Министерство внутренних дел Российской Федерации

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

Кафедра криминологии и уголовно-исполнительного права

# ДИПЛОМНАЯ РАБОТА

**на тему Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по Республике Татарстан)**

Выполнил: Осипов Никита Алексеевич
40.05.02 – Правоохранительная деятельность, год набора – 2018,
082 учебная группа

Руководитель
к.ю.н., доцент кафедры криминологии и уголовно-исполнительного права КЮИ МВД России
подполковник полиции
Хафизова Альбина Мансуровна

Рецензент:
заместитель начальника ОП № 3
«Зареченский» УМВД России по г. Казани
подполковник полиции
Казаков Руслан Равильевич

Дата защиты: "____"_____20___г. Оценка _____

Казань 2023

СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Трансформация общественных отношений с развитием информационных технологий происходит стремительно. Противодействие киберпреступности, а также меры предупреждения преступлений в киберпространстве в настоящее время недостаточно эффективны в силу многих обстоятельств, основными из которых являются следующие: недостаточное правовое регулирование деятельности субъектов в киберпространстве, отсутствие должного технического обеспечения деятельности органов внутренних дел, которое необходимо для противодействия киберпреступности, а также нехватка квалифицированных кадров. Необходимо принимать во внимание, что преступники все активнее используют информационно-телекоммуникационные технологии для совершения преступлений, как и сама киберсреда обладает значительным криминогенным потенциалом. Принимая во внимание данный факт, следует отметить, что для предупреждения киберпреступности необходимо создавать и использовать эффективные алгоритмы взаимодействия между правоохранительными и иными органами исполнительной власти, а также судами; обновление и оптимизация специальных программ и аппаратных средств; обучение сотрудников современным приемам и способам работы в интернет-пространстве.

В век высоких инновационных технологий, в обществе, в котором компьютерные технологии и телекоммуникационные системы и сеть Интернет охватывают все сферы жизнедеятельности. Но человечество, использующее информационно-телекоммуникационные технологии, не предвидело возможности злоупотребления этими технологиями. На сегодняшний день жертвами киберпреступников, действующих в информационном пространстве, могут стать не только отдельные пользователи – лица, но и целые страны. Также, следует отметить, что безопасность населения в процессе цифровизации оказывается в опасности, в зависимости преступников.

Число киберпреступлений увеличивается прямо пропорционально числу пользователей информационного пространства. Так, согласно статистическим

данным за последние пять лет, следует, что в 2018 году было зарегистрировано 174 674, в 2019 году – 294 409, в 2020 году – 510 396, в 2021 году – 517 722, в году 2022 – 522 065 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. На основе статистических данных мы видим, что за последние несколько лет преступления, совершенные с использованием компьютерных и телекоммуникационных технологий, увеличились практически в два раза, что подтверждает актуальность выбранной нами темы исследования.

Одной из важных задач национального уголовного законодательства на современном этапе развития общества является формирование механизма результативного противодействия существующей киберпреступности (киберугроз и кибератак), а также разработка мер по борьбе и контролю за появлением новых, изощренных видов преступлений, совершаемых в информационном пространстве. Следует отметить, что в настоящее время действующее уголовное законодательство в исследуемой области не в полной мере регулирует отношения, возникающие в сети Интернет, и не готово к быстрому развитию современных информационных (инновационных) технологий, что свидетельствует о необходимости доработки данного вопроса на законодательном уровне.

По нашему мнению, возрастающая роль информационного пространства как интерактивной информационно-коммуникационной среды влечет за собой появление совокупности современных рисков и угроз, повышение уязвимости информационной инфраструктуры и усиление деструктивного воздействия на общественные отношения, которые возможно использовать в киберпространстве.

**Целью дипломной работы** является комплексное исследование криминологической характеристики и предупреждения киберпреступности (по материалам МВД по Республике Татарстан).

Для решения поставленной цели, необходимо решить следующие **задачи**:

– сформулировать понятие и сущность современной киберпреступности;

– изучить уголовно-правовые и криминологические характеристики киберпреступности

– исследовать все меры предупреждения киберпреступности;

– рассмотреть возможность использования инновационных технологий в борьбе с киберпреступностью по материалам МВД по Республике Татарстан.

**Объектом** исследования выступают общественные отношения, возникающие в процессе предупреждения киберпреступности.

**Предметом** настоящей дипломной работы выступают нормы, регулирующие информационное пространство, а также инновационные технологии борьбы с противоправным использованием информационно-телекоммуникационных технологий, которые могут быть внедрены в деятельность оперативных подразделений МВД по Республике Татарстан.

**Методологическая основа исследования** включает в себя систему методов научного познания, а именно: универсально-методологический, диалектический и структурно-системный; общенаучные (анализ, синтез, индукция, дедукция, сравнение, обобщение) и частнонаучные (уголовно-статистический, изучение нормативно-правовых актов, результаты авторского социологического исследования) методы познания.

**Теоретическую основу исследования** составили научные труды и исследования в рассматриваемой нами проблеме по следующим дисциплинам: криминология, криминалистика, уголовное право, уголовно-процессуальное право, оперативно-розыскная деятельность, психология и педагогика, социология и другие науки.

**Нормативная база исследования включает** Конституцию Российской Федерации, международные правовые нормы, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации и иные нормативно-правовые акты в сфере информационного пространства и преступлений, совершаемых посредством информационно-телекоммуникационных технологий.

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

**Степень научной разработанности проблемы.** Различными аспектами исследования киберпреступности занимались такие авторы, как: В.И. Авдийского, А.И. Анапольская, А.В. Аносов, О.Р. Афанасьева, Л.А. Букалеровой, Н.Э. Войнов, В.А. Гайдук, И.М. Глотина, М.В. Гончарова, Т.А. Гончарова, И.А. Гумаров, А.А. Даненьян, А.А. Дехерт, В.Ю. Дроздов, М.М. Дубровина, М.А. Желудков, А.А. Жиркова, А.Д. Идиятуллов, М.А. Исаева, Я.Г. Ищук, О.С. Капинус, К.О. Карабеков, А.М. Королева, А.А. Магомадов, Х.Б. Магомедова, И.В. Макарова, А.Б. Марданов, Д.Ф. Минзянова, М.С. Мухина, Л.В. Набоков, В.И. Павловец, Т.В. Пинкевич, А.А. Поварчук, А.М. Попов, В.И. Робул, А.В. Сабырбаева, Н.А. Саков, С.М. Сергеев, М.М. Сериева, Е.С. Смольянинов, М.Н. Соловьев, О.А. Степанов, Ю.В. Тарасова, А.В. Терехов, П.А. Титова, П.П. Фантров, Д.М. Фарахиев, Г.Р. Фарахиева, А.А. Харламов, Н.Б. Хлыстова, А.Е. Шалагин, А.К. Шалагина, А.В. Швец, М.М. Шилков, А.А. Шишкин, В.И. Шиян, Х.Л-Э. Шуайпова и др.

**Апробация и внедрение в практику результатов исследования.** Основные положения исследования были использованы на научно-исследовательских конференциях, проходящих в КЮИ МВД России.

**Структура**. Работа состоит из введения, двух глав, включающих девять параграфов, заключения, списка использованной литературы.

# ГЛАВА 1. КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ И ОБЩЕСТВЕННАЯ ОПАСНОСТЬ

## §1. Понятие, виды и сущность киберпреступности

Исследованию киберпреступности и информационного общества в науке уделяется значительное внимание. В.И. Павловец в своих исследованиях под информационным обществом понимает: «общество, в котором социально-экономическое развитие зависит, прежде всего, от производства, переработки, хранения, распространения информации среди членов общества»[1]. С популяризацией инновационных технологий, совершенствованием информационных провайдингов, любой гражданин все больше и больше внедряется в Интернет сферу. В свою очередь Г.Р. Фарахиева пишет, что развитие информационно-коммуникационных технологий оказало существенное влияние на социальные среды несовершеннолетних. Автор считает, что информационная сфера является одной из основных, порождающей преступность, сфер в процессе цифровизации на современном этапе развития общества[2].

Можно сказать, что преступления, которые совершаются в информационном пространстве (киберпреступления), появились одновременно с популяризацией первых компьютерных сетей в экономической сфере. В настоящее время киберпреступность – проблема всего человечества. Киберпреступность развивается с развитием информационных технологий, что порождает уровень общественной опасности и степень латентности. Развитие научно-технического и социального прогресса обусловило переход от индустриального общества к постиндустриальному, что привело к масштабной

---

[1] Павловец В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования // Альманах современной науки и образования. 2018. № 1 (68). С. 104.

[2] Фарахиева Г.Р. Социальная среда как фактор вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов // Вестник Казанского юридического института МВД России. 2021. Т. 12. № 4(46). С. 555-560.

цифровизации человечества, однако наряду с этим, в равной мере, развивается и преступность, тем самым, увеличивая теневой сегмент информационного пространства.

Киберпреступность – совокупность преступлений, совершаемых в «киберпространстве» с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных. К «киберпреступлению» относится любое преступление, совершенное с применением различных способов и средств создания, обработки, передачи компьютерной информации[1].

«Киберпреступность» описывает ряд обстоятельств, при которых технология используется как средство совершения преступления. Благодаря быстрому росту инновационных достижений возникают многочисленные и постоянно меняющиеся проблемы для правительства и правоохранительных органов. Следует учитывать тот факт, что «преступный мир всегда на шаг впереди правоохранительной системы, а стремительный прогресс и процессы глобализации еще больше усложняют проблемы, связанные с противодействием преступности»[2]. Преступники одни из первых используют в своей преступной деятельности достижения технического прогресса.

Как правило, большая часть киберпреступлений обладают определенными характерными чертами, к числу которых следует относить:

1. Уровень латентности;

2. Трансграничность;

3. Специфичность подготовительных мероприятий (высокий уровень интеллектуальных возможностей);

---

[1] Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. 2018. №8. С. 12.

[2] Group-IB назвала ключевые тенденции киберпреступлений в период пандемии // Group-IB. URL: https://www.group-ib.ru/media/covid-cybercrime-trends/ (дата обращения: 11.09.2022).

4. Отсутствие непосредственного контакта – дистанционный формат преступного посягательства[1].

В нынешних реалиях киберпреступность включает в себя довольно масштабный перечень преступлений. Ряд авторов пишут, что в последние несколько лет информационное пространство применяется во всех циклах торговли людьми и наркотических средств и т.п.[2]

В свою очередь, П.А. Титова и др. авторы в своих исследованиях киберпреступность рассматривают в следующих видах:

1. Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям, а также выведение данных у наивных людей для доступа к банковским счетам.

2. Фарминг, т.е. скрытое перенаправление на ложный *IP*-адрес.

3. Распространение порнографии в информационной среде. В настоящее время в киберпорнографии набирает оборот детская порнография в информационном пространстве.

4. Незаконный оборот наркотических средств, психотропных веществ или их аналогов.

5. Кибертерроризм, выражающийся, как правило, в призывах (вербовке) к совершению террористических актов и т.д.[3]

Другие авторы предлагают рассматривать такие виды киберпреступности, как:

1. *DDoS*-атаки.

Это атака на сайт, основной целью которой является выведение его из строя путём подачи большого количества ложных запросов. В результате такой

---

[1] Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. №1. С. 104-106.

[2] Киберпреступность: понятие, виды / Н. А. Саков, А. А. Поварчук, М. М. Шилков, А. М. Королева // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции, Санкт-Петербург, 30 мая 2020 года. СПб: ГНИИ «Нацразвитие», 2020. С. 31-35.

[3] Киберпреступность / П. А. Титова, А. А. Жиркова, И. В. Макарова, А. В. Терехов // Инновационные научные исследования. 2021. № 2-1(4). С. 145.

атаки сервера, обслуживающие сайты, вынуждены обрабатывать чрезмерный объём ложных запросов, и сайт становится недоступным для простого пользователя. Популярными жертвами таких атак становятся коммерческие и информационные сайты. Хакеры в последнее время используют такой вид атак с целью вымогательства, требуя денег за прекращение атаки, или ведут информационную войну.

2. Кража личных данных.

Кража личных данных – любой вид мошенничества, в результате которого происходит похищение личной информации, к примеру паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в Интернете.

3. Онлайн мошенничество.

Обычно они представляют собой рекламу или спам, содержащие обещания вознаграждений или предложения нереальных сумм денег. Мошенничество в Интернете включает заманчивые предложения, которые «слишком хороши, чтобы быть правдой», и при нажатии на них могут вызывать помехи со стороны вредоносных программ и подвергать риску информацию[1].

Т.А. Гончарова и Л.В. Набоков в своих исследованиях рассматривают следующие виды киберпреступности:

1) неправомерный доступ к компьютерной информации;

2) распространение вредоносного программного обеспечения;

3) компьютерные хакерские атаки;

4) распространение клеветнической, экстремистской, порнографической и иной незаконной информации;

---

[1] Магомадов А.А., Шуайпова Х.Л.Э. Киберпреступление // Вопросы физико-математического образования : материалы XIII студенческой научно-практической конференции, Грозный, 16 мая 2020 года. – Махачкала: Чеченский государственный педагогический университет, ИП Овчинников М.А. (Типография Алеф), 2020. С. 229-232.

5) незаконная обработка, передача и хранение информации[1].

А.Е. Шалагин помимо вышеуказанных преступлений к киберпреступлениям относит:

– взлом учетных почт компаний и организаций (*BEC*);

– торговля контрафактной продукцией и лекарствами, поддельными документами;

– *spoofing*-атаки, которые направленны на маскировку действий для похищения данных граждан; популяризацию вредоносных программ;

– выявление поддельных платежных терминалов *PoS* для конфискации закрытой информации о банковских картах физических лиц[2];

– кибербуллинг (киберсталкинг)[3];

– популяризация ненависти, ксенофобии, геноцида, нарушения авторских прав и др.[4]

Д.М. Фарахиев рассматривает коррупцию и преступления коррупционной направленности в качестве противоправного деяния, которое может совершаться посредством информационно-телекоммуникационных технологий[5].

Таким образом, на основе проведенного исследования необходимо заявить, что киберпреступность представляет собой информационную и

---

[1] Гончарова Т.А., Набоков Л.В. Киберпреступность в России: проблемные аспекты и предупреждение преступности // Инновационная экономика и право. 2022. № 1(20). С. 121.

[2] Шалагин А.Е., Идиятуллов А.Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. 2021. Т. 12. № 2(44). С. 227-235.

[3] Шалагин А.Е., Идиятуллов А.Д., Шалагина А.К. Причины девиантного поведения подростков и молодежи // Modern Science. 2020. № 12-4. С. 274-278.

[4] Шалагин А.Е., Идиятуллов А.Д. Новые тенденции преступности в XXI веке: глобализация, цифровизация, социальный контроль // Modern Science. 2020. № 11. С.131-134.

[5] См.: Фарахиев Д.М. Коррупция как угроза национальной безопасности: пути противодействия // Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения : Материалы международной научно-практической конференции, Санкт-Петербург, 08 апреля 2022 года / Сост. Н.В. Мячин. СПб: Санкт-Петербургский университет МВД России, 2022. С. 462-467; Фарахиев Д.М., Минзянова Д.Ф. Перспективы внедрения информационно-коммуникационных технологий в деятельность оперативных подразделений полиции по противодействию коррупции // Современная наука. 2022. № 1. С. 60-63; Гумаров И.А., Фарахиев Д.М. Технология blockchain как средство противодействия коррупции // Научный компонент. 2022. № 1(13). С. 81-87.

