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 «Криминологическая характеристика и предупреждение мошенничества в сфере компьютерной информации»

Выполнил: Ахметова Дарья Радиковна
(фамилия, имя, отчество)
40.05.01 – Правовое обеспечение национальной безопасности, 2020 год набора, 101 учебная группа
(специальность, год набора, № группы)

Руководитель: к.пед.н., доцент кафедры криминологии и уголовно-исполнительного права КЮИ МВД России, полковник полиции
(ученая степень, ученое звание, должность, спец. звание)
Халметов Тимур Анварович
(фамилия, имя, отчество)

Рецензент: Начальник отдела СЧ ГСУ МВД по РТ полковник юстиции
(должность, специальное звание)
Хасанов Рамиль Ринатович
(фамилия, имя, отчество)

Дата защиты: «___» _____20___г. Оценка_____

Казань 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования дипломной работы, заключается в том, что информационно-телекоммуникационные технологии все активнее входят в нашу жизнь. Однако широкие возможности, которые дает цифровизация и цифровая трансформация экономики, нередко используются в качестве инструмента обмана и злоупотребления доверием для хищения денежных средств. Эффективным механизмом борьбы с данным видом преступлений является своевременное и эффективное предупреждение и профилактика указанных преступных посягательств. В настоящее время акцентируется большое внимание на необходимости более широкого информирования населения о способах защиты своих средств при использовании продуктов IT-технологий. Широкое распространение данного вида мошенничества и совершенствование способов его совершения требуют разработки и внедрения универсальных мер предупреждения.

Целью исследования является проведение комплексного анализа состояния и динамики преступлений в сфере компьютерных технологий, и получение новых знаний в исследуемой тематике.

Задачи дипломной работы:

1. Определить понятие, состояние и структура мошенничеств в сфере компьютерной информации;
2. Установить причины и условия совершения мошенничеств в сфере компьютерной информации;
3. Выявить характерные черты личности преступника и потерпевшего от мошенничества в сфере компьютерной информации;
4. Проанализировать общесоциальное предупреждение мошенничеств в сфере компьютерной информации;
5. Установить специально-криминологические меры предупреждения мошенничеств в сфере компьютерной информации;

6. Выявить деятельность органов внутренних дел по предупреждению мошенничества в сфере компьютерной информации.

Объектом настоящего исследования выступают общественные отношения, возникающие в процессе изучения криминологической характеристики и предупреждения мошенничества в сфере компьютерной информации.

Предметом дипломной работы выступают нормативно правовые акты, а также доктринальные положения, связанные с предупреждением мошенничеств в сфере компьютерной информации.

Степень научной разработанности проблемы. Исследованием вопроса о криминологической характеристики и предупреждения мошенничества в сфере компьютерной информации занимались такие автор как, Л.П. Александров, Ю.М. Антонян, А.В. Арестов, О.Р. Афанасьева, А.Н. Варыгин, Е.А. Винокурова, В.В. Власенко, В.А. Власов, М.С. Воробьева, А.И. Газизова, М.А Главчева, Д.А. Емельянов, Н.Д. Иващенко, К.С. Квятковский, К.В. Кецко, И.Я. Козаченко, И.М. Комаров, Т.Г. Копейко, И.И. Короленко, В.В. Лунеев, К.А. Мартынюк, А.С. Матиенко, М.Ш. Махтаев, Т.В. Молчанова, Ю.Н. Мякинина, Л.Р. Назмеева, А.Р. Новиков, А.Е. Петрова,
А.Ю. Полозовская, И.С. Попов, А.Ю. Решетников, Д.С. Романов, Р.Р. Саттаров, О.А. Старостенко, Д.С. Хайрусов и другие.

Методологическую основу дипломной работы составили теоретический метод исследования, который включает в себя такие методы, как анализ, синтез, аналогия, дедукция, индукция, обобщение, формализация, конкретизация, аналогия, также был использован практический (частный) метод исследования, который включил в себя, такие методы как наблюдение, сравнение, измерение, описание.

Теоретическую основу исследования составили научные труды и исследования по рассматриваемой нами проблеме в рамках дисциплин: криминология, уголовное право, уголовно-процессуальное право,

оперативно-розыскная деятельность, психология и педагогика, социология и другие науки.

Нормативная база исследования включает: Конституцию Российской Федерации; международные правовые нормы; Уголовный кодекс Российской Федерации; Уголовно-процессуальный кодекс Российской Федерации; Федеральный закон от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»; постановления Правительства Российской Федерации, указы Президента Российской Федерации и иные нормативные правовые акты, содержащие нормы, относящиеся к предмету настоящего исследования.

Эмпирическая основа включает в себя: материалы правоприменительной и судебной практики, статистические данные Министерства внутренних дел Российской Федерации, Генеральной прокуратуры Российской Федерации, Судебного департамента при Верховном суде Российской Федерации и иных правоохранительных органов; социологические и криминологические исследования.

Структура дипломной работы состоит из введения, двух глав, шести параграфов, заключения и списка использованной литературы.

ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Понятие, состояние и структура мошенничества в сфере компьютерной информации

В 2023 году Правительство РФ утвердило Стратегию развития отрасли связи РФ на период до 2035 года[1]. Одной из приоритетных задач и целевых показателей развития отрасли связи вышеуказанной Стратегии является, доля урегулированных в пределах установленного периода инцидентов информационной безопасности и мошеннических действий в общем числе зарегистрированных инцидентов в отраслевом центре государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Стремительное развитие компьютерных технологий и сети Интернет можно рассматривать с двух сторон. С одной, заметно упростился процесс получения информации, оказания услуг, покупок, оформления документов, у граждан появилась возможность работать удаленно и получать вознаграждение за свой труд.

С другой, резко возросло количество киберпреступлений, связанных с хищением средств, информации или доступов к ней. Пострадавшими становятся как физические лица, так и крупные компании или банки.

Как отметил заместитель председателя Совета безопасности Российской Федерации Д.А. Медведев: «Чтобы заполучить денежные средства, имущество злоумышленники, действительно, действуют весьма изощренно»[2].

---

[1] Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года: Распоряжение Правительства РФ от 24.11.2023 № 3339-р // Справ.–правовая система «КонсультантПлюс» (дата обращения: 22.10.2024).

[2] Официальный и интернет-портал правовой информации // URL: https://pravo.ru/news/222725/ (дата обращения: 22.10.2024).

Судебная статистика показывает, что обвинительными приговорами по статье 159.6 УК РФ[1] (мошенничество в сфере компьютерной информации) заканчивается совсем незначительное количество дел.

Это связано со сложностями расследования дел в сфере информационных технологий. Преступник может находиться в другой стране или установить его личность не представляется возможным.

«Каждый день появляются новые способы отъема средств у физических и юридических лиц. Чтобы максимально обезопасить себя, не стать соучастниками преступления, нужно хорошо разобраться в специфике мошенничества с деньгами в Интернете»[2].

С правовой точки зрения мошенничество в сфере компьютерной информации – любые действия, направленные на хищение собственности, денежных средств или прав на имущество путем ввода, удаления или изменения информации. Ущерб наносится не только в отношении денег и вещей, но и ценной информации – объекты интеллектуальной собственности, бизнес-идеи и многое другое.

Мошенники могут завладеть ресурсами такими способами:

«1. Введение личных данных, полученных незаконным путем.

2. Удаление информации без возможности восстановления.

3. Изменение учетной политики, которая закрывает доступ к информации законному владельцу.

4. Внедрение вирусных программ.

5. Использование дополнительных аппаратных устройств для незаконного ввода или вывода информации»[3].

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

[2] Воробьева, М.С. Криминологическая характеристика мошенничества в сфере компьютерной информации / М.С. Воробьева // Союз криминалистов и криминологов. – 2020. – № 2. – С. 130.

[3] Саттаров, Р.Р. Криминологическая характеристика преступлений, совершенных в сфере информационных технологий / Р.Р. Саттаров // Дневник науки. – 2020. – № 4(40). – С. 69.

В ч. 1 ст. 159.6 УК РФ дается легальное определение, мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

М.А. Главчева, А.М. Васильев дают следующее определение мошенничеству в сфере компьютерной информации – это преступление, которое состоит в получении незаконного доступа к компьютерной информации, краже или уничтожении данных, а также владения или использования электронной информации с целью получения выгоды[1].

Итак, мы предлагаем понимать под мошенничеством в сфере компьютерной информации – противоправное завладение чужим имуществом (движимым/недвижимым) с следующими способами путем обмана, злоупотребления доверием, присвоения, растраты, а также причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенные с использованием информационно-коммуникационных технологий.

Рассмотрим динамику и состояние преступности по исследуемой тематике. Реальный ущерб от киберпреступлений в настоящее время сложно подсчитать, при этом количество этих преступлений стремительно растет из года в год.

Состояние преступности в Российской Федерации по ст. 159.6. УК РФ «Мошенничество в сфере компьютерной информации». За 9 месяцев 2024 г. совершено 149 преступление, в 2023 г. – 417 преступлений, в 2022 г. – 334

[1] Главчева, М.А. Мошенничество в сфере компьютерной информации / М.А. Главчева, А.М. Васильев // Новости науки: социальные и гуманитарные науки : Сборник материалов XXII-ой международной очно-заочной научно-практической конференции, Москва, 21 марта 2023 года. Том 1. – Москва: Научно-издательский центр "Империя", 2023. – С. 51.

преступлений, в 2021 г. – 431 преступлений, в 2020 г. – 761 преступлений, 2019 г. – 687 преступлений[1].

Регионы с наибольшими темпами прироста зарегистрированных преступлений: Чеченская Республика – 130,3 %, Республика Мордовия – 80,8 %, Республика Калмыкия – 78,1 %.

Большая доля всех мошенничеств (85%, 350 тыс.) совершена с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации – это телефонные мошенничества с подменой номеров, мошенничества в интернете, мошенничества с электронными платежными средствами и другие виды кибермошенничеств. Их число за 11 месяцев 2024 года выросло на 7,8%. «В целом на преступления в сфере информационно-телекоммуникационных технологий или компьютерной информации приходится почти 40% от всех зарегистрированных деяний (702,9 тыс., рост на 14,3%)»[2], – отметили в Генпрокуратуре.

Высокая латентность. Реальное количество преступлений в сфере компьютерной информации гораздо больше зафиксированного в статистических данных. Главным фактором здесь выступает нежелание самих потерпевших обращаться к правоохранительным органам и стремление к использованию альтернативных способов восстановления своих прав.

На прошедшем брифинге 24.07.2024 начальник Управления уголовного розыска МВД по РТ Катипов Рефат Наримановича, отметил, что свыше 50% всех зарегистрированных преступлений – мошенничество, управление борется и пытается приостановить мошеннические попытки, которые организуют за пределами России.

---

[1] Состояние преступности в Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 22.11.2024).

[2] Генпрокуратура указала на смену традиционных видов преступности на цифровые. URL: https://tass.ru/obschestvo/22831665 (дата обращения: 10.01.2025).

Состояние преступности в Республики Татарстан по ст. 159.6. УК РФ «Мошенничество в сфере компьютерной информации». За 9 месяцев 2024 г. совершено 1 преступление, в 2023 г. – 5 преступлений, в 2022 г. – 78 преступлений, в 2021 г. – 10 преступлений, в 2020 г. – 45 преступлений, 2019 г. – 42 преступлений.

Расследованных уголовных дел по Республике Татарстан за 9 месяцев 2024 г. – 0 преступлений; за 2023 г. – 2 преступления; за 2022 г. – 1 преступление; за 2021 г. – 2 преступления; за 2020 г. – 0 преступлений; за 2019 г. – 0 преступлений.

Приостановленных уголовных дел по Республике Татарстан за 9 месяцев 2024 г. – 2 преступления; за 2023 г. – 3 преступления; за 2022 г. – 2 преступления; за 2021 г. – 11 преступления; за 2020 г. – 47 преступлений; за 2019 г. – 40 преступлений.

Следует отметить, что в настоящее время преступники активизировать и посягают на более масштабные объекты. Так, в сентябре 2024 г. преступники взломали сайт «Детского мира» и украли почти 4,5 тыс. подарочных сертификатов. Возбуждено уголовное дело по мошенничеству в сфере компьютерной информации. По версии следствия, мошенники подобрали номера и пин-коды к 4459 предоплаченным подарочным картам и сертификатам с помощью компьютерных программ. Делом занимается отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий. В ходе таких подключений, применяя компьютерные программы, заведомо предназначенные для нейтрализации средств защиты компьютерной информации, произвели подбор значений в виде номера и пин-кода к хранящимся в электронном виде предоплаченным 4459 электронным подарочным сертификатам и подарочным картам ПАО

«Детский мир», то есть электронным носителям информации, удостоверяющим право их держателя осуществить покупку товара[1].

Кроме того, преступники используют следующие способы совершения исследуемых видов преступлений: они покупают сим-карты у представителя оператора сотовой связи и с помощью интернет-бота проверяют, оформляют ли их бывшие владельцы микрозаймы, связанные с номером телефона. После этого восстанавливают доступ к личным кабинетам и оформляют экспресс-кредиты[2].

На практике зачастую преступления, предусмотренные ст. 159.6 УК РФ, сопровождаются с преступлением, предусмотренным ст. 272 УК РФ. Так, правоохранительные органы задержали троих подозреваемых в разработке и распространении вредоносного ПО «Мамонт», которое использовалось для перехвата смс и кражи денег с банковских карт. По данным МВД, задержанные могут быть причастны к более чем 300 случаям мошенничества. Злоумышленники распространяли вирус через Telegram-каналы, маскируя его под обычные приложения и видеоматериалы (сопровождая их вводящими в заблуждение вопросами, например «Это ты на видео?»). После проникновения в устройство вредоносная программа перехватывала смс-сообщения от банков, что позволяло переводить деньги на счета и кошельки злоумышленников. Задержанных оставили под подпиской о невыезде. В ходе обысков у них были изъяты улики, в том числе компьютерное оборудование, цифровые носители информации, средства связи и банковские карты. Специалисты также заблокировали ресурсы, которые применялись для совершения преступлений. Возбуждены уголовные дела по статьям 159.6 («Мошенничество в сфере компьютерной

---

[1] Хакеры украли почти 4,5 тыс. подарочных сертификатов «Детского мира». URL: https://profashion.ru/business/law/khakery-ukrali-pochti-4-5-tys-podarochnykh-sertifikatov-detskogo-mira/ (дата обращения: 10.01.2025).

[2] В Хакасии задержали подозреваемого в серии мошенничеств. URL: https://pulse19.ru/247568-v-hakasii-zaderzhali-podozrevaemogo-v-serii-moshennichestv/ (дата обращения: 10.01.2025).

информации») и 272 УК РФ («Несанкционированный доступ к компьютерной информации»)[1].

Резко снижение регистрации преступлений по ст. 159.6 УК РФ, связана с тем, что ранее возбуждали уголовное дело, даже если не был нанесен ущерб потерпевшему, в настоящее же время прокуратура не дает согласие на возбуждение уголовных дел.

Также одной из причин снижения регистрации может быть связана, с высоким уровнем латентности данного вида преступления, люди, которые попались на уловки мошенников, после осознания, понимают, что вероятность раскрытия таких преступлений не высокая, связи с чем не обращаются в полицию, либо боятся.

