознакомлен
«6» 06 2024 г. _____ (подпись) И.И. Салахов (инициалы, фамилия)

РЕЦЕНЗИЯ

на дипломную работу
Обучающего 092 взвода очной формы обучения, 2019 года набора, по специальности - 40.05.02 - Правоохранительная деятельность,
Салахова Ильфата Ильдаровича
на тему: «Выявление и предупреждение оперативными подразделениями органов внутренних дел преступлений в сфере информационно-телекоммуникационных технологий».

Тема дипломной работы, представленной слушателем 5 курса ФПС по ПВО КЮИ МВД России младшим лейтенантом полиции Салаховым И.И. представляется весьма актуальной. Это обусловлено тем, что своевременная нейтрализация криминогенных факторов, влияющих на развитие несовершеннолетних, как на потенциальных самостоятельных субъектов общества, позволяет уменьшить уровень преступности в будущем.

Тема работы «Выявление и предупреждение оперативными подразделениями органов внутренних дел преступлений в сфере информационно-телекоммуникационных технологий».

Дипломная работа состоит из введения, двух глав, шести параграфов, входящих в них, заключения, списка использованной литературы. Подобная структура обусловлена как проблематикой исследования, так и его целями, и задачами.

Во введении автор обосновал актуальность, новизну исследования, определил цели, задачи, объект и предмет исследования, а также рассмотрел методологию и методику. В первой главе «Криминологическая характеристика преступлений в сфере информационно-телекоммуникационных технологий» рассматриваются общие положения и правовая основа противодействия данным противоправным явлениям, исследуются статистические показатели, динамика и тенденции

преступности, а так же факторы, способствующие преступлениям в сфере компьютерной информации.

Во второй главе «Предупреждение отдельных видов преступлений в сфере информационно-телекоммуникационных технологий» исследуются криминологическая характеристика лиц, совершающих преступления и виктимологическая характеристика лиц, ставших жертвами от данного вида преступлений.

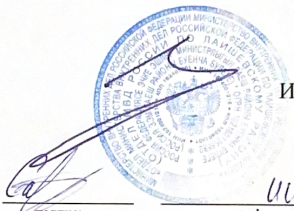
В заключении автор подводит итоги проведённого исследования и делает выводы теоретического и прикладного характера. Список источников и использованной литературы содержит нормативно-правовые акты, учебную и иную литературу. В работе все источники использованы с учётом их последних изменений, приведены выдержки из диссертационных исследований, научной литературы, каждый из которых соответствует рассматриваемой автором теме.

Таким образом, дипломная работа Салахова И.И. имеет исследовательский характер, достаточно хорошо изложенную теоретическую часть, логичное и последовательное изложение материала с соответствующими выводами и обоснованными предположениями. В ней автор показывает знание вопросов, рассматриваемой темы и действующего российского законодательства, своё умение ориентироваться в источниках права и применения его при изложении материала, а также владение современными методами исследования. В целом, работа выполнена на хорошем уровне, свидетельствующем о её достаточной самостоятельности, однако имеются некоторые спорные вопросы.

Исходя из вышесказанного, считаю, что дипломная работа Салахова И.И. на тему «Выявление и предупреждение оперативными подразделениями органов внутренних дел преступлений в сфере информационно-

телекоммуникационных технологий» может быть рекомендована к защите в Казанском юридическом институте МВД России и оценена положительно.

Рецензент:
Начальник ОМВД России
по Лаишевскому району
полковник полиции
«13» 06 2024 г.



И.К. Камалиев

С рецензией ознакомлен(а) _____ И.И.Салахов
подпись инициалы, фамилия обучающегося

«13» 06 2024 г.

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

Казанский юридический институт МВД России

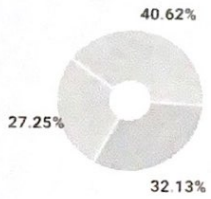
ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Жуковская Ирина Викторовна
Самоцитирование рассчитано для:
Название работы: Диплом_комп. инф
Тип работы: Не указано
Подразделение: кафедра криминологии и УИП

РЕЗУЛЬТАТЫ

СОВПАДЕНИЯ	32.13%
ОРИГИНАЛЬНОСТЬ	40.62%
ЦИТИРОВАНИЯ	27.25%
САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 03.05.2024



Структура документа: Проверенные разделы: приложение с.51-61, библиография с.44-49, титульный лист с.1, содержание с.2, основная часть с.3-43, 50
Модули поиска: ИПС Адилет; Перефразирования по eLIBRARY RU; Переводные заимствования издательства Wiley (RuEn); Сводная коллекция ЭБС, Сводная коллекция РГБ, СПС ГАРАНТ: аналитика, Модуль поиска "КЮИ МВД РФ"; Переводные заимствования по Интернету (EnRu); Переводные заимствования (RuEn); Цитирование; Издательство Wiley; Перефразирования по СПС ГАРАНТ: аналитика; Патенты СССР, РФ, СНГ; Библиография; Переводные заимствования по eLIBRARY RU (EnRu); Медицина; eLIBRARY.RU; Шаблонные фразы; Сводная коллекция вузов МВД, Кольцо вузов; СПС ГАРАНТ: нормативно-правовая документация, СМИ России и СНГ; Диссертации НББ; Перефразирования по Интернету; Интернет Плюс

Работу проверил: Жуковская Ирина Викторовна
ФИО проверяющего

Дата подписи: 04.05.2024

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

С результатами проверки ознакомлен(а) И.И.Салахов
04.05.2024