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 «Деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации»

Выполнил: Денисов Леонид Сергеевич
(фамилия, имя, отчество)
40.05.02 – Правоохранительная деятельность,
2020 год набора, 002 учебная группа
(специальность, год набора, № группы)

Руководитель: старший преподаватель кафедры
криминологии и уголовно-исполнительного
права КЮИ МВД России, подполковник полиции
(ученая степень, ученое звание, должность, спец. звание)
Битшева Альбина Владимировна
(фамилия, имя, отчество)

Рецензент: Начальник МО МВД России
«Цивильский», подполковник полиции
(должность, специальное звание)
Павлов Антон Германович
(фамилия, имя, отчество)

Дата защиты: «___» _____20___г. Оценка_____

Казань 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Развитие информационных и цифровых технологий несет для общества не только положительные результаты, например возможность обработки и хранения огромного объема информации, влияние на развитие различных сфер, но и отрицательные, связанные с рисками хищения данных и повреждения устройств посредством распространения вредоносных компьютерных программ.

Несмотря на то, что принятие регулятивных нормативных правовых актов, имеющих отношение к общественным отношениям в сфере компьютерной информации происходило с 1992 года, когда были приняты Законы РФ «О правовой охране программ для электронных вычислительных машин и баз данных» № 3523-1 «О правовой охране топологий интегральных микросхем» № 3526-1, в уголовное законодательство нормы об установлении соответствующих составов преступлений были введены только с принятием Уголовного кодекса РФ в 1996 году.

В настоящее время компьютерные технологии становятся основным инструментом реализации преступных целей и задач в виде хищения денежных средств (кибермошеннические действия (ст. 159.3, 159.6 УК РФ)), противоправного воздействия на объекты информационной инфраструктуры и на информационную безопасность государства и общества в целом (Глава 28 УК РФ, включающая ст.ст.272-274.2.). Согласно сведениям, представленным ГИАЦ МВД России, в период с января по декабрь 2024 года на территории России совершено 765365 преступлений с использованием информационно телекоммуникационных технологий, а также в сфере компьютерной информации, что на 13% превышает показатели 2023 года (676951).

Рост количества преступлений в сфере компьютерной информации свидетельствует о том, что отечественная система предупреждения преступности в данной области далека от совершенства. Требуется разработать новые и совершенствовать существующие меры, направленные на противодействие преступлениям, совершаемым с использованием

компьютерных технологий, в сфере компьютерной информации, в том числе и мер криминологического характера, преследующих цель в виде предупреждения противоправных деяний в рассматриваемой сфере. Указанные положения определяют актуальность исследуемой темы.

Цель работы заключается в комплексном исследовании вопросов предупреждения компьютерных преступлений.

Задачи работы:

1) дать характеристику состоянию и тенденциям преступности в сфере компьютерной информации;

2) рассмотреть комплекс детерминант преступности в сфере компьютерной информации;

3) дать характеристику личности киберпреступника;

4) изучить правовые основы предупреждения ОВД РФ преступлений в сфере компьютерной информации;

5) изучить организационные основы предупреждения ОВД РФ преступлений в сфере компьютерной информации;

6) выявить проблемы предупреждения преступлений в сфере компьютерной информации и пути их решения.

Теоретическая основа исследования. При написании работы использованы труды отечественных авторов, исследовавших вопросы предупреждения и пресечения преступлений в сфере компьютерной информации, среди них такие, как И. А. Зуева, Ф. Ю. Сафин, П. А. Ивлиев, А. Г. Савельева, С. А. Григорян, Н. С. Зорина, В. В. Бабурин, Н. С. Север и др.

Методологическая основа исследования представлена общенаучными методами познания, с помощью которых проведено исследование: диалектический метод, методы системного и сравнительного анализа. Использовались также такие частные научные методы, как формально-юридический, сравнительно-правовой, которые позволили рассмотреть явления в их взаимосвязи и взаимообусловленности.

Эмпирической основой исследования представлена материалами статистики, представленной Главным информационно-аналитическим центром МВД России, официально опубликованными материалами судебно-следственной практики. При исследовании вопросов предупреждения преступлений в сфере компьютерной информации также использованы результаты собственных наблюдений и практический опыт, полученный во время прохождения производственной (в том числе преддипломной) практики.

Дипломная работа имеет практическую значимость. В настоящем исследовании выявлены актуальные проблемы в сфере предупреждения преступлений в сфере компьютерной информации, сформулированы предложения по их разрешению. Реализация таких предложений может способствовать улучшению криминогенной обстановки в области компьютерной преступности.

Работа структурно состоит из введения, двух глав, разделенных на 6 параграфов, заключения и списка литературы.

ГЛАВА 1. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА

§1. Преступность в сфере компьютерной информации: понятие, состояние и тенденции

Как известно, преступность в криминологической науке определяется как социальное, исторически изменчивое, массовое, уголовно-правовое, системное явление, которое проявляется в совокупности общественно опасных уголовно наказуемых деяний и лиц, их совершивших, на определённой территории за определённый период времени. Исходя из вышеизложенного, можно сделать вывод о том, что преступность в сфере компьютерной информации образует совокупность преступлений, совершаемых в данной сфере. В отечественном уголовном законодательстве содержится самостоятельная глава, посвященная преступлениям в сфере компьютерной информации – Глава 28, которая включает в себя следующие уголовно-наказуемые деяния (Рис. 1.1. Перечень преступлений в сфере компьютерной информации по УК РФ).

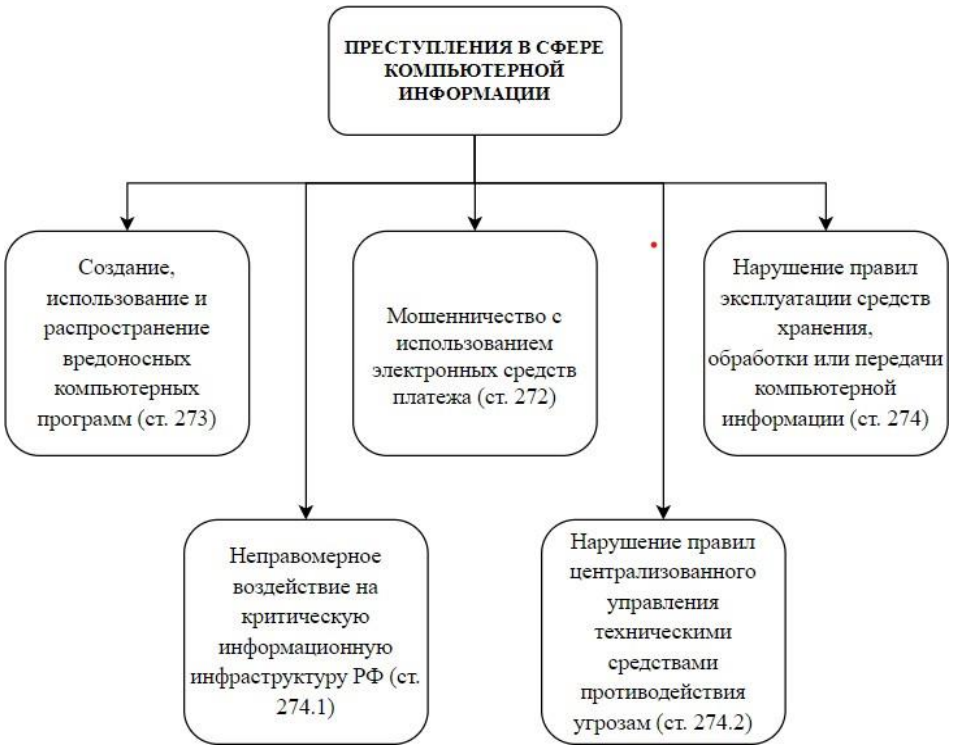

Рис. 1.1. Перечень преступлений в сфере компьютерной информации по УК РФ

Определение понятия «компьютерная информация» содержится в статье 272 Уголовного кодекса РФ:

- сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В процессе исследования возникает вполне закономерный вопрос: следует ли ограничивать структуру преступности в сфере компьютерной информации ранее перечисленными уголовно-наказуемыми деяниями или необходимо дополнить её иными преступлениями, совершаемыми в цифровом пространстве? В науке криминологии не существует общепринятого, единого подхода к рассматриваемому вопросу. Более того, в связи с развитием науки и техники, в криминологии наблюдается переизбыток понятий и категорий – преступность в сфере компьютерной информации, цифровая преступность, компьютерная преступность, киберпреступность, преступность в сфере информационно-телекоммуникационных технологий и т.д. Одни авторы, можно сказать, ставят между указанными понятиями знак равенства, другие предпринимают попытки их разграничить, что не имеет существенного значения для их профилактики и предупреждения.

И.А. Зуева определяет преступность в сфере компьютерной информации как «совокупность предусмотренных уголовным законом общественно опасных деяния, которые направлены против безопасности производства, хранения, использования либо распространения информации или информационных ресурсов и причиняющие или способные причинить вред защищаемым законодательствам благам»[1].

---

[1] Зуева И. А. Преступность в сфере компьютерной информации в России: общая характеристика / И. А. Зуева // Наука, общество, технологии: проблемы и перспективы взаимодействия в современном мире: Сборник статей II Международной научно-практической конференции, Петрозаводск, 28 июня 2022 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2022. – С. 69-73.

По мнению Ф.Ю. Сафина, «преступность в сфере компьютерной информации представляет собой совокупность противоправных уголовно-наказуемых деяний, совершаемых с использованием новых информационных технологий, которые позволяют совершать преступления дистанционно, а также скрывать свою «личность» и результаты преступной деятельности путем «анонимизации» действий, при наличии временного разрыва между началом активных противоправных действий и наступлением негативных последствий»[1].

В настоящем исследовании мы придерживаемся подхода, согласно которому преступность в сфере компьютерной информации представляет собой совокупность уголовно-наказуемых деяний, включенных в Главу 28 УК РФ, а также ряд иных преступлений, совершаемых в цифровом, то есть, киберпространстве. К числу таких деяний следует отнести:

- кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ);

- мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

- мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

- интернет-вымогательство (ст. 163 УК РФ, без квалифицирующего признака в виде «совершение посредством информационно-телекоммуникационных технологий»).

Таким образом, преступность в сфере компьютерной информации образуют деяния, предусмотренные Главой 28 Уголовного закона, а также различные формы хищений чужого имущества, совершаемые в данной сфере. Путем анализа положений уголовного законодательства раскроем сущность преступлений в сфере компьютерной информации.

---

[1] Сафин Ф. Ю. Отдельные аспекты преступности в сфере компьютерной информации / Ф. Ю. Сафин // Научная сессия ГУАП: гуманитарные науки: Сборник докладов традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики, Санкт-Петербург, 14–22 апреля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. – С. 221-222.

Деяние, предусмотренное статьей 272 УК РФ (Неправомерный доступ к компьютерной информации), посягает на общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. Для наступления уголовной ответственности по статье 272 УК РФ необходимо наличие общественно-опасных последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации.

Статья 273 предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, которые образуют объективную сторону исследуемого преступления.

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Обязательным условием для привлечения лица к уголовной ответственности является наступление таких альтернативных общественно-опасных последствий, как уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Уголовная ответственность по статье 274.1 УК РФ наступает за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Критическая информационная инфраструктура, согласно Закону «О безопасности критической информационной инфраструктуры Российской Федерации» – это объекты критической

информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.[1]

Объекты критической информационной инфраструктуры, согласно вышеназванному законодательному акту, – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Неправомерное воздействие оказывается путем создания, распространения и (или) использования компьютерных программ либо иной компьютерной информации.

Статья 274.2 УК РФ устанавливает ответственность за нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств.

Для определения состояния преступности в сфере компьютерной информации необходимо проанализировать статистические материалы, представленные Главным информационно-аналитическим центром МВД России (ГИАЦ МВД России). В материалах ГИАЦ МВД России имеется раздел, в котором содержатся сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[2].

В 2020 году с использованием информационно-телекоммуникационных технологий, а также в сфере компьютерной информации совершено 510396

---

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г № 187 ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 12.09.2024).

[2] Состояние преступности в России за 2020-2024 гг. [Электронный ресурс] // Главный информационно-аналитический центр МВД России URL: https://мвд.рф/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen (дата обращения 11.09.2024).

противоправных деяний (+ 73%), из них 267613 относятся к категории тяжких и особо тяжких.

Показатели 2021 года выше показателей предыдущего на 1,4% (всего совершено 517722 киберпреступлений). Таким образом, рост преступности в исследуемой сфере, несмотря на увеличение доли тяжких и особо тяжких преступлений (288312), был существенно приостановлен. По мнению МВД России, данный результат был связан с успешной работой специализированных подразделений по расследованию IT-преступлений[1].

Данная тенденция сохранилась в 2022 году. Количество киберпреступлений составило 522065, прирост 0,8%. За отчетный период совершено 272233 тяжких и особо тяжких преступлений, что на 5,6% меньше показателей 2021 года. Специалисты в сфере информационной безопасности объяснили данные показатели тем, что значительная часть мошенников, а также иных киберпреступников являются жителями Украины, и в связи с началом спецоперации были вынуждены покинуть страну и искать новое место жительства для продолжения преступной деятельности. Вторая причина – прекращение работы мировых платежных систем на территории России. Так, злоумышленники испытывают трудности с переводом средств на международные кошельки и трансформацию их в криптовалюту[2].

В период с января по декабрь 2023 года на территории России совершено 676951 преступлений с использованием информационно телекоммуникационных технологий, а также в сфере компьютерной информации, что на 30% превышает показатели 2022 года.