техническую стороны процесса цифровизации общества, которая детерминирует преступность, совершаемую посредством информационных технологий. На наш взгляд, киберпреступность образует неразрывное звено, синтез нескольких сфер отношений, представленных информационной и технической составляющей.

Поскольку термин законодательно не закреплен, мы предлагаем следующее авторское определение киберпреступности, под которым мы понимаем общественно опасное деяние или совокупность преступлений, совершаемых посредством информационно-телекоммуникационных технологий (включая технические средств, компьютерные сети и системы, а равно их программные элементы).

## §2. Правовое регулирование киберпреступности

В современных условиях ежедневной цифровизации населения киберпреступность активно развивается и инвестирует большие средства в развитие и решение криминальных задач. Киберпреступники уделяют больше внимания новым цифровым технологиям, таким как: большие данные, искусственный интеллект, квантовые технологии, технологии беспроводной связи, системы распределенного реестра (блокчейн), производственные технологии, промышленный Интернет, компоненты робототехники и сенсорики, технологии виртуальной и дополненной реальностей.

Само словосочетание «киберпреступность» говорит о том, что преступления совершаются непосредственно через сеть Интернет либо через информационно-телекоммуникационные сети. Преступник совершает преступление удаленно, и неважно, к какому виду соучастника преступления

он относится, будь то исполнитель, организатор, подстрекатель или же пособник[1].

Основы кибербезопасности были заложены в Доктрине информационной безопасности Российской Федерации (далее – Доктриной ИБ), утвержденной Указом Президента Российской Федерации № 46 от 5 декабря 2016 года. Обеспечение кибербезопасности в соответствии с Доктриной ИБ, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации, осуществляющими федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере, и осуществляет правовое, оперативно-розыскное, научно-технического направления на обнаружение, предотвращение и отражение киберугроз[2].

В сфере правового регулирования киберпреступности отдельного внимания заслуживает проект Конвенции ООН «О противодействии использованию информационно-коммуникационных технологий в преступных целях», созданный российскими разработчиками. В нём представлены цели, заключающиеся в профилактике выявления правонарушений в информационной сфере на ранних стадиях, обеспечение наказуемости данных нарушений, непосредственное сотрудничество стран в решении подобных вопросов, заключающееся в создании и развитии кадров и оказания помощи друг другу (ст. 1).[3]

---

[1] Швец А.В., Гайдук В.А. Проблемы и особенности выявления, документирования и правового регулирования киберпреступности в Российской Федерации // Вестник Амурского государственного университета. Серия: Гуманитарные науки. 2021. № 94. С. 17-21.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50, ст. 7074.

[3] О противодействии использованию информационно-коммуникационных технологий в преступных целях: Проект Конвенции ООН от 29.06.2021 URL: unodc.org

В данной конвенции подробно раскрываются многие специфичные информационные термины. Например, «бот-сеть» означает два и более устройств ИКТ, в модуль которых скачаны вирусные программы, управление которыми производится тайно. Установлена также ответственность за незаконное получение информации в электронной форме (гл. 2), описываются действия, связанные с раскрытием лиц, подозреваемых в данном нарушении (ст. 48). Для эффективности борьбы с подобными инцидентами, в ст. 57 Конвенции каждому государству предлагается сформировать информационный центр, который будет работать круглосуточно.

Анализируя данную Конвенцию, следует отметить, что в ней собрано значительное количество сведений, благодаря которым можно усовершенствовать меры по борьбе с киберпреступностью. В ней: представлена конкретная программа по осуществлению обучения квалифицированных специалистов, занимающихся осуществлением информационной безопасности; акцентируется внимание на необходимости проведения всеми странами единой политики в борьбе с киберпреступностью и активной взаимопомощи. Исходя из совокупности всех этих факторов, данный проект переведён с русского на многие языки и в электронной форме был официально опубликован на официальных сайтах ООН и МИД России.

К сожалению, против этого проекта выступили представители незначительного числа делегаций, приводившие в качестве главного контраргумента отсутствие необходимости внесения дополнительных изменений в Конвенцию, принятую в Будапеште в 2001 г. По их мнению, представленных в ней положений достаточно, чтобы разрешать все имеющиеся в информационной сфере вопросы. По-видимому, такая неоднозначная реакция обусловлена тем, что не все страны ООН имеют желание проектировать долгосрочный алгоритм сотрудничества в решении вопросов борьбы с

киберпреступностью. Вследствие этого российский проект не получил должного уровня одобрения[1].

Итак, одними из ключевых правовых регуляторов информационной безопасности в Российской Федерации выступают:

– Конституция Российской Федерации;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

– Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ;

– Указ Президента РФ от 02.07.2021 года № 400 «О Стратегии национальной безопасности Российской Федерации»;

– Доктрина информационной безопасности РФ 2016 года, утверждена Указом Президента РФ от 05.12.2016 года № 646.

Обращение политики государства на обеспечение высокого уровня информационной безопасности, противодействие киберпреступлениям, защиты информации и жизнедеятельности граждан от преступного посягательства на сферы функционирования страны является важной задачей, способной при ее грамотной реализации защитить информационные ресурсы от деструктивного воздействия и предотвратить утечку и разглашение информации[2].

На сегодняшний день компьютеризация общества коснулась всех сфер жизнедеятельности человека, обусловив необходимость формирования механизма правового регулирования отношений, возникающих в сфере компьютерной информации.

Интернет-пространство формирует новую сферу для жизни и взаимодействия современного общества, в связи с чем количество преступных деяний в сети «Интернет» значительно повышается с каждым годом, а уровень

---

[1] Даненьян А.А Международное правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261-269.

[2] Соловьев М.Н. Правовые основы регулирования противодействия киберпреступности, безопасность личности в информационном пространстве // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : Сборник статей Международной научно-практической конференции, Москва, 30 октября 2019 года / отв. ред. В.О. Лапин. М.: Академия управления МВД России, 2019. С. 214-220.

раскрываемости киберпреступлений, по данным Генеральной прокуратуры РФ, составляет 4,4%[1], что объясняется доступностью и широким распространением цифровых технологий.

Несмотря на пробелы в законодательстве, декларативность и противоречия предписаний, отсутствие единого системного, комплексного подхода к регулированию информационной безопасности, противодействию киберпреступности, Россия постепенно выстраивает определенную линию национальной стратегии защиты информации и своих граждан в глобальном информационно-цифровом пространстве, тесно сотрудничает с другими странами в области разработки и подписания совместных международных соглашений по борьбе с киберпреступностью, защиты интересов личности от преступных посягательств на персональные данные, выстраивает стратегию перехода на отечественное программное обеспечение и программно-аппаратные комплексы защиты информации.

## §3. Уголовно-правовая характеристика киберпреступности

Традиционно уголовно-правовая классификация выражается «в систематизации преступлений по определенным признакам, предусмотренным в УК РФ». Такие признаки (критерии классификации преступлений) последовательно различаются: на уровне единичного – дифференциации составов преступлений – ими служат отдельные признаки составов преступлений (главным образом объективной стороны), на уровне особенного (Особенной части УК РФ) – родовой объект, на уровне всеобщего (Общей части УК РФ) – общественная опасность в целом, ее характер и степень. С учетом множества закрепленных законодателем объективных и субъективных признаков преступлений (по которым они могут быть разделены на группы)

[1] О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Официальный сайт Генеральной Прокуратуры. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения 15.09.2022)

расширяются как возможности классификации преступлений, так и варианты классификаций. Это, в свою очередь, требует оценки пригодности тех или иных классификаций для уголовно-правового анализа.

Таким образом, в доктрине уголовного права компьютерные преступления могут быть представлены: как преступления в сфере компьютерной информации; информационные компьютерные преступления; киберпреступления (интернет-преступления). К преступлениям в сфере компьютерной информации относятся: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ)[1].

Круг информационных компьютерных преступлений образуют преступления, совершаемые в сфере использования информационно-телекоммуникационных (компьютерных) технологий. Это преступления в сфере компьютерной информации, а также иные преступления, которые совершаются в сфере использования информационно-телекоммуникационных (компьютерных) технологий.

Объект киберпреступности в свою очередь различается.

Во-первых, непосредственным объектом преступления, предусмотренного ст. 274 УК РФ является общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Во-вторых, непосредственным объектом преступления, предусмотренного ст. 272 УК РФ является общественные отношения,

---

[1] Шишкин А.А. Уголовно-правовая характеристика киберпреступности // Молодежь и наука: шаг к успеху : Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок молодых ученых. В 5-ти томах, Курск, 19–20 марта 2020 года / Ответственный редактор А.А. Горохов. Курск: Юго-Западный государственный университет, 2020. С. 373-375.

обеспечивающие правомерный доступ, создание, обработку, преобразование и использование охраняемой законом компьютерной информации самим создателем, а также потребление ее иными пользователями.

В-третьих, непосредственным объектом преступления, предусмотренного ст. 159.6 УК РФ является общественные отношения, сложившиеся в сфере электронного документооборота.

В-четвертых, непосредственным объектом преступления, предусмотренного ст. 228.1 УК РФ является общественные отношения в сфере оборота наркотических средств, психотропных веществ или их аналогов, обеспечивающие безопасность здоровья населения.

Поскольку объект киберпреступлений может быть разный, так, и предмет преступного посягательства в сфере информационного пространства может быть различный.

Объективная сторона киберпреступлений характеризуется действием, с высокой степенью общественной опасности, поскольку совершаются с использованием информационно-телекоммуникационных технологий. Также, в правоприменительной практике суды указывают на причинно-следственную связь и последствия, которые наступили в момент информационного посягательства и после такового.

Так, к примеру, ДД.ММ.ГГ, действия гражданина 1 заключались в приобретении smart-карты «…» с индивидуальным кодом «…», которая была предназначена для подключения к спутниковому телевидению через приемник. Помимо указанных действий, гражданин 1 имел корыстную заинтересованность[1].

Субъект – физическое вменяемое лицо, достигшее возраста уголовной ответственности. В ряде случаев, преступником может быть специальных субъект, с дополнительными признаками.

---

[1] Приговор Хасавюртовского городского суда № 1-261/2020 от 20 июля 2020 г. по делу № 1-261/2020. URL: https://sudact.ru/regular/doc/SlYwK6TxKKNT/ (дата обращения: 20.09.2022)

Субъективная сторона киберпреступлений выражается в форме умысла, как правило прямого. В некоторых преступлениях большое внимание уделяется целям или мотивам.

Например, 11 мая 2020 года, в дневное время, гражданин А.Ю.В. и С.Д.Н., каждый из которых был в состоянии опьянения, вызванного употреблением алкоголя, находились на улице по адресу: адрес, где гражданин С.Д.Н. нашел банковскую карту адрес выпущенную на имя В., оборудованную системой бесконтактных платежей, и утерянную по невнимательности В.. В этот момент у гражданина С.Д.Н. возник преступный умысел, направленный на мошенничество, то есть хищение денежных средств с использованием электронных средств платежа, путем умолчания перед работниками торговых организаций и сферы услуг о незаконном владении им указанной банковской картой[1].

В другом случае А. умышленно, тайно, из корыстных побуждений похитил следующее имущество: из комнаты – лежащий на диване мобильный телефон марки «Айфон 7», стоимость которого согласно заключению специалиста №200/2-15 от 27.05.2020г. составляет 14000 рублей, вместе с не представляющими материальной ценности силиконовым чехлом, защитным стеклом, сим-картой оператора сотовой связи ТЕЛЕ2, банковской картой ПАО «Сбербанк» (№), а также из кухни – не представляющие материальной ценности банку кофе, пачку сигарет, а всего имущество на общую сумму 14000 рублей, принадлежащее Потерпевший №1, причинив последней значительный материальный ущерб на указанную выше сумму[2].

Таким образом, можно сделать вывод о том, что киберпреступность — это любое противоправное действие или серия действий, которые осуществляются с использованием технологий и интернета, направленные на

---

[1] Приговор Чусовского городского суда № 1-175/2020 от 24 ноября 2020 г. по делу № 1-175/2020. URL: https://sudact.ru/regular/doc/kQeGaLsl08H8/ (дата обращения: 20.09.2022).

[2] Приговор Коминтерновского районного суда г. Воронежа № 1-525/2020 от 24 июля 2020 г. по делу № 1-525/2020. URL: https://sudact.ru/regular/doc/nV1W3qNJLirI/ (дата обращения: 20.09.2022).

нанесение ущерба физическим или юридическим лицам, их правам и интересам. К киберпреступлениям относятся кража и хищение информации, незаконный доступ к ресурсам, распространение вирусов, мошенничество, кибершпионаж, кибертерроризм и др. Киберпреступность стала серьезной проблемой в наше время, и требует специальных знаний и навыков для противодействия ей.

Судебно-следственная практика, статистические данные, а также материалы, представленные средствами массовой информации, свидетельствуют о том, что киберпреступления образуют такие противоправные деяния, которые закреплены в Главе 28 действующего Уголовного закона, а также иные действия, закрепленные в Уголовном Кодексе РФ, которые сопряжены с использованием информационно-коммуникационных технологий.

# ГЛАВА 2. ОСОБЕННОСТИ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ КИБЕРПРЕСТУПНОСТИ

## §1. Состояние и динамика киберпреступности в России и в Республике Татарстан

За последние годы в Российской Федерации отмечается рост преступлений как в сфере информационных технологий, так и совершаемых с их использованием. Виды киберпреступлений весьма разнообразны и связаны со всеми сферами общественных отношений. Сегодня жертвами преступников в виртуальном пространстве могут стать не только люди, но и целые государства. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете[1].

Анализируя судебную, а также следственную практику, стоит отметить, что наиболее распространенными преступлениями с применением информационно-телекоммуникационных технологий являются создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ); мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Следует подчеркнуть, что мошенничество с использованием платежных (банковских) карт (ст. 159.3 УК РФ) в 2020 г. выросло в 8 раз по сравнению с аналогичными преступлениями, предусмотренными гл. 28 УК РФ[2].

---

[1] Карабеков К.О. Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2022. № 22-2. С. 25-27.

[2] Войнов Н.Э. Киберпреступность в Российской Федерации: современное состояние и актуальные проблемы // Киберпреступность: риски и угрозы: сб. ст. рос. научно-практ. круглого стола с междунар. участием (Санкт-Петербург, 11 февраля 2021 г.). СПб.: Астерион, 2021. С. 143-147.