Еще одной проблемой является квалификация ст. 159.6 УК РФ, так у правоприменителя возникают проблемы при квалификации преступлений в сфере компьютерной информации и приоритет отдается в пользу уже известных составов ст. 272, 159 УК РФ. Однако возникают сомнения в правильности оценки подобного деяния как мошенничества. Если для мошенничества характерны признаки обмана и злоупотребления доверием, то в ситуациях, когда для завладения чужим имуществом используются возможности компьютерных технологий, мы не сможем отыскать многих из этих признаков. Таким образом, квалификация мошенничества в сфере компьютерной информации имеет ряд трудностей, связанных с наличием близких по содержанию составов преступлений, не раскрытыми в полной мере существенными признаками состава, а также с общими проблемами квалификации постоянно растущих преступлений в области информационных технологий.

Криминологическая структура мошенничества в сфере компьютерной информации может включать следующие элементы[2]:

---

[1] В Саратовской области задержали подозреваемых в разработке вредоносного ПО «Мамонт». URL: https://habr.com/ru/news/895690/ (дата обращения: 31.03.2025).

1. Способ совершения преступления. Выделяют, например, неправомерный доступ к информационной инфраструктуре кредитной организации, воздействие вредоносного программного обеспечения на компьютерные устройства и другие.

2. Обстановка преступления. У преступников могут быть соответствующие компьютерные устройства, программно-аппаратные и другие технические средства.

3. Личность преступника. В структуре личности преступника выделяют социально-демографические признаки, социальные функции и нравственно-психологические характеристики. От особенностей личности зависит тот вид мошенничества, на котором специализируется преступник.

Также существует криминалистическая типология мошенничества в сфере компьютерной информации в зависимости от степени организованности и уголовно-правовой квалификации.

Криминологическая типология мошенничества в сфере компьютерной информации может быть выполнена по ряду классификационных признаков:

«1. По способу получения доступа к хранилищу информации:

– путём взлома пароля защитной программы или менеджера паролей;

– получением кодовой комбинации методами фишинга;

– в результате подбора пароля посредством внешнего подключения специального устройства;

– посредством кражи или подделки электронного ключа»[1].

2. По цели противоправного поступка:

– для хищения конфиденциальной, уникальной или значимой для третьего лица информации;

---

[2] Криминология : учебник для вузов / В.И. Авдийский [и др.] ; под редакцией В.И. Авдийского, Л.А. Букалеровой. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 56 с.

[1] Хайрусов, Д.С. Криминология : учебное пособие для среднего профессионального образования / Д.С. Хайрусов. – Москва : Издательство Юрайт, 2024. – 45 с.

– для удаления или изменения информации таким образом, чтобы данные утратили свою ценность;

– для блокировки учётной записи, с целью получения денежных сумм или имущества, в обмен на алгоритм снятия ограничений доступа к компьютеру.

3. По инструменту совершения злонамеренных действий:

– посредством ручного ввода информации и изменения данных реестра на атакуемом компьютере;

– путём заражения вредоносными кодами посредством загрузки файлов со съёмного носителя или генерирования при помощи устройства ввода информации;

– в результате установки специализированного программного обеспечения или стандартных программ со скрытыми модулями, которые выполняют определённый алгоритм в течение заданного интервала времени.

Также существует типология в зависимости от степени организованности: «организованное» и «несложное», или «простое», мошенничество в сфере компьютерной информации.

Таким образом, мы можем сделать следующие выводы:

1. Под мошенничеством в сфере компьютерной информации – противоправное завладение чужим имуществом (движимым/недвижимым) с следующими способами путем обмана, злоупотребления доверием, присвоения, растраты, а также причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенные с использованием информационно-коммуникационных технологий.

2. В ходе анализа статистических данных по Российской Федерации и Республике Татарстан, мы можем утверждать, что идет снижение регистрации данного вида преступления. Наиболее распространённые причины снижения регистрации: проблема квалификации (разграничение между ст. ст. 159, 159.6, 272 УК РФ), страх людей обратиться в полицию.

§2. Причины и условия совершения мошенничества в сфере компьютерной информации

Актуальность исследования причин и условий совершения мошенничества в сфере компьютерной информации обусловлена несколькими факторами:

1. Массовый переход в киберпространство. В нём осуществляются предпринимательские правоотношения, банковские расчёты и даже взаимоотношения между гражданином и государством.

2. Развитие информационных технологий. Они создают возможности для ведения полноценной экономической деятельности посредством интернета.

3. Безнаказанность мошенников. Жертвы не обращаются в правоохранительные органы, считая это бесполезным. Проблема усугубляется тем, что электронный платёж сложно проследить, а незначительность ущерба зачастую не позволяет возбудить уголовное дело.

Постоянно совершенствующиеся способы преступлений. Это связано с появлением нового программного обеспечения и компьютерных устройств.

Таким образом, изучение причин и условий совершения мошенничества в сфере компьютерной информации важно для разработки мер по борьбе с этим явлением и совершенствованию законодательства.

Для изучения причинного комплекса мошенничества в сфере компьютерной информации, необходимо для начала дать определение причинам и условиям преступности.

Под причинами преступности принято понимать те жизненные явления, которые порождают совершению преступления, держат ее на стабильном уровне, способствуют увеличение или уменьшение.

«Причины преступности – это негативные социальные явления и процессы, обусловленные закономерностями функционирования общества,

которые порождают и воспроизводят преступность и преступления как своё закономерное следствие»[1].

Причины преступности[2]:

1. Социальное окружение и влияние. Взаимодействие с криминальными группировками, присутствие в насильственной или конфликтной среде, а также негативные влияния со стороны близких людей могут стать факторами, способствующими преступности.

2. Экономические факторы. Неустойчивая экономическая ситуация, высокий уровень безработицы и неравенство в распределении благ могут создавать условия, при которых люди склонны к совершению преступлений в попытке обеспечить себя и своих близких.

3. Низкий уровень образования и социальной адаптации. Отсутствие образования и навыков, неспособность адаптироваться к социальным изменениям и нормам могут привести к возникновению преступного поведения.

4. Психологические факторы. Низкий уровень самоконтроля, склонность к агрессии и насилию, неадекватное решение проблем и конфликтов, а также отсутствие эмоционального контроля могут быть связаны с преступной деятельностью.

Условия преступности – это явления которые способствуют совершению преступности. В научной литературе принято выделять сопутствующие, достаточные, необходимые условия преступности[3].

---

[1] Афанасьева, О.Р. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 96 с.

[2] Полозовская, А.Ю. Причины и условия совершения компьютерных преступлений / А.Ю. Полозовская // Следственная деятельность: проблемы, их решение, перспективы развития : материалы III Всероссийской молодёжной научно-практической конференции, Москва, 25 ноября 2019 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2020. – С. 805.

[3] Газизова, А.И. Условия преступности / А.И. Газизова // Современные научные исследования и инновации. – 2019. – № 5(97). – С. 41.

«Условия преступности – это различные явления социальной жизни, которые не порождают преступность, но содействуют, способствуют её возникновению и существованию»[1].

В своих исследованиях Н.Д. Иващенко условия преступности подразделяет на три основные группы:

«1. Сопутствующие (они образуют общий фон событий и явлений, обстоятельства места и времени).

2. Необходимые (без таких условий событие могло бы не наступить).

3. Достаточные (совокупность всех необходимых условий)»[2].

Условиями преступности могут быть как обстоятельства, относящиеся к состоянию внешней среды (активность правоохранительных органов, латентность конкретных видов деяний, различное отношение общества к разным видам преступных деяний, материальные условия среды), так и характеризующие самого преступника (криминальный профессионализм, алкогольная или наркотическая зависимость и т.д.).

Рассмотрев эти два понятия, необходимо перейти к рассмотрению причин и условии совершения мошенничеств в сфере компьютерной информации.

Причины и условия совершения мошенничеств в сфере компьютерной информации:

1. Рост числа электронных устройств и их пользователей, а также увеличение объёма информации, хранимой в ЭВМ.

Рост числа электронных устройств и их пользователей связан с появлением и всеобщим распространением персональных компьютеров (ПК). Они стали широко применяться не только в науке и производстве, но и в системе общего образования, сфере обслуживания, быту. ПК вошли в дом как один из видов бытовой техники наряду с телевизорами, магнитофонами.

---

[1] Криминология. Общая часть : учебник для вузов / В.П. Ревин, В.Д. Малков, В.В. Ревина, Ю.С. Жариков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 88 с.

[2] Иващенко, Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы / Н.Д. Иващенко // Столица науки. – 2020. – № 6(23). – С. 270.

Увеличение объёма информации, хранимой в ЭВМ, связано с тем, что объём обрабатываемых данных постоянно растёт. Поэтому компьютерам требуется всё больше и больше памяти, особенно в многозадачном режиме, когда одновременно запускается сразу несколько программ[1].

Также с каждым поколением вычислительных машин развиваются их аппаратные возможности: ЭВМ становятся более мощными и универсальными, расширяется количество обрабатываемых типов данных.

2. Недостаточность мер по защите ЭВМ и их систем, а также не всегда серьёзное отношение руководителей к вопросу обеспечения информационной безопасности и защите информации.

Некоторые проявления этих факторов[2]:

2.1. Недостаточность защиты программного обеспечения. Например, несовершенный алгоритм шифрования сохраняемых паролей (как в системе Windows 95).

2.2. Недостаточность защиты технических средств защиты компьютерной техники. Например, уязвимость портов персонального компьютера, через которые подключается периферийное оборудование.

2.3. Неконтролируемый доступ сотрудников и обслуживающего персонала к клавиатуре компьютера.

2.4. Низкий профессионализм или отсутствие служб информационной безопасности. Также может отсутствовать должностное лицо, отвечающее за режим секретности и конфиденциальность компьютерной информации.

2.5. Отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения конфиденциальной информации.

2.6. Недостаточное финансирование мероприятий по защите информации.

---

[1] Молчанова, Т.В. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий / Т.В. Молчанова, В.А. Аксенов // Вестник экономической безопасности. – 2020. – № 2. – С. 98.

[2] Криминология : учебник для вузов / О.С. Капинус [и др.] ; под общей редакцией О.С. Капинус. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 182 с.

Для решения этих проблем необходимо принимать комплексные меры по обеспечению информационной безопасности, включая организационные (разработка положений, регламентов и процессов взаимодействия) и технические (использование криптографических, антивирусных систем и других инструментов).

3. Уязвимость программного обеспечения и технических средств защиты компьютерной техники.

Уязвимость программного обеспечения – это недостаток (слабость) программы, который позволяет злоумышленникам получить незаконный доступ к её функциям или хранящимся в ней данным. Изъяны могут появиться на любом этапе жизненного цикла, от проектирования до выпуска готового продукта.

В зависимости от стадии появления уязвимости делятся на[1]:

3.1. Уязвимости проектирования. Возникают на этапе проектирования. К ним относятся неточности алгоритмов, несогласованности в интерфейсе между разными модулями или в протоколах взаимодействия с аппаратной частью, внедрение неоптимальных технологий.

3.2. Уязвимости реализации. Появляются на этапе написания программы или внедрения в неё алгоритмов безопасности. Это – некорректная организация вычислительного процесса, синтаксические и логические дефекты.

3.3. Ошибки конфигурации. Распространёнными их причинами являются недостаточно качественная разработка и отсутствие тестов на корректную работу дополнительных функций. К этой категории также можно относить слишком простые пароли и оставленные без изменений учётные записи по умолчанию.

3.4. Уязвимости технических средств включают в себя, например, уязвимости микропрограмм в постоянных запоминающих устройствах,

---

[1] Криминология. Особенная часть : учебник для вузов / Ю.С. Жариков, В.П. Ревин, В.Д. Малков, В.В. Ревина. – 2-е изд. – Москва : Издательство Юрайт, 2024. – 87 с.

программируемых логических интегральных схемах, базовой системы ввода-вывода, программного обеспечения контроллеров управления, интерфейсов управления.

Чтобы минимизировать влияние уязвимостей и ущерб от них, рекомендуется оперативно устанавливать выпускаемые разработчиками исправления (патчи) для приложений или включить автоматический режим обновления, не устанавливать сомнительные программы, использовать специальные сканеры уязвимостей или специализированные функции антивирусных продуктов.

4. Возможность выхода пользователей в мировые информационные сети для обмена информацией, заключения контрактов, осуществления платежей.

Выход пользователей в мировые информационные сети для обмена информацией, заключения контрактов и осуществления платежей возможен благодаря глобальным вычислительным сетям. Они объединяют разрозненные сети и позволяют пользователям обмениваться данными со всеми другими участниками глобальной сети, где бы они ни находились.

Для обмена информацией в глобальных сетях, например, в интернете, используются электронная почта, службы мгновенного обмена сообщениями, доски объявлений, форумы, онлайн-конференции и веб-сообщества[1].

Для заключения контрактов в мировых информационных сетях применяются технологии смарт-контрактов, которые обеспечивают взаимодействие пользователей без участия посредников. Информационная система без участия человека выявляет соответствие реальной ситуации определённым условиям и при совпадении условий с заданными параметрами проводит трансакцию.

---

[1] Копейко, Т.Г. Причины и условия совершения мошенничества при получении выплат / Т.Г. Копейко // Гуманитарные, социально-экономические и общественные науки. – 2021. – № 4-2. – С. 105.

Для осуществления платежей используются электронные международные платежные системы, которые позволяют совершать денежные переводы по всему миру. Использование таких платформ экономит время, обеспечивает связь между компаниями и клиентами, упрощает проведение международных платежей.

5. Использование в преступной деятельности современных технических средств, в том числе ЭВМ.

Это может быть связано с совершением компьютерных преступлений.

К таким преступлениям относятся, например:

– введение ложной информации в ЭВМ;

– незаконное использование ЭВМ;

– нарушение обработки информации;

– кража информации.

Многие государства вынуждены реагировать на участившиеся случаи использования ЭВМ во вред другим людям и организациям путём принятия специальных уголовных законов.

6. Недостаточность защиты средств электронной почты.

Недостатки защиты средств электронной почты[1]:

6.1. Отсутствие надёжной защиты протоколов. Это позволяет создавать письма с фальшивыми адресами и не даёт гарантии, что автор – действительный автор сообщения.

6.2. Лёгкость изменения электронных писем. Стандартное письмо не содержит средств проверки собственной целостности и при передаче через множество серверов может быть прочитано и изменено.

6.3. Отсутствие гарантий доставки письма. Несмотря на возможность получить сообщение о доставке, часто это означает лишь, что сообщение

[1] Винокурова, Е.А. Некоторые особенности развития мошенничества в интернете в Российской Федерации / Е.А. Винокурова // Инновации в науке и практике : Сборник трудов по материалам Всероссийского конкурса научно-исследовательских работ, Уфа, 30 мая 2020 года. – Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2020. – С. 99.

дошло до почтового сервера получателя, но не обязательно до самого адресата.

6.4. Выбор алгоритма шифрования, не обеспечивающего надёжную защиту. Это может быть связано с тем, что национальное законодательство страны пребывания или регистрации не рекомендует использовать алгоритмы шифрования высокой надёжности.

6.5. Системные или несистемные сбои при применении защищённых протоколов передачи данных или средств криптографической защиты.

6.6. Бэкдоры в криптоалгоритмах, незадекларированные возможности программ, позволяющие разработчикам расшифровать информацию.

6.7. Действия вредоносных, вирусных программ, перехватывающих данные в пути или на сервере.