В 2024 году количество аналогичных преступлений составило 765365 (+ 13%).

---

[1] Рост киберпреступности замедлился в 2021 году - [Электронный ресурс] // Право.ru: законодательство, судебная система, новости и аналитика. Все о юридическом рынке. https://pravo.ru/news/236839/ (дата обращения 12.09.2024).

[2] Эксперт объяснил, чем обосновано первое за пять лет снижение киберпреступности в России - [Электронный ресурс] // Газета СПБ РУ - новости Санкт-Петербурга https://gazeta.spb.ru/2497344-ekspert-obyasnil-chem-obosnovano-pervoe-za-pyat-let-snizhenie-kiberprestupnosti-v-rossii (дата обращения 12.09.2024).

Таким образом, тенденция постепенного снижения показателей прироста киберпреступлений являлась временной. Современная система профилактики и предупреждения киберпреступлений далека от совершенства. Действительно, приостановлению существенного роста IT-преступлений в России в 2021 и 2022 годах скорее способствовали внешние факторы, нежели деятельность правоохранительных и иных органов, к задачам которых относится противодействие преступлениям в сфере высоких технологий.

Также следует отметить, что в отдельных регионах темпы прироста IT-преступлений превышают показатели по России (Рисунок 1.2. Регионы с наибольшими темпами прироста зарегистрированных преступлений).

Рисунок 1.2 Регионы с наибольшими темпами прироста зарегистрированных преступлений

В то же время в отдельных субъектах РФ наметились положительные тенденции в виде снижения киберпреступлений либо уменьшении темпов их прироста (Рисунок 1.3. Регионы с наименьшими темпами прироста зарегистрированных преступлений). Это – Ямало-Ненецкий АО, где количество преступлений снизилось на 46%, а также Ненецкий АО, Республика Марий Эл,

Забайкальский край, Калужская область, в которых наблюдаются наименьшие темпы прироста зарегистрированных преступлений.

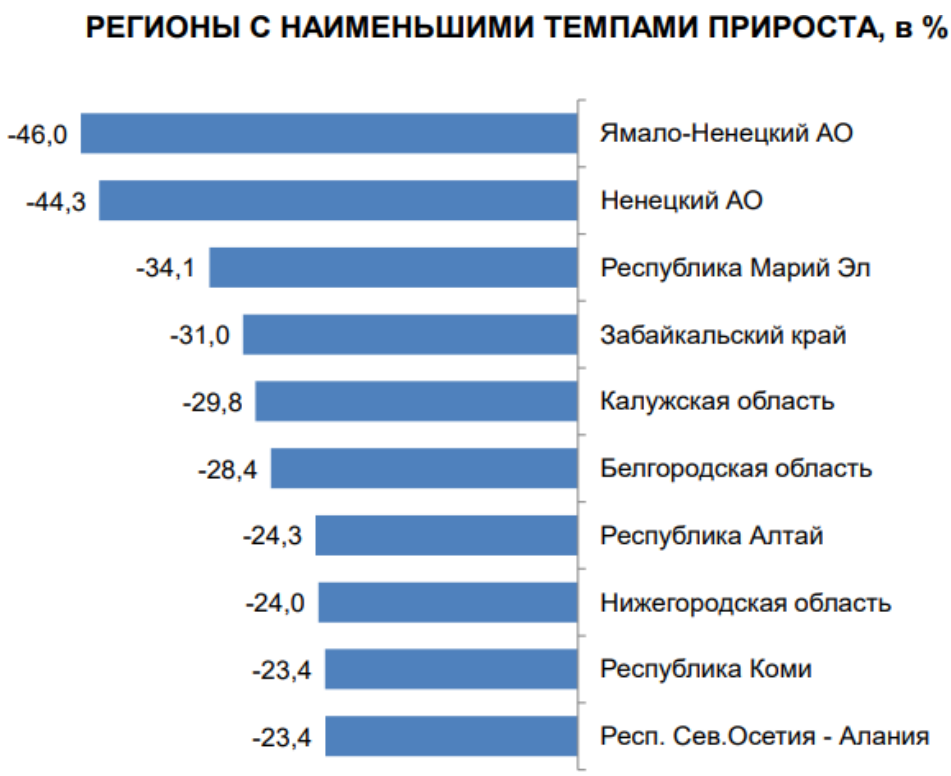

Рисунок 1.3. Регионы с наименьшими темпами прироста зарегистрированных преступлений

Таким образом, за последние 5 лет количество киберпреступлений увеличилось на 120% и достигло своего рекордного значения. Темпы прироста были приостановлены в 2021, 2022 годах, однако, как справедливо отмечают специалисты в сфере информационной безопасности, данное обстоятельство связано с политическими причинами и условиями. В отдельных регионах имеет место снижение количества IT-преступлений (Чеченская Республика), в то же время в других субъектах темпы прироста превышают показатели по России.

Современная преступность в сфере компьютерной информации имеет следующую структуру:

- кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ);

- мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

- мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);
- интернет-вымогательство (ст. 163 УК РФ).

§2. Элементы криминологической характеристики преступлений в сфере компьютерной информации

Важнейшими элементами криминологической характеристики преступлений в сфере компьютерной информации являются их причины и условия. Следует отметить, что преступность в сфере компьютерной информации обусловлена комплексом причин и условий. Это - общие причины и условия преступности, а также отдельные факторы, непосредственно детерминирующие противоправное поведение киберпреступника.

Кратко охарактеризуем общие причины и условия преступности в современной России. Традиционно факторы преступности разделяют на социально-экономические, политические, идеологические, законодательные (правовые), технические и т.д.

Социально-экономические факторы обусловлены негативными процессами, событиями, происходящими в социальной сфере общества, в сфере экономических отношений. К примеру, такое социально-экономическое явление, как безработица, обуславливает имущественную преступность, преступность в сфере незаконного оборота оружия и боеприпасов, наркотических средств и психотропных веществ. Под воздействием указанного фактора формируется корыстная мотивация, вследствие которой и возникает решение осуществить кражу чужого имущества, сбыт оружия или наркотиков.

Политические факторы обусловлены соответствующими событиями, явлениями и процессами, имеющими место в политической сфере общества. Преступность, как правило, обуславливается политической нестабильностью, сменой власти, политического режима, отношениями между центром и субъектами и т.д.

Правовые факторы, в первую очередь, связаны с несовершенством законодательства в той или иной сфере, его несоответствием практике. Что

касается технических условий, то развитие высоких технологий, цифровизация общественной жизни позволяют организовать и совершать преступные деяния бесконтактным способом.

Рассмотрим причины и условия преступлений в сфере компьютерной информации. Как отмечает большинство авторов, ключевым фактором киберпреступлений становится развитие и постоянное совершенствование самого киберпространства. К примеру, если в первом десятилетии XXI века сфера интернет-коммуникаций была представлена социальными сетями (ВКонтакте, Ask), функционирующими преимущественно в различных браузерах (Mozilla Firefox, Opera), а также электронной почтой, то в последующем были разработаны мобильные приложения для обмена мгновенными сообщениями, с функциями аудио и видео-звонков, системой идентификации по биометрическим данным. Иными словами, сфера киберпреступной деятельности существенно расширилась. Одни преступники пользуются традиционными методами (например, взлом оборудования путем направления вирусов на электронную почту), другие реализуют преступные цели в современных мессенджерах (например, рассылка фишинговых ссылок в WhatsApp).

В материалах Главного информационно-аналитического центра МВД России представлены сведения о наиболее распространенных способах и методах совершения киберпреступлений (Рисунок 1.1. Методы и способы совершения киберпреступлений в России в 2024 году).

Метод, способ совершения преступления	**Количество преступлений**	**+,- в %**
расчетные (пластиковые) карты	132849	4,5
компьютерная техника	36385	24,9
программные средства	12175	59,2
фиктивные электронные платежи	1608	21,4
сеть Интернет	526794	38,2
средства мобильной связи	302865	42,2

Рисунок 1.1. Методы и способы совершения киберпреступлений в России в 2024 году

Как видим, значительная часть киберпреступлений совершается посредством сети Интернет. Также распространение получили факты противоправного использования средств мобильной связи и расчетных карт.

Следует обозначить еще один фактор, обуславливающий преступность в сфере компьютерной информации. Современные информационные технологии способствуют анонимизации преступников, что вызывает у последних чувство безнаказанности и мотивирует на совершение противоправных деяний. Анонимность не позволяет правоохранительным органам в полном объеме выявлять и раскрывать преступления, устанавливать всех участников преступных сообществ, так как в таких условиях реальная связь между участниками отсутствует. Согласно мнению П.А. Ивлиева, «получая данные о пользователях, спецслужбы, борющиеся с реальной преступностью, узнают лишь о компьютере или сервере, с которого совершалось преступления или с которого преступник связывался с сообщниками. Но далеко не всегда принадлежность № человеку говорит о том, что этим IP пользуется только владелец. Мы не можем с точностью утверждать, что за каждым конкретным IP скрывается один человек. Тем более, что в цифровом пространстве существуют специальные методы анонимизации через использование поддельного или подставного IP. Для этого используются прокси-сервера, специальные браузеры (к примеру, TOR), расширения для обычных браузеров»[1]

Как было отмечено выше, анонимность лиц, причастных к преступлениям сфере компьютерной информации, оказывает существенное влияние на их раскрываемость. Показатели раскрываемости киберпреступлений за последние 5 лет представлены в виде рисунка (Рисунок 1.2. Раскрываемость киберпреступлений в России в 2020-2024 гг.).

[1] П. А. Ивлиев. Анонимность в интернете: проблемы и особенности. Международный журнал гуманитарных и естественных наук. –2021. – № (4-2). С. 7-10.

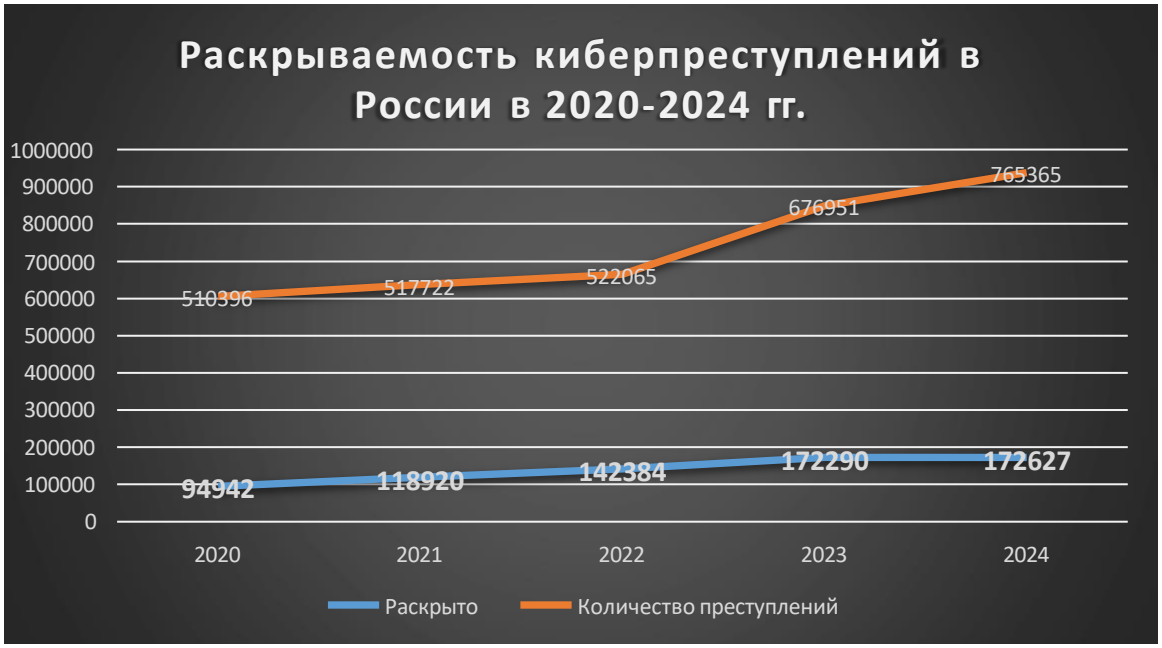

Рисунок 1.2. Раскрываемость киберпреступлений в России в 2020-2024 гг.

Как видим, показатели раскрываемости киберпреступлений за последние 5 лет не составляли более 27 % (2020 – 18%, 2021 – 23%, 2022 – 27%, 2023 – 25%, 2024 – 22%). Дело в том, что механизм раскрытия преступлений в сфере компьютерной информации довольно сложный и требует значительных временных затрат. В условиях ограниченности сил и средств, вызванных кадровыми проблемами, а также проблемами разработки и внедрения в систему правоохранительных органов, в первую очередь органов внутренних дел, новых технологий, рост показателей раскрываемости практически невозможен. В отдельных регионах показатели раскрываемости существенно превышают показатели по России (Рис.1.5. Регионы с наибольшей раскрываемостью киберпреступлений в 2024 году).

Рис.1.5. Регионы с наибольшей раскрываемостью киберпреступлений в 2024 году

Низкий процент раскрываемости зарегистрирован в Смоленской, Тверской, Амурской областях, в Приморском крае, в Республике Хакасия (Рис.1.6. Регионы с наибольшей раскрываемостью киберпреступлений в 2023 году).

Рис.1.6. Регионы с наибольшей раскрываемостью киберпреступлений в 2024 году

Таким образом, преступность в сфере компьютерной информации обусловлена как общими причинами и условиями, детерминирующими

преступность в России, так и конкретными факторами. Развитие киберпространства, цифровизация общественной жизни, а также иные явления и процессы, связанные с информацией и информационными технологиями, порождают преступность в данной сфере.