Рассмотрим количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий за 2019 по 2022 гг. (рисунок 1):

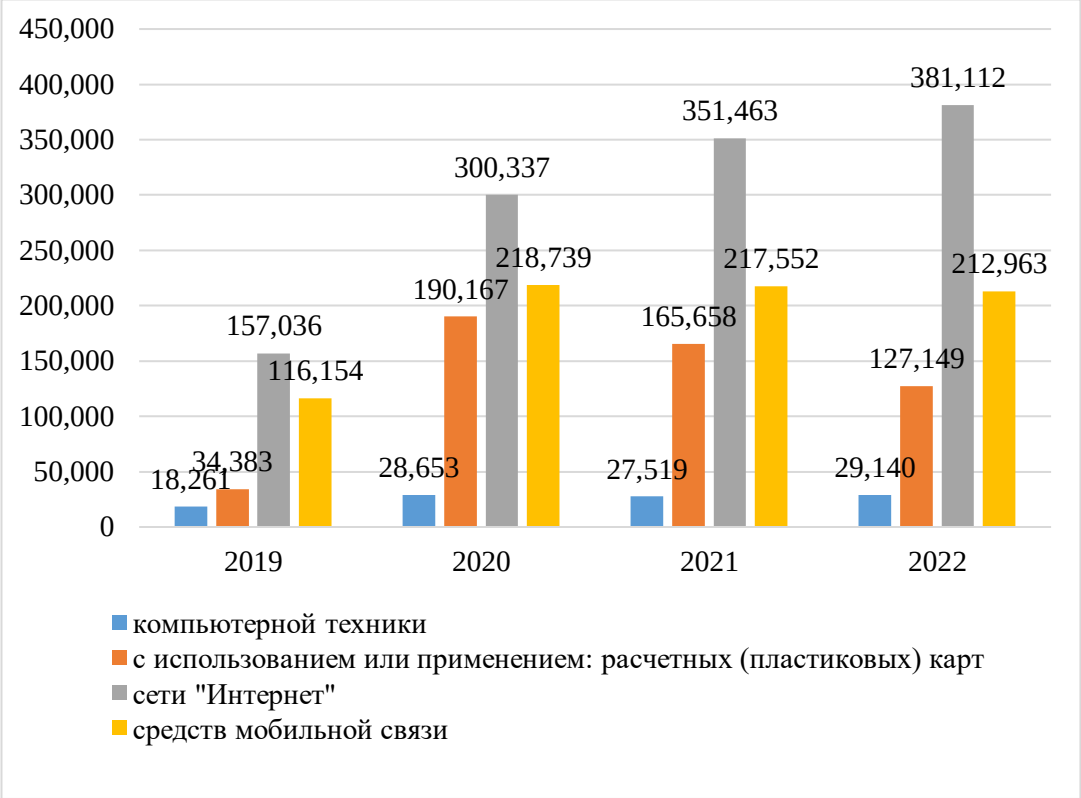



Рисунок 1. Количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий за 2019 по 2022 гг. на территории Российской Федерации

Год за годом стабильными остаются показатели киберпреступлений. Также следует отметить, что имеется прирост количества преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (рисунок 2):

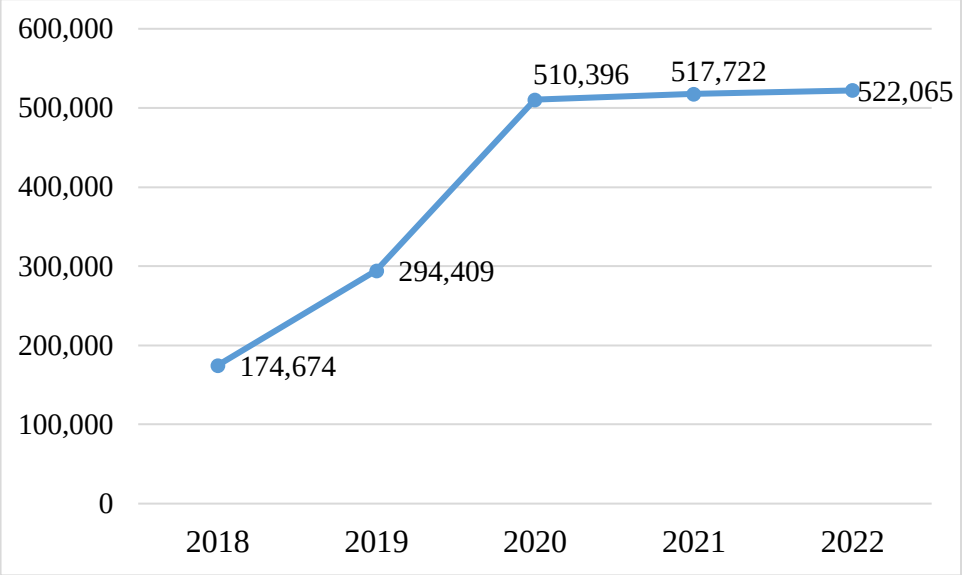



Рисунок 2. Количество зарегистрированных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий в период времени с 2019 по 2022 гг. на территории Российской Федерации

Наиболее распространенные преступления, совершаемые посредством информационно-телекоммуникационных технологий, можно представить ниже (рисунок 3):

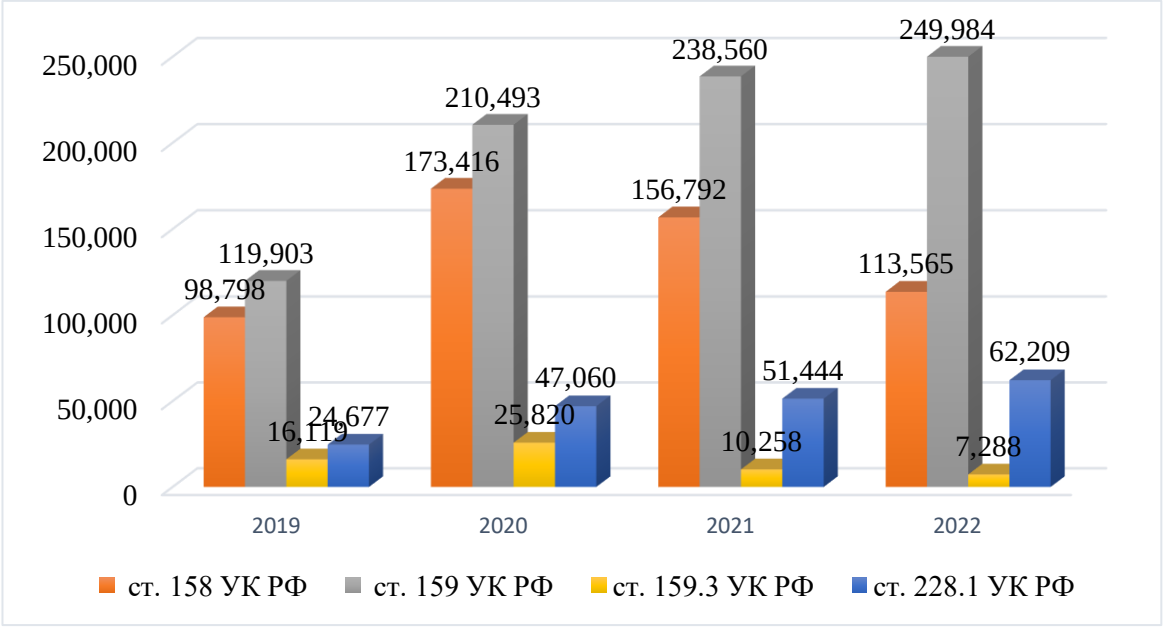



Рисунок 3. Количество зарегистрированных преступлений, предусмотренных ст.ст. 158, 159, 159.3 и 228.1 УК РФ на территории Российской Федерации

С развитием информационных технологий появляются широкие возможности для совершения различных киберпреступлений, в частности, «псевдо онлайн» торговля с предоплатой; с использованием электронных платежных систем; телефонное мошенничество с использованием персональных данных пользователей банковских продуктов (фишинг); банковские операции; вымогательство денежных средств за обеспечение сохранности данных; сохраняют свою актуальность преступления, связанные с игровыми и развлекательными порталами с незаконным контентом; продолжает сохраняться доминирующая роль *IT*-компаний, осуществляющих разработку антивирусного программного обеспечения и поддержку современных информационных сервисов; мошенничество на сайтах бесплатных объявлений (например, «Авито», «Юла»), кражи денежных средств с банковских счетов юридических и физических лиц, взломы хранилищ персональных данных пользователей (так называемое «Облако»); появляются новые виды вирусов.

Повышение роли информационно-телекоммуникационных технологий отражается на современных тенденциях киберпреступности. Сохраняется актуальность правонарушений, направленных на извлечение персональных данных граждан и организаций с целью их незаконного использования. Несмотря на активную работу правоохранительных органов, продолжает оставаться актуален кибертерроризм, носящий завуалированный характер. Совершение тяжких преступлений, связанных с особой жестокостью и совершением актов насилия посредством высоких технологий, преступления, угрожающие общественной безопасности, например, создание «групп смерти» в сети «В Контакте». Нарушение авторских прав (незаконное распространение контента, имеющего ограничения авторскими правами), совершенствуются преступления, совершаемые с технологиями использования искусственного интеллекта для автоматизации прикладных задач. Продолжают пользоваться популярностью у хакеров специальные программы, незаметно работающие на

любых устройствах и использующие их мощности для майнинга криптовалют, распространяются вирусы, использующие уязвимость устаревших компьютерных систем, компонентов компьютеров и серверов. Наблюдается высокий риск утечки биометрических данных в связи с тем, что в настоящее время осуществляется их активное накопление (в финансовой, правоохранительной, миграционной и иных сферах). Усиливается организованность хакеров и хакерских групп в связи с расширением сфер криминальных интересов, усложняются применяемые преступные схемы, поскольку существующие системы безопасности являются многоступенчатыми и требуют привлечения навыков нескольких узконаправленных специалистов, в связи с увеличением количества техники и поддерживающего её программного обеспечения растёт число узкоспециализирующихся лиц, совершающих киберпреступления (хакеры, фрикеры, крэкеры, вирусоописатели, вирмайкеры, крипторы, скамеры и т.п.). Сохраняется стабильным число преступлений, связанных с кибернаёмничеством, а также с организацией незаконного оборота наркотических средств и психотропных веществ, их прекурсоров, оружия и боеприпасов и иных предметов, запрещенных к свободному обороту, а также с распространения проституции, нелегальной миграцией, порнографией, с использованием сети Интернет. Усиливаются интересы киберпреступников, направленные на взлом компьютерных систем и баз данных (например, мобильных операторов с целью получения паспортных данных пользователей, банковских карт, данных электронных кошельков и т.п.). Сохраняется высокая роль *IT*-компаний, осуществляющих разработку антивирусного программного обеспечения и поддержку современных информационных сервисов, которые укрепляют защиту программных продуктов и обеспечивают функционирование информационных систем. Для совершения масштабных преступлений киберпреступники объединяются в организованные группы или преступные сообщества, в том числе транснациональные, появляются новые вирусы, например, новые виды шифровальщиков, шифрующие сведения из массива

информации и впоследствии дают повод злоумышленникам для вымогательства денежных средств за их дешифровку[1].

Продолжают сохраняться риски совершения киберпреступлений с территории Украины и иных недружественных стран, совершаемых на почве политических разногласий. Имеются тенденция роста преступлений в сфере высоких технологий в глобальном масштабе и на государственном уровне, так как экономически развитые страны различными деструктивными способами, в том числе используя нетрадиционные методы, будут стараться влиять на рост экономик развивающихся стран, в частности, путем изучения общественного мнения, с использованием конфиденциальных данных граждан и навязывая им контент, дискредитирующий действующую государственную власть; путем скрытого финансирования общественных объединений, целью которых является подрыв государственного строя; путем внедрения в информационные системы предприятия вредоносного программного обеспечения, например, с целью шпионажа и др.

Таким образом, киберпреступность может принимать различные формы: от атак на конкретные устройства, нацеленные на получение несанкционированного доступа, вымогательства и кражи денег путем блокирования доступа к файлам или компьютерным системам до атак на облачную инфраструктуру, конечная цель которых является компрометация виртуальных машин и использование их в качестве оружия.

Очевидно, что избежать этого возможно путем профилактики киберпреступлений, основным важным фактором которой является соблюдение мер информационной безопасности, а также своевременные разъяснения сотрудниками банка мер безопасности при использовании гражданами различных банковских продуктов. Представляется необходимым объединять усилия не только на государственном уровне, но и на международной арене в

---

[1] Тарасова Ю.В. Тенденции киберпреступности в Российской Федерации // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции, Санкт-Петербург, 29 сентября 2021 года. СПб: ГНИИ «Нацразвитие», 2021. С. 6-13.

борьбе с данными видами преступности, вовремя реагировать на киберинциденты и ставить в приоритет кооперацию и обмен оперативной информацией в целях обеспечения глобальной кибербезопасности.

Итак, следует отметить, что официальные статистические данные не отображают реальную картину происходящего, поскольку велика степень латентности. В связи с чем, в целях понимания феномена киберпреступности, предлагаем рассмотреть динамику и тенденцию развития киберпреступности в нынешней России:

1. Увеличение роли инновационных технологий, которые порождают увеличение киберпреступности; повышение организованности преступных сообществ, а так же расширение границ преступного информационного мира;

2. К наиболее распространенным киберпреступлениям относятся:

– мошенничество (в любом виде);

– хищение денежных средств;

– вымогательство;

– незаконный оборот наркотических средств, психотропных веществ или их аналогов;

– распространение порноматериалов;

– кибербуллинг;

– кибертерроризм.

3. Киберпреступность будет трансформироваться в целях сокрытия преступных действий.

Если ранее совершавшие эти преступления лица, обладали специальными познаниями в области IT-технологий, то в настоящее время за киберпреступлениями стоят частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически, в том числе и по заказу организованных преступных групп.

## §2. Причины и условия совершения киберпреступлений

Криминальный комплекс киберпреступности становится все более многофункциональным, что связано с поступательным совершенствованием информационных (инновационных) технологий и их широким применением, как физическими лицами, так и иными лицами во всех сферах общественной и государственной жизни общества. Основополагающим факторам, влияющим на киберпреступность в составе общей преступности в стране, помимо общесоциальных факторов, является несовершенство правового регулирования общественных отношений в информационном пространстве.

*Правовые причины и условия, способствующие совершению киберпреступности.*

Правовое регулирование информационного пространства на сегодняшний день так и не нашло свое отражение в законодательстве России. Отрицательные аспекты общественных проявлений имеют место тогда, когда отсутствует социальный и общественный контроль. Реализация данного вида контроля в сфере киберпреступности затрудняется в связи с объективными причинами. Следует отметить, что низкий уровень правовой культуры и правовой регламентации в информационном пространстве «порождает» правовой нигилизм и отсутствие безопасности в интернет-пространстве[1].

В то же время законодатель слишком мало внимания уделяет охране общественных отношений в области информационных технологий.

*Социально-экономические факторы в детерминации киберпреступности проявляются в трех группах социальных явлений.*

1. Социальные явления, которые связаны с прогрессом:

– развитие инновационных технологий и внедрение их во все сферы жизнедеятельности общества;

– увеличение количества пользователей Интернет-пространства;

---

[1] Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общей редакцией О. С. Капинус. 2-е изд., перераб. и доп. М. : Юрайт, 2022. С. 1000.

– популяризация электронных кошельков и оплаты посредством Интернет-пространства;

– отсутствие прямого контакта при совершении разнообразных операций в Интернет-пространстве.

Вышесказанное подтверждает рост мошенничества, незаконного оборота наркотиков, порнографии, хищений персональных данных, кибербуллинга, кибертерроризма и др.

2. Экономический кризис и его отрицательный результат:

– низкий уровень экономического развития страны;

– криминализация экономической деятельности

– высокий уровень безработицы.