Единственного надёжного способа защиты электронной почты не существует, безопасность систем можно обеспечить только с помощью комплекса мер.

7. Небрежность в работе пользователей ЭВМ.

Небрежность в работе пользователей ЭВМ – это одна из причин, способствующих совершению преступлений в сфере компьютерной информации.

Пользователи не всегда серьёзно относятся к обеспечению конфиденциальности информации и часто пренебрегают элементарными требованиями по её защите.

Например[1]:

- не уничтожают файлы, содержащие информацию ограниченного доступа, с компьютеров общего пользования;

- наделяют нескольких лиц правом доступа к любым компонентам сети;

---

[1] Ульянов, М.В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения / М.В. Ульянов // Правопорядок: история, теория, практика. – 2022. – № 4(35). – С. 105.

- устанавливают сетевые серверы в общедоступных местах;

- небрежно хранят записи паролей;

- используют упрощённые пароли, устанавливаемые для защиты информации.

Также к небрежности в работе пользователей ЭВМ относят нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда полное их отсутствие.

8. Непродуманная кадровая политика в вопросах приёма на работу и увольнения[1]:

Несоответствие реальных условий труда локальным актам компании. Например, если в договоре прописан минимальный должностной оклад, а по факту большая часть заработанных денег выплачивается «в конверте».

Неправильное оформление трудовых договоров. Они должны быть оформлены строго в соответствии с трудовым законодательством.

Ознакомление работника с локальными нормативными актами после подписания трудового договора. Это нужно сделать до того, как сотрудник подпишет договор.

Отсутствие условий труда на рабочем месте в трудовом договоре. С 1 января 2014 года условия труда на рабочем месте являются обязательным условием в содержании трудового договора.

Оформление кадровых документов неуполномоченными работниками. Это может привести к трудовым спорам, когда приказы об увольнении, о применении дисциплинарного взыскания или выплате премий подписываются, несмотря на отсутствие полномочий.

Для продуманной кадровой политики рекомендуется проводить кадровые проверки, чтобы независимые эксперты проверили соответствие документооборота текущему законодательству.

---

[1] Попов, И.С. Преступления в сфере компьютерной информации в России и зарубежных государствах / И.С. Попов // XVII Неделя науки молодежи СВАО : Сборник статей по итогам работы научных конференций и круглых столов, Москва, 18–30 апреля 2022 года. – Москва: Издательство «Стратагема-Т», 2022. – С. 668.

9. Низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать компьютерные преступления. Это выражается в отсутствии специального образования и необходимых навыков в использовании компьютерных технологий

10. Отсутствие скоординированности в работе государственных и общественных структур в сфере обеспечения информационной безопасности.

Для решения проблемы предлагается, например[1]:

10.1. Создать единую систему борьбы с киберпреступлениями. Для этого можно заключить соглашение об электронном обмене информацией между органами государственной власти и службами при взаимодействии с банками, операторами связи.

10.2. Создать межведомственный орган по координации деятельности. Центром координации может стать созданный при ФСБ Национальный координационный центр по компьютерным преступлениям.

10.3. Укрепить управленческую вертикаль. Это касается субъектов принятия решений на всех уровнях власти, а также органов, осуществляющих контроль в отношении критически важных объектов информационной безопасности.

10.4. Повысить уровень сотрудничества и взаимодействия всех сил, служб и государственных органов, отвечающих за обеспечение информационной безопасности, в том числе путём проведения учений.

10.5. Привлечь к решению вопросов обеспечения национальной информационной безопасности представителей бизнеса и гражданского общества.

Также, для более подробного уяснения мошенничества в сфере компьютерной информации, необходимо рассмотреть вопрос о способах совершения данного вида преступления. Несмотря на то, что новые способы

[1] Решетников, А.Ю. Криминология : учебное пособие для вузов / А.Ю. Решетников, О.Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 78 с.

мошенничества появляются чуть ни каждый день, все преступления можно условно разделить на несколько категорий:

«– хищение уникальной информации и данных;

– блокировка учетных данных пользователя и дальнейшее вымогательство денег за предоставление доступа;

– удаление или изменение информации в целях утраты ее ценности;

– взлом защищенных программ пользователя;

– получение кодов доступа путем фишинга;

– подбор паролей с использованием специальных устройств;

– изменение данных в реестре зараженного вирусами компьютера;

– установка специального вредоносного программного обеспечения, которое выполняет заранее заданный алгоритм по установленному графику»[1].

Следует отметить, что мошенники внедряют вирус, который меняет доменное имя сайта и переводит на сайт-копию. После этого обычно приходит смс с просьбой ввести код (после этого с баланса мобильного списываются деньги) или ввести пароль банковской карты (таким образом исчезают средства с карт-счета).

Также, злоумышленники пользуются тем, что бухгалтеры часто ищут на просторах Интернета шаблоны форм документов. Мошенники создают поддельные сайты ведомств, а также известных справочно-правовых систем. Причем подделки могут быть на первых строках в поисковике.

Там злоумышленники выкладывают зараженные документы. После скачивания на компьютере запускается программа удаленного доступа. С ее помощью хакеры, к примеру, могут дистанционно менять банковские реквизиты в договорах, указывая вместо данных получателя свои данные.

---

[1] Короленко, И.И. Особенности преступлений в сфере компьютерной информации / И.И. Короленко, В.Д. Божко // Актуальные вопросы публичного управления, экономики, права в условиях цифровизации : сборник научных статей Медународной научно-практической конференции, Курск, 11–12 мая 2023 года / Курская академия государственной и муниципальной службы. Том 1. – Курск: Б. и., 2023. – С. 389.

Чтобы избежать подобного, ЦБ РФ рекомендует[1]:

– установить и регулярно обновлять антивирус;

– настроить запрет на установку программ;

– обращать внимание на адрес сайта. Например, официальные сайты госорганов, как правило, маркируются синим кружочком с галкой;

– быть осторожными при работе с сайтами, если в их адресной строке нет знака замочка. Его отсутствие свидетельствует о небезопасном соединении;

– обращать внимание на формат скачиваемого документа. Безопасными считаются форматы pdf, docx, xlsx, jpg, png.

Также можно скачать формы неунифицированных документов, используемых в бухгалтерской работе, с нашего сайта – это безопасно и бесплатно.

Еще один блок причины и условия совершения мошенничества в сфере компьютерной информации[2]:

1. Объективные условия. К ним относятся вид деятельности или род занятия потерпевшего, форма собственности предприятия или физического лица, юридическое положение и категория доступности используемой компьютерной информации, назначение и структура информационно-производственного процесса и другие.

2. Субъективные условия. К ним относятся факторы социально-психологического и организационно-управленческого характера, например, отступление от технологических режимов обработки информации, отсутствие или несоответствие средств защиты информации её категории, нарушение правил работы с охраняемой законом компьютерной информацией.

---

[1] Центробанк предупредил бухгалтеров о мошенниках // https://www.consultantkirov.ru/news/news-from-igk/tsentrobank-predupredil-bukhgalterov-o-moshennikakh.html (дата обращения:17.11.2024).

[2] Квятковский, К.С. Преступления в сфере компьютерной информации, компьютерные преступления и киберпреступность: соотношение понятий / К.С. Квятковский // Молодой ученый. – 2022. – № 42(437). – С. 109.

3. Особенности современных сетевых технологий. Анонимность и оперативность действий в интернете, а также возможность свободно перемещаться в пространстве, используя различные точки доступа, упрощают и удешевляют совершение мошенничества.

4. Корыстная мотивация. Особенность компьютерных преступлений позволяет при минимальных временных и физических затратах получить значительную экономическую выгоду.

Для предотвращения рисков компании стать жертвой компьютерного мошенничества рекомендуется уделять особое внимание информационной защищённости, иметь высококвалифицированных IT-специалистов, специалистов в области информационной безопасности и надёжное программное обеспечение.

Основные факторы, способствующие совершению мошенничеств в сфере компьютерной информации, включают:

1. Цифровизация и объём данных: массовое распространение электронных устройств и увеличение объёма информации, хранящейся в цифровом виде.

2. Пробелы в защите и управленческая халатность: недостаточный уровень защитных мер для компьютерных систем и зачастую несерьёзное отношение руководителей к вопросам обеспечения информационной безопасности.

3. Технические уязвимости: наличие уязвимостей в программном обеспечении и аппаратных средствах компьютерной техники.

4. Глобальная связность: возможность широкого доступа пользователей к мировым информационным сетям для обмена данными, заключения сделок и проведения платежей.

5. Техническая оснащенность преступности: активное использование злоумышленниками современных технических средств, включая компьютеры, в своей криминальной деятельности.

6. Уязвимость электронной почты: недостаточный уровень защиты средств электронной почты.

7. Человеческий фактор: невнимательность и недостаточная осведомленность пользователей компьютерной техники.

8. Кадровые риски: непродуманная кадровая политика, особенно в части найма и увольнения персонала.

9. Недостаточная подготовка правоохранителей: низкий уровень специальной подготовки сотрудников правоохранительных органов, ответственных за предупреждение, раскрытие и расследование киберпреступлений.

10. Отсутствие системной координации: недостаток скоординированных действий между государственными и общественными структурами в сфере обеспечения информационной безопасности.

Также к условиям совершения мошенничеств в сфере компьютерной информации относят анонимность в интернете, которая позволяет злоумышленникам оставаться незамеченными в виртуальном пространстве.

§3. Характерные черты личности преступника и потерпевшего от мошенничества в сфере компьютерной информации

Личность преступника – совокупность социально-психологических свойств и качеств человека, являющихся причинами и условиями совершения преступлений.

Структура личности преступника включает четыре взаимосвязанных элемента:

«1. Социально-демографические характеристики. Данные о поле, возрасте, социальном положении личности. Важное значение имеет род занятий, вид деятельности, место жительства, а также материально-технические и жилищные условия, в которых проживает личность.

2. Образовательно-культурные характеристики. Отражают уровень интеллектуального развития личности, её образование, род трудовой и творческой деятельности, а также интересы и культурные потребности.

3. Функциональные характеристики. Закрепляют роль индивидуума в социуме, в частности посредством его принадлежности к социальным общностям, группам по интересам. Помимо этого, функциональная составляющая личности преступника отражает характерные особенности его взаимодействия с другими членами общества, а также отношение к социальным и государственным институтам.

4. Социально-психологические характеристики. Отражают систему ценностей, мировоззрение, нравственную позицию, моральные устои, этические принципы человека»[1].

В криминологии выделяют следующие типы личности преступника[2]:

1. Случайный. Совершает преступление впервые, при этом противоправная деятельность расходится с социально-положительной характеристикой и окружающей обстановкой, которая была до совершения преступного посягательства.

2. Ситуационный. Совершает преступление впервые, при этом мотивом для совершения преступления выступает сложная социально-экономическая, бытовая или иная обстановка.

3. Неустойчивый. Совершает преступление впервые, однако в его характеристике отмечаются уже имеющиеся эпизоды административных правонарушений и иной антисоциальной деятельности эпизодического характера.

4. Злостный. Совершает преступления неоднократно.

---

[1] Криминология и предупреждение преступлений : учебник для среднего профессионального образования / В.И. Авдийский [и др.] ; под редакцией В.И. Авдийского, Л.А. Букалеровой. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 39 с.

[2] Козаченко, И.Я. Криминология : учебник и практикум для вузов / И.Я. Козаченко, К.В. Корсаков.- Москва : Издательство Юрайт, 2024. – 77 с.

5. Особо злостный. Совершает преступления на профессиональной основе, неоднократно или степень их общественной опасности относится к опасным и особо опасным преступлениям.

6. Личность преступника является предметом комплексного изучения и рассмотрения специалистами различных отраслей знаний (криминологии, социологии, психологии, психиатрии и т. д.).

Изучению личности преступника в научном сообществе всегда уделялось должное внимание. Данным обстоятельством продиктовано существование различных формулировок понятия данного явления.

Так, В.В. Лунеев под личностью преступника понимает: «человека, виновно совершившего уголовно наказуемое деяние, обладающего совокупностью социальных криминологически значимых свойств, которые во взаимодействии с криминогенными факторами внешней среды обусловили преступное поведение»[1].

По мнению Ю.М. Антоняна: «личность преступника выступает в качестве совокупности социально значимых негативных свойств, образовавшихся в процессе многообразных и систематических взаимодействий с другими людьми»[2].

Эффективным механизмом борьбы с мошенничеством в сфере компьютерной информации является инновационное, своевременное и эффективное предупреждение и профилактика указанных преступных посягательств. При этом важным элементом преступного поведения, требующего внимательного рассмотрения в целях закономерного исследования преступности в данной сфере, является личность преступника и потерпевшего[3].

---

[1] Лунеев В.В. Курс мировой и российской криминологии. В 2 т. Т. 1. Общая часть. В 3 кн. Кн. 3: учебник для вузов / В.В. Лунеев. М.: Юрайт, 2023. С. 24.

[2] Антонян Ю.М. Криминология: учебник для вузов / Ю.М. Антонян. 3-е изд., перераб. и доп. М.: Юрайт, 2023. С. 80.

[3] Кецко К.В. Отдельные особенности личности экономического преступника, действующего в сфере электронной коммерции // Право и государство: теория и практика. 2022. № 7(211). С. 135.

Проведение исследования личности преступника и потерпевшего в сфере компьютерной информации позволит в числе прочего сформировать и внедрить разнообразные эффективные меры, направленные на предупреждение преступлений в данной сфере. Эффективности данных мер можно добиться только всесторонним и объективным изучением личности преступника и потерпевшего, следует узнать, чем мотивировано его преступное поведение, как связано с его взглядами, жизненными позициями и иными факторами.

Особый интерес в криминологические характеристики мошенничества в сфере компьютерной информации представляют данные о личности мошенников. При этом в основу характеристик личности правонарушителя первоначально должны быть положены базовые, классические характеристики, такие как: социально-демографическая и правовая характеристики; нравственно-психологическая характеристика; основные психические и психофизиологические особенности; социальное поведение.

Актуальность изучения личности мошенника в сфере компьютерной информации обусловлена рядом факторов:

1. Постоянное развитие преступности в этой сфере. Это связано с применением информационных технологий в коммерческой деятельности, образовательной системе, базах данных.

2. Необходимость повышения эффективности выявления, раскрытия и расследования мошенничества. Для этого нужны не только юридические знания, но и специальные навыки в сфере информационных технологий.

3. Важность выявления мотивов преступного поведения. Это позволяет формировать на их основе эффективные меры предупреждения преступлений.

На основании официальных статистических данных можно составить обобщённый криминологический портрет личности «компьютерного» мошенника. Это поможет эффективно предупреждать имущественные преступления в сфере компьютерной информации.

В основном рассматриваемые преступления совершают лица мужского пола возрастом от 14 лет, среди которых заметно увеличение числа лиц в возрастной группе от 20 до 40 лет. Зачастую они обладают профильным образованием и достаточно высоким уровнем знаний в области информационных технологий. Их мотивацией часто выступает азарт, порой преобладающий над корыстью, но чаще всего присутствуют оба мотива.

Так, согласно сведениям, размещенным на официальном сайте Судебного департамента при Верховном Суде РФ[1], преимущественно лицами, осужденными за совершение рассматриваемой категории преступлений, являются мужчины в возрасте 18 – 35 лет, имеющие высшее или среднее профессиональное образование.