§3. Личность компьютерного преступника как объект профилактического воздействия

Для предупреждения преступности существенное значение имеет характеристика личности преступника, что влияет на выбор тех или иных методов, способов и средств оказания предупредительного воздействия. Рассмотрим особенности личности преступника, совершающего противоправные деяния в сфере компьютерной информации, то есть, киберпреступника.

Личность преступника является одной из базовых криминологических категорий. В науке криминологии можно встретить следующие определения рассматриваемой категории.

Личность преступника, по мнению И.А. Макаренко, «представляет собой устойчивую криминалогически значимую совокупность психофизиологических свойств и качеств, мотивационных установок эмоциональной и рациональной сфер человеческого сознания, отразившихся в следах преступления в процессе подготовки, совершения и сокрытия следов преступления, а также его постпреступного поведения» [1]

Структура личности преступника, согласно мнению, А.О. Девятовой, «состоит из ряда симптомов, которые в совокупности влияют на совершение проступка. Подструктурами являются:

1. Биофизиологические признаки, составляющие личность преступника, – это физиологическое состояние ее нервной системы, текущее состояние

---

[1] Криминалистика: история и перспективы развития : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. — М. : Издательство Юрайт, 2019. — 167 с.

здоровья и т.д. Этот фактор исследуется в связи с тем, что личностные черты часто определяются генетически.

2. Социально-демографические характеристики. Они включали ряд показателей, таких как возраст, пол, социальное и семейное положение, уровень образования, род занятий, национальные характеристики.

3. Морально-психологические характеристики, которые определяют личность преступника в криминологии, включают в себя черты мировой идентичности, ценностей, убеждений и жизненной ориентации, которая определяется решительностью и настойчивостью в достижении задуманного человека и в целом влияет на совокупность привычек и установок человека. Считается, что человек становится личностью только при формировании собственной системы ценностей и отношения к общественному порядку, а также умение брать на себя ответственность за свои решения и действия сами.

4. Наконец, окончательные характеристики, раскрывающие понятие преступника – его интеллектуальные, эмоциональные и волевые качества»[1].

По мнению А.Г. Савельевой, «основными составляющими структуры личности преступника являются группы, объединяющие ряд элементов:

– социально-демографическая группа (связи, роли, социальный статус и т. д.);

– уголовно-правовая группа (личностный или групповой характер преступного поведения, направление преступного поведения, ранняя преступная деятельность, наказание и признаки его цели и т. д.);

– морально-психологическая группа (психические свойства, психологическая характеристика, моральные ценности и т. д.)»[2].

---

[1] Девятова А.О. Личность преступника: понятие и криминологическая характеристика // Отечественная юриспруденция. – 2019. №7 (32). – С. 75-78.

[2] Савельева, А. Г. Структурные элементы личности преступника как объекта изучения криминологии / А. Г. Савельева // Право. Общество. Государство: Сборник научных трудов студентов и аспирантов / Отв. ред. Е. В. Трофимов. Том 11. – Санкт-Петербург: Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2020. – С. 166-169.

Обобщая вышеназванное, можно сказать, что криминологическая характеристика личности преступника, причастного к преступлениям в сфере компьютерной информации, складывается из таких элементов, как его социальный статус, социальные функции, нравственная и психологическая характеристика личности. Социальный статус, как элемент криминологической характеристики охватывает такие признаки уровень образования преступника, его положение в обществе.

Исследователи отмечают, что согласно статистическим данным, возрастные границы киберпреступников — от 15 до 40 лет, как правило, они имеют техническое образование, либо образование в сфере IT-технологий, либо имеют навыки и опыт общения с компьютерными и иными технологиями. Исследователи акцентируют внимание на нижней границе возраста киберпреступников — ими в некоторых случаях становятся несовершеннолетние в возрасте от 15 лет. Наблюдается преобладание среди них молодого поколения. Это объясняется меньшей «компьютеризацией» старшего поколения, а также тем, что навыки владения компьютером вырабатываются в дошкольном, юном возрасте. Наиболее криминально активными считаются лица в возрасте от 16 до 25 лет и от 26 до 35 лет. В возрасте от 16 до 17 лет совершается большая часть сетевых преступлений, ведь именно в этом возрасте возникает потребность в утверждении себя как личности, самоопределении, а также получении максимального количества материальных благ, не имея реальной возможности добиться этого. Это связано так же с доступностью к высоким технологиям практически всех возрастов, доступностью информации в сфере киберпространства, а также условиями среды воспитания, когда высокие технологии становятся частью обыденной жизни.

Киберпреступники чаще всего имеют следующие психологические характеристики: тип личности, склонный к депрессии, к личностным переживаниям, неврозам, страдают тревожностью и обидчивостью, в ряде случаев обладают завышенным самомнением. Самооценка занижена, совершая преступление «дистанционно» киберпреступник ощущает чувство

превосходства над потерпевшим. Анонимность дает преступнику преимущество и ощущение безнаказанности. Киберпреступник характеризуется нигилистическим отношением к законности, считает возможным устанавливать и руководствоваться собственной моралью и правилами поведения, навязывая это поведении и другим лицам, игнорируют общественные ценности и нормы поведения. Некоторые киберпреступники так же характеризуются инфантильностью, безответственностью, отсутствием понимания последствий своих действий.

Личность киберпреступника является актуальным объектом исследований современных учёных - криминологов. Так, С.А. Григорян под рассматриваемой категорией понимает «совокупность нравственно-психологических, уголовно-правовых и социально-демографических качеств личности, выражающихся в преступном поведении индивида при совершении «киберпреступлений». По мнению автора, «все киберпреступники делятся на два типа:

- обычные «киберпреступники», совершающие противоправные действия отдельных видов преступной деятельности (мошеннические действия, наркоторговля посредством сети-Интернет и т.д.);

- преступники в среде компьютерной информации и технологий, которые могу совершать противоправную деятельность только в киберпространстве (например, несанкционированный доступ к компьютерной информации и ресурсам и т.д.)»[1].

Н.С. Зориной определены два вида личности киберпреступников. К первому типу относятся традиционные киберпреступники, которые совершают традиционные преступления, такие как мошенничество и вымогательство, где используются общедоступные ресурсы и возможности (таких, как электронная почта или социальные сети).

---

[1] Григорян, С. А. Особенности личности современного «киберпреступника»/ С. А. Григорян // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2022. – № 8(147). – С. 103-106.

Второй тип – хакеры, которые совершают экономические киберпреступления в сфере компьютерной информации, такие как незаконный сбор сведений, составляющих коммерческую, налоговую либо банковскую тайну, где присутствует неправомерный доступ к компьютерной информации, либо используются вредоносные программы[1].

Согласно мнению В.В. Бабурина, «киберпреступник — это человек с высоким уровнем компьютерной грамотности и знаний в области информационных технологий, который использует данные навыки для совершения преступлений». Автор, исходя из структуры киберпреступности, выделяет следующие типы личности киберпреступников: кибермошенник; кибервор; киберпреступник в сфере компьютерной информации; в сфере распространения наркотических и иных запрещенных законом веществ; кибертеррорист; киберэкстремист; киберпреступник, распространяющий порнографические материалы[2].

Более узкий подход к определению типов личности киберпреступников характерен для исследований Н.С. Севера. По мнению автора, «обычно киберпреступников можно разделить на лиц, несанкционированно получающих доступ к охраняемой законом информации (ст. 272 УК РФ), и на лиц, использующих вредоносное ПО как специфическую разновидность компьютерной информации для реализации собственных преступных устремлений (ст. 273 УК РФ). Отдельно в данном случае выделяются лица, совершающие преступления при нарушении правил эксплуатации систем хранения и обработки информации (ст. 274 УК РФ) и в процессе нарушений

---

[1] Зорина Н. С. К вопросу о личности киберпреступника и его жертве в сфере компьютерной информации и информационных технологий / Н. С. Зорина // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». – 2022. – № 25. – С. 92-96.

[2] Бабурин В. В. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан / В. В. Бабурин, К. О. Карабеков // Психопедагогика в правоохранительных органах. – 2024. – Т. 29, № 1(96). – С. 113-119.

режима охраны критической информационной инфраструктуры (ст. 274.1 УК РФ)»[1].

В исследованиях Ю.В. Белевитиной типология киберпреступников также разработана исходя из анализа положений статей 272-274.2 УК РФ. Автором определены следующие типы личности преступников в сфере компьютерной информации:

- лица, владеющие высочайшими познаниями в данной специфической области, специализирующиеся на совершении специальных киберпреступлений (субкультура «хакер»);

– лица, имеющие готовый алгоритм совершения преступных действий, слабо разбирающийся в деталях и процессах, происходящий в информационных системах, совершающие при помощи электронных устройств «неспецифические» для киберпространства деяния (мошенничество, кражи, отмывание денежных средств, и т.д.);

– лица, ранее совершавшие преступления, «переквалифицировавшиеся» в киберпреступников из-за широких возможностей киберпространства, а также представители организованной преступности, способные объединить лиц, имеющие специальные знания для совершения преступлений, направляющие основные усилия на максимальное извлечение выгоды[2].

Нередко к преступлениям в сфере компьютерной информации имеют причастность организованные группы. Организованный характер носят мошеннические действия, совершаемые путем применения информационно-телекоммуникационных технологий, и сопровождаемые неправомерным доступом к компьютерной информации.

Классическая организованная группа состоит из следующих участников:

---

[1] Север Н. С. Особенности криминологической характеристики личности киберпреступников / Н. С. Север // Вестник Волгоградского государственного университета. Серия 9: Исследования молодых ученых. – 2022. – № 20. – С. 108-110.

[2] Белевитина, Ю. В. Криминологический портрет личности киберпреступника в современной России / Ю. В. Белевитина // Инновационная наука. – 2022. – № 12-2. – С. 61-64.

1) организатор, который осуществляет руководство преступной деятельностью, занимается подбором иных участников, распределяет полученные преступные доходы и т.д.;

2) исполнитель – осуществляет неправомерный доступ к компьютерной информации, содержащейся на технических устройствах организации, откуда по указанию организатора выводит имеющиеся денежные средства на банковские карты, Киви-кошельки и т.д.;

3) лицо, осуществляющее подбор абонентских номеров, банковских карт, на которые перечисляются денежные средства.

Научный и практический интерес представляет третья категория участников организованной преступной деятельности в сфере компьютерной информации – лица, осуществляющие подбор абонентских номеров, банковских карт, на которые перечисляются денежные средства. Действующие сотрудники правоохранительных органов, а также специалисты в области IT-технологий обозначают таких лиц как «дроповоды». Соответственно, лица, которые предоставляют абонентские номера, банковские карты называются «дропами»[1].

Специалисты выделяют следующие разновидности дропов:

- разводной дроп — используется втемную. Человека обманом заставляют участвовать в схеме, присылать сканы документов, получать или отправлять товар, снимать наличные, передавать данные карты и т. д.;

- неразводной дроп — понимает, что ему предстоит делать, и осознанно идет на сотрудничество с дроповодом за вознаграждение[2].

Дроповоды обладают следующими характеристиками:

---

[1] Алымов Д.А., Криминалистическая характеристика типовых следов преступника, осуществляющего криминальную деятельность в виртуальном пространстве (на примере дроповодов). Вестник Томского государственного университета. – 2024. – № (506). – С. 185-192.

[2] Дроповоды: кто скрывается за украденными личностями - [Электронный ресурс] // Рейтинг партнерских программ, партнерок URL: https://partnerkin.com/blog/stati/dropovody_kto_skryvaetsya_za_u (дата обращения: 16.12.2024).

- в своей преступной деятельности используют зашифрованные мессенджеры, VPN, TOR (анонимный браузер) и другие средства для поддержания анонимности;

- для затруднения отслеживания применяют запутанные и нестандартные маршруты сетевых операций;

- реализуют психологические методы для обмана участников транзакций и кражи данных;

- стараются не оставлять следов, не называют дропам своего настоящего имени, используют анонимные номера телефонов.

С нравственно-психологической точки зрения, для указанной группы преступников характерны такие свойства, как высокий уровень цинизма, сильно выраженная корыстная мотивация, желание самоутвердиться.

Рассмотрим пример из практики. Так, гражданин З. находился в федеральном розыске и скрывался в городе С. В связи с нахождением в розыске, З. не имел легального источника дохода, поэтому решил заняться преступной деятельностью, а именно мошенничеством в сфере компьютерной информации, что также сопровождалось неправомерным доступ к компьютерной информации, содержащейся в компьютерных системах организаций «Х» и «А».

В целях осуществления преступной деятельности, З. посредством сети Интернет изучил возможность хищения хранящихся на счетах безналичных денежных средств, путём неправомерного доступа к охраняемой законом компьютерной информации посредством сети Интернет. Также З. был осведомлен о необходимости для совершения хищения наличия у похитителей большого количества банковских счетов и карт, а также сим-карт операторов связи, оформленных на лиц, достоверно неосведомленных об использовании их счетов и карт в преступных целях (далее подставных лиц), скорейшего вывода безналичных денежных средств с подконтрольных счетов, на которые они перечислены непосредственно при хищении, на другие подконтрольные счета и скорейшего их обналичивания во избежание отмены или блокирования операций при обнаружении хищения.