3. Виртуализация жизнедеятельности, распространение социальных сетей, сервисов по определению местонахождения, в частности доступа в них со смартфонов, и, как результат, применение преступниками «пробелов» в программном обеспечении телефонов (смартфонов), и невозможность обеспечить надежность источников их разработки[1].

*В качестве организационно-технических факторов киберпреступности выступают следующие обстоятельства.*

Методы, способы и средства совершения кибепреступлений в настоящее время изощрены и идут на шаг впереди от систем безопасности информационных сетей и систем, а также мер противодействия и предупреждения. В данном аспекте следует говорить о халатности руководителей и (или) ответственных лиц по вопросам обеспечения безопасности данных и защите сведений. При этом не следует забывать и о обычных пользователей Интернет-пространства.

---

[1] Исаева М.А. Детерминанты информационных преступлений // Технологии формирования правовой культуры в современном образовательном пространстве : Материалы V Всероссийской научно-практической конференции с международным участием, Волгоград, 27 апреля 2021 года. Волгоград: Волгоградский государственный аграрный университет, 2021. С. 251-256.

К организационно-техническому блоку детерминант киберпреступности следует также относить низкий уровень профессионализма сотрудников правоохранительных органов, в компетенцию которых входит борьба с киберпреступностью; слабое инфраструктурное оснащение правоохранительных органов; дефицит кадрового потенциала.

Правоохранительные органы, занимающиеся борьбой с киберпреступностью зачастую, не обладают необходимыми специальными знаниями в сфере инновационных (компьютерных) технологий, что в последнем сказывается на процессе раскрытия и расследования преступлений, совершаемые посредством информационных технологий.

*Самодетерминация киберпреступности* как преступный фактор является результатом невозможности контролировать данные, содержащиеся в информационном пространстве. В данном контексте следует говорить о любых данных (к примеру, Интернет-ресурсы, связанные с детской порнографией; со способами незаконного приобретения незаконного оборота наркотических средств; со способами незаконного приобретения информации (персональных данных) и т.п.). К информации, носящей конфиденциальных характер, доступ доступен лишь определенному количеству пользователей (либо одному человеку).

Как уже отмечалось, киберпреступность обладает высоким уровнем латентности, что сказывается на преступности в целом. Зарегистрированные преступления, как правило, связаны с большими финансовыми потерями, и если они не являются значительными, жертвы преступлений предпочитают не сообщать о них в органы внутренних дел; с другой стороны – жертвы преступлений не желают предавать данные факты огласке в целях сохранения своей социального статуса или репутации (характерно для юридических и должностных лиц)[1].

[1] Дехерт А.А., Фантров П.П. Детерминанты гиперлатентности преступлений, совершенных в виртуальном пространстве // Высокие технологии и инновации в науке : Сборник избранных

Высокая латентность и появление все новых криминальных угроз в виртуальном пространстве снижают эффективность деятельности по предупреждению киберпреступности, которая, в отличие от субъектов профилактики, ограниченных законодательными рамками, а также границами своих государств, языковыми, политическими, религиозными и иными особенностями, не признает национальных границ, является трансграничной. Не лишним будет отметить, что трудности расследования такого рода преступлений связаны с растущими скоростями обмена информацией и перманентным появлением технологических новаций. Специфичность указанных характеристик требует межгосударственного подхода к противодействию киберпреступлениям, эффективность которого недостижима без международного сотрудничества.

Следует выделять и *психологические факторы, детерминирующие киберпреступность*.

В процессе исследования мы выделяем следующие особенности киберпреступности:

– «самодостаточность», которая обуславливается наличием социально-экономических, культурно-нравственных, в том числе субкультурных и других социальных институтов, позволяющие населению представить иллюзию полноценного существования;

– конфиденциальность. Информационно пространство – идеальное место для «бегства» от реальности, проблем, ответственности, трансформации социальной роли и статуса и др., не требующее колоссальных изменений;

– невидимость, которая дает возможность избежать психологических контактов и связанных с ними возможных отрицательных последствий;

– минимизация власти через опосредованное восприятие атрибутов более высокого социального положения и способность их игнорировать;

---

статей Международной научной конференции, Санкт-Петербург, 27 ноября 2021 года. СПб: ГНИИ «Нацразвитие», 2021. С. 229-232.

– развитие информационной среды, киберкультуры в процессе взаимодействия.

К психологическим факторам киберпреступности может быть отнесено такое явление современного мира, как консьюмеризм – психология потребления. Это формирование определенной прослойки индивидуалистов с повышенными запросами, живущих только сегодняшним днем и считающих возможным удовлетворение потребностей любыми средствами. Эти люди ориентированы на быстрое достижение успеха, обладают определенными способностями для этого, склонны к риску.

Таким образом, вышеуказанные причины и условия, детерминирующие киберпреступность необходимо принимать во внимание в целях предупреждения преступлений, совершаемых посредством информационно-телекоммуникационных технологий, в том числе минимизации киберпреступности.

## §3. Криминологическая характеристика личности преступника, совершающего киберпреступления

Криминологическая характеристика личности преступника, совершающего киберпреступления является неотъемлемым элементом криминологического исследования в целом. Исследованием личности преступника, в том числе киберпреступника занимались множество авторов.

В криминологии под личность преступника следует понимать комплекс социально значимых качеств человека, которые сформировались в процессе коммуникации и обусловили криминальное поведение человека. С учетом указанного, В.И. Робул характеризует киберпреступника как «человека, который совершает противоправное деяние в контексте киберпреступности»[1]. По нашему мнению, данное определение, приведенное В.И. Робулом является

[1] Робул В.И. Некоторые характеристики личности киберпреступника // Международный научный журнал «Вестник науки», 2019. №8. С. 21-23.

весьма узким, так как автор рассматривает лишь уголовно-правовую характеристику личности преступника, совершающего преступления посредством информационно-телекоммуникационных технологий, не принимая во внимание психологические и криминологические аспекты.

На наш взгляд, наиболее актуальное определение личности приведено в исследовании А.Б. Марданова. Так, по мнению автора, личность киберпреступника – это: «совокупность социально значимых свойств личности, которые привели к совершению преступления в сфере компьютерной информации, совершенного умышленно или по неосторожности»[1]. По мнению О.Р. Афанасьева под личности киберпреступника следует понимать комплекс социально-демографических, морально-психологических и уголовно-правовых качеств личности, которые выражаются в совершении киберпреступлений[2].

Исследование характерных черт личности киберпреступника дает возможность выделить в отдельную категорию лиц, совершающих преступления в информационном пространства и посредством информационно-телекоммуникационных технологий.

На наш взгляд, личность киберпреступника – это совокупность характерных качеств и черт личности, сформировавшееся под влиянием факторов, детерминирующих преступное поведение в информационном пространстве.

Анализ отечественной и зарубежной практики, изучение научных источников показывают, что возраст компьютерных правонарушителей колеблется в широких границах (в среднем 15-45 лет). Согласно исследованиям, на момент совершения преступления возраст преступников не превышает 20 лет - 33%, 13% – старше 40 лет, 54% – от 20 до 40 лет. Итак, киберпреступники – это не всегда молодые люди, как считали раньше. Свыше 80% таких лиц – мужчины. В то же время процент женщин быстро растет в

---

[1] Марданов А.Б. Криминологическая характеристика личности киберпреступника // Публичное и частное право, 2018. №2. С. 111 – 118.

[2] Криминология : учебник и практикум для вузов / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. М. : Юрайт, 2022. С. 313.

силу профессиональной ориентации некоторых специальностей и должностей, которые занимают в основном женщины. При этом размер убытков от преступлений, совершенных мужчинами, в четыре раза больше, чем от преступлений, совершенных женщинами.

Рассматривая образовательный уровень киберпреступников, следует отметить, что преступники обладают высокими интеллектуальными возможностями и способностями. При этом преступники имеют высшее или неоконченное высшее образование в 29,7% случаев, среднее специальное образование зарегистрировано у 37,4% осужденных (приложение №2). На наш взгляд данные показатели обусловлены необходимостью обладания навыков и умения пользования информационными и инновационных технологиями (к примеру, в сфере программирования).

Следует отметить, что среди осуждённых лиц за киберпреступления 23,4% - рабочие, 14.4 % – служащие (приложение №3).

Нынешние киберпреступники мотивированы в финансово-материальном плане, и торговля конфиденциальной информации, особенно от юридических лиц, стала обычным явлением. Зачастую системные администраторы тех или иных организаций встают на криминальный путь. Данная проблема популяризируется в условиях экономического кризиса и сокращения кадров в компаниях и организациях[1].

Киберпреступники совершают многоэпизодные преступления, которые в большинстве случаев не были привлечены к ответственности в силу латентности данного вида преступления. Согласно данным Судебного Департамента при Верховном Суде РФ следует, что в 8% случаев преступники имеют неснятую или непогашенную судимость, около 5% – рецидивисты. В 14,6% случаев киберпреступления носят групповой характер.

Затрагивая вопрос психического развития и здоровья данной группы преступников, заметим, что более 95 % из них не имеют психических

[1] Криминология : учебник и практикум для вузов / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. М. : Юрайт, 2022. С. 316.

отклонений, что позволяет сделать вывод, о том, что преступления совершаются умышленно, они хорошо спланированы. Лиц признанных невменяемыми среди интернет-преступников нет.

Исследуя уголовно-правовую характеристику личности интернет-преступников, нельзя не отметить то обстоятельство, что «компьютерные» преступники в большинстве случаев ранее не имели судимости, совершали преступление впервые, но среди интернет-преступников только 59% ранее не судимы. Остальные же уже были ранее судимы или с недавно снятой судимостью, что позволяет сделать вывод о рецидивном характере киберпреступности.

Известно, что компьютерные преступления совершаются определенным кругом лиц: высококвалифицированными программистами; специалистами в области телекоммуникационных систем; мошенниками со знаниями в сфере *IT* технологий.

Значительная часть преступных деяний в сети Интернет – анонимна, что свидетельствует о тщательной подготовке преступления и об активной деятельности по его сокрытию.

Согласно изученным материалам правоприменительной практики по преступлениям, совершенным посредством информационно-телекоммуникационных технологий и статистической отчетности мы предлагаем следующую классификацию киберпреступников:

1. В зависимости от преступления и степени овладения компьютерными навыками:

– граждане, обладающие наивысшим уровнем знаний в конкретной сфере и специализирующиеся на совершении конкретных киберпреступлений;

– граждане, у которых заранее готов алгоритм совершения преступлений, слабо знакомые с деталями и процессами, происходящими в информационных системах, использующие электронные устройства для совершения «неспецифических» для информационного пространства действий (к примеру, ст.ст. п. «г» ч. 3 ст. 158, 159.3, 159.6, 242 и т.д.);

– ранее судимые граждане.

2. В зависимости от территориальности:

– граждане, которые совершают лишь преступления в информационном пространстве (в том числе посредством информационно-телекоммуникационных технологий);

– граждане, которые совершают преступления как в информационном пространстве (в том числе посредством информационно-телекоммуникационных технологий), так и иные виды преступления.

3. В зависимости от мотивационных установок:

– корыстный тип. К данной категории следует относить лиц с явно выраженными стремлениями к приобретению материальных и иных благ посредством совершения киберпреступлений;

– насильственный тип. К данной категории следует относить лиц, у которых отсутствует контакт в информационном пространстве, однако это не исключает совершения киберпреступлений посредством психологического влияния и иных противозаконных действий;

– социально-дезорганизующий или «игровой» тип. К данной категории следует относить лиц, преследующих цель нарушение социальные и правовых норм, деструктивное воздействие на общество и социальные группы;

– протестующий тип. К данной категории следует относить лиц, протестующих в информационном пространстве (ст.ст. 207.1, 207.2, 207.3 УК РФ и др.);

– самоутверждающийся тип. К данной категории следует относить лиц, которые пытаются получить высокий неформальный социальные статус;

– неосторожный тип.

Таким образом, можно сделать вывод о том, что киберпреступность — это новое явление, которое благодаря развитию технологий стало возможным только в последние десятилетия. Киберпреступники используют различные технические средства для достижения своих целей, что делает их труднее выслеживаемыми и защищенными от преследования.

Киберпреступность требует новых методов обнаружения и предотвращения, поскольку традиционные методы правоохранительных органов не обладают достаточной эффективностью для решения этой проблемы.

Наконец, киберпреступность может вызывать серьезный ущерб даже в странах с высокой уровнем развития, поэтому она должна быть воспринята как одна из главных угроз нашей современной жизни и контролироваться с регулярной проверкой и обнаружением.

# ГЛАВА 3. ПРЕДУПРЕЖДЕНИЕ КИБЕРПРЕСТУПНОСТИ В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ

## §1. Общесоциальные меры предупреждения киберпреступности

Со вступлением всего мирового сообщества в новую эпоху информационных технологий невозможно представить жизнь человека без использования достижений технического и научного прогресса. Всеобщая компьютеризация и информатизация населения способствуют качественному и быстрому решению повседневных задач, а также достижению определенных целей.

Предупреждение киберпреступлений требует серьезных усилий со стороны органов государственной власти и общества и может быть эффективным лишь в процессе применении разнообразных общесоциальных и специально-криминологических мер.

Исключительным условием эффективности предупредительных мероприятий в сфере киберпреступности является их социально-экономическая целесообразность. Следует отметить, что предупредительные мероприятия должны быть направлены не только на эффективность, но и на системность их реализации. Системность в разработке и реализации мер предупреждения киберпреступности включает в себя действия разнообразных уровней

превентивной деятельности, дифференцированных по объему, функциям и признакам, и в то же время взаимодействующих при решении задач предупредительного характера[1].

Обеспечение своевременной и эффективной предупредительной деятельности в сфере высоких технологий представляет собой определенную проблему для органов внутренних дел, решение которой во многом зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов общесоциальных и специальных мер предупреждения исследуемой категории преступлений.

Меры общесоциального предупреждения реализуются посредством использования комплексных возможностей государства, которые обеспечивают прогрессивное совершенствование общества, отношений людей в социально-экономическом, социально-политическом, нравственно-духовном, семейно-бытовом аспектах. Данные мероприятия направлены на достижение масштабных целей, которые ставятся государством.

М.А. Желудков и другие, к наиболее распространенным превентивным направлениям киберпреступности относят (на основе зарубежного опыта):

1. Обеспечение безопасности стратегических и государственных информационных систем от информационных атак и актов кибертерроризма (Эстония, Канада, Германия и др.);

2. Совершенствование правового регулирования (Канада, Япония, Германия и др.);

3. Обеспечение безопасности информации и персональных данных (Франция, Чехия и др.);

4. Взаимодействие правоохранительных органов государств (Япония и др.)[2].

---

[1] Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. М. : Академия управления МВД России, 2021. С. 87.

[2] Желудков М.А., Попов А.М., Дубровина М.М. Особенности противодействия киберпреступности в России и зарубежных странах // Вестник Волгоградской академии МВД России. 2018. № 3(46). С. 97-102.

На федеральном (государственном) уровне в настоящее время в деятельности органов исполнительной власти необходимым является создание разборчивого свода правил и инструкций, регулирующих доступ правоохранительных органов к данным, находящимся в распоряжении интернет-провайдеров и иных организаций частного сектора, вовлеченных в исследуемый процесс.