К мотивам указанных лиц относятся: безделье, вандализм, выражение неудовлетворенности собственной карьерой, доказательство превосходства над техникой, извлечение личной или финансовой выгоды, месть, получение от общества того, что оно якобы задолжало, попытка добиться расположения со стороны других людей, проявления собственного «я», развлечение, самовыражение, случайность.

В зависимости от мотивообразующих факторов выделяют лиц: «с ярко выраженным корыстным мотивом; с отличительной особенностью устойчивого сочетания профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма, и изобретательности; с информационными болезнями или компьютерными маниями»[2].

Типовой криминологический портрет личности мошенника в сфере компьютерной информации:

---

[1] Официальный сайт МВД России. URL: https://http://www.cdep.ru/ (дата обращения: 24.10.2024).

[2] Назмеева, Л.Р. Мошенничество в сфере компьютерной информации: криминологическая характеристика личности преступника / Л.Р. Назмеева, Т.В. Соловьева // Ученые записки Казанского юридического института МВД России. – 2023. – Т. 8, № 2(16). – С. 62.

1. Мужчина в возрасте до 35 лет. Городской житель, имеющий среднее специальное или высшее техническое образование.

2. Не состоящий в семейном браке (холост либо разведён).

3. Обладающий профессиональными навыками и опытом работы на компьютерных устройствах.

4. Безработный (недавно уволенный с работы или службы) либо работающий специалист в области IT-технологий (системный администратор, инженер-программист, менеджер по продажам компьютерных устройств, технический директор).

5. В прошлом судимости не имел и к уголовной ответственности не привлекался, но компьютерные преступления совершал неоднократно.

6. Преступные деяния предпочитает совершать в одиночку, так как обладает низкой социальной коммуникативностью и по характеру является индивидуалистом, эгоцентричной личностью.

С психологической точки зрения, компьютерный преступник является неординарной и мыслящей личностью, который достаточно замкнут и скромен в общении со сверстниками или коллегами, поскольку большую часть времени проводит за компьютером в «виртуальном» мире, предпочитая его «живому» общению.

Анализируя особенности мошенников, следует отметить, что они нередко являются замкнутыми и необщительными людьми, предпочитая общение в социальных сетях и редко имея друзей в реальной жизни. При этом они могут обладать высокой самооценкой и считать себя гениями, что влияет на их отношение к жертвам. Им присущ аналитический склад ума и развитое логическое мышление; при планировании преступления они проявляют творческий подход.

Рассматривая личность преступника, занимающегося совершением исследуемых деяний, мы видим, что его специфической, отличительной чертой является нацеленность не на личностные ориентиры и качества потерпевшего, а на техническую возможность совершения преступного

деяния. Такое построение своей деятельности и позволяет преступнику достигать желаемого результата.

А.Е. Петрова под личностью потерпевшего понимает следующее это человек, организация или группа лиц, пострадавших от действий преступника или другого правонарушителя[1].

Исследование личности потерпевшего можно рассматривать в двух аспектах[2]:

1. «Статическая область». К ней относятся возраст, пол, национальность, служебное положение и т. д. Ряд этих признаков требуется выяснить по непосредственному требованию закона, причём некоторые из них могут прямо влиять на квалификацию преступления (например, возраст при половых преступлениях).

2. «Динамическая область». Это поведение потерпевшего в период, непосредственно предшествовавший событию преступления, и в период события преступления, и связь этого поведения с поведением преступника.

Изучение личности потерпевшего позволяет выдвигать возможные следственные версии, устанавливать истинные мотивы преступления, избирать наиболее эффективную тактику проведения следственных действий с участием потерпевшего (таких как допрос, очная ставка и другие).

---

[1] Петрова, А.Е. Типичные свойства личности потерпевшего, преступника и связь между ними, как элементы характеристики хищений предметов, имеющих особую ценность / А.Е. Петрова // Социально-экономические, организационные, политические и правовые аспекты обеспечения эффективности государственного и муниципального управления : Материалы IV Всероссийской научно-практической конференции молодых ученых, Барнаул, 27 ноября 2021 года. – Барнаул: Алтайский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»., 2022. – С. 399.

[2] Мякинина, Ю.Н. Криминалистическая характеристика потерпевшего / Ю.Н. Мякинина, М.А. Сазонова // Грядущим поколениям завещаем: творить добро в защиту права : Материалы Всероссийской научно-практической конференции студентов с международным участием, Оренбург, 23–24 марта 2022 года / Под редакцией Е.В. Ерохина. – Оренбург: Общество с ограниченной ответственностью Типография "Агентство Пресса", 2022. – С. 464.

К специальным методам исследования личности и поведения потерпевшего относятся анализ следственной и судебной статистики, изучение материалов судебно-психологической и судебно-психиатрической экспертиз, социально-психологические и судебно-психологические исследования конфликтных ситуаций.

Актуальность изучения личности потерпевшего от мошенничества в сфере компьютерной информации обусловлена рядом факторов:

1. Важность информации о личностных характеристиках потерпевшего. Она позволяет более подробно охарактеризовать личность преступника, мотивы совершения преступления, точно определить круг людей, среди которых следует искать преступника, и спланировать поисковые действия, чтобы найти наиболее важные доказательства по делу.

2. Возможность глубже понять обстоятельства преступления. Изучение криминально значимых характеристик личности и поведения жертвы (до, вовремя и после совершения преступления) помогает выявить те, что указывают на оригинальность, направленность и мотивы преступника, его общие (типичные) и индивидуальные свойства.

3. Создание криминалистической типологии потерпевших. Выявление характеристик потерпевших, характерных для конкретного вида преступлений, их анализ, обобщение и систематизация позволяют создать типологию, которая дополнительно обогащает криминалистическую характеристику отдельных видов преступлений.

Кроме того, полученные в ходе исследований материалы могут стать основой для проведения практических мероприятий виктимологического характера.

«Потерпевшие же от таких преступлений, наоборот, напротив, могут быть малознакомы с информационными технологиями, иметь сравнительно небольшой опыт онлайн-покупок (платежей) и т.д. Такие люди обычно являются пользователями различных платежных систем, которые мошенники используют в своих целях. Кроме того, потерпевшие нередко раскрывают

личную информацию, будучи невнимательными к предупреждениям банков и платежных систем о сохранении конфиденциальности: они могут сообщать посторонним свои паспортные данные, информацию о реквизитах банковской карты (номере, CVC-коде, сроке действия), пин-коде и т.д.»[1].

Еще одной категорией потерпевших являются лица, потерявший деньги при онлайн-пожертвованиях. Эти лица, как правило, характеризуются доверчивостью и сострадательностью, готовностью всегда прийти на помощь.

Обращаясь к вопросу о типичных потерпевших от мошенничества в сфере компьютерной информации можно отметить, что ими могут являться как физические, так и юридические лица. Отсутствие непосредственного контакта между преступником и потерпевшим порождает не нацеленность на личностные качества и ориентиры потерпевшего, единственным критерием выступает наличие у последнего соответствующих материальных благ.

Личность потерпевшего от мошенничества в сфере компьютерной информации включает в себя различные характеристики, которые могут помочь в расследовании преступления.

К объективным условиям деятельности потерпевшего относятся[2]:

- вид деятельности или род занятия потерпевшего;
- форма собственности предприятия или физического лица;
- юридическое положение и категория доступности используемой компьютерной информации;

---

[1] Матиенко, А.С. Понятие и система преступлений в сфере компьютерной информации / А.С. Матиенко // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». – 2022. – Т. 4, № 14-2. – С. 16.

[2] Мартынюк, К.А. Криминалистическое изучение личности потерпевшего при расследовании мошенничества в сети интернет / К.А. Мартынюк // Актуальные проблемы раскрытия и расследования преступлений, совершаемых с использованием интернета : Сборник материалов Всероссийской научно-практической конференции, Белгород, 23 сентября 2021 года / Под редакцией Н.А. Жуковой. – Федеральное государственное автономное образовательное учреждение высшего образования«Белгородский государственный национальный исследовательский университет»: Белгородский государственный национальный исследовательский университет, 2021. – С. 159.

– вид права собственности на обрабатываемую и используемую компьютерную информацию (информационные ресурсы), а также средства её обработки;

– назначение и структура организации информационно-производственного процесса, характер потребляемых ресурсов и выпускаемой продукции;

– система учёта и отчётности по документам на машинном носителе информации, её соответствие действующему законодательству, правилам, положениям и иным нормативным документам;

– кадровое и материально-техническое обеспечение обработки компьютерной информации;

– вид используемых средств вычислительной техники, связи и телекоммуникаций, их тактико-технические характеристики и соответствие категории обрабатываемых информационных ресурсов;

– погодные условия;

– наличие необходимых помещений и вспомогательного оборудования;

– наличие, техническое состояние и соответствие средств защиты информации, а также охраны объектов информатизации категории обрабатываемых информационных ресурсов;

– наличие необходимой организационно-распорядительной документации, регламентирующей порядок обработки и использования охраняемой законом компьютерной информации, её соответствие специальным требованиям защиты информации.

К субъективным характеристикам потерпевшего относятся, например[1]:

– вид деятельности или род занятия потерпевшего;

– форма собственности предприятия или физического лица;

[1] Старостенко, О.А. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно- телекоммуникационных технологий / О.А. Старостенко // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 5. – С. 268.

– юридическое положение и категория доступности используемой компьютерной информации;

– вид права собственности на обрабатываемую и используемую компьютерную информацию (информационные ресурсы), а также средства её обработки;

– назначение и структура организации информационно-производственного процесса, характер потребляемых ресурсов и выпускаемой продукции;

– система учёта и отчётности по документам на машинном носителе информации, её соответствие действующему законодательству, правилам, положениям и иным нормативным документам;

– кадровое и материально-техническое обеспечение обработки компьютерной информации;

– вид используемых средств вычислительной техники, связи и телекоммуникаций, их тактико-технические характеристики и соответствие категории обрабатываемых информационных ресурсов;

– погодные условия;

– наличие необходимых помещений и вспомогательного оборудования;

– наличие, техническое состояние и соответствие средств защиты информации, а также охраны объектов информатизации категории обрабатываемых информационных ресурсов;

– наличие необходимой организационно-распорядительной документации, регламентирующей порядок обработки и использования охраняемой законом компьютерной информации, её соответствие специальным требованиям защиты информации.

Выявление и изучение криминально значимых характеристик личности и поведения жертвы (до, вовремя и после совершения преступления) позволяет глубже понять многие обстоятельства преступления.

Криминологические характеристики личности потерпевшего от мошенничества в сфере компьютерной информации[1]:

1. Ненадлежащее отношение к вопросу обеспечения информационной безопасности.

2. Нежелание потерпевших финансовых структур подавать сообщения в правоохранительные органы о совершённых в отношении их преступлениях, чтобы не потерять клиентов.

3. Правовая и компьютерная неграмотность пользователей.

4. Высокая виктимность в силу активного использования гаджетов, интернет-сервисов и электронных средств платежа.

При совершении преступления важную роль играют субъективные качества потерпевшего, его поведение. Небрежность, нерасторопность или самонадеянность чаще всего провоцируют преступника.

Также к криминологической характеристике личности потерпевшего можно отнести нежелание подавать сообщения в правоохранительные органы о совершённых в отношении него преступлениях, чтобы не потерять клиентов.

Таким образом, характерные черты личности преступника при мошенничестве в сфере компьютерной информации:

1. Преимущественно мужчины в возрасте от 14 лет, при этом характерно увеличение среди них лиц от 20 до 40 лет.

2. Профильное образование и хорошие технические навыки.

3. Азарт как мотив преступления, иногда даже вытесняющий на второй план корысть, но чаще ими движут оба мотива одновременно.

4. Замкнутость, предпочтение общения в социальных сетях, в реальной жизни малый круг общения.

5. Завышенная самооценка, восприятие себя как гениев, к своим жертвам отношение с пренебрежением.

---

[1] Лунеев, В.В. Криминология : учебник для вузов / В.В. Лунеев. – Москва : Издательство Юрайт, 2024. – 68 с.

6. Любовь к риску, аналитический склад ума, логическое мышление, при реализации преступных замыслов проявление творческого подхода.

Характерные черты личности потерпевшего при мошенничестве в сфере компьютерной информации:

1. Обладание материальными благами, доступ к которым осуществляется, в том числе посредством преодоления программно-технической защиты.

2. Недостаточное внимание к соблюдению мер защиты компьютерной информации.

ГЛАВА 2. ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Общесоциальное предупреждение мошенничества в сфере компьютерной информации

Актуальность изучения вопроса общесоциального предупреждения мошенничества в сфере компьютерной информации обусловлена рядом факторов:

1. Увеличение количества таких преступлений. В интернете существенно выросло число мошеннических действий, возрос причиняемый ущерб, изменились способы совершения и «инструментарий» мошенников.

2. Безнаказанность мошенников. Жертвы не обращаются в правоохранительные органы, считая это бесполезным. Проблема усугубляется тем, что электронный платёж сложно проследить, а незначительность ущерба зачастую не позволяет возбудить уголовное дело.

3. Необходимость повышения безопасности информационных систем. В том числе актуально разрабатывать и внедрять собственные программные средства защиты, что особенно важно в условиях санкций.

За мошенничество в сфере компьютерной информации назначается наказание по статье 159.6. УК РФ[1] большое значение имеет наличие или отсутствие квалифицирующих признаков преступления. Если их нет, то преступнику может быть назначено одно из следующих наказаний:

1. Обязательные работы сроком до 360 часов.

2. Штраф до 120 000 рублей.

3. Исправительные работы сроком до 1 года.

4. Принудительные работы на 2 года.

5. Лишение свободы на срок до 2 лет.

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

Если причиненный ущерб не превышает 2500 рублей, то за мошенничество наступает лишь административная ответственность по статье 7.27 КоАП РФ[1].

В случае наличия квалифицирующего состава преступления грозит более серьезное наказание. Более подробную информацию об этом можно получить в статье 159.6 УК РФ. К квалифицирующим признакам относятся[2]:

1. Действия, причинившие крупный ущерб потерпевшему, а также совершенные по предварительному сговору группой лиц.

2. Действия, совершенные с использованием служебного положения.

3. Мошеннические действия в отношении банковского счета или электронных кошельков.

Если в отношении человека совершены мошеннические действия в сфере компьютерной информации, нужно обратиться в полицию, в специальный отдел, расследующий киберпреступления. Написать заявление по установленной форме, в нем обязательно указываете[3]:

1. Сайт, на котором в отношении потерпевшего было совершено преступление.

2. Реквизиты карты, банковского счета, электронного кошелька, с которого были похищены или списаны деньги.

3. Все имеющиеся данные лица, с которым вы общались – электронная почта, номера в мессенджерах, профили в социальных сетях.

4. Обязательно приложить скриншоты переписки, если таковые имеются.

---

[1] Кодекс Российской Федерации об административные правонарушения: Федеральный закон от 30.12.2001 № 195-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

[2] Уголовное право. Общая часть. Семестр I : учебник для вузов / И.А. Подройкина [и др.] ; ответственные редакторы И.А. Подройкина, Е.В. Серегина, С.И. Улезько. – 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 37 с.

[3] Варыгин, А.Н. Основы криминологии и профилактики преступлений : учебное пособие для вузов / А Н. Варыгин, В.Г. Громов, О.В. Шляпникова ; под редакцией А. Н. Варыгина. – 2-е изд. – Москва : Издательство Юрайт, 2024. – 15 с.