З. не владел техническими навыками, позволяющими осуществить неправомерный доступ к компьютерной информации, поэтому посредством мессенджера «Jabber» преступил в преступный сговор неустановленным лицом. Данное лицо выполняло функции, связанные с получением неправомерного доступа к компьютерной информации, принадлежащей организациям «Х» и «А». Согласно материалам уголовного дела, неустановленное лицо осуществило несанкционированную загрузку и установку программного обеспечения в персональные компьютеры организации «Х», в результате чего получен удаленный доступ, в том числе возможность получать снимки содержимого рабочего стола ПК, воспроизводить нажатие клавиш клавиатуры и движение указателя, а также удаленно управлять ПК «Х», повлекший модификацию и копирование компьютерной информации из корыстной заинтересованности. Далее, неустановленное лицо установило в ПК «Х» программное обеспечение «qiwicashier.exe», что позволило управлять (администрировать) счетом организации «Х» в платежной системе «QIWI» КИВИ Банк (АО) и беспрепятственно производить транзакции находящихся на указанном счете денежных средств.

Денежные средства организации «Х» зачислялись на «QIWI-кошельки», которые были зарегистрированы на абонентские номера лиц, не осведомленных о преступной деятельности. Подбор абонентских номеров осуществлял гражданин Б., который также был вовлечен в организованную группу. Обналичивание похищенных денег также отнесено к функциям Б[1].

В настоящее время государственном принимаются меры, направленные на противодействие деятельности дропов. Так, в целях борьбы с вовлечением подростков в преступные дропперские схемы Банком России инициирована мера, в соответствии с которой родители или законные представители будут получать уведомления о выдаче карт их детям и обо всех операциях по ним.

---

[1] Приговор Первомайского районного суда г. Краснодара от 19.07.2018 по делу № 1-50/2018 - [Электронный ресурс]. – URL: https://судебныерешения.рф/35324463/extended (дата обращения: 17.12.2024).

Нововведение коснется подростков от 14 до 18 лет. Способ информирования взрослых о финансовых операциях по счету несовершеннолетнего банк укажет в договоре[1].

Следующая мера – установление лимита по переводам. Согласно сведениям, представленным Центральным Банком, данные по дропперам попадают в базу Банка России о мошеннических операциях, эти сведения доступны всем банкам и правоохранителям. Сама база формируется на основе сведений банков о случаях и попытках мошенничества (это финансовые операции, по которым клиенты банка заявили о своем несогласии). Если сведения о клиенте попадают в базу данных ЦБ, то банк может приостановить ему действие карты или услуги онлайн-банкинга. Если банк этого не сделал, с 15 мая 2025 года для такого человека вводится лимит - он не сможет переводить себе или другим людям больше 100 тыс. руб. в месяц. При этом, если сведения о противоправных действиях человека поступают в базу данных от правоохранительных органов, банк обязан заблокировать человеку карты и доступ к онлайн-банку[2].

Ключевой мерой в борьбе с дропами может стать принятие законопроекта № 909076-8 «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» (об уточнении ответственности за неправомерный оборот электронных средств платежа). Проект предусматривает ответственность за передачу из корыстной заинтересованности клиентом оператора по переводу денежных средств предоставленного ему оператором по переводу денежных средств электронного средства платежа и (или) доступа к нему другому лицу для осуществления таким лицом неправомерных операций[3].

---

[1] Банки начнут сообщать родителям о платежах и переводах детей - [Электронный ресурс] // Российская газета URL: https://rg.ru/2025/03/29/banki-nachnut-soobshchat-roditeliam-o-platezhah-i-perevodah-detej.html (дата обращения: 17.12.2024).

[2] Не более 100 тысяч в месяц: как будет работать новый закон для борьбы с дропперами - [Электронный ресурс] // Российская газета URL: https://rg.ru/2025/05/14/ne-prinimajte-na-svoj-schet.html (дата обращения: 17.12.2024).

[3] Законопроект № 909076-8 «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» (об уточнении ответственности за неправомерный оборот электронных средств платежа) - [Электронный ресурс] // Система обеспечения

Исследования, проведенные в рамках настоящей главы, позволяют сделать следующие выводы.

Преступность в сфере компьютерной информации представляет собой систему уголовно-наказуемых деяний, включенных в Главу 28 УК РФ, а также ряд иных преступлений, совершаемых в цифровом, то есть, киберпространстве: кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);интернет-вымогательство (ст. 163 УК РФ).

Что касается состояния и тенденции преступности в сфере компьютерной информации, то за последние 5 лет количество киберпреступлений увеличилось на 149% и достигло своего рекордного значения. Темпы прироста были приостановлены в 2021, 2022 годах, однако, как справедливо отмечают специалисты в сфере информационной безопасности, данное обстоятельство связано с политическими причинами и условиями. В отдельных регионах имеет место снижение количества IT-преступлений, в то же время в других субъектах темпы прироста превышают показатели по России. Рост количества преступлений в сфере компьютерной информации обусловлен как общими причинами и условиями, детерминирующими преступность в России, так и конкретными факторами. Развитие киберпространства, цифровизация общественной жизни, а также иные явления и процессы, связанные с информацией и информационными технологиями, порождают преступность в данной сфере.

Что касается личности преступника, то обобщенный портрет лица, совершившего киберпреступления, можно описать следующим образом:

- лицо возрасте до 30 лет, в большинстве случаев имеющее профессиональное образование в области информационных технологий, либо соответствующие навыки, ранее не судимое, преимущественно мужского пола.

законодательной деятельности URL: https://sozd.duma.gov.ru/bill/909076-8 (дата обращения: 17.12.2024).

Черты личности характеризуются правовым нигилизмом, нежеланием жить по правилам, установленным обществом, руководство корыстными, хулиганскими или иными мотивами, испытывают чувство безнаказанности и превосходства в связи с обезличенностью персоны в киберпространстве.

Преступления в сфере компьютерной информации, как правило, носят организованный характер. Преступная цель достигается посредством усилий следующих категорий лиц: организатор, хакер, дроповод, дроп.

ГЛАВА 2. Деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации.

§1. Правовые основы предупреждения ОВД РФ преступлений в сфере компьютерной информации

Деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации основана на нормативно-правовых актах общего характера, посвященных вопросам противодействия преступности в целом, а также специальных нормативно-правовых актах, нормы которых регламентируют предупреждение киберпреступлений и иных правонарушений в цифровом пространстве.

Правовая и организационная основы системы профилактики правонарушений, общие правила ее функционирования, основные принципы, направления, виды профилактики правонарушений и формы профилактического воздействия, полномочия, права и обязанности субъектов профилактики правонарушений и лиц, участвующих в профилактике правонарушений определены Федеральным законом от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»[1]. Несмотря на то, что ряд уголовно-наказуемых деяний совершается посредством информационно-телекоммуникационных технологий, в том числе и путем оказания противоправного воздействия на цифровую инфраструктуру, понятия киберпреступления, кибербезопасность, а также схожие по смыслу и содержанию категории не нашли отражения в исследуемом нормативно-правовом акте. Так, в качестве самостоятельных направлений профилактики законодатель выделяет противодействие терроризму, экстремистской деятельности, незаконному обороту наркотиков, незаконной миграции,

[1] Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23 июня 2016 г. № 182-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 18.12.2024).

коррупции. Объектами, которым должно быть уделено отдельное внимание при профилактике правонарушений, выступают безопасность дорожного движения, пожарная безопасность, экологическая безопасность, безнадзорность и беспризорность несовершеннолетних.

Полагаем, что законодательство в сфере профилактики и предупреждения преступлений должно соответствовать наиболее актуальным тенденциям, характерным для преступности. В связи с вышеизложенным, считаем необходимым дополнить часть 1 статьи 6 Закона «Об основах системы профилактики правонарушений в Российской Федерации» новым пунктом и изложить её в следующей редакции:

Статья 6. Основные направления профилактики правонарушений

1. Профилактика правонарушений осуществляется по следующим основным направлениям:

1) защита личности, общества и государства от противоправных посягательств;

17. противодействие преступления и иным правонарушениям, совершаемым посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации, обеспечение защищенности граждан, общества и государства от противоправных деяний, совершаемых посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации.

В статье 7 Закона № 182 - ФЗ закреплено положение, в соответствии с которым федеральные органы исполнительной власти и органы государственной власти субъектов Российской Федерации в целях реализации государственной политики в сфере профилактики правонарушений в соответствии с требованиями бюджетного законодательства Российской Федерации и законодательства Российской Федерации в сфере стратегического планирования разрабатывают государственные программы Российской Федерации в сфере профилактики правонарушений и государственные

программы субъектов Российской Федерации в сфере профилактики правонарушений соответственно.

Противодействие преступности на территории Республики Татарстан, помимо законов РФ и подзаконных актов, осуществляется в соответствии с Постановлением Кабинета Министров Республики Татарстан от 16 октября 2013 года № 764 «Об утверждении государственной программы Республики Татарстан «Обеспечение общественного порядка и противодействие преступности»[1]. Структура и содержание данной Программы соответствует государственной программе, утвержденной Правительством РФ, за исключением анализа и оценки криминогенной обстановки.

Что касается правовых актов, непосредственно регламентирующих вопросы предупреждения преступлений в сфере компьютерной информации, то в Законе № 182-ФЗ упомянут Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[2]. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. При определении основных информационных угроз, в Доктрине акцентируется внимание на возрастании масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличении числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий.

---

[1] Об утверждении государственной программы Республики Татарстан «Обеспечение общественного порядка и противодействие преступности»: Постановление Кабинета Министров Республики Татарстан от 16 октября 2013 № 764 «Сборник постановлений и распоряжений Кабинета Министров Республики Татарстан и нормативных актов республиканских органов исполнительной власти», 22.10.2013, N 78, ст. 2624.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации, N 50, 12.12.2016, ст.7074

Помимо вышеизложенного, отмечается высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

В конце 2024 года Правительством РФ утверждена Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий[1]. В Концепции определены принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение ее создания и функционирования, а также закреплено

[1] Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: Распоряжение Правительства РФ от 30.12.2024 N 4154-р - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 05.01.2025).

определение понятия «противоправные деяния, совершенные с использованием информационно-коммуникационных технологий»:

- общественно опасные деяния, за которые предусмотрена уголовная либо административная ответственность, совершенные с использованием (применением) информационно-коммуникационных технологий или в сфере компьютерной информации, в том числе с использованием (применением) электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет", информационной инфраструктуры, компьютерной техники, программных средств, онлайн-сервисов, средств коммуникации (в том числе средств мобильной связи, сервисов обмена мгновенными сообщениями, IP-телефонии), электронных средств платежа, операций с цифровой валютой и цифровыми финансовыми активами.

Основные функции государственной системы противодействия киберпреступлениям заключаются в следующем:

- создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком Российской Федерации, кредитными организациями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети "Интернет" и иных информационных технологий;

- принятие на региональном и муниципальном уровнях соответствующих целевых программ, предусматривающих формирование системы профилактики правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий;

- организация и проведение научно-исследовательских и опытно-конструкторских работ по разработке и применению криминалистических средств и методов выявления, раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также сбора доказательств;

- повышение уровня материального и технического оснащения федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих функции по выработке и реализации государственной политики в сфере противодействия противоправным деяниям, а также уровня правовой и социальной защищенности их сотрудников, включая обеспечение правовой защиты сотрудников правоохранительных и следственных органов и т.д.

Концепция разработана в соответствии с положениями Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ[1]. Данный нормативно-правовой акт, не является прямой правовой основой предупреждения киберпреступности, но содержит положения, которые могут способствовать этому:

- установка основных правил и способов защиты прав на информацию, защиты самой информации путём принятия основных правовых, организационных и технических (программно-технических) мер по её защите;

-запрет на требование от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и на получение такой информации помимо воли гражданина. Исключение могут составлять только случаи, прямо предусмотренные федеральными законами.

На основании вышеизложенного можно сделать следующие выводы.

Правовая основа деятельности ОВД РФ по предупреждению компьютерной преступности складывается:

1. Из нормативно-правовых актов общего характера:

- Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации»;

- Федеральный закон «О полиции»;

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 07.01.2025).

- Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации»;

- Приказ МВД России «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений»;

- нормативно-правовые акты, утверждающие программы по предупреждению преступности на федеральном, региональном и местном уровнях.

2. Из специальных нормативно-правовых актов:

- Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

- Распоряжение Правительства РФ от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий».

§2. Организационные основы предупреждения ОВД РФ преступлений в сфере компьютерной информации

Организация деятельности ОВД РФ по предупреждению преступлений в сфере компьютерной информации представляет собой комплекс мероприятий, направленных на создание необходимых условий для реализации данной цели. Одним из элементов организации является создание служб и подразделений органов внутренних дел и наделение их полномочиями по предупреждению компьютерных преступлений. Ключевая роль в предупреждении преступности принадлежит оперативным подразделениям органов внутренних дел. На протяжении нескольких десятилетий существенный вклад в предупреждение преступлений на территории Российской Федерации вносят подразделения уголовного розыска, осуществляющие оперативно-розыскное противодействие

преступлениям общеуголовной направленности, в том числе преступным посягательствам, совершаемым в сфере компьютерной информации – кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) путем выявления лиц, причастных к ним, и принятием мер, направленных на задержание фигурантов.

Так, оперативными сотрудниками Управления уголовного розыска МВД по Республике Татарстан совместно с сотрудниками УМВД России по г. Казани задержан молодой человек, который выполнял функции курьера преступной организации, специализирующейся на дистанционном мошенничестве. Задержанный пояснил, что осенью 2024 года искал работу и в мессенджере «Telegram» обнаружил объявление о работе и связался с «работодателем». Суть работы заключалась в следующем. Фигурант должен был забирать денежные средства у обманутых граждан и перечислять их на соответствующие банковские счета. Вознаграждение за преступную деятельность составлять 10% от полученной суммы[1]. Следует отметить, что лица-организаторы данной преступной деятельности ввиду ряда объективных причин не были установлены.