Наличие четкого правового регулирования, отвечающего основным требованиям международного законодательства о защите данных, сегодня может обеспечить выполнение требований по обеспечению прав и свобод человека и верховенства закона.

Между правоохранительными органами ощущается нехватка подготовленных кадров. Все это обусловливает необходимость повышения квалификации сотрудников, занимающихся расследованием уголовных преступлений в сфере высоких технологий, в том числе в области технических знаний. Расследования преступлений в сфере информационных технологий проводятся специалистами в области юриспруденции, но в этой области также требуется углубленная техническая подготовка, которая не предназначена для юристов. В подтверждение этому мы обратились к современным федеральным государственным образовательным стандартам (ФГОС 3+) в области права и специальностей. В перечень обязательных пунктов практически не входит ни одна дисциплина, которая бы осуществлялась с помощью информационных технологий. Профессиональный уровень подготовки специалистов напрямую влияет на эффективность расследования уголовных преступлений в области компьютерных данных. Подготовка специалистов должна осуществляться комплексно, в том числе путем приобретения практических навыков, с использованием современных информационных технологий[1].

[1] Магомедова Х.Б. Отдельные аспекты предупреждения киберпреступности // Проблемы совершенствования законодательства : сборник научных статей студентов юридического факультета. Махачкала : ООО «АЛЕФ», 2019. С. 90-92.

Основополагающим элементом общесоциального уровня предупреждения кибепреступности является мониторинг состояния информационного пространства в сфере криминальных проявлений. Необходимо принимать во внимание показатели преступности с использованием информационно-телекоммуникационных технологий; латентность киберпреступлений; причины и условия, детерминирующие киберпретупления; криминологическое прогнозирование, тенденция и динамика преступлений, совершаемых в информационном пространстве.

Социально-политический блок превентивных общесоциальных мер киберпреступности в юриспруденции является основным, поскольку уголовная политика государства: «во многом зависит от укрепления роли государственной власти, рационализации подходов к выработке решений в формировании уголовной политики, от создания условий для эффективной работы механизмов, основанных на саморегулировании и препятствующих развитию дестабилизирующих факторов»[1]. Важными элементами в данном блоке предупредительных мер являются мероприятия, которые направлены на нормализацию политической стабильности государства; усиление политической власти; формирование эффективного правового регулирования цифровых технологий и киберпреступности; разработка стратегий и планов уголовной и цифровой политики.

К социально-экономическому блоку превентивных общесоциальных мер киберпреступности как правило относят нормализацию экономической стабильности страны, укрепление кредитно-денежной политики, совершенствование мероприятий по социальной защите общества, повышение уровня жизнедеятельности государства, уменьшение уровня безработицы и др.

Социально-правовому блоку превентивных общесоциальных мер киберпреступности в настоящее время, в век высокий технологий отводится большое внимание, а именно государству необходимо формировать

[1] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т.В. Пинкевич. Москва: Юрлитформ, 2020. С. 163.

законодательную базу, отвечающую современным реалиям: принятие ряда нормативно-правовых актов, внесение изменений в ряд существующий нормативно-правовых актов, которые регулируют формирование и использование цифровых технологий, охрана общественных отношений, которые возникают в связи с их использованием в этой сфере, защита личности, общества и государства не только от их применения инновационных технологий в быту и на производстве, но и в преступных целях.

Большое внимание необходимо отводить нормативным требованиям (предписаниям) в сфере предупреждения киберпреступности в соответствии с международно-правовыми нормами и международными обязательствами России; заключениям и ратификации международных Конвенций, договоров и соглашений по борьбе с цифровой преступностью – киберпреступностью.

Организационно-управленческий блок превентивных общесоциальных мер киберпреступности направлены на осуществление организационных аспектов предупредительной деятельности, принятию государственных решений в сфере охраны, контроля и надзора со стороны органов государственной власти, а также по взаимодействию государства, общественности и иных частных спектров жизнедеятельности.

## §2. Специальные и индивидуальные меры предупреждения киберпреступности

Специально-криминологическое предупреждение заключается в деятельности по предотвращению, пресечению и раскрытию преступлений; выявлению и устранению (нейтрализации) детерминант преступности, причин и условий конкретных преступлений; оздоровлению социальной микросреды, коррекции поведения лиц, исправлению лиц, от которых можно ожидать совершения преступлений или уже совершивших преступления.

Специально-криминологические меры предупреждения преступлений подразумевают деятельность, непосредственно направленную на причины и условия совершения преступлений[1]. Исходя из общих задач специально-криминологического предупреждения, а также на основе анализа причин и условий, способствующих совершению преступлений с использованием высоких технологий, целесообразно сосредоточить внимание на разработке следующего комплекса мер:

*1. Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий*.

В научном сообществе преобладает точка зрения, что основной целью предупреждения преступлений в сфере высоких технологий является создание определенных правил использования информации, максимально ограничивающих условия и возможности неправомерного воздействия на нее. В то же время, в качестве окончательной цели предупреждения рассматриваемых преступлений целесообразно рассматривать создание системы международных и государственных гарантий информационной безопасности, обеспечивающих должный уровень защищенности личности, общества и государства в сфере создания, передачи, хранения, обработки и использования информации, а также функционирования соответствующих электронных средств и информационно-телекоммуникационных систем.

Реализация предлагаемых целей и задач по предупреждению преступлений в сфере высоких технологий предполагает разработку системы предупредительных мер на основе качественной научной проработки всех аспектов криминологического воздействия на причины и условия совершения данного вида преступлений. Однако в настоящее время у научного сообщества отсутствует единый подход к организации данной работы и содержанию

---

[1] Организация деятельности органов внутренних дел по предупреждению преступлений (термины, определения): учебное пособие / под ред. А. В. Аносов, В. И. Старков, Е. Ю. Титушкина [и др]. М., 2016. С. 75.

профилактических мер, направленных как на преступность в сфере высоких технологий в целом, так и на отдельные ее проявления, в частности.

Основным результатом научно-исследовательской работы должен явиться адаптированный перенос ее результатов в правоприменительную практику. Координация усилий правоохранительных органов должна осуществляться уже на этапе сбора криминологической информации (начиная с этапа регистрации заявлений и сообщений о преступлениях) и в дальнейшем представлять собой единую информационную систему, позволяющую беспрепятственно обмениваться информацией, в том числе научными разработками и методиками, в процессе предупреждения, раскрытия и расследования высокотехнологичных преступлений[1].

*2. Совершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями в сфере высоких технологий (научно-методическое обеспечение).*

Реализация мер по предупреждению киберпреступности в данном направлении обеспечивается путем совершенствования подзаконных актов и различного рода инструктивно-регламентирующей документации, которые в силу своей специфики способны оказать оперативное воздействие на ситуацию в случаях, когда законодательное решение проблемы затруднено в силу разных причин. Кроме того, качественное методическое обеспечение способствует эффективному применению законодательных норм в практической деятельности.

В силу разнородности нормативной базы (правоохранительных органов и иных государственных учреждений, общественных организаций, коммерческих структур, и т.п.) неизбежно возникают проблемы взаимодействия в процессе правоприменения, которые не позволяют эффективно противодействовать преступности. Несогласованность субъектов предупреждения преступлений в

---

[1] Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. 2018. № 4(48). С. 93-97.

этой сфере зачастую предоставляет дополнительные возможности для преступных комбинаций.

К отдельным направлениям совершенствования научно-методического обеспечения противодействия киберпреступности относятся:

– унификация и легитимизация терминов и определений, связанных с данным направлением деятельности. Так, само понятие «преступления в сфере высоких технологий» включает в себя не только преступления, предусмотренные гл. 28 УК РФ, но и те, где информационно-телекоммуникационные сети или компьютерная информация выступают в качестве средства или орудия совершения преступного деяния. При этом непосредственный объект состава преступления зачастую включает в себя и другие общественные отношения, такие как отношения в сфере собственности, экономической деятельности, здоровья населения и общественной нравственности и т. д. (мошенничество с использованием платежных карт (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), незаконные организация и (или) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ст. 171.2 УК РФ), сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (ст. 228.4 УК РФ) и др.) Данный аспект напрямую связан с особенностями квалификации деяний, совершенных с использованием высокотехнологичных средств[1];

– формирование правовых механизмов, сужающих пространство для совершения противоправных деяний. В частности, целесообразно рассмотреть вопрос о законодательном закреплении обязанности производителей и продавцов компьютерной техники, средств связи предустанавливать в

[1] Харламов, А.А. Проблемные вопросы квалификации мошенничества с использованием платежных карт // Вестник Уральского юридического института МВД России. 2017. № 1. С. 44-47.

производимую продукцию антивирусные продукты в целях защиты от несанкционированного доступа к компьютерной информации. С другой стороны, меры профилактики могут быть направлены не только на потенциального преступника, но и на органы (организации), представляющие интерес для злоумышленников в сфере высоких технологий. В частности, такой мерой могла бы стать система страхования информационных рисков, которая предусматривает страхование средств передачи, обработки или хранения охраняемой компьютерной информации, а также информационно-телекоммуникационных сетей и оборудования от неправомерного блокирования, уничтожения, модификации либо несанкционированного копирования электронной информации. При этом перед заключением страхового договора собственник (владелец) информационного ресурса либо информационно-телекоммуникационной сети и соответствующего оборудования обязан провести ряд установленных мер по защите информации и оборудования (установка сертифицированного программного обеспечения, антивирусная защита и т. д.). Данная мера направлена на уменьшение наносимого материального ущерба и снижение количества происходящих по их вине несанкционированных проникновений в компьютерные системы;

– обеспечение своевременности реагирования законодательства на изменяющиеся условия функционирования систем защиты информации и информационных ресурсов. При этом для решения задач совершенствования нормативного правового обеспечения деятельности по предупреждению киберпреступлений необходимо обращаться к зарубежной практике правового регулирования данной деятельности, в частности опыта Китайской народной республики по созданию «Золотого щита[1]». Кроме того, для предупреждения совершения компьютерных преступлений в сети Интернет, представляется возможным в федеральном законе «Об информации, информационных

[1] China Net -- Интернет Китай // http://www.china.com.cn/chinese/zhuanti/283732.htm

технологиях и о защите информации»[1] закрепить обязанность для физических лиц при регистрации сайтов, веб-страничек, получении аккаунтов в социальных сетях указывать свои персональные данные (Ф. И. О., год рождения, данные паспорта);

– разработка новых прикладных методик противодействия компьютерной преступности, в том числе в процессе оперативно-розыскной профилактики. По словам С. М. Сергеева, до настоящего времени исследования, касающиеся вопросов «деанонимизации» пользователей сети Интернет, не проводились, соответственно, практика лишена каких-либо научно обоснованных рекомендаций и предложений[2]. В частности, представляется необходимым законодательно закрепить полномочия правоохранительных органов на осуществление мониторинга опубликованных в сети Интернет материалов экстремистского или иного противоправного характера, а при необходимости обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения.

*3. Принятие организационно-управленческих мер предупреждения киберпреступности.*

Данное направление характеризуется комплексом мер, направленных на совершенствование практической деятельности субъектов предупреждения преступлений в сфере высоких технологий. К ним следует отнести:

– создание системы подготовки сотрудников правоохранительных органов по специальностям «Защита информации и информационно-телекоммуникационных сетей» и «Информационная безопасность» в образовательных учреждениях МВД, ФСБ, МО, ФТС России и др. Данная мера

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Российская газет. 2006. № 165.

[2] Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. 2017. № 1(73). С. 137-140.

позволит обеспечить комплектование правоохранительных органов компетентными и профессиональными сотрудниками;

– переход от преимущественно территориального принципа работы правоохранительных органов в сфере предупреждения преступлений к функциональному. Существующая структура правоохранительных органов и принципы организации работы отдельных подразделений вызывают проблемы координации как внутри самих этих ведомствах, так и в рамках межведомственного взаимодействия. Одной из главных особенностей высокотехнологичной преступности является ее многоэпизодность и трансграничный характер. По этой причине на практике зачастую возникают сложности с определением места совершения преступления, а значит и территориального органа, который должен заниматься его раскрытием и расследованием. В виртуальном мире понятие территориальности достаточно условно, поэтому существовавшая долгие годы практика проведения разбирательства «по месту совершения преступления» в сочетании с бюрократизмом уголовно-процессуальной системы не способствует принятию своевременных мер по изобличению преступников и документированию их деятельности;

– совершенствование информационно-аналитического обеспечения деятельности по противодействию преступлениям в сфере высоких технологий. Данная работа связана решением целого ряда задач, включающих сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации;

– перевод на новый уровень организацию взаимодействия правоохранительных органов со средствами массовой информации. Использование средств массовой информации в системе противодействия высокотехнологичной преступности должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями; проведение правовой пропаганды, направленной на

формирование правосознания и нетерпимость к преступным проявлениям; информирование населения о средствах и методах защиты от высокотехнологичных преступных посягательств, о новых формах и схемах осуществления компьютерных преступлений. В силу специфики преступлений с использованием высоких технологий профилактический эффект от своевременного доведения данной информации чрезвычайно высок, особенно если передаваемая в средствах массовой информации (далее – СМИ) информация отвечает требованиям систематичности, наступательности, наглядности и своевременности. К работе со СМИ необходимо привлекать и общественные организации, такие как союз потребителей, союз обманутых соинвесторов (вкладчиков) и т. д. Общественно-корпоративные сообщества (Ассоциация российских банков, союзы предпринимателей и т. д.) также могут сыграть большую роль в противодействии киберпреступности.

Обеспечение комплексного подхода к профилактической деятельности обуславливается в зависимости направлений и мер профилактических направленностей. На наш взгляд, к данным следует относить:

– вовлечение всей системы профилактики киберпреступлений и средств минимизации отрицательных явлений, воздействующих на увеличение цифровой преступности – киберпреступности;

– взаимодействие и активизация государственных и общественных организаций в области профилактики киберпреступности;

– применение форм и методов превенции и профилактики киберпреступности, строящиеся на итогах научных исследованиях;

– выработка и осуществление государственных и региональных программ по профилактике киберпреступности.

Следующим направлением профилактической деятельности киберпреступности является стабильная оценка результативности использования нормативной базы в сфере цифровых технологий. Целесообразно осуществлять устойчивый анализ правоприменительной

практики; ведение статистической отчетности по уголовным делам, связанным с киберпреступностью.

Специально-криминологические и индивидуальные меры предупреждения киберпреступности , как и общесоциальное предупреждение требуют комплексного подхода. На наш взгляд, необходимо активизировать виктимологическую профилактику в целях повышения защитного уровня общества, т.е. пользователей информационного пространства и инновационных технологий. Исследование жертвы кибепреступлений необходимо, как правило, в целях первичной профилактики. На наш взгляд, аналогичная задача ставится и перед исследователями, которые рассматривают виктимологические аспекты предупреждения преступлений и киберпреступлений.

Применительно к индивидуальному проявлению кибервиктимности можно говорить о «виктимном поступке», отражающем единичный факт проявления кибервиктимизма. По нашему мнению, кибервиктимный поступок – это деяние, которое обладает признаками умысла, как правило косвенного) либо неосторожности, которое способствует совершению в отношении них преступлений посредством информационно-телекоммуникационных технологий.