Как показывает практика, расследование преступлений в сфере компьютерной информации идет очень сложно и длительно. Порой в действиях не усматривается состав мошенничества, т.к. пострадавший добровольно передает средства и не осознает, за что платит. Иногда возникают сложности с поисками злоумышленника, которые используют несуществующие аккаунты и профили, номера телефонов, зарегистрированные на иных лиц.

Именно по этой причине юридическая консультация или помощь опытного юриста заметно повышают шансы на успех. Квалифицированный адвокат в рамках своей компетенции может отыскать аналогичные случаи и других пострадавших.

Групповое заявление дает больше шансов, что уголовное дело по статье 159.6 УК РФ будет возбуждено, а следственно-розыскные действия будут проведены должным образом. Запишитесь за консультацию онлайн и подробно опишите ситуацию.

Для общесоциального предупреждения мошенничеств в сфере компьютерной информации можно предпринять следующие меры[1]:

Информировать население о новых способах обмана. Для этого нужно создавать веб-сайты, посвящённые информированию пользователей об основных техниках мошенничества, и освещать соответствующую информацию в СМИ.

Повышать уровень правовой культуры граждан. Для этого в школах, средних и высших учебных заведениях нужно проводить лекции и семинары.

Укреплять авторитет правоохранительных органов. Это необходимо, чтобы потенциальный преступник осознавал реальную возможность быть пойманным и понести за это уголовное наказание.

Некоторые меры общесоциального предупреждения мошенничеств в сфере компьютерной информации[2]:

---

[1] Антонян, Ю.М. Криминология : учебник для среднего профессионального образования / Ю.М. Антонян. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 38 с.

1. Совершенствование правовой политики, в том числе уголовной. Наведение правопорядка в области электронных сделок и платежей позволит сократить количество правонарушений, совершаемых мошенниками.

Некоторые меры, которые помогают защитить граждан от мошеннических операций:

С 25 июля 2024 года вступает в силу закон[1]. По нему банки обязаны приостанавливать на два дня переводы, если информация о получателе денег содержится в базе данных Банка России о случаях и попытках мошеннических операций. В противном случае кредитной организации придётся вернуть клиенту деньги в течение 30 календарных дней.

Банки обязаны отключать доступ к дистанционному обслуживанию клиентам, которые занимаются выводом и обналичиванием похищенных денег. Их платёжные инструменты будут блокироваться, если при информационном обмене от правоохранительных органов поступили сведения об участии человека в мошеннической схеме.

Оператор после перевода денежных средств обязан возместить клиенту сумму в 30-дневный срок, если получит от Банка России информацию о том, что проведённая операция содержит признаки перевода без добровольного согласия клиента.

Также для разрешения правовых споров в сфере электронной коммерции предлагается разработать Федеральный закон «Об электронных сделках», где будут закреплены нормы, регулирующие все вопросы, касающиеся сделок, совершение которых происходит электронным способом.

---

[2] Емельянов, Д.А. Предупреждение мошенничества в сети Интернет / Д.А. Емельянов // Право и законность: вопросы теории и практики : сборник материалов XII Всероссийской научно-практической конференции, Абакан, 22–23 апреля 2022 года. – Абакан: Издательство ФГБОУ ВО «Хакасский государственный университет им. Н. Ф. Катанова», 2022. – С. 87.

[1] О внесении изменений в Федеральный закон «О национальной платежной системе»: Федеральный закон от 24.07.2023 № 369-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 15.11.2024).

2. Развитие международного сотрудничества по борьбе с транснациональной компьютерной преступностью. Необходимо решать вопросы разграничения юрисдикции двух или нескольких государств, закреплять национальные уголовно-правовые нормы с международными.

Для развития международного сотрудничества по борьбе с транснациональной компьютерной преступностью необходимо[1]:

1. Достичь общего понимания криминальных угроз в киберпространстве. Для этого нужно активно взаимодействовать технических экспертов, сотрудников правоохранительных органов, представителей научного сообщества и международных полицейских организаций.

2. Создать специальные ведомства или подразделения на международном уровне. Они должны иметь чёткий мандат деятельности и правила сотрудничества с компетентными органами различных государств.

3. Унифицировать процессуальные нормы и протоколы. Это позволит сделать цифровые доказательства, обрабатываемые в одной стране, допустимыми в другой.

4. Заключить универсальный международный договор о борьбе с компьютерными преступлениями. Он должен учитывать накопившийся опыт международных соглашений в этой области и особенности национального законодательства стран-участниц. Например, таким универсальным регулятором могла бы стать отдельная Конвенция ООН о компьютерных преступлениях.

Некоторые международно-правовые основы сотрудничества в области борьбы с компьютерной преступностью: Конвенция Совета Европы о киберпреступности 2001 года, Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на Одиннадцатом

[1] Решетников, А.Ю. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А.Ю. Решетников, О.Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 88 с.

Конгрессе Организации Объединённых Наций по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 года, Глобальная программа кибербезопасности, утверждённая Международным союзом электросвязи в 2007 году.

3. Информирование населения о видах мошенничества и способах противодействия ему. Для этого нужно использовать все возможные способы доведения информации до населения, специализируя её подачу под потребности различных возрастных групп граждан.

Для информирования населения о видах мошенничества и способах противодействия ему можно использовать различные способы доведения информации, адаптируя её под потребности разных возрастных групп граждан.

Для людей пожилого возраста эффективным каналом информирования может быть использование ближайших родственников из противоположной возрастной категории – детей и внуков, которые становятся «проводниками» для доставки необходимой информации лицам старшего возраста. Для детей младшего школьного возраста подойдут игровые механики, например, конкурсы, а также подача материала в формате обучающей видеорекламы. Для граждан старше 45 лет эффективным каналом донесения информации может быть размещение социальной рекламы, в том числе на справочно-информационных порталах в интернете, в центрах государственных услуг, городских поликлиниках.

Также можно использовать информационные кампании на популярных ресурсах и в средствах массовой информации, рекламу, интерактивное общение с пользователями.

4. Развитие навыков цифровой гигиены. Одной из основных составляющих является поддержание электронной безопасности. Для этого нужно использовать надёжные пароли и регулярно их обновлять, а также активировать двухфакторную аутентификацию для защиты личных данных от несанкционированного доступа.

Для развития навыков цифровой гигиены и поддержания электронной безопасности рекомендуется:

4.1. Использовать сложные пароли. Они должны содержать заглавные и строчные буквы, специальные символы. Пароли желательно регулярно менять.

4.2. Включить двухфакторную аутентификацию. Это дополнительный уровень защиты любого аккаунта в интернете. Для входа в аккаунт система запросит не только пароль, но и код, который придёт в SMS или электронном письме.

4.3. Остерегаться вирусов. Устанавливать надёжные антивирусные программы, своевременно обновлять ПО. Не посещать сомнительные ресурсы.

4.4. Сохранять конфиденциальность в соцсетях. Не размещать материалы, по которым можно понять, где находится дом или место работы. Не ставить отметки геолокации, когда отправляетесь в кино или кафе.

4.5. Быть внимательным. При установке новых приложений или регистрации на сайтах, убедиться в надёжности ресурса. Не игнорировать пользовательские соглашения и тщательно проверять, даёте ли вы разрешение на доступ к личной информации.

4.6. Регулярно обновлять программное обеспечение. Обновления часто содержат патчи для обнаруженных уязвимостей.

4.7. Делать резервные копии важных данных. Это поможет сохранить информацию в случае взлома или технической неисправности.

4.8. Следить за новостями в сфере безопасности. Чтобы быть в курсе последних угроз и способов их предотвращения.

Таким образом, общесоциальное предупреждение мошенничеств в сфере компьютерной информации может включать следующие меры:

1. Совершенствование правовой политики, в том числе уголовной.

2. Создание и функционирование социально-правового контроля.

3. Нормативно-правовое регулирование криминологической экспертизы.

4. Создание нормативного акта по регулированию общественных отношений в интернете.

5. Развитие международного сотрудничества по борьбе с транснациональной компьютерной преступностью.

6. Профилактика, влияние на правосознание людей. Например, призывы не сообщать личную информацию, не переводить денежные средства и данные банковских карт.

Также важно обучать пользователей основам безопасности в сети интернет, чтобы предостеречь себя от потенциальных опасностей. Например, не открывать подозрительные ссылки или скачивать файлы с ненадёжных источников.

§2. Специально-криминологические меры предупреждения мошенничества в сфере компьютерной информации

Предупреждение преступлений в криминологии рассматривается как особый вид деятельности государства и общества, направленный на поиск эффективных средств и методов воздействия на преступность.

Специально-криминологическое предупреждение – это «социальный процесс, основой которого является применение отвечающих требованиям законности специальных методов и приемов регулирования социальных отношений в целях ликвидации тех их отрицательных последствий, которые могут вызвать совершение преступлений»[1].

Специально-криминологическое предупреждение – это воздействие на социальные группы, отдельных лиц и организации или сферы деятельности,

[1] Варыгин, А.Н. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А.Н. Варыгин, В.Г. Громов, О.В. Шляпникова ; под редакцией А. Н. Варыгина. – 2-е изд. – Москва : Издательство Юрайт, 2024. – 45 с.

в отношении которых есть основания полагать, что они обладают повышенной криминогенностью или виктимностью.

Цель такого предупреждения – выявить и устранить (блокировать, нейтрализовать) причины, условия и иные детерминанты преступности.

Наряду с этим специально-криминологическое предупреждение включает в себя предотвращение замышляемых и подготавливаемых, пресечение начатых преступлений.

При специальном предупреждении преступности на основе криминологических исследований выделяются повышенно-криминогенные и повышенно-виктимные социальные группы, сферы деятельности и объекты. К первым можно, например, отнести несовершеннолетних из неблагополучных семей, лиц без определённого источника дохода, группы населения, находящегося за чертой бедности. К повышенно-виктимным – владельцев больших капиталов и такие объекты, как хранилища ценностей.

Актуальность исследования специально-криминологических мер предупреждения мошенничеств в сфере компьютерной информации обусловлена рядом факторов:

1. Трансформация видов и способов мошенничества. Построение «цифровой экономики», удешевление средств автоматизированной обработки (передачи) данных и экспонентный рост числа пользователей современными компьютерными технологиями открыли новые возможности для представителей криминального мира. Как следствие, виды и способы мошенничества быстро и существенно трансформируются, придавая ему всё большее виртуальное измерение.

2. Специфика преступлений в сфере компьютерной информации. Она порождает сложности как в обнаружении фактических действий злоумышленника, так и в определении потенциальной возможности совершения преступного деяния.

Таким образом, актуальность исследования заключается в необходимости разработки эффективных мер по предупреждению

мошенничеств в сфере компьютерной информации с учётом современных тенденций и вызовов.

Поскольку мошенничество в сфере компьютерной информации сопряжено с воздействием на психику человека, то представляется, что основные предупредительные меры должны быть направлены на работу с жертвой преступления, а, следовательно, на первый план в предупреждении мошенничества должна выйти виктимологическая профилактика.

Субъектами предупреждения должны стать, прежде всего, органы внутренних дел, так как борьба с мошенническими в сфере компьютерной информации относится к их компетенции.

Объекты предупреждения – это граждане, способные стать жертвой мошенничества в сфере компьютерной информации.

В целях виктимологической профилактики предлагается реализация следующих мер предупредительного характера.

Во-первых, задача органов внутренних дел состоит в своевременном информировании населения о новых способах преступного посягательства. Для этого необходимо использовать ряд мер, к которым, в частности, можно отнести[1]:

1) размещение информации о мошеннических действиях на официальных сайтах МВД России;

2) публикация информации в иных источниках – в газетах, на телевидении, по радио;

3) выступление участковых уполномоченных полиции на сходах граждан.

Во-вторых, действенной мерой должен стать мониторинг новых способов мошенничества, совершаемого организованными группами со стороны сотрудников следственных и оперативных подразделений органов

[1] Власов, В.А. Отдельные актуальные правовые аспекты мошенничества с использованием компьютерной информации / В.А. Власов, В.А. Кондратова, И.В. Морозова // Аграрное и земельное право. – 2020. – № 11(191). – С. 159.

внутренних дел, изучение следственной и судебной практики других регионов страны, обмен информацией о мошеннических действиях и практическим опытом.

В-третьих, важным моментом является разработка виктимологической памятки для населения по безопасному использованию сети Интернет, чтобы не стать жертвой мошенничества. В подобной памятке следует разместить информацию о способах мошенничества, совершаемого с использованием сети Интернет. Так И.М. Комаров говорит о необходимости создания единого интернет-портала помощи жертвам, пострадавшим от мошенничества[1].

В-четвертых, в целях ограничения доступа к сайтам, созданным для совершения мошенничества, предлагается дополнить ч. 1 ст. 15.3 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2], в которой предоставить Генеральному прокурору РФ и его заместителям право обращаться в Роскомнадзор с требованием о принятии мер по ограничению доступа к данным информационным ресурсам.

К специально-криминологическим мерам предупреждения мошенничества в сфере компьютерной информации относятся[3]:

1. Организационно-техническое ограничение анонимности пользователей в сети «Интернет». Обязательная идентификация возможна в случаях, предусмотренных федеральным законом (например, при

---

[1] Комаров, И.М. Проблемы расследования мошенничества в сфере компьютерной информации (правовыве и криминалистические проблемы) / И.М. Комаров // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью : Сборник научных трудов по материалам V Всероссийской научно-практической конференции (симпозиума), Краснодар, 15 ноября 2019 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 185.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

[3] Афанасьева, О.Р. Криминология : учебник и практикум для вузов / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 89 с.

регистрации в социальных сетях, размещении объявлений о продаже товаров и оказании услуг).

Организационно-технические меры по ограничению анонимности пользователей в сети «Интернет»[1]:

1.1. Идентификация в публичных Wi-Fi-сетях. При подключении пользователя к таким сетям необходимо провести идентификацию его личности и устройства, с которого он заходит в сеть. Для идентификации личности нужно пройти обязательную авторизацию – данные о пользователе могут быть получены из документов, удостоверяющих личность, по номеру его мобильного телефона или из учётной записи на портале «Госуслуг». А mac-адрес устройства идентифицируется при подключении к сети.

1.2. Идентификация в сервисах обмена мгновенными сообщениями. Пользователь сообщает свой абонентский номер организатору сервиса, а тот проверяет его через оператора связи. В базу данных оператора связи заносится уникальный идентификационный номер пользователя сервиса.

Также, согласно Федеральному закону №97-ФЗ от 05.05.2014, владельцам страничек в социальных сетях или личных сайтов с суточной аудиторией более трёх тысяч пользователей запрещено анонимное использование собственных блогов в сети.

2. Мониторинг информационных ресурсов. Его проводят государственные органы, отраслевые структуры и общественные организации для обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества.

Мониторинг информационных ресурсов проводят организации, уполномоченные Правительством Российской Федерации. Он направлен на выявление информации и ресурсов, доступ к которым подлежит

---

[1] Махтаев, М.Ш. Криминалистическое обеспечение предупреждения преступлений (правонарушений) : учебное пособие для вузов / М.Ш. Махтаев. – Москва : Издательство Юрайт, 2024. – 45 с.

ограничению, в том числе в целях обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества.