Распространение киберпреступности стало причиной принятия в 2022 году организационно-управленческого решения в виде создания в системе органов внутренних дел подразделений по борьбе с киберпреступностью. Приказом МВД России от 29 декабря 2022 г. № 1110 утверждено Положение об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации[2]. В соответствии с указанным нормативно-правовым актом,

---

[1] Сотрудники уголовного розыска МВД по Республике Татарстан задержали курьера мошенников - [Электронный ресурс] // Официальный сайт МВД по Республике Татарстан URL: https://16.мвд.рф/news/item/57929558/ (дата обращения: 11.01.2025).

[2] Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: Приказ МВД России от 29 декабря 2022 г. № 1110 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 12.01.2025).

Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России) является самостоятельным структурным подразделением центрального аппарата Министерства внутренних дел Российской Федерации, обеспечивающим и осуществляющим в пределах компетенции функции Министерства по выработке и реализации государственной политики и нормативно-правовому регулированию в области организации противодействия противоправным деяниям, совершаемым с использованием (в сфере) информационно-коммуникационных технологий.

В территориальных органах внутренних дел на уровне субъектов функционируют отделы по борьбе с противоправным использованием информационно-коммуникационных технологий (ОБК), деятельность которых регламентирована Приказом МВД России от 14.02.2023 № 71 «Об утверждении Типового положения о подразделении по борьбе с противоправным использованием информационно-коммуникационных технологий территориального органа Министерства внутренних дел Российской Федерации на региональном уровне»[1].

Ведомственным нормативно-правовым актом установлены задачи подразделений по борьбе с киберпреступлениями:

1) выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе связанных с организованными формами преступности, выявление и установление лиц, их подготавливающих, совершающих или совершивших;

2) осуществление системного анализа криминалистически значимой информации в установленной сфере деятельности;

---

[1] Об утверждении Типового положения о подразделении по борьбе с противоправным использованием информационно-коммуникационных технологий территориального органа Министерства внутренних дел Российской Федерации на региональном уровне: Приказ МВД России от 14.02.2023 № 71 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 13.01.2025).

3) обеспечение взаимодействия структурных подразделений территориального органа МВД России с органами исполнительной власти и участниками информационного обмена субъекта Российской Федерации в установленной сфере деятельности;

4) координация по поручению руководителя (начальника) территориального органа МВД России деятельности оперативных подразделений территориального органа МВД России в установленной сфере деятельности.

5) противодействие распространению в информационно-телекоммуникационной сети Интернет информации, создающей угрозу причинения вреда жизни, здоровью и имуществу граждан.

Деятельность подразделений по борьбе с киберпреступлениями носит разносторонний характер. Об этом свидетельствует перечень задач, определенных в Приказе МВД России от 14.02.2023 № 71. Задачи ОБК могут быть распределены по следующим группам.

Во-первых, задачи, связанные с осуществлением оперативно-розыскной деятельности.

1. Выявление, предупреждение, пресечение и раскрытие преступлений:

- связанных с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных компьютерных программ, нарушением правил эксплуатации информационно-телекоммуникационных сетей и средств хранения, обработки или передачи компьютерной информации, нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования;

- связанных с нарушением неприкосновенности частной жизни, тайны переписки и сообщений, передаваемых по сетям электрической связи,

посредством неправомерного доступа к компьютерной информации и (или) использования вредоносного программного обеспечения;

- связанных с нарушением авторских и смежных прав, совершенных по совокупности с неправомерным доступом к компьютерной информации и (или) использованием вредоносного программного обеспечения;

- против собственности и в сфере экономической деятельности, совершенных по совокупности с неправомерным доступом к компьютерной информации и (или) использованием вредоносного программного обеспечения;

- против жизни и здоровья, половой неприкосновенности и половой свободы, а также семьи и несовершеннолетних, связанных с использованием и распространением запрещенной информации в информационно-телекоммуникационных сетях, включая сеть Интернет.

2. Выявление и пресечение деятельности транснациональных, межрегиональных организованных групп и преступных сообществ (преступных организаций), совершающих преступления с использованием (в сфере) информационно-коммуникационных технологий.

3. Проведение оперативно-розыскных мероприятий по поступившим обращениям и иной информации о подготавливаемых, совершаемых или совершенных преступлениях, а также заявлениям и сообщениям о преступлениях, об административных правонарушениях, о происшествиях в установленной сфере деятельности.

4. Осуществление в пределах компетенции оперативного сопровождения уголовных дел, участие в проведении следственных действий, в том числе по поручениям следователя и дознавателя.

5. Осуществление в информационно-телекоммуникационной сети Интернет поисковых мероприятий, направленных на выявление угроз информационной безопасности граждан, общества и государства, в том числе информации, распространение которой в Российской Федерации запрещено.

6. Участие в установленном порядке в проведении мероприятий по получению доступа, съема и фиксации информации, содержащейся на

электронных носителях и в информационно-телекоммуникационных сетях, в рамках имеющихся технических возможностей.Во-вторых, задачи аналитического характера.

1. Мониторинг и анализ оперативной обстановки на территории субъекта Российской Федерации, разработка мер по оперативному реагированию на ее изменение в установленной сфере деятельности.

2. Анализ административной практики и непосредственное осуществление в пределах своих полномочий производства по делам об административных правонарушениях в соответствии с законодательством Российской Федерации.

3. Сбор, обобщение и анализ информационно-справочных материалов в области современных информационно-коммуникационных технологий, которые могут быть использованы в оперативно-служебной деятельности подразделения.

Изучение программных продуктов, информационно-телекоммуникационных сетей, мобильных и компьютерных устройств в рамках материалов оперативно-розыскной деятельности подразделения.

5. Осуществление в пределах компетенции сбора, хранения, обработки, анализа и учета данных, в том числе оперативно-розыскной информации и электронно-цифровых следов преступлений, полученных в результате оперативно-служебной деятельности подразделения.

6. Предоставление в установленном порядке сведений, необходимых для формирования ведомственной и государственной статистической отчетности.

В-третьих, задачи организационно-координационного характера.

1. Осуществление взаимодействия с региональными операторами связи, организациями, оказывающими услуги в области информационных коммуникаций и в кредитно-финансовой сфере, с другими участниками обмена информацией по вопросам предоставления сведений о пользователях их услугами (оказанных им услуг), а также иных сведений при осуществлении оперативно-розыскной деятельности.

2. Координация работы по организации взаимодействия оперативных подразделений территориального органа МВД России с органами

исполнительной власти субъекта Российской Федерации в установленной сфере деятельности.

3. Организация и участие в проведении комплексных оперативно-профилактических операций, оперативно-профилактических мероприятий в установленной сфере деятельности.

К субъектам предупреждения преступлений в сфере компьютерной информации, помимо оперативных подразделений, относятся службы и подразделения, деятельность которых не связана с осуществлением оперативно-розыскной деятельности. Таковым является служба участковых уполномоченных полиции. Если предупредительная деятельность оперативных подразделений преимущественно связана с выявлением лиц, причастных к преступлениям, и принятием мер, направленных на их задержание, то службы участковых уполномоченных полиции преследуют цель в виде оказания профилактического воздействия на граждан-потенциальных жертв преступлений в сфере компьютерной информации. В соответствии с Приказом МВД России от 29.03.2019 № 205 «О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности» участковый уполномоченный полиции при несении службы на обслуживаемом административном участке принимает меры, направленные на предупреждение и пресечение преступлений и иных правонарушений[1].

Задачи по недопущению совершения в отношении граждан компьютерных преступлений реализуются в рамках профилактического обхода административного участка путем проведения информационно-разъяснительной работы среди жителей. Согласно мнению В.Ю. Белицкого, «разъяснительные беседы с населением участковому уполномоченному необходимо проводить с

---

[1] О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности: Приказ МВД России от 29.03.2019 № 205 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 13.01.2025).

учетом персонифицированных свойств и качеств личности, обратив внимание на то, что высока вероятность стать жертвой мошенников следующих категорий граждан:

1) молодежи, а равно иных лиц с недостаточным уровнем образования, культуры и правосознания, которые не имеют постоянного места работы, но желают получать доход без должных и необходимых трудовых затрат;

2) лиц старшего и пожилого возраста, не владеющих знаниями как современных информационно-телекоммуникационных технологий, так и недостаточно ориентирующихся в быстроменяющихся социальных условиях;

3) жадных, стремящихся к личному обогащению людей;

4) доверчивых, наивных, податливых, склонных к внушению людей, а равно иных категорий граждан, у которых отсутствует или недостаточно развита критичность мышления»[1].

Сущность информационно-разъяснительной работы заключается в доведении до граждан информации о наиболее актуальных способах и методах совершения преступлений в сфере компьютерной информации. Полагаем, что в текущих условиях, связанных с ограниченностью сил и средств службы участковых уполномоченных полиции, традиционный профилактический обход (общение с каждым из жителей домов, расположенных на административном участке) не является эффективным. Наиболее рациональный способ предотвращения мошенничеств – создание в мессенджерах, в частности, в WhatsApp, соответствующей беседы с жителями дома и участкового уполномоченного полиции, в котором участковый будет распространять информацию о наиболее распространенных способах совершения киберпреступлений. О фактах поступления подозрительных звонков жители будут уведомлять участкового, иных жителей дома в беседе. Тем самым,

[1] Белицкий, В. Ю. Предупреждение совершения мошенничеств участковым уполномоченным полиции / В. Ю. Белицкий // Вестник Барнаульского юридического института МВД России. – 2017. – № 2(33). – С. 132-133.

создаются условия для организации взаимодействия участкового уполномоченного полиции с жителями административного участка.

Помимо органов внутренних дел, в системе предупреждения преступлений в сфере компьютерной информации присутствуют иные органы, взаимодействие с которыми является одним из элементов организации деятельности по предупреждению рассматриваемой разновидности преступлений. К числу таких органов следует отнести Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Роскомнадзор предоставляет сведения о месте нахождения и персональных данных лица, на чьё имя зарегистрирован домен в сети Интернет, используемый в целях совершения преступлений в сфере компьютерной информации. Также Роскомнадзор вправе заблокировать сайты по требованию правоохранительных служб, в том числе и органов внутренних дел, если на них содержится информация, противоречащая законодательству РФ.

Существенным условием для предупреждения компьютерных преступлений является организация взаимодействия ОВД РФ с банковскими организациями в лице Банка России. Так, с 2023 года осуществляется онлайн - обмен информацией между Банком России и МВД. Сотрудники полиции в рамках проверки сообщения о преступлении и производства предварительного расследования по уголовным делам о преступлениях в сфере компьютерной информации, могут оперативно получать данные о финансовых операциях из автоматизированной системы Банка России ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности). Согласие клиента для этого не потребуется. На базе ФинЦЕРТ создана система информационного обмена между участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере

информационной безопасности. В информационном обмене с системой участвуют более 1000 организаций, включая все российские банки[1].

К элементам организации предупреждения преступлений в сфере компьютерной информации, исходя из положений Приказа МВД России от 24 августа 2023 г. № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений», относится осуществление в установленном порядке комплексного анализа оперативной обстановки на соответствующей территории и объектах, результатах работы, выявление и прогнозирование тенденций и отклонений, выработка на этой основе своевременных, обоснованных и оптимальных управленческих решений. Информационно-аналитическую работу в системе органов внутренних дел выполняют специально созданные подразделения. Они входят в структуру Федерального казённого учреждения «Главный информационно-аналитический центр МВД России» (ФКУ «ГИАЦ МВД России»).

Функции по осуществлению информационно-аналитической деятельности также выполняют организационно-аналитические (штабные) аппараты органов внутренних дел на окружном, региональном и районном уровнях.

На основании вышеизложенного можно сделать следующие выводы. Организация деятельности ОВД РФ по предупреждению преступлений в сфере компьютерной информации представляет собой комплекс мероприятий, направленных на создание необходимых условий для реализации данной цели.

К организационным элементам относятся: создание и обеспечение деятельности служб и подразделений, к полномочиям которых отнесена реализация мер по пресечению, предотвращению и профилактике преступлений киберпреступлений; организация взаимодействия ОВД РФ с иными субъектами системы профилактики преступлений в сфере компьютерной информации;

---

[1] С 21 октября текущего года Банк России и МВД России начнут онлайн-обмен информацией для противодействия кибермошенникам - [Электронный ресурс] // Новости: ГАРАНТ.РУ URL: https://www.garant.ru/news/1653676/ (дата обращения: 17.01.2025).

осуществление комплексного анализа оперативной обстановки на соответствующей территории и объектах, результатах работы, выявление и прогнозирование тенденций и отклонений, выработка на этой основе своевременных, обоснованных и оптимальных управленческих решений.

§3. Проблемы предупреждения преступлений в сфере компьютерной информации и пути их решения

Рассмотрим проблемные аспекты реализации задач, связанных с предупреждением преступлений в сфере компьютерной информации, и определим пути их решения.