В криминологии викитимологическую профилактику рассматривают в нескольких аспектах. Организационный аспект виктимологической профилактики имеет характерные черты, которые связаны со специальной подготовкой сотрудников органов внутренних дел и иных служб и органов государственной власти. Отсутствие должного уровня профессиональных знаний и навыков не позволяет сотрудникам правоохранительных органов оперативно проводить профилактические мероприятия. Данное обстоятельство обусловлено с отсутствием в настоящее время приемлемых методических рекомендаций по организации и тактике виктимологической профилактики

киберпреступлений и определенных методов деятельности с потерпевшими от данных преступлений[1].

Субъектами реализации виктимологической профилактики киберпреступлений выступают государство в лице правоохранительных органов и общественные организации, а также иные негосударственные структуры. Виктимологическая профилактика данного вида преступлений охватывает разные по объему формы поведения, которые являются закономерным следствием разнообразных видов виктимизации: легкомыслие в поведении, чрезмерная любознательность, небрежность пользователей, незнание основных мер информационной безопасности, возрастные и интеллектуальные качества и др. В качестве механизма регулирования защиты потерпевших от киберпреступлений выступают не только правовые нормы, но и морально-нравственные, предпринимательские и этические нормы поведения. Таким образом, виктимологическая профилактика направлена на широкую социальную профилактику для минимизации киберпреступности как общественно опасного явления.

Итак, предлагаем реализовывать виктимологическую профилактику в информационном пространстве по следующим направлениям:

– увеличение результативности информационной безопасности; совершенствование безопасности программно-технических средств сети Интернет;

– превенция спам-сообщений и всплывающих окон в сети Интернет;

– предотвращение применение сети Интернет как информационного ресурса в целях превенции.

Подытоживая исследования настоящего параграфа следует отметить, что в целях сокращения киберпреступлений на современном этапе развития общества следует воздействовать на следующие направления:

---

[1] Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. М. : Академия управления МВД России, 2021. С. 105.

– противодействие анонимность пользователь информационного пространства – деанонимизация пользователей информационного пространства;

– организация полноценного взаимодействия правоохранительных органов, негосударственных субъектов предупреждения и граждан в целях реализации положений виктимологической профилактики;

– правовое регулирование экономических отношений в сети Интернет, что позволяет устранить экономическую основу этого вида преступлений: вопросы электронной формы сделки по гражданскому законодательству, вопросы регулирования деятельности и ответственности ЭПС, интернет-аукционов, участников дистанционной торговли.

Таким образом, своевременная разработка и комплексное использование специально-криминологических мер предупреждения преступлений в сфере высоких технологий способствует значительному повышению уровня информационной безопасности России и эффективности борьбы с противоправными деяниями в данной сфере. При этом следует учитывать, что предложенные предупредительные меры будут иметь практический эффект только в случае взаимодействия государственных органов с институтами гражданского общества (общественными объединениями, органами местного самоуправления, средствами массовой информации, образовательными и научными учреждениями, и т. д.) на основе планирования и программирования совместной деятельности с учетом специфики работы каждого из заинтересованных субъектов профилактики.

## §3. Использование инновационных технологий в борьбе с киберпреступностью по материалам МВД по Республики Татарстан

Масштабное увеличение использования инновационных технологий в информационном обществе такими же темпами ставит перед правоохранительными органами новые задачи в сфере противодействия

совершенствованию киберпреступности, а также развития знаний, навыков и умений по раскрытию и расследованию киберпреступлений. Однако при всей существующей четкости элементов стратегии профессионального развития сотрудников органов внутренних дел в данной сфере в настоящее время не существует единой стратегии такой подготовки.

Современная преступность ежедневно подвергается трансформации, появляются новые способы совершения противоправных действий, меняется область концентрации преступных элементов. Данные трансформации затронули и процесс хищения денежных средств посредством краж и мошенничеств. По результатам работы органов внутренних дел в 2022 году Республика Татарстан среди регионов Приволжского федерального округа продолжает занимать первое место по числу расследованных «дистанционных» краж и мошенничеств – 2817 преступлений, а также по количеству лиц, в отношении которых были направлены уголовные дела в суд – 1793 лица.

За последние три года наиболее распространенным способом совершения дистанционных хищений в отношении граждан, проживающих на территории Республики Татарстан, являются телефонные звонки от мошенников, которые представляются сотрудниками Банковских учреждений, Собственной безопасности и иных правоохранительных органов (более 20% от всех совершенных краж и мошенничеств исследуемой категории в отношении жителей Республики Татарстан). Механизм совершения данных преступлений следующий: потерпевшим поступает телефонный звонок от мошенников, в ходе разговора последние предоставляют ложные данные об оформлении кредитов на потерпевшего, после чего получают необходимые данные о банковских счетах и похищают денежные средства.

Так, в 2022 году 44-летняя жительница Казани стала очередной жертвой телефонных мошенников. Женщина перевела на неизвестный счет более двух миллионов рублей. В один из дней июля ей позвонили с незнакомого абонентского номера и представились сотрудником банка. В ходе разговора мошенник сообщил, что от ее имени пытаются получить кредит. После чего,

женщине позвонил лжесотрудник правоохранительных органов в целях подтверждения сказанного первым мошенником. В результате преступных действий жительница Казани перевела на «безопасный счет» денежные средств в размере двух миллионов шестисот тридцати восьми рублей[1].

В ноябре 2022 года в Казани 23-летняя жительница стала жертвой мошенников, поверив злоумышленникам, перевела деньги на «безопасные счета», оформила кредиты и предоставила дистанционный доступ к своему телефону. Мошенники также представились сотрудниками правоохранительных органов[2].

На втором месте по количеству заявлений и обращений, поступающих от жителей Республики Татарстан, занимают мошенничества при покупке товара в сети Интернет (16,7%), когда потерпевшие не получают заказанный и оплаченный товар, либо получают «пустые» посылки. Так, в декабре 2020 года в суд было направлено уголовное дело в отношении 27-летнего жителя Пермской области, который мошенническими действиями похитил более миллиона рублей у 62 женщин (14 из которых жители Республики Татарстан) под предлогом продажи меховых изделий через социальные сети. 13 сентября 2021 года суд приговорил преступника к 3 годам 9 месяцам лишения свободы.

На третьем месте располагается такой способ совершения краж и мошеннических действий посредством информационно-телекоммуникационных технологий, как «предоставление услуг». До 14,6% от всех совершенных преступлений выросло число краж и мошенничеств под предлогом оказания каких-либо услуг («поездки на «*BlaBlaCar*», поиск попутчиков в сети Интернет, иные разнообразные Интернет-услуги). При

---

[1] Жительница Казани перевела мошенникам 2,6 миллиона рублей. URL: https://m.business-gazeta.ru/news/558111 (дата обращения: 26.01.2023).

[2] 23-летняя жительница Казани, поверив мошенникам, лишилась свыше 500 тыс. рублей. URL: https://tatcenter.ru/news/23-letnyaya-zhitelnicza-kazani-poveriv-moshennikam-lishilas-svyshe-500-tys-rublej/ (дата обращения: 26.01.2023).

совершении 39,7% преступлений, подозреваемые использовали возможности Интернет-соединений.

Четвертое место занимает хищение денежных средств при осуществлении покупок товаров на сайтах бесплатных объявлений.

В данном направлении сотрудниками оперативного аппарата Республики осуществляется виктимологическая профилактика и информирование, направленное на конфиденциальность персональных данных, данных банковских счетов и т.д.

Помимо иных регионов страны, сотрудниками оперативного аппарата Республики осуществляется работа по выявлению и задержанию лиц, совершающих данные преступления на территории Республики Татарстан. Так, в конце декабря 2021 года в ходе проведения оперативно-розыскных мероприятий установлены и задержаны четверо жителей Ульяновской области, которые в арендованном доме на территории пос. Вознесение г. Казани организовали преступный «колл-центр». Реализуя свой преступный умысел, преступники, используя средства связи, совершали мошенничества в отношении жителей других регионов страны под предлогом предоставления компенсации за ранее приобретенные биологически активные добавки и лекарственные препараты. Общая сумма ущерба составила более десяти миллионов рублей. Также в конце февраля 2022 года в процессе сопровождения данного уголовного дела сотрудниками Управления уголовного розыска МВД по Республике Татарстан в Краснодарском крае был задержан организатор данной преступной группы, выходец одной из стран СНГ, который был арестован. Всего сотрудниками было установлено 8 фигурантов и 11 эпизодов совершения аналогичных преступлений организованной группой на общую сумму двенадцать миллионов рублей.[1]

[1] Результаты работы по предупреждению, выявлению и раскрытию краж с банковских крат граждан и мошенничеств с использованием информационно-телекоммуникационных технологий URL: https://16.мвд.рф /press_slujba/press_reliz/item/29195688

На сегодняшний день между МВД по Республике Татарстан и банковскими организациями налажен алгоритм совместных действий. Во всех крупных финансовых учреждениях уже внедрена системы фрод мониторинга, ориентированная на обнаружение попыток совершения мошеннических действий. Заложенный в нее набор правил, списков и фильтров позволяет вычислять подозрительные транзакции и блокировать их до момента перевода денег. Только службой безопасности Сбербанка в первом полугодии 2022 год предотвратил 452 преступления[1]. А в целях экономии времени на исполнение запросов по движению денежных средств заключено соглашение по использованию электронного документооборота, что значительно облегчает жизнь полицейским.

С сотовыми операторами связи МВД по Республике Татарстан также налажено полное взаимодействие. По сайту федерального агентства «Россвязь» можно посмотреть, каким операторам связи принадлежат абонентские и *IP*-номера. Также можно вычислить электронный ящик, карту, через которую пополняется баланс. Следует отметить, что сотруднику полиции придется проанализировать огромное количество информации, прежде чем у него получится установить злоумышленника и привлечь его к ответственности.

С учетом тенденции роста преступности исследуемой категории МВД по Республике Татарстан одним из первых в России разработало алгоритм их раскрытия, закрепив его в Приказе МВД по Республике Татарстан от 2017 года. Данный алгоритм установил обязательный порядок и сроки принятия процессуальных решений, а также систему производства следственных действий и проведения оперативно-розыскных мероприятий. Создание специализированной следственно-оперативной группы МВД по борьбе с преступлениями в сфере информационно-телекоммуникационных технологий (далее – ССОГ). На наш взгляд, это одно из самых своевременных и

[1] За полгода Сбербанк предотвратил попытки финансового мошенничества на 250 миллионов рублей URL:https://www.irk.ru/news/20220825/fraud/

правильных решений. В 2019 году с учетом продолжающегося роста «дистанционной» преступности ССОГ была усилена, а ее руководителем был назначен заместитель Министра – начальник ГСУ МВД по Республике Татарстан. В состав данной группы на сегодня входят руководители и сотрудники ведущих служб аппарата Республики.

Исходя из этого, актуальным становится вопрос о разработке и реализации стратегии обучения сотрудников органов внутренних дел, целью которой будет обеспечение необходимого уровня их квалификации и компетентности в расследовании киберпреступлений, с акцентом на деятельность с электронными доказательствами, криминалистический анализ компьютерного оборудования в системе уголовного правосудия и помощь другим ведомствам в реализации кибербезопасности.

Основные преимущества использования информационных технологий заключаются, во-первых, в высвобождении времени у должностных лиц, что позволяет сосредоточить усилия на раскрытии уже совершенных преступлений, а во-вторых, в возможностях искусственного разума, способного выполнять сложнейшие расчеты при выявлении факторов, способствующих совершению преступления, и продумывать алгоритмы борьбы с ними.

Сложность в борьбе с киберпреступностью вызвана, прежде всего, тем, что преступники достаточно быстро приспосабливаются к методам защиты информации, учатся находить пробелы в программном обеспечении и использовать данные недостатки в свою пользу. Современные хакеры (например, появившаяся в 2016 году группа «*Silence*») в начале своей деятельности анализировали опыт, тактику и инструменты других подобных хакерских групп (*MoneyTaker, Cobalt* (*Anunak* или *Carbanak*)) и даже, совершая ошибки при осуществлении хакерских атак, могли на ходу пытаться их устранить. Также преступники анализируют отчеты антивирусных и *Threat Intelligence* компаний. Часто подобные преступления совершаются лицами, которые в прошлом или в настоящий момент занимаются легальной деятельностью в сфере программирования или реверсинжиниринга.

Возможности модификации легальных программ и иные технические обновления значительно упрощают деятельность хакеров и киберпреступность «молодеет». Сооснователь *Group-IB* Дмитрий Волков утверждает, что киберпреступником сегодня стать намного легче, чем 5-7 лет назад[1].

Соответственно, возникают вопросы, как же обеспечить эффективную борьбу с киберпреступлениями. Глава Сбербанка Герман Греф считает, что необходимо создать в России отдельное министерство, которое занималось бы чрезвычайными ситуациями в информационной сфере. На наш взгляд, прежде всего, необходимо обеспечить надлежащую подготовку и технологическое оснащение сотрудников, которые буду заниматься кибербезопасностью. Так, на конференции *CyberCrimeCon* 2018 было принято решение о функционировании центра инновационных навыков и компетенций в сфере безопасности информационного пространства *CyberSchool*. Основываясь на 15-летнем опыте расследования киберпреступлений и борьбы с онлайн мошенничеством, специалисты *Group-IB* сформировали уникальные образовательные программы и форматы обучения, ориентированные на широкую аудиторию – от учащихся школ и высших учебных заведений до специалистов *IT*-сферы[2].

Также большое внимание следует уделить международному сотрудничеству в сфере информационной защиты, т.к. атаки хакерских групп, в большинстве случаев направлены не на конкретную страну, а на ряд государств. Такие группы спонсируются, в частности, Северной Кореей (*Lazarus*), Пакистаном, Китаем, США, Россией (*Silence, MoneyTaker*), Ираном и Украиной. С учетом такого международного масштаба, одолеть киберпреступность возможно лишь совместными усилиями. В 2018 году при совместной операции, проведенной сотрудниками испанской национальной полиции, при поддержке правоохранительных органов Румынии, Тайваня и

---

[1] Группа Silence-новая угроза для банков. URL: https://www.group-ib.ru/resources/threat-research/silence.html (дата обращения: 10.10.2022).

[2] «Сбербанк» представил статистику финансовых киберпреступлений. URL: https://tproger.ru/news/sberbank-cyberattack-statistics/ (дата обращение: 10.10.2022).

Республики Беларусь был задержан лидер хакерской группы *Cobalt* (также известной, как *Carbank* или *Anunak*)[1].

Рассматривая международное сотрудничество следует обратить внимание на исследования Д.М. Фарахиева, который рассматривает превентивные аспекты в сфере незаконного оборота наркотических средств, психотропных веществ или их аналогов в информационном пространстве. Исходя из вышеизложенного, в целях совершенствования деятельности по предупреждению преступлений в сфере незаконного оборота наркотических средств в киберпространстве Д.М. Фарахиев и Д.Ф. Минзянова предлагают проведение следующих мероприятий на международном уровне:

«1.1. Наладить взаимодействие между правоохранительными органами России и зарубежных стран в области борьбы с наркопреступностью в интернет-пространстве. Положительный опыт наблюдается в организации взаимодействия между представителями *Europol* и Генеральной прокуратурой *Frankfurt am Main* и Федеральным управлением уголовной полиции (совместно с *Europol*, *Eurojust* и коллегами из Нидерландов и различных агентств США)[2].