Также мониторинг защищённости информационных ресурсов осуществляют Центр защиты информации и специальной связи ФСБ РФ и территориальные органы безопасности. Цель таких мероприятий – определить способность ресурсов противостоять угрозам информационной безопасности. Под мониторинг попадают информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, подключённые к интернету.

При выявлении по результатам мониторинга признаков информации и ресурсов, доступ к которым подлежит ограничению, федеральный орган исполнительной власти направляет информацию в уполномоченные государственные органы для рассмотрения и принятия решений.

3. Повышение эффективности применения уголовно-правовых норм. Например, норм с двойной превенцией, предусмотренных статьями 159.6, 272, 273, 274 и 274.1 УК РФ[1].

Для повышения эффективности применения уголовно-правовых норм с двойной превенцией, в том числе предусмотренных статьями 159.6, 272, 273, 274 и 274.1 УК РФ, можно предпринять следующие шаги:

3.1. Сократить латентность преступлений. Для этого, например, внедрить системы автоматизированного учёта и информационные базы данных, в том числе биометрические сканеры, в сфере оборота оружия. Также можно мониторить интернет-ресурсы, в том числе с использованием искусственного интеллекта, для блокировки запрещённой информации и обнаружения преступной деятельности.

---

[1] Уголовное право. Общая часть : учебник для вузов / А.В. Наумов [и др.] ; ответственные редакторы А.В. Наумов, А.Г. Кибальник.- 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 48 с.

3.2. Обеспечить неотвратимость уголовной ответственности. Для этого, например, стимулировать сообщения в правоохранительные органы о готовящемся или совершённом преступлении, что облегчит предотвращение опасного деяния и его дальнейшее расследование.

3.3. Руководиться при рассмотрении уголовных дел положениями федеральных законов, которые регламентируют вопросы создания, распространения, передачи, защиты информации и применения информационных технологий.

3.4. Тщательно изучать собранные в ходе предварительного расследования доказательства. Они должны в полной мере устанавливать все обстоятельства, предусмотренные статьёй 73 УПК РФ.

3.5. Организовать взаимодействие между следственными органами и прокурорами. Это поможет избежать нарушений и затягивания сроков следствия.

4. Установление ограничений на трудовую деятельность в кредитно-финансовой сфере и на должностях, связанных с эксплуатацией и обслуживанием информационных (информационно-коммуникационных) технологий, лицам, ранее привлекавшимся к ответственности за мошенничество в сфере компьютерной информации.

5. Подготовка высококвалифицированных следователей и экспертов-криминалистов в сфере борьбы с высокотехнологичными преступлениями, оснащение их современной криминалистической техникой, предполагает:

5.1. Освоение специальных знаний. Специалисты должны изучать основы функционирования глобальных компьютерных сетей и телекоммуникационных систем, механизмы реализации сетевого обмена, современные операционные системы, механизмы взлома вычислительных систем и методы противодействия им. Также в рамках обучения рассматриваются аппаратные и программные средства фиксации полученной информации и выявления подозрительных событий.

5.2. Изучение особенностей совершения и квалификации преступлений в сфере высоких технологий. Учебный материал должен включать в себя последние научные и практические данные ведущих учёных и практиков в этой области.

Оснащение современной криминалистической техникой включает обеспечение следователей и экспертов-криминалистов такими средствами, как:

5.1.1. Для работы на месте происшествия. Унифицированные чемоданы со средствами и инструментами для изъятия и фиксации следов, цифровой фотокомплект, спутниковый навигатор, лазерный дальномер-рулетка, ультрафиолетовый осветитель, комплект фонарей для осмотра места происшествия.

5.1.2. Для лабораторных исследований. Сравнительные криминалистические микроскопы, передвижные криминалистические лаборатории, приборы для исследования денежных знаков, оттисков печатей и штампов и другие.

Также с развитием IT-технологий экспертно-криминалистические подразделения оснащаются новыми аппаратно-программными средствами, что расширяет возможности экспертного сопровождения расследования высокотехнологичных преступлений.

6. Привлечение специалистов в области IT-технологий для раскрытия и расследования сложных технотронных преступлений, является одной из мер противодействия компьютерной преступности.

Такие специалисты помогают в поиске, извлечении, восстановлении и оперативной обработке данных в электронном виде, связанной с обнаружением и исследованием информации на электронных носителях и цифровых устройствах[1].

---

[1] Афанасьева, О.Р. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 36 с.

Например, в 2022 году в структуре центрального аппарата МВД России было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий, которое занимается предупреждением, выявлением, пресечением и раскрытием преступлений и иных правонарушений в сфере информационно-коммуникационных технологий.

Также для расследования преступлений в сфере высоких технологий в Министерстве внутренних дел Российской Федерации сформировано специальное подразделение. Его задача – обучить и модернизировать навыки и профессиональные компетенции следователей, привлекаемых к раскрытию преступлений в сфере высоких технологий.

7. Создание единой для правоохранительных органов базы данных с элементами искусственного интеллекта по учёту технотронных преступников, совершённых ими преступных деяний и обнаруженных следов преступлений.

Такая база данных с соответствующим программным обеспечением могла бы в автоматическом режиме сопоставлять изъятые с места преступлений «цифровые следы», компьютерные вирусы, а также сведения о технотронных преступниках, совершённых ими и доказанных преступных деяний. В случае выявления определённых совпадений предоставлять сведения о нераскрытых преступлениях и лицах, с большой долей вероятности их совершивших.

Использование криминалистических учётов с элементами искусственного интеллекта, по мнению автора, будет способствовать раскрытию сложных технотронных преступлений и более эффективному их расследованию.

Подводя итог, мы можем сделать вывод, что к специально-криминологические меры предупреждения мошенничества в сфере компьютерной информации:

1. Организационно-техническое ограничение анонимности пользователей в сети «Интернет». Обязательная идентификация возможна в случаях, предусмотренных федеральным законом (например, при регистрации в социальных сетях, размещении объявлений о продаже товаров и оказании услуг).

2. Мониторинг информационных ресурсов. Его проводят государственные органы, отраслевые структуры и общественные организации для обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества.

3. Повышение эффективности применения уголовно-правовых норм. Например, норм с двойной превенцией, предусмотренных статьями 159.6, 272, 273, 274 и 274.1 УК РФ.

4. Установление ограничений на трудовую деятельность в кредитно-финансовой сфере и на должностях, связанных с эксплуатацией и обслуживанием информационных (информационно-коммуникационных) технологий, лицам, ранее привлекавшимся к ответственности за мошенничество в сфере компьютерной информации.

5. Подготовка высококвалифицированных следователей и экспертов-криминалистов в сфере борьбы с высокотехнологичными преступлениями, оснащение их современной криминалистической техникой.

6. Привлечение специалистов в области IT-технологий для раскрытия и расследования сложных технотронных преступлений.

7. Создание единой для правоохранительных органов базы данных с элементами искусственного интеллекта по учёту технотронных преступников, совершённых ими преступных деяний и обнаруженных следов преступлений.

§3. Деятельность органов внутренних дел по предупреждению мошенничества в сфере компьютерной информации

Деятельность органов внутренних дел по предупреждению преступлений – это деятельность служб, подразделений и сотрудников в пределах их компетенции, направленная на недопущение преступлений путём выявления, устранения или нейтрализации причин, условий и обстоятельств, способствующих их совершению, оказания профилактического воздействия на лиц с противоправным поведением.

Одной из наиболее актуальной темы органов внутренних дел является предупреждение мошенничества, особенно в связи с высоким ростом данных преступлений. Как нам известно, первоочередной задачей органов внутренних дел является обеспечение защиты прав и свобод человека и гражданина, а также законных интересов общества и государства. При этом Россия признает себя правовым демократическим государством, где права и свободы человека представляют наивысшую ценность. Это обуславливает актуальность, так как совершение преступления всегда сопровождается тем, что потерпевшее лицо претерпевает определенные неудобства, которые выражаются в нарушении, либо в ограничении прав, свобод и законных интересов. Поэтому деятельность государства должна быть направлена на недопущение преступности в обществе. Однако в современных условиях невозможно представить такое общество, в котором будет отсутствовать преступность. В связи с чем государство возлагает на органы внутренних дел определенные задачи, связанные с предупреждением преступности[1].

[1] Романов, Д.С. Деятельность органов внутренних дел по предупреждению и профилактике преступлений с использование сети Интернет / Д.С. Романов // Молодой исследователь: от идеи к проекту : Материалы IV студенческой научно-практической конференции, Йошкар-Ола, 15 июня 2020 года. – Йошкар-Ола: Марийский государственный университет, 2020. – С. 311.

Также актуальность деятельности органов внутренних дел по предупреждению мошенничеств в сфере компьютерной информации подтверждают ряд факторов:

1. Распространённость киберпреступлений. С развитием информационно-телекоммуникационных технологий (ИТТ) и их широким использованием по всему миру возникают и новые угрозы безопасности.

2. Разрушительные последствия. Киберпреступления могут быть разрушительными для отдельных личностей, организаций и даже государств.

3. Сложное раскрытие и установление лица, подлежащего привлечению в качестве обвиняемого. На момент совершения преступления лицо может находиться в любом месте страны и даже за её пределами.

Для противодействия преступлениям в сфере информационных технологий в структуре МВД России более 14 лет функционирует специальное подразделение – Управление «К». Подразделение занимается не только борьбой с уже совершёнными преступлениями, но и уделяет большое внимание профилактике противоправных деяний и защите граждан от мошенничества в ИТ-сфере.

Меры, которые помогают органам внутренних дел предупреждать мошенничества в сфере компьютерной информации[1]:

1. Повышение осведомлённости пользователей. Обучение людей основам безопасности в сети, их правам и обязанностям, а также методам защиты от киберугроз.

2. Разработка и применение новых технических решений. Использование машинного обучения, искусственного интеллекта и аналитических систем позволяет раннее обнаруживать угрозы,

[1] Александров, Л.П. Предупреждение и раскрытие оперативными подразделениями внутренних дел фактов мошенничества в сфере информационных технологий / Л.П. Александров // Молодежь, наука и цивилизация : Материалы международной студенческой научной конференции, Красноярск, 19 мая 2022 года / Отв. редактор Н.Н. Цуканов. Том Выпуск 24. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. – С. 366.

предотвращать кибератаки и обеспечивать быструю реакцию на инциденты безопасности.

Органы внутренних дел является центральным органом обеспечения соблюдения законности за происходящими в обществе социальными процессами. Для реализации данной задачи так и тех, которые также имеют законодательное закрепление необходим механизм, при помощи которого будет регламентироваться и регулироваться данная деятельность. Деятельность органов внутренних дел по предупреждению преступности представляет особую систему, имеющую специфические особенности.

В качестве нормативной базы по данному направлению деятельности следует назвать следующие правовые акты: Конституцию Российской Федерации[1], положения Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» [2], Федерального закона от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»[3], а также Приказ МВД России от 24.08.2023 № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений»[4], в котором отражены основные задачи органов внутренних дел по профилактике правонарушений. В частности, п. 2 определяет, что субъекты ведомственной системы решают следующие основные задачи:

---

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства РФ, 01.07.2020. № 31, ст. 4398.

[2] Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

[3] Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних: Федеральный закон от 24.06.1999 № 120-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

[4] О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений: Приказ МВД России от 24.08.2023 № 619 // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

– выявляют и анализируют причины и условий, порождающие правонарушения и условия, способствующие совершению правонарушений или облегчающие их совершение, принимают в пределах своих полномочий меры по их устранению и нейтрализации;

– выявляют лиц, подготавливающих правонарушения, принимают к ним меры в соответствии с законодательством Российской Федерации;

– обеспечивают в установленном порядке надзор (контроль) за лицами, противоправные и антиобщественные деяния которых дают основания в соответствии с законодательством Российской Федерации проводить в отношении них такие мероприятия и принимать меры правового воздействия для предупреждения совершения ими правонарушений;

– осуществляют меры по обеспечению безопасности граждан от противоправных посягательств на улицах и в иных общественных местах, объектах транспорта и транспортной инфраструктуры, а также имущественной безопасности всех форм собственности от преступных посягательств; – обеспечивают привлечение граждан, общественных объединений и иных организаций для оказания помощи (содействия) в рамках реализации своих прав в сфере профилактики правонарушений, информируют граждан о способах защиты от противоправных посягательств[1].

Сущность задач состоит в том, что органы предварительного расследования в соответствии со ст. 73 УПК РФ[2] имеют обязанность в установлении обстоятельств, которые способствовали совершению преступлений, а также органы предварительного расследования обязаны вносить представлении о принятии мер по устранению обстоятельств,

---

[1] О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений: Приказ МВД России от 24.08.2023 № 619 // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

[2] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

способствовавших совершению преступления или других нарушений закона[1]. Это вытекает из ст. 158 УПК РФ и п. 4.1.1 Приказа МВД России от 24.08.2023 г. № 619[2].

При этом и другие подразделения органов внутренних дел проводят ежедневную работу по данным направлениям. В частности, участковые уполномоченные полиции и сотрудники подразделений по делам несовершеннолетних проводят профилактические беседы, а также ведут профилактический учет лиц, которые склонны к совершению преступлений[3]. Также на участковых уполномоченных полиции возложена обязанность по осуществлению надзора за лицами, освободившимися из мест лишения свободы. Данные профилактические меры позволяют осуществлять деятельность, которая дает положительные эффекты. Однако стоит сказать о том, что выполнение данных задач нередко сопровождается определенными проблемы. Это обуславливает большое количество причин и условий. В частности, большая загруженность должностных лиц органов внутренних дел не позволяет осуществлять должный надзор за лицами, в отношении которых установлен административный надзор. Также не всегда должным образом проводиться профилактическая работа с несовершеннолетними. Есть еще и другие проблемы, но в большей степени они взаимосвязаны и обуславливаются нехваткой квалифицированных кадров. Поэтому одной из решений данных проблем может являться привлечение новых квалифицированных кадров, что позволит снизить нагрузку с тех сотрудников, которые уже имеют многолетний опыт работы по выполнению

---

[1] О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений: Приказ МВД России от 24.08.2023 № 619 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

[2] Там же.

[3] Новиков, А. Р. Основные направления деятельности органов внутренних дел по предупреждению преступлений / А. Р. Новиков // Социально-экономические и правовые меры борьбы с преступлениями и иными правонарушениями : Всероссийская конференция: сборник научных трудов, Рязанский филиал Московского университета МВД России им. В.Я. Кикотя, 04 апреля 2024 года. – Рязань: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 115.

данных задач. Это определенным образом поспособствует повышению эффективности работы органов внутренних дел по всем направлениям деятельности.

Несомненно, деятельность органов внутренних дел по предупреждении преступности не может осуществляться без наличия принципов, которые являются основными началами, идеями, которые отражают сущность осуществляемой деятельности. При рассмотрении данного вопроса необходимо обратиться к ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» от 23.06.2016 г. № 182-ФЗ[1], в котором в статье 4 закреплены следующие принципы:

1) приоритет прав и законных интересов человека и гражданина при осуществлении профилактики правонарушений. Сущность данного принципа состоит в том, что права и законные интересы человека и гражданина представляют наивысшую ценность для государства. Поэтому четкое и неукоснительное их соблюдение является важной составляющей профилактики правонарушений. В свою очередь, органы внутренних дел не должны допускать каких-либо нарушений, а также унижать чести и достоинства лиц, в отношении которых проводятся мероприятия по профилактике правонарушений.