Часть проблем носит организационный характер. Как было отмечено ранее, базовым элементом системы обеспечения общественного порядка и противодействия преступности, в том числе и преступлениям в сфере компьютерной информации, является полиция. К сожалению, организация деятельности современной российской полиции по противодействию преступности далека от совершенства. Ключевая проблема на данный момент, которая систематически обсуждается на уровне государственных органов – кадровый дефицит в полиции. Если министр внутренних дел РФ В.А. Колокольцев в 2023 году заявил о некомплекте в 100 тыс. сотрудников[1], то в ноябре текущего года данный показатель составил 173 тыс. или около 20% всего личного состава[2]. Об аналогичной проблеме заявляют руководители территориальных подразделений. Например, к началу 2024 года в МВД по Татарстану недоукомплектованность сотрудниками превышала 17%. Данные

---

[1] «Скоро останетесь одни в своих креслах»: МВД не хватает 100 тысяч сотрудников - [Электронный ресурс] // Газета.Ru URL: https://www.gazeta.ru/social/2023/10/11/17718175 (дата обращения: 17.01.2025).

[2] Нехватка сотрудников МВД достигла почти 20% - [Электронный ресурс] // РБК URL: https://www.rbc.ru/society/26/11/2024/6745d1979a794754b06006c5 (дата обращения: 18.01.2025).

о нехватке кадров в ведомстве раскрыл на заседании Госсовета РТ временно исполняющий обязанности главы МВД по РТ Алексей Соколов[1].

Помимо количественных, некомплект имеет и качественный характер. Дело в том, что в процессе решения задач, связанных с кадровым обеспечением, система органов внутренних дел пополняется сотрудниками с относительно невысокой квалификацией. Предупреждение преступлений в сфере компьютерной информации требует от действующих сотрудников знаний и в области юриспруденции, и в области информационной безопасности. То есть, обязательным условием для эффективного противодействия криминальным явлениям в сфере компьютерной информации выступает наличие «универсальных» сотрудников, которые, помимо знания норм уголовного, уголовно-процессуального, оперативно-розыскного и иного законодательства, владеют техническими знаниями, умениями и навыками по выявлению кибепреступников, установлению их местонахождения, а также недопущению осуществления ими преступной деятельности (например, блокировка действий, направленных на хищение денежных средств) и т.д. Наличие в системе органов внутренних дел представителей IT-профессий – залог разработки новых и совершенствования имеющихся методов и способов предупреждению преступлений в сфере компьютерной информации.

В связи с чем современная российская полиция испытывает острую нехватку в сотрудниках? К основным причинам кадрового дефицита, как количественного, так и качественного, относят факторы социально-экономического характера. Путем личного общения с действующими и бывшими сотрудниками ОВД, а также посредством анализа форумов и сообществ, связанных с деятельностью полиции, функционирующих в социальных сетях и мессенджерах, установлено, что большая часть полицейских принимает решение об увольнении из службы в связи с отсутствием должного

[1] «Некомплект» в МВД по РТ превысил 17%: «Тема заезжена…» - [Электронный ресурс] // БИЗНЕС Online — Новости Казани URL: https://www.business-gazeta.ru/news/623284 (дата обращения: 18.01.2025).

уровня материального обеспечения и устраивается на работу в сферу услуг (такси, доставка), где заработная плата существенно превышает размер материального вознаграждения сотрудника ОВД. Немаловажными факторам также являются снижение престижа профессии, отсутствие поддержки среди населения.

В настоящее время предпринимаются попытки разрешения проблемы, связанной с отсутствием сотрудников полиции, владеющих знаниями в сфере информационных технологий, путем реализации мер, направленных на повышение квалификации действующих сотрудников. То есть, по мнению руководителей, если направить сотрудника полиции на повышение квалификации, допустим, на шесть месяцев, из него получится IT-специалист, который должен будет выявлять, пресекать, предупреждать противоправные деяния в сфере компьютерной информации. При этом не учитывается тот факт, что продолжительность обучения по IT-специальностям в образовательных учреждениях составляет 4,5-5 лет, а практические навыки преимущественно вырабатываются в процессе осуществления трудовой деятельности. Таким образом, повышение квалификации в сфере информационных технологий является неэффективным способом решения кадровых проблем.

Нами предлагается несколько иной, более действенный способ разрешения проблемы в виде организации взаимодействия полиции с IT-компаниями. Взаимодействие осуществляется следующим путем:

- IT-компания выделяет территориальному органу внутренних дел своего работника, который за дополнительную плату оказывает помощь соответствующим подразделениям полиции в разработке методов выявления, пресечения, предупреждения и раскрытия киберпреступлений.

Другой способ – альтернативная служба для IT- специалистов в полиции вместо службы в Вооруженных силах РФ. В соответствии с действующим законодательством, IT-специалистам предоставляется отсрочка от военной службы. При этом срок работы в аккредитованных IT-компаниях у претендента на отсрочку должен быть не менее 11 месяцев в течение года, предшествующего

дате начала призыва. Но если специалист устроился в IT-компанию в течение года после окончания обучения в вузе или научной организации, требование о стаже работы не применяется. Для иных IT-специалистов предлагается вышесказанная альтернативная служба в полиции, что позволит специалистам оказать помощь сотрудникам полиции в предупреждении преступлений в сфере компьютерной информации, и в то же время совершенствовать умения и навыки.

Помимо отсутствия высококвалифицированных кадров, в системе правоохранительных органов, в первую очередь, в органах внутренних дел, существуют другие организационные проблемы. В ходе беседы с действующими сотрудниками отдела по борьбе с киберпреступлениями МВД по Республике Татарстан (ОБК МВД по РТ) установлено, что на практике у подразделения отсутствуют четко сформулированные задачи. К примеру, практически любая информация, поступившая в территориальный орган внутренних дел, в которой имеется упоминание об IT-технологиях, автоматически направляется в ОБК, тогда как данная информация относится к сфере деятельности иных служб и подразделений полиции (например, БЭП, НОН, УР, ЦПЭ и т.д.). В связи с чем, нагрузка на сотрудников подразделения по борьбе с киберпреступлениями растет, что не позволяет решить задачи по борьбе с преступлениями в сфере компьютерной информации. Также действующие сотрудники отметили отсутствие высокопроизводительного компьютерного оборудования, беспроводного высокоскоростного Интернета (Wi-Fi), что не позволяет выявить киберпреступников и принять меры по привлечению их к уголовной ответственности.

В настоящее время не уделяется должного внимания вопросам привлечения граждан к содействию полиции, иным правоохранительным органам в решении задач, связанных с противодействием преступлениям в сфере компьютерной информации на добровольной основе. Существенный вклад в предупреждение преступности вносят добровольные народные дружины – основанное на членстве общественное объединение, участвующее в охране общественного порядка во взаимодействии с органами внутренних дел

(полицией) и иными правоохранительными органами, органами государственной власти и органами местного самоуправления.

Высокой степенью эффективности обладали народные дружины, функционировавшие в Советском союзе. Институт народных дружинников в настоящее время только зарождается. Для модернизации такого института гражданского общества, как народные дружины, необходимо в давно известное название привлечь новый смысл и содержание. По мнению, С.П. Зимина «целесообразным будет не только патрулирование улиц и проведение дежурств, но и использование, например, веб-камер дистанционного наблюдения, специальных интернет-программ коммуникации между дружинниками и полицией. Интересным будет также использование специальной формы одежды с нашивками (например, символ города или поселка), а не простых повязок»[1].

В современной криминологической науке предлагается трансформировать традиционные народные дружины в «кибердружины». Более того, еще в 2018 году был разработан соответствующий законопроект «О кибердружинах», который не внесен в Государственную Думу РФ. В проекте закона кибердружина определена как общественное объединение, взаимодействующее с правоохранительными органами и органами государственной власти для противодействия распространению в сети Интернет противоправной информации, а также поддержки безопасной информационной среды в сети Интернет[2].

Правовые акты, регламентирующие вопросы деятельности кибердружин, разработаны органами местного самоуправления. Например, в Республике Татарстан, это Постановление исполнительного комитета Тукаевского района Республики Татарстан от 07.10.2020 г. № 3991 «О создании кибердружины»[3].

---

[1] Зимин С.П. Народные дружины как форма предупреждения преступности гражданским обществом // Science Time. 2021. №7 (91). – С. 17-20.

[2] Проект федерального закона о кибердружинах (законопроект не был внесен в Государственную Думу) // СПС «КонсультантПлюс» (дата обращения: 22.01.2025).

[3] О создании кибердружины: Постановление исполнительного комитета Тукаевского района Республики Татарстан от 07.10.2020 г. № 3991 - [Электронный ресурс] // Тукаевский

Анализ положений данного правового акта, а также иных правовых документов иных муниципальных образований республики, свидетельствует о том, что кибердружины преследуют цели, которые преимущественно связаны с выявлением противоправной информации с признаками террористической, экстремистской деятельности, а также с незаконным оборотом наркотиков, порнографией и т.д. То есть, противодействие киберпреступлениям, например, имущественного характера (мошенничества, кражи) не является приоритетным направлением деятельности кибердружин Республики Татарстан, тогда как в 2023 году общественным советом при ГУ МВД России по Ростовской области принято решение о создании кибердружин для борьбы с интернет-мошенничеством[1].

Следующая проблема – сама компьютерная преступность. Большинство процессов, протекающих в сфере компьютерной информации, ввиду ряда объективных причин не подлежит контролю со стороны государства. В диссертационном исследовании К.Н. Евдокимова выдвинута частная научная теория «Анекселенктотичной (неконтролируемой) технотронной преступности». По мнению автора, «анекселенктотичная технотронная преступность – новый вид высокотехнологической преступности, пришедшей на смену традиционной компьютерной преступности и являющийся дальнейшей формой развития преступности с использованием высоких технологий, которая в силу латентного, организованного, профессионального, трансграничного, транснационального характера и самодетерминации вышла из-под контроля личности, общества и государства, представляя опасность практически для всех жизненно важных общественных отношений»[2].

муниципальный район URL: https://tukay.tatarstan.ru/postanovleniya-i-rasporyazheniya-rik.htm?pub_id=2514334 (дата обращения: 22.01.2025).

[1] В Ростовской области создадут кибердружину для борьбы с мошенниками - [Электронный ресурс] // Свежие новости за сегодня в Ростове и Ростовской области URL: https://don24.ru/rubric/obschestvo/sverka-nuzhno-ukazat-avtora-snimka-v-rostovskoy-oblasti-sozdadut-kiberdruzhinu-dlya-borby-s-moshennikami.html (дата обращения: 23.01.2025).

[2] Евдокимов, К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореферат дис. ... доктора юридических наук: 12.00.08 / Евдокимов Константин

Следует согласиться с указанным мнением. Так, в основе преступлений в сфере компьютерной информации лежит корыстная мотивация, то есть, финансовый интерес. Действия по легализации преступных доходов, полученных в результате совершения преступлений в сфере компьютерной информации, преимущественно осуществляются посредством криптовалют, оборот которых не подлежит полному и всестороннему контролю финансовыми и налоговыми органами государства. Использование цифровой валюты позволяет скрыть источник происхождения средств и конечного бенефициара - их получателя, что фактически исключает возможность выявления и конфискации использовавшейся при совершении экономических преступлений цифровой валюты. В 2024 году государством предприняты попытки урегулирования оборота криптовалюты:

1. С 1 сентября 2024 года у российского бизнеса появилась возможность проводить международные расчёты в криптовалюте. Цифровые деньги во внешнеэкономической деятельности приобретают статус платёжного средства, но расплачиваться ими можно только под контролем Банка России.

2. С 1 ноября 2024 года в России станет легальна и добыча криптовалюты. Поправки в закон о цифровых финансовых активах разрешают добывать криптовалюту юридическим лицам и индивидуальным предпринимателям, но только после их включения в специальный реестр[1].

Вышеуказанные меры не способны оказать влияние на процессы использования криптовалюты в преступной деятельности. Дело в том, что значительная часть операций с криптовалютой совершается на платформах-обменниках, расположенных на территории зарубежных стран, которые не предоставляют сведения о лицах – владельцах крипто-кошельков. Вывод денежных средств, как правило, осуществляется в мобильных приложениях, в

Николаевич; [Место защиты: ФГКОУ ВО «Университет прокуратуры Российской Федерации»]. - Москва, 2022. - 73 с.

[1] Криптовалюта выходит из тени. Как меняется правовое регулирование цифровых денег- [Электронный ресурс] // Аналитические статьи: ГАРАНТ.РУ URL: https://www.garant.ru/article/1759006/ (дата обращения: 24.01.2025).

специальных чат-ботах, функционирующих в мессенджерах наподобие «Telegram», в анонимном браузере «TOP».

Отсутствие контроля над финансовыми операциями – не единственный признак анекселенктотичной (неконтролируемой) технотронной преступности. В последнее время актуальным становится использование технологии искусственного интеллекта (ИИ) в различных сферах жизнедеятельности, например, в науке, искусстве, программировании и т.д. Возможности искусственного интеллекта применяются в целях реализации преступных целей. Так, распространение получили «дипфейки» – подложные картинки и видео, созданные на основе других изображений[1]. Например, в 2021 году в социальных сетях получило видеообращение основателя Т-банка Олега Тинькова. На видео в кадре сидит человек, похожий на Тинькова, который обещает выгоду от инвестиций. «Давайте бегом за бонусом. Мы дарим +50% к вашей сумме вложений. Например, вы инвестируете 20 000 рублей, а на счет для работы получаете 30 000 рублей, а там с нашим экспертом и все 70 000 за месяц можно заработать. Фальшивое видео опубликовано фейковой страницей Tinkoff Bonus в Facebook, аватарка которой напоминает логотип банка. По данным Fakecheck, при попытке перехода по ссылкам рядом с дипфейком пользователь попадает на лендинг с логотипами банка и «Тинькофф Инвестиций», где после ответов на вопросы про инвестиции его попросят оставить имя, email и телефон. Далее происходит дальнейшая психологическая «обработка» потенциальной жертвы – инвестора, с высылкой реквизитов, куда нужно перевести деньги для получения бонуса, а также установлением данных карт[2].