1.2. Учредить Международный информационно-антинаркотический центр (далее – Центр) и наделить его следующими полномочиями:

а) балансирование антинаркотической политики;

б) выработка и предложение результативных научно обоснованных инициатив в области борьбы с наркопреступностью, преимущественно в интернет-пространстве;

в) содействие органам, занимающимся предупреждением киберпреступности, в том числе в сфере незаконного оборота наркотических средств;

---

[1] Мухина М.С. Противодействие в сфере киберпреступности // Уголовно-правовые и криминологические направления противодействия преступности : Сборник материалов Межрегиональной научно-практической конференции профессорско-преподавательского состава, аспирантов и студентов, Симферополь, 29 марта 2019 года. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2019. С. 260-267.

[2] Организация правоохранительной системы в некоторых федеративных странах мира. URL: https:// komitetgi.ru/upload/iblock/538/538b9dcf40eca849375fa5f15da10d26.pdf (дата обращения: 10.10.2022).

г) формирование баз данных, которые содержат в себе веб-сайты, на которых пропагандируют наркотические средства, в целях дальнейшего решения вопроса о блокировке негативных веб-сайтов и др.

Деятельность данного Центра должна быть направлена на совершенствование механизма предупреждения преступлений в сфере незаконного оборота наркотических средств в интернет-пространстве посредством разработанной многофункциональной инновационной многоязычной *Web*-платформы»[1].

На современном этапе развития общества в процессе цифровизации большое внимание следует отводить возможностям использования искусственного интеллекта и иных инновационных технологий. Так, к примеру, Д.М. Фарахиев рассматривает следующие возможности использования инновационных технологий в процессе противодействия коррупции и преступлениям коррупционной направленности:

1) массив больших данных *(bigdata)*, поскольку данный инструментарий способствует использованию фрагментированных сведений в целях составления общей картины системной коррупционной активности. Наряду с этим возникает возможность высокоавтоматизированного сбора статистических данных по большому количеству параметров коррупционных проявлений: о наиболее вероятных коррупционных отношениях, о вновь возникающих динамических рисках коррупции, о статистике преступлений коррупционной направленности, связанных с определенным уровнем полномочий должностного лица. Это помогает объективно оценить коррупционные риски отдельных государственных должностей с учетом их местонахождения,

[1] Минзянова Д.Ф., Фарахиев Д.М. Инновационный подход к раскрытию и предупреждению преступлений в сфере незаконного оборота наркотических средств, совершаемых в Интернет-пространстве // Ученые записки Казанского юридического института МВД России. 2022. Т. 7. № 1 (13). С. 74-80.

социально-экономических условий, а также культурно-исторических особенностей субъекта[1];

2) внедрение и использование *blockchain* систем. Данная система представляет собой весьма сложный механизм, которые способствует оперативному и результативному отбору и обработке информации. В качестве положительных характерных черт *blockchain*-систем следует отразить следующее: прозрачность; отсутствие посредников; безопасность, надежность.

Итак, безопасность *blockchain*-систем заключается в том, что пользователи получают открытый и закрытый криптографические ключи, которые в свою очередь открывают «ворота» к блокам системы *blockchain*. Следует отметить, что оба криптографических ключа запаролены, что дает возможность избежать трансформации информации. Также система оснащена системой *KYC* (функция биометрии) для подтверждения личности пользователя.

Надежность *blockchain*-систем подтверждается наличием математических алгоритмов, которые лежат в основе деятельности данной технологии, которые не допускают изменение или добавлений в систему. Соответствие проверяется посредством достижения соглашений между всеми пользователями, так как все сведения представляют собой единую цепочку блоков, которые соответствуют друг другу и располагаются в последовательном порядке, поскольку каждый новый блок добавляется поверх предыдущего.

Основополагающее преимущество – прозрачность *blockchain*-систем. Все сведения о валютных операциях, контрактах являются общедоступными. Следовательно, каждый может ознакомиться с активами и операциями пользователя в свободной форме, что дает возможность отслеживать

---

[1] Фарахиев Д.М., Минзянова Д.Ф. Перспективы внедрения информационно-коммуникационных технологий в деятельность оперативных подразделений полиции по противодействию коррупции // Современная наука. 2022. № 1. С. 60-63.

сомнительное поведение и действия, а также вычислять противоправные операции коррумпированных должностных лиц[1].

Примерный принцип работы технологии *blockchain* представлен в приложении № 4.

На наш взгляд, весьма остро стоит вопрос объема и уровня информационно-технического обеспечения органов внутренних дел в процессе выявления, раскрытия и (или) предупреждения дистанционного хищения денежных средств. Однако, как показывает практика, применение современных баз данных в процессе раскрытия подобных преступлений, совершаемых посредством информационно-коммуникационных технологий – *«Palantir»*, *«Osiris»*, *«UNODC Sherloc»*, «ПСКОВ» и ряда других – представляется малоэффективным. Огромные вычислительные мощности и серьезный штат профессиональных сотрудников необходимы для качественного функционирования подобных систем. Таким образом, большое внимание в борьбе с дистанционным хищением денежных средств, следует отводить укреплению умственного и технического потенциала правоохранителей.

Одной из основных функций органов внутренних дел, в том числе их оперативных подразделений, является профилактическая деятельность, выражающаяся в комплексе оперативно-профилактических мероприятий. Это информирование граждан об уже распространенных и новых способах дистанционного хищения, разработка алгоритма действий в случае вероятного хищения денежных средств, виктимологическая профилактика, в том числе в отношении отдельной категории граждан, которые в силу определенных особенностей (возрастных, психофизиологических), не могут самостоятельно обезопасить себя от преступных посягательств, связанных с дистанционным хищением денежных средств.

Нами предлагается создание специализированного приложения для пользователей смартфонов с доступом к *online*-банкам и системе-*NFC*,

---

[1] Гумаров И.А., Фарахиев Д.М. Технология blockchain как средство противодействия // Научный компонент. 2022. № 1(13). С. 81-87.

позволяющего распознавать и блокировать нежелательные звонки и *SMS*-сообщения, целью которых является дистанционное хищение денежных средств. Так в 2021 г. МВД России сообщило, что запустит новый мобильный сервис «Антимошенник» в целях борьбы с телефонным мошенничеством. Данный сервис будет функционировать на базе официального приложения МВД России: при звонке с неизвестного номера система сопоставит его со списком мошеннических номеров, которые уже внесены в базу данных МВД России, и направит исходящему пользователю сообщение-предупреждение. В результате чего, такие абонентские номера можно будет заблокировать[1].

В целях формирования и внедрения специализированного приложения можем обратиться к зарубежному опыту. Так, в США существует программа *«National Do Not Call Registry»* (национальный реестр номеров, на которые запрещается звонить). В Канаде существует Центр по борьбе с мошенничеством, который информирует населения о деятельности телефонных мошенников. Каждый год центром выявляется более 5 тысяч телефонных номеров и более 15 тысяч электронных адресов, которыми пользуются мошенники. Используя этот опыт, можно повысить эффективность противодействия дистанционному хищению денежных средств посредством телефонной связи в нашей стране. В США, например, применяются такие методы борьбы, как *«jamming»* (технология глушения или срыва телефонного сигнала), а также ведется работа по информированию населения с помощью компьютерных программ.

Также необходимо отметить, что введение биометрических параметров населения может стать отправной точкой для новых схем дистанционного хищения денежных средств (к примеру, могут быть использованы программы, позволяющие в точности копировать голоса любой жертвы или их родственников). Во многих программах имеется функция, позволяющая менять

---

[1] Сабырбаева А.В. Электронные доказательства как новый вид доказательств при расследовании современных форм мошенничества // Review of law sciences. 2020. №3 (120). С. 215-220.

голос, и их использование не требует особых навыков. В целях противодействия таким преступлениям следует установить уголовную ответственность за данную категорию преступлений на законодательном уровне.

В процессе раскрытия и расследования дистанционного хищения денежных средств сотрудники оперативных подразделений должны использовать различные информационно-коммуникационные технологии, к примеру, такие как *Big Data*. На наш взгляд, возможность централизованного сбора и анализа виртуального следа имеет перспективное значение, так как, по мнению экспертов, в ближайшие несколько лет большие данные *«Big Data»* будут наиболее уязвимы для кибератак – до 70%. И тенденции оцифровки информации предполагают, что риски будут только увеличиваться. Несмотря на это, на сегодняшний день, в условиях цифровизации за счет использования разнообразных аналитико-инновационных технологий становится возможным осуществлять прогнозирование и последующий контроль фактов дистанционного хищения денежных средств.

Представляется практически необходимым и целесообразным совершенствование и использование возможностей системы ИБД-Ф «Дистанционное мошенничество» в целях собирания, систематизации, обработки и анализа расследуемых преступлений, связанных с дистанционным хищением денежных средств и иными видами киберпреступности. Система ИБД-Ф дает возможность собирать и сравнивать данные в автоматизированном режиме[1].

На наш взгляд, одним из наиболее эффективных направлений внедрения достижений криминалистики и результатов научных исследований в практику борьбы с дистанционным хищением денежных средств является образовательный процесс. Таким образом, все более актуальными в интересах

---

[1] Анапольская А.И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств, совершаемых в сфере функционирования электронных расчетов // Вестник ТГУ. 2019. № 5 (145). С. 224.

органов внутренних дел становятся вопросы совершенствования организации подготовки специалистов, которые обладают знаниями в области информационно-коммуникационных технологий, а также вопросы повышения квалификации сотрудников следственных, криминалистических и оперативных подразделений в борьбе с дистанционным хищением денежных средств.

Также большое значение имеет взаимодействие оперативных подразделений с органами Федеральной службы исполнения наказания и лицами, оказывающими содействие органам, осуществляющим оперативно-розыскную деятельность, направленное на получение оперативно-значимой информации о местонахождении лиц или группы лиц, совершающих дистанционные хищения денежных средств. Однако надо отметить, установление местонахождения преступников затрудняется в связи с латентностью данного вида преступления. Несмотря на это, ряд авторов считают, что одним из эффективных направлений в борьбе с дистанционным хищением денежных средств является использование специальных технических средств в учреждениях уголовно-исполнительной системы. Для этого используется специальная радиочастотная технология, которая позволяет срывать телефонные сигналы. Основной принцип ее работы – это «глушение» сигналов с помощью радиоволн, работающих в диапазоне рабочих частот операторов мобильной связи. Но у данной технологии есть существенный минус, она также «глушит» звонки государственных служб и жителей ближайших жилых районов. Для решения этой проблемы используется экспериментальная технология *«Managed access system»* (система управляемого доступа), благодаря которой можно блокировать только те звонки, которые исходят от заключенных. Особенностью этой системы является то, что она позволяет разворачивать зону, защищающую от сигналов сотовых телефонов на определённом участке.

Таким образом, в условиях агрессивных действий криминального мира лишь общественное мнение может положительно повлиять на процесс создания условий и возможностей для правоохранительных органов оперативно

использовать современные криминалистические методы, инструменты и рекомендации при выявлении и расследовании преступлений, связанных с дистанционным хищением денежных средств и иных видов киберпреступности.

На наш взгляд, в борьбе с такого рода преступлениями оперативные подразделения должны использовать все возможности информационно-коммуникационных технологий. Стремительный процесс цифровизации на современном этапе развития общества открывает перспективы совершенствования информационных платформ системы МВД России и внедрения в деятельность оперативных подразделений полиции информационно-коммуникационных технологий в целях эффективной борьбы с киберпреступностью.

Итак, все выше исследованные инновационные технологии в борьбе с киберпреступлениями возможно внедрить в деятельность оперативного аппарата МВД по Республике Татарстан, и их использование эффективно отразится на общей картине преступлений в сфере информационно-телекоммуникационных технологий.

# ЗАКЛЮЧЕНИЕ

С популяризацией инновационных технологий, совершенствованием информационных провайдингов, любой гражданин все больше и больше внедряется в Интернет сферу. Исследованию киберпреступности и информационного общества в науке уделяется значительное внимание. Преступления, которые совершаются в информационном пространстве (киберпреступления), появились одновременно с популяризацией первых компьютерных сетей в экономической сфере. В настоящее время киберпреступность – проблема всего человечества.

С развитием информационных технологий появляются широкие возможности для совершения различных киберпреступлений, в частности, псевдо онлайн торговля с предоплатой; с использованием электронных платежных систем; телефонное мошенничество с использованием персональных данных пользователей банковских продуктов (фишинг); банковские операции; вымогательство денежных средств за обеспечение сохранности данных; сохраняют свою актуальность преступления, связанные с игровыми и развлекательными порталами с незаконным контентом; продолжает сохраняться доминирующая роль IT-компаний, осуществляющих разработку антивирусного программного обеспечения и поддержку современных информационных сервисов; мошенничество на сайтах бесплатных объявлений (например, «Авито», «Юла»), кражи денежных средств с банковских счетов юридических и физических лиц, взломы хранилищ персональных данных пользователей (так называемое «Облако»); появляются новые виды вирусов.

Продолжают сохраняться риски совершения киберпреступлений с территории Украины и иных недружественных стран, совершаемых на почве политических разногласий. Имеются тенденции роста преступлений в сфере высоких технологий в глобальном масштабе и на государственном уровне, так как экономически развитые страны различными деструктивными способами, в

том числе используя нетрадиционные методы, осуществляют влияние на экономические процессы развивающихся стран, в частности, путем изучения общественного мнения, с использованием конфиденциальных данных граждан и навязывая им контент, дискредитирующий действующую государственную власть; путем скрытого финансирования общественных объединений, целью которых является подрыв государственного строя; путем внедрения в информационные системы предприятия вредоносного программного обеспечения, например, с целью шпионажа и др.

Поскольку термин «киберпреступность» законодательно не закреплен, на основе исследования, предлагается авторское определение киберпреступности, под которым мы понимаем общественно опасное деяние или совокупность преступлений, совершаемые посредством информационно-телекоммуникационных технологий (включая технические средства, компьютерные сети и системы, а равно их программные элементы).

В процессе исследования криминологической характеристики киберпреступности, мы рассматриваем причины и условия, детерминирующие преступность в информационном пространстве в нескольких аспектах.

Итак, правовое регулирование информационного пространства на сегодняшний день так и не нашло свое отражение в законодательстве России. Отрицательные аспекты общественных проявлений имеют место тогда, когда отсутствует социальный и общественный контроль. Реализация данного вида контроля в сфере киберпреступности затрудняется в связи с объективными причинами. В то же время законодатель слишком мало внимания уделяет охране общественных отношений в области информационных технологий. Их разработка позволила практически безнаказанно совершать киберпреступления.

Социально-экономические факторы в детерминации киберпреступности проявляются в трех группах социальных явлений. 1. Социальные явления, которые связаны с прогрессом: – развитие инновационных технологий и внедрение их во все сферы жизнедеятельности общества; – увеличение количества пользователей Интернет-пространства; – популяризация

электронных кошельков и оплаты посредством Интернет-пространства; – отсутствие прямого контакта при совершении разнообразных операций в Интернет-пространстве. 2. Экономический кризис и его отрицательный результат: – низкий уровень экономического развития страны; – криминализация экономической деятельности – высокий уровень безработицы. 3. Виртуализация жизнедеятельности, распространение социальных сетей, сервисов по определению местонахождения, в частности доступа в них со смартфонов, и, как результат, применение преступниками «пробелов» в программном обеспечении телефонов (смартфонов), и невозможность обеспечить надежность источников их разработки.