2) законность. Данный принцип нам говорит о том, что деятельность по предупреждению преступности должна осуществляться только в соответствии с установленным законодательством. Применение иных форм и методов, направленных на профилактику правонарушений не допускается, так как в этой связи будут нарушены права и законные интересы лиц, в отношении которых осуществляются такие мероприятия.

3) обеспечение системности и единства подходов при осуществлении профилактики правонарушений. Системность и единство говорит о том, что

---

[1] Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

профилактика правонарушений представляет сложный процесс, который имеет свою структуру, а также единые подходы при осуществлении профилактики правонарушений, что выражается в том, что в каждом конкретном случае применяются подходы, которые едины по своей природе, то есть методы и средства, направленные на осуществление профилактики систематизированы и единообразны.

4) открытость, непрерывность, последовательность, своевременность, объективность, достаточность и научная обоснованность принимаемых мер профилактики правонарушений. Данный принцип говорит о том, что с мерами, направленными на осуществление профилактики, может ознакомиться любой человек и гражданин. Однако непрерывность означает то, что профилактические мероприятия осуществляются всегда, даже в тех случаях, когда нам может показаться, что такая деятельность не проводиться. Своевременность говорит о том, что профилактические мероприятия должны применяться в тот момент, когда возникают какие-либо предпосылки для совершения антиобщественных действий либо уже в момент совершения противоправного действия, либо же после, но общим является то, что данные меры должны применены в нужное время для того, чтобы были достигнуты задачи по профилактике преступности.

5) компетентность при осуществлении профилактики правонарушений. Данный принцип, безусловно, очень важен, так как от уровня профессионализма сотрудника органов внутренних дел напрямую зависит эффективность осуществления профилактики преступности. От высокого уровня профессионализма в выигрышном положении окажутся все. Ведь и молодые сотрудники будут перенимать опыт у высококвалифицированных сотрудников, так и лица, в отношении которых осуществляются профилактические меры, будут направлены на правильный путь.

6) ответственность субъектов профилактики правонарушений и их должностных лиц за обеспечение прав и законных интересов человека и гражданина. Ответственность субъектов предусматривает то, что сотрудник

органов внутренних дел должен помнить о том, что осуществляет деятельность в соответствии с действующем законодательством, что предполагает наличие у него властных полномочий. Однако наличие норм, предусматривающих ответственность субъектов профилактики правонарушений и их должностных лиц говорит о том, что посредством этого повышается уровень законности осуществляемой деятельности[1].

В настоящее время для более правильного понимания дефиниции «предупреждение преступности» необходимо изучить такие понятия, как «профилактика», «предотвращение», «пресечение», а также определить их соотношение с понятием «предупреждение». При сравнении, по-нашему мнению, следует уделить внимание на смысловое значение данных понятий.

Традиционно в криминологии под предупреждением преступности понимается многоуровневая система целенаправленных государственных и общественных мер по выявлению, устранению, ослаблению и нейтрализации причин и условий преступности ее отдельных видов преступлений, а также по удержанию от перехода или возврата на преступный путь лиц условия жизни и поведение которых указывает на такую возможность.

В частности, в Большом юридическом словаре мы можем увидеть, что под профилактикой преступности понимается совокупность предупредительный мероприятий, которые направлены на сохранение и укрепление урегулированности общественного порядка[2].

Слово «предупредить» в толковом словаре русского языка понимается как заранее известить либо уведомить, а слово «предотвратить» – заранее отвести, устранить, в свою очередь, «пресечь» – прекратить сразу[3].

В криминологии понятие «пресечение» употребляется только по отношению к конкретным преступлениям. Как нам известно из курса

---

[1] Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

[2] Большой юридический словарь / под ред. А. Я. Сухарева, В. Е. Крутских. – М., 2001. – С. 502.

[3] Ожегов, С.И. Толковый словарь / С.И. Ожегов, Я.О. Шведова. – М., 1992. – С. 598-599.

уголовного права, пресечь преступление можно на стадии приготовления или покушения на преступление. В связи с этим пресечение нельзя включать в понятие «предупреждение». Объясняется это тем, что в таком случае лицо уже совершает преступления, пусть и не в оконченном виде.

Таким образом, нами были рассмотрены основные задачи органов внутренних дел по предупреждению преступности, а также принципы данной деятельности. Задачи определяют основные направления, по которым необходимо проводить качественную работу для достижения необходимого уровня правопорядка в стране. От качества выполнения задач зависит общий уровень состояния преступности на территории нашего государства. Поэтому важно отметить, что в руководящих документах были отражены основные задачи, стоящие перед органами внутренних дел по профилактике преступности. При этом, как уже было сказано, принципы являются основополагающими началами, идеями построения всей системы мер по осуществлению профилактики преступности. Их содержание определяет качественный характер выполняемой деятельности в данной области.

Деятельность органов внутренних дел по предупреждению мошенничеств в сфере компьютерной информации включает следующие мероприятия[1]:

1. Создание специализированных отделов в органах внутренних дел, которые занимаются раскрытием и расследованием преступлений, связанных с дистанционными мошенничествами.

Это положительно сказывается на эффективности оперативного сопровождения, качестве и сроках расследования уголовных дел. В небольших территориальных отделах ОВД РФ закрепление за расследованием уголовных дел, связанных с дистанционными

[1] Власенко, В.В. Профилактика органами внутренних дел на региональном уровне правонарушений, совершаемых с использованием информационно-телекоммуникационных технологий (по материалам Ставропольского края) / В.В. Власенко, И.Б. Кулиев // Пробелы в российском законодательстве. – 2021. – Т. 14, № 3. – С. 139.

мошенничествами, должно осуществляться следователем (дознавателем), специально закреплённым за данным направлением и изучившим методику расследования этой категории преступлений.

Например, в 2016 году такой отдел был создан в Управлении уголовного розыска ГУ МВД по Алтайскому краю. Его основные направления работы – раскрытие краж с банковских карт и социальных мошенничеств.

Также в 2022 году указом президента Владимира Путина в структуре МВД России было создано управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК). Среди основных задач управления – предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе министерства.

2. Выявление фактов продажи «виртуальных карт» в неофициальных торговых точках, без процедуры оформления на конкретное лицо. Именно такие «безымянные карты», как правило, используются для осуществления мошенничеств.

Для выявления фактов продажи виртуальных карт в неофициальных торговых точках и их использования в мошеннических целях могут применяться следующие меры[1]:

2.1. Банковские системы мониторинга. Они анализируют миллионы банковских операций и выявляют признаки, которые указывают на оформление карты в недобросовестных целях. Например, система реагирует на переоформление банковской карты на другой номер, после чего сразу проводятся мелкие операции наподобие оплаты товара в магазине. Это может

[1] Совершенствование деятельности ОВД по противодействию компьютерной преступности в РФ / М.Ю. Кузнецов, И.А. Политкин, Р.Ф. Мусугалиев, М.А. Вашаев // Лучшая научно-исследовательская работа 2022 : Сборник статей XXXVI Международного научно-исследовательского конкурса, Пенза, 30 июня 2022 года / Под общей редакцией Г.Ю. Гуляева. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 93.

означать, что владелец продал карту злоумышленникам, и те пытаются вести себя как рядовые клиенты.

2.2. Уголовная ответственность. Передача оформленной на лицо без целей дальнейшего персонального использования банковской карты и средств доступа к системам дистанционного банковского обслуживания в случае их последующего использования для совершения неправомерных операций с денежными средствами влечёт уголовную ответственность по ст. 187 УК РФ.

Также для защиты от мошенничества с банковскими картами рекомендуется не передавать никому реквизиты своей карты, использовать только надёжные источники для оплаты товаров и услуг и при наличии сомнений в безопасности денежных средств самостоятельно перезвонить в банк по номеру телефона, указанному на обороте пластиковой банковской карты.

3. Блокировка любого типа интернет-сети в учреждениях для лиц, содержащихся под стражей, так как значительная часть преступлений данной категории совершается осуждёнными и отбывающими наказание в местах лишения свободы.

Согласно Федеральному закону от 09.03.2021 №44-ФЗ[1], оператор связи может прекратить предоставление услуг по абонентским номерам подвижной радиотелефонной связи в случаях выявления фактов использования этих номеров подозреваемыми, обвиняемыми и осуждёнными на территории следственного изолятора или исправительного учреждения. Решение принимает директор ФСИН России или его заместитель либо начальник территориального органа уголовно-исполнительной системы, в ведении которого находится учреждение.

---

[1] О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы: Федеральный закон от 09.03.2021 № 44-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

Также осуждённым запрещено иметь при себе, хранить и пользоваться средствами связи и комплектующими к ним. Это предусмотрено статьёй 82 Уголовно-исполнительного кодекса РФ и Правилами внутреннего распорядка исправительных учреждений.

4. Установление запрета на возможность получения микрозаймов, кредитов по сети «Интернет» без фактического удостоверения личности гражданина, его состояния в момент взятия финансовой услуги, установления его платёжеспособности и предоставления документов, удостоверяющих личность.

Установить запрет на получение микрозаймов и кредитов по сети «Интернет» можно через самозапрет. Это добровольный отказ от кредитов и займов в банках или микрофинансовых организациях (МФО).

Чтобы установить самозапрет, нужно заполнить шаблонное заявление на «Госуслугах», в МФЦ, лично в банке или микрофинансовой организации и выбрать опции – отказ от выдачи займов банками или МФО, запрет на личное и/или дистанционное оформление кредитов. Для подачи заявления нужны паспорт и СНИЛС.

Самозапрет распространяется только на выдачу нецелевых и необеспеченных залогом кредитов. На ипотеку, автокредит и займы на образование с господдержкой услуга не распространяется.

Запрет начнёт действовать не позднее окончания дня получения заявления квалифицированным бюро кредитных историй (если заявление было подано до 22 часов по мск) или на следующий день (если заявление было подано после 22 часов по мск).

Снять запрет можно также через «Госуслуги» или МФЦ.

5. Проведение разъяснительных бесед и публикация в средствах массовой информации, на официальных сайтах региональных управлений МВД России сюжетов с подробным описанием методик работы мошенников, которые постоянно обновляются и приобретают новые формы.

Проведение разъяснительных бесед и публикация сюжетов с подробным описанием методик работы мошенников являются частью профилактических мероприятий, которые проводятся сотрудниками органов внутренних дел на территории Российской Федерации[1].

Разъяснительные беседы проводят участковые уполномоченные полиции и сотрудники уголовного розыска. Во время встреч они информируют граждан об основных способах мошенничества, а также рассказывают о мерах предосторожности. Например, рекомендуют не доверять звонкам от незнакомцев, не переходить по сомнительным ссылкам и не разглашать свои персональные данные и данные банковских карт и счетов третьим лицам.

В интернете на официальных сайтах Министерства внутренних дел Российской Федерации в разделе «Для граждан» или «Дополнительные страницы» выкладываются информативные видеоролики о том, как защитить себя от мошенников и что делать, если всё же вы стали жертвой мошенников. Эти разделы регулярно обновляются, добавляются новые способы мошенничеств, а также основные способы и рекомендации по их предупреждению.

С самого начала возникновения проблемы МВД по Республике Татарстан предприняты ряд мер: разработаны методические рекомендации и алгоритмы работы по раскрытию и расследованию данных видов преступлений, которые для изучения и использования в служебной деятельности направлены в территориальные ОВД.

В целях эффективного взаимодействия между службами в сентябре 2019 года приказом МВД по Республике Татарстан создана специализированная следственно-оперативная группа по борьбе с преступлениями в сфере информационно-телекоммуникационных

---

[1] Решетников, А.Ю. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А.Ю. Решетников, О.Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 67 с.

технологий. На уровне территориальных ОВД также созданы линейные следственно-оперативные группы.

Таким образом, деятельность органов внутренних дел по предупреждению мошенничеств в сфере компьютерной информации включает следующие мероприятия:

1. Создание специализированных отделов в органах внутренних дел, которые занимаются раскрытием и расследованием преступлений, связанных с дистанционными мошенничествами.

2. Выявление фактов продажи «виртуальных карт» в неофициальных торговых точках, без процедуры оформления на конкретное лицо. Именно такие «безымянные карты», как правило, используются для осуществления мошенничеств.

3. Блокировка любого типа интернет-сети в учреждениях для лиц, содержащихся под стражей, так как значительная часть преступлений данной категории совершается осуждёнными и отбывающими наказание в местах лишения свободы.

4. Установление запрета на возможность получения микрозаймов, кредитов по сети «Интернет» без фактического удостоверения личности гражданина, его состояния в момент взятия финансовой услуги, установления его платёжеспособности и предоставления документов, удостоверяющих личность.

5. Проведение разъяснительных бесед и публикация в средствах массовой информации, на официальных сайтах региональных управлений МВД России сюжетов с подробным описанием методик работы мошенников, которые постоянно обновляются и приобретают новые формы.

Для противодействия преступлениям в сфере информационных технологий в структуре МВД России функционирует специальное подразделение – Управление «К». Также в ведомстве есть Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России).

ЗАКЛЮЧЕНИЕ

Таким образом, под мошенничеством в сфере компьютерной информации мы понимаем, хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Криминологическая характеристика мошенничеств в сфере компьютерной информации включает следующие аспекты:

1. В 2023 году специалисты зафиксировали 207,1 тысяч мошеннических сайтов. Это на 86% больше, чем в предыдущем году. Основные скачки роста количества таких ресурсов пришлись на март, сентябрь и октябрь.

Также изученная криминологическая характеристика показывает, что преступность в этой сфере отличается высоким уровнем латентности, что обусловлено несовершенством законодательства и совокупностью других причин. Наиболее типичным предметом посягательства выступают электронные денежные средства и ценные бумаги, обладающие высокой ликвидностью.

2. Специфические характеристики деяния. К ним относятся способы и механизмы совершения преступления, механизм образования следов, средства, обстановка, место преступления, его предмет и объект.

3. Личностные характеристики мошенников. Это преимущественно мужчины в возрасте от 14 лет, при этом характерно увеличение среди них лиц от 20 до 40 лет. В основном это люди с профильным образованием, наличием хороших технических навыков. Часто их мотивом становится азарт, иногда даже вытесняя на второй план корысть, однако, чаще ими движут оба мотива одновременно. Такие мошенники пользуются компьютерной терминологией и специфической лексикой, непонятной для

лиц, не входящих в круг айтиспециалистов. Они бывают, зачастую замкнуты, предпочитают общение в социальных сетях, в реальной жизни имеют малый круг общения. Самооценка таких мошенников часто завышена, они воспринимают себя как гениев, к своим жертвам относятся с пренебрежением, любят риск. При наличии у следствия серьёзных доказательств, легко идут на сотрудничество.

4. Группы интернет-мошенников. Преступниками могут быть как специалисты с достаточно высокой квалификацией, так и просто дилетанты. Интернет-мошенники делятся на две большие группы: лица, которые находятся с потерпевшим в деловых или трудовых отношениях, и лица, которые не имеют деловых отношений с потерпевшим.

Для предупреждения мошенничеств в сфере компьютерной информации можно рекомендовать, например, виктимологическую профилактику, направленную на предупреждение традиционных форм мошенничества. Важно повышать осведомлённость в области информационной безопасности, в частности, у пользователей систем интернет-банкинга и онлайн-кошельков.

Также для предупреждения мошенничеств в сфере компьютерной информации рекомендуется:

1. Не передавать свои технические устройства незнакомым и малознакомым лицам.