Технологии искусственного интеллекта находятся в свободном доступе (например, ChatGPT в Telegram) и не контролируются со стороны государства.

---

[1] «Темная сторона» нейросетей: от «умного» фишинга до дронов-террористов - [Электронный ресурс] // РБК Тренды URL: https://trends.rbc.ru/trends/industry/62a3332f9a7947fc4dd296d8 (дата обращения: 24.01.2025).

[2] «Всех обнял!»: образ Олега Тинькова использовали в дипфейк-рекламе - [Электронный ресурс] // Forbes.ru URL: https://www.forbes.ru/milliardery/439255-vseh-obnal-obraz-olega-tin-kova-ispol-zovali-v-dipfejk-reklame (дата обращения: 25.01.2025).

Также к проблемам предупреждения преступлений в сфере компьютерной информации относятся проблемы, обусловленные напряженной политической обстановкой в мире. Как отмечено в Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, существенное негативное влияние на криминогенную обстановку в информационно-коммуникационной сфере оказывает сложная международная ситуация, в том числе связанная с деятельностью спецслужб недружественных государств и неонацистских формирований, курируемых иностранными спецслужбами. Основная масса преступлений совершается специализирующимися на мошенничествах транснациональными организованными преступными группами, связанными с организацией хищения персональных данных граждан Российской Федерации и работой действующих с территорий недружественных государств колл-центров, с использованием которых похищаются средства граждан. То есть, пресечь деятельность преступных организаций, действующих за пределами Российской Федерации не представляется возможным.

Помимо вышеизложенного, существенное влияние на эффективность деятельности правоохранительных органов по борьбе с преступлениями в сфере компьютерной информации влияет такое социально-опасное явление, как коррупция. Субъектами коррупционных преступлений выступают должностные лица органов, осуществляющих оперативно-розыскную деятельность, предварительное расследование по уголовным делам о преступлениях в сфере компьютерной информации.

Так, Балашихинский суд вынес обвинительный приговор в отношении бывшего следователя СК РФ Марата Тамбиева. Суд установил, что Тамбиев, будучи руководителем Мещанского, а потом Тверского следственного отдела СК, с 2020 по 2022 год получил взятки на сумму более 7,5 млрд рублей в биткоинах от подследственных, обвиняемых в неправомерном обороте средств платежей. Часть денег, как установило следствие, он получил по предварительному сговору со следователем Кристиной Ляховенко, которая

сфальсифицировала доказательства по делу. Как позже выяснилось, на криптокошельках группировки Infraud Organization после возбуждения дела было более 5200 биткоинов, что соответствовало на тот момент более 14 млрд рублей. Тамбиев согласился «помочь» хакерам за половину от этой суммы.

За материальное вознаграждение, по данным суда, следователи помогали выносить решения об избрании обвиняемым меры пресечения в виде домашнего ареста вместо заключения под стражу. А также принимали меры, направленные на избежание ареста их имущества, и оказывали другие услуги. Когда уже другим следователям удалось вскрыть защищенный ноутбук Тамбиева, то в нем обнаружили папку «Пенсия», а в ней - пароли от многочисленных криптокошельков. В итоге суд признал Марата Тамбиева виновным в получении взяток, превышении должностных полномочий»[1].

Негативные примеры имеются и в системе МВД России. Так, в августе 2023 года возбуждено уголовное дело о взятке в отношении бывших сотрудников Бюро специальных технических мероприятий МВД РФ Георгия Сатюкова и Дмитрия Соколова, которые, по мнению следствия, в период с 2019 по 2021 год от сисадмина криптобиржи World Exchange Services Pte. Ltd Алексея Иванова получали взятки, предназначенные за «общее покровительство»[2].

На основании вышеизложенного, можно сделать следующие выводы.

В качестве правовой основы деятельности ОВД РФ по предупреждению преступлений в сфере компьютерной информации выступают:

- нормативно-правовые актах общего характера, посвященные вопросам противодействия преступности в целом;

---

[1] Суд вынес приговор по делу о рекордной взятке в биткоинах - [Электронный ресурс] // Российская газета URL: https://rg.ru/2024/10/09/bitkoiny-ot-hakerov.html (дата обращения: 25.01.2025).

[2] Крупнейшие взятки в России - [Электронный ресурс] // Коммерсантъ URL: https://www.kommersant.ru/doc/7214606 (дата обращения: 25.01.2025).

- специальные нормативно-правовые акты, нормы которых регламентируют предупреждение киберпреступлений и иных правонарушений в цифровом пространстве.

Несмотря на актуальность преступлений, совершаемых путем использования информационно-телекоммуникационных технологий, в сфере компьютерной информации, ни федеральное, ни ведомственное законодательство не рассматривают данные криминальные явления в качестве направлений профилактики и предупреждения, которым должно быть уделено особое внимание. Полагаем, что законодательство в сфере профилактики и предупреждения преступлений должно соответствовать наиболее актуальным тенденциям, характерным для преступности. В связи с вышеизложенным, считаем необходимым дополнить часть 1 статьи 6 Закона «Об основах системы профилактики правонарушений в Российской Федерации» новым пунктом и изложить её в следующей редакции:

Статья 6. Основные направления профилактики правонарушений

1. Профилактика правонарушений осуществляется по следующим основным направлениям:

1) защита личности, общества и государства от противоправных посягательств;

17. противодействие преступления и иным правонарушениям, совершаемым посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации, обеспечение защищенности граждан, общества и государства от противоправных деяний, совершаемых посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации.

Соответствующие изменения необходимо внести в ведомственное законодательство – в Приказ МВД России № 619.

Организация деятельности ОВД РФ по предупреждению преступлений в сфере компьютерной информации включает в себя следующие мероприятия:

- создание и обеспечение деятельности служб и подразделений, к полномочиям которых отнесена реализация мер по пресечению, предотвращению и профилактике преступлений киберпреступлений;

- организация взаимодействия ОВД РФ с иными субъектами системы профилактики преступлений в сфере компьютерной информации;

- осуществление комплексного анализа оперативной обстановки на соответствующей территории и объектах, результатах работы, выявление и прогнозирование тенденций и отклонений, выработка на этой основе своевременных, обоснованных и оптимальных управленческих решений.

Проблемы предупреждения преступлений в сфере компьютерной информации носят комплексный характер:

- количественный и качественный дефицит кадров системе органов внутренних дел;

- специфика самой компьютерной преступности;

- международные проблемы, обусловленные наличием конфликта во взаимоотношениях России с другими государствами, относящимися к категории недружественных;

- коррупция в самой сфере противодействия компьютерной преступности.

ЗАКЛЮЧЕНИЕ

Исследования, проведенные в рамках настоящей дипломной работы, позволяют сделать следующие выводы.

В первой главе рассмотрена криминологическая характеристика преступлений в сфере компьютерной информации. Преступность в сфере компьютерной информации представляет собой систему уголовно-наказуемых деяний, включенных в Главу 28 УК РФ (Преступления в сфере компьютерной информации), а также ряд иных преступлений, совершаемых в цифровом, то есть, киберпространстве. Это – кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ); интернет-вымогательство (с. 163 УК РФ).

Далее определено состояние преступности в сфере компьютерной информации. Согласно статистическим данным, представленным ГИАЦ МВД России (Раздел «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации»), за последние пять лет наблюдается устойчивая тенденция роста преступлений в рассматриваемой сфере. Если в 2020 году с использованием информационно-телекоммуникационных технологий, а также в сфере компьютерной информации совершено 510396 противоправных деяний, в 2024 году данный показатель составил 765365. Таким образом, прирост за последние пять лет составил 149%. Если сравнивать показатели 2023 и 2024 годов, то прирост равен 13%. Темпы прироста были приостановлены в 2021, 2022 годах, однако, данное обстоятельство связано с политическими причинами и условиями.

Стоит отметить, что в отдельных регионах наметились положительные тенденции в виде снижения прироста киберпреступлений. Это – Ямало-Ненецкий АО, где количество преступлений снизилось на 46%, а также

Ненецкий АО, Республика Марий Эл, Забайкальский край, Калужская область. В некоторых субъектах темпы прироста IT-преступлений превышают показатели по России.

Далее рассмотрена структура криминологической характеристики преступлений в сфере компьютерной информации. Преступность в данной области обусловлена общими причинами и условиями преступности, а также отдельными факторами, непосредственно детерминирующими противоправное поведение киберпреступника. Ключевым фактором киберпреступлений становится развитие и постоянное совершенствование самого киберпространства, что позволяет разрабатывать новые способы реализации преступных целей. К примеру, значительная часть преступлений совершается в современных мессенджерах, которые пользуются популярностью у граждан (Telegram, WhatsApp).

Следующий фактор – современные информационные технологии способствуют анонимизации преступников, что вызывает у последних чувство безнаказанности и мотивирует на совершение противоправных деяний. Анонимность киберпреступников – одна из ключевых причин низкой раскрываемости преступлений в сфере компьютерной информации. За последние 5 лет показатели раскрываемости не составляли более 27 % (в 2024 – 22%). К регионам с наибольшей раскрываемостью относятся Республика Дагестан, Свердловская область, Республика Ингушетия, Чеченская Республика (48.6 – 31.1%). Низкая раскрываемость характерна для Ненецкой АО, Республики Марий Эл, Республики Мордовия, Приморского края (9.6 – 15.7%).

На основе личного опыта, полученного в результате прохождения производственной практики был сделан вполне обоснованный вывод о том, что механизм раскрытия преступлений в сфере компьютерной информации довольно сложный и требует значительных временных затрат. В условиях ограниченности сил и средств, вызванных кадровыми проблемами, а также проблемами разработки и внедрения в систему правоохранительных органов, в

первую очередь органов внутренних дел, новых технологий, рост показателей раскрываемости практически невозможен.

Существенное значение для предупреждения компьютерных преступлений имеет изучение личности компьютерного преступника. Обобщенный портрет киберпреступника следующий:

- лицо возрасте до 30 лет, в большинстве случаев имеющее профессиональное образование в области информационных технологий, либо соответствующие навыки, ранее не судимое, преимущественно мужского пола. Черты личности характеризуются правовым нигилизмом, нежеланием жить по правилам, установленным обществом, руководство корыстными, хулиганскими или иными мотивами, испытывают чувство безнаказанности и превосходства в связи с обезличенностью персоны в киберпространстве.

На практике сотрудники правоохранительных органов преимущественно сталкиваются с такими типами киберпреступников, как хакеры, специализирующиеся на взломе информационных систем, традиционные преступники, использующие в преступных целях общедоступные информационные технологии, например, кибермошенники.

Во второй главе исследована деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации. Деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации основана на нормативно-правовых актах общего характера, посвященных вопросам противодействия преступности в целом, а также специальных нормативно-правовых актах, нормы которых регламентируют предупреждение киберпреступлений и иных правонарушений в цифровом пространстве.

В ходе анализа Федерального закона «Об основах системы профилактики правонарушений в Российской Федерации», выступающего в качестве правовой основы предупреждения компьютерных преступлений, установлено, в указанном нормативно-правовом акте понятия киберпреступления, кибербезопасность, а также схожие по смыслу и содержанию категории не

нашли отражения. Далее был сделан вывод о том, что законодательство в сфере профилактики и предупреждения преступлений должно соответствовать наиболее актуальным тенденциям, характерным для преступности. В связи с вышеизложенным, необходимо дополнить часть 1 статьи 6 Закона «Об основах системы профилактики правонарушений в Российской Федерации» новым пунктом и изложить её в следующей редакции:

Статья 6. Основные направления профилактики правонарушений

1. Профилактика правонарушений осуществляется по следующим основным направлениям:

1) защита личности, общества и государства от противоправных посягательств;

17. противодействие преступления и иным правонарушениям, совершаемым посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации, обеспечение защищенности граждан, общества и государства от противоправных деяний, совершаемых посредством информационно-телекоммуникационных технологий, в сфере компьютерной информации.

Соответствующие изменения необходимо внести в ведомственное законодательство – в Приказ МВД России № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений».

Деятельность по предупреждению компьютерных преступлений также основана на следующих нормативно-правовых актах:

- Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

- Распоряжение Правительства РФ от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий».

Эффективное предупреждение компьютерных преступлений возможно при должной организации такой деятельности. Организация деятельности ОВД РФ по предупреждению преступлений в сфере компьютерной информации представляет собой комплекс мероприятий, направленных на создание необходимых условий для реализации данной цели.

К субъектам предупреждения в системе органов внутренних дел относятся:

- подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий;

- подразделения уголовного розыска;

- служба участковых уполномоченных полиции

Если предупредительная деятельность оперативных подразделений преимущественно связана с выявлением лиц, причастных к преступлениям, и принятием мер, направленных на их задержание, то службы участковых уполномоченных полиции преследуют цель в виде оказания профилактического воздействия на граждан-потенциальных жертв преступлений в сфере компьютерной информации.

Актуальным в последнее время является взаимодействие по вопросам предупреждения компьютерных преступлений с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Роскомнадзор:

- предоставляет сведения о месте нахождения и персональных данных лица, на чьё имя зарегистрирован домен в сети Интернет;

-блокирует сайты по требованию правоохранительных служб, в том числе и органов внутренних дел, если на них содержится информация, противоречащая законодательству РФ.

Существенным условием для предупреждения компьютерных преступлений является организация взаимодействия ОВД РФ с банковскими организациями в лице Банка России.

Проблемы предупреждения преступлений в сфере компьютерной информации заключаются в следующем. В первую очередь, качественный и

количественный кадровый дефицит в органах внутренних дел. Предлагаем разрешить данную проблему путем организации взаимодействия полиции с IT-компаниями. Взаимодействие осуществляется следующим путем:

Способ № 1. IT-компания выделяет территориальному органу внутренних дел своего работника, который за дополнительную плату оказывает помощь соответствующим подразделениям полиции в разработке методов выявления, пресечения, предупреждения и раскрытия киберпреступлений.

Способ № 2. Альтернативная служба для IT- специалистов в полиции вместо службы в Вооруженных силах РФ. В соответствии с действующим законодательством, IT-специалистам предоставляется отсрочка от военной службы. При этом срок работы в аккредитованных IT-компаниях у претендента на отсрочку должен быть не менее 11 месяцев в течение года, предшествующего дате начала призыва. Но если специалист устроился в IT-компанию в течение года после окончания обучения в вузе или научной организации, требование о стаже работы не применяется. Для иных IT-специалистов предлагается вышесказанная альтернативная служба в полиции, что позволит специалистам оказать помощь сотрудникам полиции в предупреждении преступлений в сфере компьютерной информации, и в то же время совершенствовать умения и навыки.

Следующая проблема – не используется в полном объеме потенциал содействия граждан. На законодательном уровне не закреплен правовой статус «кибердружин», тогда как на местном уровне разработаны правовые акты, регламентирующие вопросы их деятельности.

Проблемой также является характер самой компьютерной преступности. Большинство процессов, протекающих в сфере компьютерной информации, ввиду ряда объективных причин не подлежит контролю со стороны государства. Это, в частности, использование в преступной деятельности цифровой валюты, что позволяет скрыть источник происхождения средств и конечного их получателя, что фактически исключает возможность выявления и конфискации использовавшейся при совершении экономических преступлений цифровой валюты.

Также к проблемам предупреждения преступлений в сфере компьютерной информации относятся проблемы, обусловленные напряженной политической обстановкой в мире. Так, значительная часть киберпреступлений совершается специализирующимися на мошенничествах транснациональными организованными преступными группами, связанными с организацией хищения персональных данных граждан РФ и работой действующих с территорий недружественных государств колл-центров, с использованием которых похищаются средства граждан. То есть, пресечь деятельность преступных организаций, действующих за пределами Российской Федерации не представляется возможным.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

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

1. Конституция Российской Федерации от 12.12.1993 г.: Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации www.pravo.gov.ru, 04.07.2020. № 0001202007040001 (дата обращения: 10.09.2024).

2. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.09.2024).

3. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23 июня 2016 г. № 182-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 18.12.2024).

4. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 01.01.2025).

5. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г № 187 ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 12.09.2024).

6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 07.01.2025).

7. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации, N 27 (ч.II), 05.07.2021, ст.5351

8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации, N 50, 12.12.2016, ст.7074

9. Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности»: Постановление Правительства РА от 15 апреля 2014 года № 345 Собрание законодательства Российской Федерации, N 18 (ч.IV), 05.05.2014, ст.2188/

10. Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: Распоряжение Правительства РФ от 30.12.2024 N 4154-р - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 05.01.2025).

11. Об утверждении государственной программы Республики Татарстан «Обеспечение общественного порядка и противодействие преступности»: Постановление Кабинета Министров Республики Татарстан от 16 октября 2013 № 764 «Сборник постановлений и распоряжений Кабинета Министров Республики Татарстан и нормативных актов республиканских органов исполнительной власти», 22.10.2013, N 78, ст. 2624.

12. О Программе профилактики правонарушений и преступлений в г. Казани на 2016 - 2025 годы: Постановление Исполнительного комитета города Казани Республики Татарстан от 04 декабря 2015 № 4267 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 01.01.2025).

13. О создании кибердружины: Постановление исполнительного комитета Тукаевского района Республики Татарстан от 07.10.2020 г. № 3991 - [Электронный ресурс] // Тукаевский муниципальный район URL: https://tukay.tatarstan.ru/postanovleniya-i-rasporyazheniya-rik.htm?pub_id=2514334 (дата обращения: 22.01.2025).

14. О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений: Приказ МВД России от 24 августа 2023 г. № 619 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 03.01.2025).

15. Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: Приказ МВД России от 29 декабря 2022 г. № 1110 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 12.01.2025).

16. Об утверждении Типового положения о подразделении по борьбе с противоправным использованием информационно-коммуникационных технологий территориального органа Министерства внутренних дел Российской Федерации на региональном уровне: Приказ МВД России от 14.02.2023 № 71 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 13.01.2025).

17. О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности: Приказ МВД России от 29.03.2019 № 205 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 13.01.2025).

II. Монографии, учебники, учебные пособия:

18. 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, 2025. — 356 с

19. 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, 2025. — 178 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, 2025. — 339 с.

21. Решетников, А. Ю. Криминология: учебник для вузов / А. Ю. Решетников, О. Р. Афанасьева. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 166 с.

22. Лунеев, В. В. Криминология: учебник для вузов / В. В. Лунеев. — Москва: Издательство Юрайт, 2025. — 686 с.

III. Статьи, научные публикации:

23. Алымов Д.А., Криминалистическая характеристика типовых следов преступника, осуществляющего криминальную деятельность в виртуальном пространстве (на примере дроповодов). Вестник Томского государственного университета. – 2024. – № (506). – С. 185-192.

24. Бабурин В. В. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан / В. В. Бабурин, К. О. Карабеков // Психопедагогика в правоохранительных органах. – 2024. – Т. 29, № 1(96). – С. 113-119.

25. Белевитина, Ю. В. Криминологический портрет личности киберпреступника в современной России / Ю. В. Белевитина // Инновационная наука. – 2022. – № 12-2. – С. 61-64.

26. Белицкий, В. Ю. Предупреждение совершения мошенничеств участковым уполномоченным полиции / В. Ю. Белицкий // Вестник Барнаульского юридического института МВД России. – 2017. – № 2(33). – С. 132-133.

27. Григорян, С. А. Особенности личности современного «киберпреступника»/ С. А. Григорян // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2022. – № 8(147). – С. 103-106.

28. Девятова А.О. Личность преступника: понятие и криминологическая характеристика // Отечественная юриспруденция. – 2019. №7 (32). – С. 75-78/

29. Евдокимов, К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореферат дис. ... доктора юридических наук: 12.00.08 / Евдокимов Константин Николаевич; [Место защиты: ФГКОУ ВО «Университет прокуратуры Российской Федерации»]. - Москва, 2022. - 73 с.

30. Зимин С.П. Народные дружины как форма предупреждения преступности гражданским обществом // Science Time. 2021. №7 (91). – С. 17-20.

31. Зорина Н. С. К вопросу о личности киберпреступника и его жертве в сфере компьютерной информации и информационных технологий / Н. С. Зорина // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». – 2022. – № 25. – С. 92-96.

32. Зуева И. А. Преступность в сфере компьютерной информации в России: общая характеристика / И. А. Зуева // Наука, общество, технологии: проблемы и перспективы взаимодействия в современном мире: Сборник статей II Международной научно-практической конференции, Петрозаводск, 28 июня 2022 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2022. – С. 69-73.

33. Ивлиев П.А.. Анонимность в интернете: проблемы и особенности. Международный журнал гуманитарных и естественных наук. –2021. – № (4-2). С. 7-10.

34. Савельева, А. Г. Структурные элементы личности преступника как объекта изучения криминологии / А. Г. Савельева // Право. Общество. Государство: Сборник научных трудов студентов и аспирантов / Отв. ред. Е. В. Трофимов. Том 11. – Санкт-Петербург: Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2020. – С. 166-169.

35. Сафин Ф. Ю. Отдельные аспекты преступности в сфере компьютерной информации / Ф. Ю. Сафин // Научная сессия ГУАП: гуманитарные науки: Сборник докладов традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики, Санкт-Петербург, 14–22 апреля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. – С. 221-222.

36. Север Н. С. Особенности криминологической характеристики личности киберпреступников / Н. С. Север // Вестник Волгоградского

государственного университета. Серия 9: Исследования молодых ученых. – 2022. – № 20. – С. 108-110.

IV. Эмпирические материалы:

37. Приговор Первомайского районного суда г. Краснодара от 19.07.2018 по делу № 1-50/2018 - [Электронный ресурс]. – URL: https://судебныерешения.рф/35324463/extended (дата обращения: 17.12.2024).

38. Сотрудники уголовного розыска МВД по Республике Татарстан задержали курьера мошенников - [Электронный ресурс] // Официальный сайт МВД по Республике Татарстан URL: https://16.мвд.рф/news/item/57929558/ (дата обращения: 11.01.2025).

V. Справочная литература:

39. Банки начнут сообщать родителям о платежах и переводах детей - [Электронный ресурс] // Российская газета URL: https://rg.ru/2025/03/29/banki-nachnut-soobshchat-roditeliam-o-platezhah-i-perevodah-detej.html (дата обращения: 17.12.2024).

40. В Ростовской области создадут кибердружину для борьбы с мошенниками - [Электронный ресурс] // Свежие новости за сегодня в Ростове и Ростовской области URL: https://don24.ru/rubric/obschestvo/sverka-nuzhno-ukazat-avtora-snimka-v-rostovskoy-oblasti-sozdadut-kiberdruzhinu-dlya-borby-s-moshennikami.html (дата обращения: 23.01.2025).

41. «Всех обнял!»: образ Олега Тинькова использовали в дипфейк-рекламе - [Электронный ресурс] // Forbes.ru URL: https://www.forbes.ru/milliardery/439255-vseh-obnal-obraz-olega-tin-kova-ispol-zovali-v-dipfejk-reklame (дата обращения: 25.01.2025).

42. Дроповоды: кто скрывается за украденными личностями - [Электронный ресурс] // Рейтинг партнерских программ, партнерок URL: https://partnerkin.com/blog/stati/dropovody_kto_skryvaetsya_za_u (дата обращения: 16.12.2024).

43. Законопроект № 909076-8 «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» (об уточнении ответственности за неправомерный оборот электронных средств платежа) - [Электронный ресурс] // Система обеспечения законодательной деятельности URL: https://sozd.duma.gov.ru/bill/909076-8 (дата обращения: 17.12.2024).

44. Криптовалюта выходит из тени. Как меняется правовое регулирование цифровых денег- [Электронный ресурс] // Аналитические статьи: ГАРАНТ.РУ URL: https://www.garant.ru/article/1759006/ (дата обращения: 24.01.2025).

45. Крупнейшие взятки в России - [Электронный ресурс] // Коммерсантъ URL: https://www.kommersant.ru/doc/7214606 (дата обращения: 25.01.2025).

46. Не более 100 тысяч в месяц: как будет работать новый закон для борьбы с дропперами - [Электронный ресурс] // Российская газета URL: https://rg.ru/2025/05/14/ne-prinimajte-na-svoj-schet.html (дата обращения: 17.12.2024).

47. «Некомплект» в МВД по РТ превысил 17%: «Тема заезжена…» - [Электронный ресурс] // БИЗНЕС Online — Новости Казани URL: https://www.business-gazeta.ru/news/623284 (дата обращения: 18.01.2025).

48. Нехватка сотрудников МВД достигла почти 20% - [Электронный ресурс] // РБК URL: https://www.rbc.ru/society/26/11/2024/6745d1979a794754b06006c5 (дата обращения: 18.01.2025).

49. Проект федерального закона о кибердружинах (законопроект не был внесен в Государственную Думу) // СПС «КонсультантПлюс» (дата обращения: 22.01.2025).

50. Рост киберпреступности замедлился в 2021 году - [Электронный ресурс] // Право.ru: законодательство, судебная система, новости и аналитика. Все о юридическом рынке. https://pravo.ru/news/236839/ (дата обращения 12.09.2024.

51. С 21 октября текущего года Банк России и МВД России начнут онлайн-обмен информацией для противодействия кибермошенникам - [Электронный ресурс] // Новости: ГАРАНТ.РУ URL: https://www.garant.ru/news/1653676/ (дата обращения: 17.01.2025).

52. «Скоро останетесь одни в своих креслах»: МВД не хватает 100 тысяч сотрудников - [Электронный ресурс] // Газета.Ru URL: https://www.gazeta.ru/social/2023/10/11/17718175 (дата обращения: 17.01.2025).

53. Состояние преступности в России за 2020-2024 гг. [Электронный ресурс] // Главный информационно-аналитический центр МВД России URL: https://мвд.рф/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen (дата обращения 11.09.2024).

54. Суд вынес приговор по делу о рекордной взятке в биткоинах - [Электронный ресурс] // Российская газета URL: https://rg.ru/2024/10/09/bitkoiny-ot-hakerov.html (дата обращения: 25.01.2025).

55. «Темная сторона» нейросетей: от «умного» фишинга до дронов-террористов - [Электронный ресурс] // РБК Тренды URL: https://trends.rbc.ru/trends/industry/62a3332f9a7947fc4dd296d8 (дата обращения: 24.01.2025).

56. Эксперт объяснил, чем обосновано первое за пять лет снижение киберпреступности в России - [Электронный ресурс] // Газета СПБ РУ - новости Санкт-Петербурга https://gazeta.spb.ru/2497344-ekspert-obyasnil-chem-obosnovano-pervoe-za-pyat-let-snizhenie-kiberprestupnosti-v-rossii (дата обращения 12.09.2024).