2. Не переходить по ссылкам на сомнительные сайты.

3. Не сообщать незнакомым лицам свои персональные данные, а также информацию о банковских картах и счетах (номера, коды доступа, пароли и т. д.).

4. Использовать антивирусное программное обеспечение и регулярно обновлять его.

5. Не устанавливать и не сохранять без предварительной проверки антивирусной программой файлы, полученные из ненадёжных источников.

6. Проверять все новые файлы, сохраняемые на компьютере.

7. По возможности не сохранять в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически менять их.

Если гражданин пострадал от мошеннических действий, связанных с незаконными банковскими операциями, ему необходимо незамедлительно обратиться в банк, сообщить, что списание денежных средств произошло против воли собственника, заблокировать карту, получить выписку о движении денежных средств по счёту (по возможности), а также обратиться в любой территориальный орган МВД России (подразделение полиции) лично либо по телефону.

Предложения по совершенствованию статьи 159.6 «Мошенничество в сфере компьютерной информации» Уголовного кодекса Российской Федерации:

1. Исключить пункт «в» из части 3 статьи. По мнению некоторых экспертов, он противоречит научно обоснованным критериям дифференциации уголовной ответственности.

2. Дополнить статью дополнительным абзацем. Например, когда хищение совершается путём использования учётных данных собственника или иного владельца имущества с последующим удалением, модификацией либо блокированием охраняемой законом компьютерной информации.

3. Изменить систему квалифицирующих признаков. Добавить в статью пункт о мошенничестве, совершённом лицом, на которое по службе или работе возложены обязанности по обеспечению эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования.

Также предлагается использовать кодификатор компьютерных преступлений и способов их совершения, разработанный Интерполом, для упрощения разработки и интеграции новых составов в отечественное законодательство.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы Российской Федерации:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства РФ, 01.07.2020. № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

4. Кодекс Российской Федерации об административные правонарушения: Федеральный закон от 30.12.2001 № 195-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

6. Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних: Федеральный закон от 24.06.1999 № 120-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

7. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 17.11.2024).

8. О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы: Федеральный закон от 09.03.2021 № 44-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

9. О внесении изменений в Федеральный закон «О национальной платежной системе»: Федеральный закон от 24.07.2023 № 369-ФЗ // Справ.–правовая система «КонсультантПлюс» (дата обращения: 15.11.2024).

10. О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений: Приказ МВД России от 24.08.2023 № 619 // Справ.–правовая система «КонсультантПлюс» (дата обращения: 29.10.2024).

11. Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года: Распоряжение Правительства РФ от 24.11.2023 № 3339-р // Справ.–правовая система «КонсультантПлюс» (дата обращения: 22.10.2024).

II. Монографии, учебники, учебные пособия:

12. Антонян, Ю.М. Криминология : учебник для среднего профессионального образования / Ю.М. Антонян. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 388 с.

13. Афанасьева, О.Р. Криминология : учебник и практикум для вузов / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 356 с.

14. Афанасьева, О.Р. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 356 с.

15. Большой юридический словарь / под ред. А. Я. Сухарева, В. Е. Крутских. – М., 2001. – С. 502.

16. Варыгин, А.Н. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А.Н. Варыгин, В.Г. Громов, О.В. Шляпникова ; под редакцией А. Н. Варыгина. – 2-е изд. – Москва : Издательство Юрайт, 2024. – 165 с.

17. Козаченко, И.Я. Криминология : учебник и практикум для вузов / И.Я. Козаченко, К.В. Корсаков.- Москва : Издательство Юрайт, 2024. – 277 с.

18. Криминология : учебник для вузов / В.И. Авдийский [и др.] ; под редакцией В.И. Авдийского, Л.А. Букалеровой. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 339 с.

19. Криминология : учебник для вузов / О.С. Капинус [и др.] ; под общей редакцией О.С. Капинус. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 1132 с.

20. Криминология и предупреждение преступлений : учебник для среднего профессионального образования / В.И. Авдийский [и др.] ; под редакцией В.И. Авдийского, Л.А. Букалеровой. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 339 с.

21. Криминология. Общая часть : учебник для вузов / В.П. Ревин, В.Д. Малков, В.В. Ревина, Ю.С. Жариков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 178 с.

22. Криминология. Особенная часть : учебник для вузов / Ю.С. Жариков, В.П. Ревин, В.Д. Малков, В.В. Ревина. – 2-е изд. – Москва : Издательство Юрайт, 2024. – 206 с.

23. Лунеев, В.В. Криминология : учебник для вузов / В.В. Лунеев. – Москва : Издательство Юрайт, 2024. – 686 с.

24. Махтаев, М.Ш. Криминалистическое обеспечение предупреждения преступлений (правонарушений) : учебное пособие для вузов / М.Ш. Махтаев. – Москва : Издательство Юрайт, 2024. – 229 с.

25. Ожегов, С. И. Толковый словарь / С. И. Ожегов, Я. О. Шведова. – М., 1992. – С. 598-599.

26. Решетников, А.Ю. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А.Ю. Решетников, О.Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 168 с.

27. Уголовное право. Общая часть : учебник для вузов / А.В. Наумов [и др.] ; ответственные редакторы А.В. Наумов, А.Г. Кибальник.- 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 448 с.

28. Уголовное право. Общая часть. Семестр I : учебник для вузов / И.А. Подройкина [и др.] ; ответственные редакторы И.А. Подройкина, Е.В. Серегина, С.И. Улезько. – 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 307 с.

29. Хайрусов, Д.С. Криминология : учебное пособие для среднего профессионального образования / Д.С. Хайрусов. – Москва : Издательство Юрайт, 2024. – 95 с.

30. Хайрусов, Д.С. Криминология : учебное пособие для среднего профессионального образования / Д.С. Хайрусов. – Москва : Издательство Юрайт, 2024. – 95 с.

III. Статьи, научные публикации:

31. Александров, Л.П. Предупреждение и раскрытие оперативными подразделениями внутренних дел фактов мошенничества в сфере информационных технологий / Л.П. Александров // Молодежь, наука и цивилизация : Материалы международной студенческой научной конференции, Красноярск, 19 мая 2022 года / Отв. редактор Н.Н. Цуканов. Том Выпуск 24. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. – С. 365-368.

32. Арестов, А.В. Преступления в сфере компьютерной информации: проблемы квалификации преступных деяний по статьям 272 и 273 УК РФ /

А.В. Арестов // Социально-экономические процессы современного общества : Материалы II Всероссийской научно-практической конференции с международным участием, Чебоксары, 25 мая 2023 года / Гл. редактор Э.В. Фомин. – Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2023. – С. 188-192.

33. Винокурова, Е.А. Некоторые особенности развития мошенничества в интернете в Российской Федерации / Е.А. Винокурова // Инновации в науке и практике : Сборник трудов по материалам Всероссийского конкурса научно-исследовательских работ, Уфа, 30 мая 2020 года. – Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2020. – С. 99-106.

34. Власенко, В.В. Профилактика органами внутренних дел на региональном уровне правонарушений, совершаемых с использованием информационно-телекоммуникационных технологий (по материалам Ставропольского края) / В.В. Власенко, И.Б. Кулиев // Пробелы в российском законодательстве. – 2021. – Т. 14, № 3. – С. 138-143.

35. Власов, В.А. Отдельные актуальные правовые аспекты мошенничества с использованием компьютерной информации / В.А. Власов, В.А. Кондратова, И.В. Морозова // Аграрное и земельное право. – 2020. – № 11(191). – С. 159-162.

36. Воробьева, М.С. Криминологическая характеристика мошенничества в сфере компьютерной информации / М.С. Воробьева // Союз криминалистов и криминологов. – 2020. – № 2. – С. 130-138.

37. Газизова, А.И. Условия преступности / А.И. Газизова // Современные научные исследования и инновации. – 2019. – № 5(97). – С. 41.

38. Главчева, М.А. Мошенничество в сфере компьютерной информации / М.А. Главчева, А.М. Васильев // Новости науки: социальные и гуманитарные науки : Сборник материалов XXII-ой международной очно-заочной научно-практической конференции, Москва, 21 марта 2023 года. Том 1. – Москва: Научно-издательский центр "Империя", 2023. – С. 50-52.

39. Емельянов, Д.А. Предупреждение мошенничества в сети Интернет / Д.А. Емельянов // Право и законность: вопросы теории и практики : сборник материалов XII Всероссийской научно-практической конференции, Абакан, 22–23 апреля 2022 года. – Абакан: Издательство ФГБОУ ВО «Хакасский государственный университет им. Н.Ф. Катанова», 2022. – С. 87-88.

40. Иващенко, Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы / Н.Д. Иващенко // Столица науки. – 2020. – № 6(23). – С. 269-276.

41. Квятковский, К.С. Преступления в сфере компьютерной информации, компьютерные преступления и киберпреступность: соотношение понятий / К.С. Квятковский // Молодой ученый. – 2022. – № 42(437). – С. 108-112.

42. Кецко К.В. Отдельные особенности личности экономического преступника, действующего в сфере электронной коммерции // Право и государство: теория и практика. 2022. № 7(211). С. 135 - 138.

43. Комаров, И.М. Проблемы расследования мошенничества в сфере компьютерной информации (правовыве и криминалистические проблемы) / И.М. Комаров // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью : Сборник научных трудов по материалам V Всероссийской научно-практической конференции (симпозиума), Краснодар, 15 ноября 2019 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 182-185.

44. Копейко, Т.Г. Причины и условия совершения мошенничества при получении выплат / Т.Г. Копейко // Гуманитарные, социально-экономические и общественные науки. – 2021. – № 4-2. – С. 104-108.

45. Короленко, И.И. Особенности преступлений в сфере компьютерной информации / И.И. Короленко, В.Д. Божко // Актуальные вопросы публичного управления, экономики, права в условиях цифровизации

: сборник научных статей Медународной научно-практической конференции, Курск, 11–12 мая 2023 года / Курская академия государственной и муниципальной службы. Том 1. – Курск: Б. и., 2023. – С. 388-391.

46. Мартынюк, К.А. Криминалистическое изучение личности потерпевшего при расследовании мошенничества в сети интернет / К.А. Мартынюк // Актуальные проблемы раскрытия и расследования преступлений, совершаемых с использованием интернета : Сборник материалов Всероссийской научно-практической конференции, Белгород, 23 сентября 2021 года / Под редакцией Н.А. Жуковой. – Федеральное государственное автономное образовательное учреждение высшего образования«Белгородский государственный национальный исследовательский университет»: Белгородский государственный национальный исследовательский университет, 2021. – С. 158-160.

47. Матиенко, А.С. Понятие и система преступлений в сфере компьютерной информации / А.С. Матиенко // Вестник студенческого научного общества ГОУ ВПО "Донецкий национальный университет". – 2022. – Т. 4, № 14-2. – С. 16-20.

48. Молчанова, Т.В. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий / Т.В. Молчанова, В.А. Аксенов // Вестник экономической безопасности. – 2020. – № 2. – С. 93-98.

49. Мякинина, Ю.Н. Криминалистическая характеристика потерпевшего / Ю.Н. Мякинина, М.А. Сазонова // Грядущим поколениям завещаем: творить добро в защиту права : Материалы Всероссийской научно-практической конференции студентов с международным участием, Оренбург, 23–24 марта 2022 года / Под редакцией Е.В. Ерохина. – Оренбург: Общество с ограниченной ответственностью Типография "Агентство Пресса", 2022. – С. 462-465.

50. Назмеева, Л.Р. Мошенничество в сфере компьютерной информации: криминологическая характеристика личности преступника /

Л.Р. Назмеева, Т.В. Соловьева // Ученые записки Казанского юридического института МВД России. – 2023. – Т. 8, № 2(16). – С. 62-66.

51. Новиков, А. Р. Основные направления деятельности органов внутренних дел по предупреждению преступлений / А. Р. Новиков // Социально-экономические и правовые меры борьбы с преступлениями и иными правонарушениями : Всероссийская конференция: сборник научных трудов, Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 04 апреля 2024 года. – Рязань: Московский университет МВД РФ им. В.Я. Кикотя, 2024. – С. 114-118.

52. Петрова, А.Е. Типичные свойства личности потерпевшего, преступника и связь между ними, как элементы характеристики хищений предметов, имеющих особую ценность / А.Е. Петрова // Социально-экономические, организационные, политические и правовые аспекты обеспечения эффективности государственного и муниципального управления : Материалы IV Всероссийской научно-практической конференции молодых ученых, Барнаул, 27 ноября 2021 года. – Барнаул: Алтайский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»., 2022. – С. 398-400.

53. Полозовская, А.Ю. Причины и условия совершения компьютерных преступлений / А.Ю. Полозовская // Следственная деятельность: проблемы, их решение, перспективы развития : материалы III Всероссийской молодёжной научно-практической конференции, Москва, 25 ноября 2019 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2020. – С. 802-805.

54. Попов, И.С. Преступления в сфере компьютерной информации в России и зарубежных государствах / И.С. Попов // XVII Неделя науки молодежи СВАО : Сборник статей по итогам работы научных конференций и

круглых столов, Москва, 18–30 апреля 2022 года. – Москва: Издательство «Стратагема-Т», 2022. – С. 668-670.

55. Романов, Д.С. Деятельность органов внутренних дел по предупреждению и профилактике преступлений с использование сети Интернет / Д.С. Романов // Молодой исследователь: от идеи к проекту : Материалы IV студенческой научно-практической конференции, Йошкар-Ола, 15 июня 2020 года. – Йошкар-Ола: Марийский государственный университет, 2020. – С. 310-312.

56. Саттаров, Р.Р. Криминологическая характеристика преступлений, совершенных в сфере информационных технологий / Р.Р. Саттаров // Дневник науки. – 2020. – № 4(40). – С. 69.

57. Совершенствование деятельности ОВД по противодействию компьютерной преступности в РФ / М.Ю. Кузнецов, И.А. Политкин, Р.Ф. Мусугалиев, М.А. Вашаев // Лучшая научно-исследовательская работа 2022 : Сборник статей XXXVI Международного научно-исследовательского конкурса, Пенза, 30 июня 2022 года / Под общей редакцией Г.Ю. Гуляева. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 91-94.

58. Старостенко, О.А. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий / О.А. Старостенко // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 5. – С. 267-269.

59. Ульянов, М.В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения / М.В. Ульянов // Правопорядок: история, теория, практика. – 2022. – № 4(35). – С. 102-108.

IV. Диссертации, авторефераты диссертаций:

60. Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации:

диссертация ... кандидата Юридических наук: 12.00.08 / Фролов М.Д. ;[Место защиты: ФГАОУ ВО «Российский университет дружбы народов»], 2019. – 211 с.

61. Камко, А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей [Электронный ресурс] : диссертация ... кандидата юридических наук / А. С. Камко. — Красноярск : СФУ, 2020.

V. Иные источники:

62. Состояние преступности в Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 22.11.2024).

63. Официальный и интернет-портал правовой информации // URL: https://pravo.ru/news/222725/ (дата обращения: 22.10.2024).

64. Официальный сайт МВД России. URL: https://http://www.cdep.ru/ (дата обращения: 24.10.2024).

65. Центробанк предупредил бухгалтеров о мошенниках // https://www.consultantkirov.ru/news/news-from-igk/tsentrobank-predupredil-bukhgalterov-o-moshennikakh.html (дата обращения: 17.11.2024).