К организационно-техническому блоку детерминант киберпреступности следует также относить низкий уровень профессионализма сотрудников правоохранительных органов, в компетенцию которых входит борьба с киберпреступностью; слабое инфраструктурное оснащение правоохранительных органов; дефицит кадрового потенциала. Правоохранительные органы, занимающиеся борьбой с киберпреступностью зачастую не обладают необходимыми специальными знаниями в сфере инновационных (компьютерных) технологий, что последнее сказывается на процессе раскрытия и расследования преступлений, совершаемые посредством информационных технологий.

Самодетерминация киберпреступности как преступный фактор является результатом невозможности контролировать данные, содержащиеся в информационном пространстве. В данном контексте следует говорить о любых данных (к примеру, Интернет-ресурсы, связанные с детской порнографией; со способами незаконного приобретения незаконного оборота наркотических средств; со способами незаконного приобретения информации (персональных данных) и т.п.). К информации, носящей конфиденциальных характер, доступ доступен лишь определенному количеству пользователей (либо одному человеку).

Большое внимание в криминологических исследованиях уделяется личности преступника, в нашем случае киберпреступника. На основе анализа мнений криминологов, мы под личностью киберпреступника понимаем совокупность характерных качеств и черт личности, сформировавшееся под влиянием факторов, детерминирующих преступное поведение в информационном пространстве.

Как правило, киберпреступниками в большинстве случаев являются мужчинами с высшим или неоконченным высшим образованием, поскольку киберпреступники должны обладать высокими навыками и умениями пользования информационными и инновационных технологиями (к примеру, в сфере программирования). Следует отметить, что среди осуждённых лиц за киберпреступления 23,4% были рабочими, 14,4% – служащие. Нынешние киберпреступники мотивированы в финансово-материальном плане, и торговля конфиденциальной информации, особенно от юридических лиц, стала обычным явлением. Зачастую системные администраторы тех или иных организаций встают на криминальный путь. Данная проблема популяризируется в условиях экономического кризиса и сокращения кадров в компаниях и организациях.

Большое внимание в процессе исследования уделялось предупреждению киберпреступности. Предупреждение киберпреступлений требует серьезных усилий со стороны органов государственной власти и общества и может быть эффективным лишь в процессе применении разнообразных общесоциальных и специально-криминологических мер.

Меры общесоциального предупреждения реализуются посредством использования комплексных возможностей государства, которые обеспечивают прогрессивное совершенствование общества, отношений людей в:

1) социально-экономическом: к данному блоку превентивных общесоциальных мер киберпреступности как правило относят нормализацию экономической стабильности страны, укрепление кредитно-денежной политики, совершенствование мероприятий по социальной защите общества,

повышение уровня жизнедеятельности государства, уменьшение уровня безработицы и др.;

2) социально-политическом: важными элементами предупредительных мер в данном направлении являются мероприятия, которые направлены на нормализацию политической стабильности государства; усиление политической власти; формирование эффективного правового регулирования цифровых технологий и киберпреступности; разработка стратегий и планов уголовном и цифровой политики;

3) социально-правовом: в век высокий технологий к данному блоку превенции отводится большое внимание, а именно государству необходимо формировать законодательному базу, отвечающая современным реалиям: принятие ряда нормативно-правовых актов, внесение изменений в ряд существующий нормативно-правовых актов, которые регулируют формирование и использование цифровых технологий, охрану общественных отношений, которые возникают в связи с их использованием в этой сфере, защиту личности, общества и государства не только от их применения инновационных технологий в быту и на производстве, но и в преступных целях.

4) организационно-управленческом: данные мероприятия направлены на осуществление организационных аспектов предупредительной деятельности, принятию государственных решений в сфере охраны, контроля и надзора со стороны органов государственной власти, а также по взаимодействию государства, общественности и иных частных спектров жизнедеятельности.

Фундаметальным элементом общесоциального уровня предупреждения кибепреступности является мониторинг состояния информационного пространства в сфере криминальных проявлений.

Специально-криминологические и индивидуальные меры предупреждения киберпреступности, как и общесоциальное предупреждение требуют комплексного подхода. Исследование жертвы кибепреступлений необходимо, как правило, в целях первичной профилактики. На наш взгляд, аналогичная задача ставится и перед исследователями, которые рассматривают

виктимологические аспекты предупреждения преступлений и киберпреступлений.

Обеспечение комплексного подхода к профилактической деятельности обуславливается в зависимости от направлений и мер профилактических направленностей.

Рассмотрев основные традиционные меры предупреждения киберпреступлений, автором исследовались инновационные технологии борьбы с преступлениями, совершаемых посредством информационно-телекоммуникационных технологий.

Основные преимущества использования информационных технологий заключаются, во-первых, в высвобождении времени у должностных лиц, что позволяет сосредоточить усилия на раскрытии уже совершенных преступлений, а во-вторых, в возможностях искусственного разума, способного выполнять сложнейшие расчеты при выявлении факторов, способствующих совершению преступления, и продумывать алгоритмы борьбы с ними.

Большое внимание отводится *blockchain* системам. Данная система представляет собой весьма сложный механизм, которые способствует оперативному и результативному отбору и обработке информации. В качестве положительных характерных черт *blockchain*-систем следует отразить следующее: прозрачность; отсутствие посредников; безопасность, надежность.

Итак, безопасность *blockchain*-систем заключается в том, что пользователи получают открытый и закрытый криптографические ключи, которые в свою очередь открывают «ворота» к блокам системы *blockchain*. Следует отметить, что оба криптографических ключа запаролены, что дает возможность избежать трансформации информации. Также система оснащена системой *KYC* (функция биометрии) для подтверждения личности пользователя. Надежность *blockchain*-систем подтверждается наличием математических алгоритмов, которые лежат в основе деятельности данной технологии, которые не допускают изменение или добавлений в систему.

Примерный принцип работы технологии *blockchain* представлен в приложении № 4.

На наш взгляд, весьма остро стоит вопрос объема и уровня информационно-технического обеспечения органов внутренних дел в процессе выявления, раскрытия и (или) предупреждения дистанционного хищения денежных средств. Однако, как показывает практика, применение современных баз данных в процессе раскрытия подобных преступлений, совершаемых посредством информационно-коммуникационных технологий – «*Palantir*», «*Osiris*», «*UNODC Sherloc*», «ПСКОВ» и ряда других – представляется малоэффективным. Огромные вычислительные мощности и серьезный штат профессиональных сотрудников необходимы для качественного функционирования подобных систем. Таким образом, большое внимание в борьбе с дистанционным хищением денежных средств, следует отводить укреплению умственного и технического потенциала органов правоохранительной деятельности.

В процессе раскрытия и расследования дистанционного хищения денежных средств сотрудники оперативных подразделений должны использовать различные информационно-коммуникационные технологии, к примеру, такие как *Big Data*. На наш взгляд, возможность централизованного сбора и анализа виртуального следа имеет перспективное значение, так как, по мнению экспертов, в ближайшие несколько лет большие данные «*Big Data*» будут наиболее уязвимы для кибератак – до 70%. И тенденции оцифровки информации предполагают, что риски будут только увеличиваться. Несмотря на это, на сегодняшний день, в условиях цифровизации за счет использования разнообразных аналитико-инновационных технологий становится возможным осуществлять прогнозирование и последующий контроль фактов дистанционного хищения денежных средств.

Таким образом, в условиях агрессивных действий криминального мира лишь общественное мнение может положительно повлиять на процесс создания условий и возможностей для правоохранительных органов оперативно

использовать современные криминалистические методы, инструменты и рекомендации при выявлении и расследовании преступлений, связанных с дистанционным хищением денежных средств и иных видов киберпреступности. Исследованные инновационные технологии в борьбе киберпреступлениями возможно внедрить в деятельность оперативного аппарата МВД по Республике Татарстан, и их использование эффективно отразятся на общей картине преступлений в сфере информационно-телекоммуникационных технологий.

# 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: 14.09.2022).

2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Российская газета. – 2001. – № 249.

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Российская газета. 2006. № 165.

4. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ // Российская газета. – 2016. – № 139.

5. О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ // Российская газета. – 2010. – № 295.

6. О прокуратуре Российской Федерации: Федеральный закон от 17.01.1992 № 2202-1 // Российская газета. – 1995. – № 22.

7. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Российская газета. – 1996. – № 113-115.

8. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Российская газета. – 1995. – № 160.

9. О стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27 (часть II). – Ст. 5351.

10. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02 июля 2021 № 400 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

11. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901.

12. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

13. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 // Российская газета. – 2013. – № 282.

14. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: Указание Генпрокуратуры России № 738/11, МВД России № 3 от 25.12.2020 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

15. О деятельности органов внутренних дел по предупреждению преступлений (вместе с «Инструкцией о деятельности органов внутренних дел по предупреждению преступлений»): Приказ МВД России от 17.01.2006 № 19 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

16. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: Приказ МВД России от 19.06.2012 № 608 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

## II. Монографии, учебники, учебные пособия

17. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие: в 2 ч. / А. В. Аносов [и др.]. – М.: Академия управления МВД России, 2019. – С. 5.

18. Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общей редакцией О. С. Капинус. – 2-е изд., перераб. и доп. – М. : Юрайт, 2022. – С. 1000.

19. Криминология : учебник и практикум для вузов / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. – М. : Юрайт, 2022. – С. 316.

20. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. – М. : Юрайт, 2022. – С. 217.

21. Криминология : учебник для вузов / В. И. Авдийский [и др.] ; под редакцией В. И. Авдийского, Л. А. Букалеровой. – 2-е изд., перераб. и доп. – М. : Юрайт, 2022. – С. 231.

22. Криминология: Общая часть: учебник / под общей редакцией Ф.К. Зиннурова. – Казань : КЮИ МВД России, 2019. – С. 358.

23. Криминология: учебник / В.Ю. Дроздов, Н.Б. Хлыстова – М.: КНОРУС, 2019. – С. 210.

24. Организация деятельности органов внутренних дел по предупреждению преступлений (термины, определения): учебное пособие / под ред. А. В. Аносова, В. И. Старкова, Е. Ю. Титушкиной [и др]. – М., 2016. – С. 75.

25. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. – М. : Юрайт, 2022. – С. 103.

26. Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т.В. Пинкевич. – М. : Юрлитформ, 2020. – С. 163

27. Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. – М. : Академия управления МВД России, 2021. – С. 105.

## III. Статьи, научные публикации

28. Анапольская А.И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств, совершаемых в сфере функционирования электронных расчетов // Вестник ТГУ. – 2019. – №5 (145). – С. 224.

29. Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. – 2018. – № 4 (48). – С. 93-97.

30. Войнов Н.Э. Киберпреступность в Российской Федерации: современное состояние и актуальные проблемы // Киберпреступность: риски и угрозы: сб. ст. рос. научно-практ. круглого стола с междунар. участием (Санкт-Петербург, 11 февраля 2021 г.). – СПб.: Астерион, 2021. – С. 143-147.

31. Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2018. – № 8. – С. 12.

32. Гончарова Т.А., Набоков Л.В. Киберпреступность в России: проблемные аспекты и предупреждение преступности // Инновационная экономика и право. – 2022. – № 1 (20). – С. 121.

33. Гумаров И.А., Фарахиев Д.М. Технология blockchain как средство противодействия // Научный компонент. – 2022. – № 1 (13). – С. 81-87.

34. Даненьян А.А. Международное правовое регулирование киберпространства // Образование и право. – 2020. – № 1. – С. 261-269.

35. Дехерт А.А., Фантров П.П. Детерминанты гиперлатентности преступлений, совершенных в виртуальном пространстве // Высокие технологии и инновации в науке : сборник избранных статей Международной

научной конференции, Санкт-Петербург, 27 ноября 2021 года. – СПб: ГНИИ «Нацразвитие», 2021. – С. 229-232.

36. Желудков М.А., Попов А.М., Дубровина М.М. Особенности противодействия киберпреступности в России и зарубежных странах // Вестник Волгоградской академии МВД России. – 2018. – № 3 (46). – С. 97-102.

37. Исаева М.А. Детерминанты информационных преступлений // Технологии формирования правовой культуры в современном образовательном пространстве : Материалы V Всероссийской научно-практической конференции с международным участием, Волгоград, 27 апреля 2021 года. – Волгоград: Волгоградский государственный аграрный университет, 2021. – С. 251-256.

38. Карабеков К.О. Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2022. – № 22-2. – С. 25-27.

39. Киберпреступность / П. А. Титова, А. А. Жиркова, И. В. Макарова, А. В. Терехов // Инновационные научные исследования. – 2021. – № 2-1 (4). – С. 145.

40. Киберпреступность: понятие, виды / Н. А. Саков, А. А. Поварчук, М. М. Шилков, А. М. Королева // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции, Санкт-Петербург, 30 мая 2020 года. – СПб: ГНИИ «Нацразвитие», 2020. – С. 31-35.

41. Магомадов А.А., Шуайпова Х.Л.Э. Киберпреступление // Вопросы физико-математического образования : материалы XIII студенческой научно-практической конференции, Грозный, 16 мая 2020 года. – Махачкала: Чеченский государственный педагогический университет, ИП Овчинников М.А. (Типография Алеф), 2020. – С. 229-232.

42. Магомедова Х.Б. Отдельные аспекты предупреждения киберпреступности // Проблемы совершенствования законодательства :

сборник научных статей студентов юридического факультета. – Махачкала : ООО «АЛЕФ», 2019. – С. 90-92.

43. Марданов А.Б. Криминологическая характеристика личности киберпреступника // Публичное и частное право. – 2018. – №2. – С. 111-118.

44. Минзянова Д.Ф., Фарахиев Д.М. Инновационный подход к раскрытию и предупреждению преступлений в сфере незаконного оборота наркотических средств, совершаемых в Интернет-пространстве // Ученые записки Казанского юридического института МВД России. – 2022. – Т. 7. – № 1 (13). – С. 74-80.

45. Мухина М.С. Противодействие в сфере киберпреступности // Уголовно-правовые и криминологические направления противодействия преступности : Сборник материалов Межрегиональной научно-практической конференции профессорско-преподавательского состава, аспирантов и студентов, Симферополь, 29 марта 2019 года. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2019. – С. 260-267.

46. Павловец В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования // Альманах современной науки и образования. – 2018. – № 1 (68). – С. 104.

47. Робул В.И. Некоторые характеристики личности киберпреступника // Международный научный журнал «Вестник науки». – 2019. – №8. – С. 21-23.

48. Сабырбаева А.В. Электронные доказательства как новый вид доказательств при расследовании современных форм мошенничества // Review of law sciences. – 2020. – №3 (120). – С. 215-220.

49. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. – 2017. – № 1(73). – С. 137-140.

50. Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – С. 104-106.

51. Соловьев М.Н. Правовые основы регулирования противодействия киберпреступности, безопасность личности в информационном пространстве // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : Сборник статей Международной научно-практической конференции, Москва, 30 октября 2019 года / отв. ред. В.О. Лапин. – М.: Академия управления МВД России, 2019. – С. 214-220.

52. Тарасова Ю.В. Тенденции киберпреступности в Российской Федерации // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции, Санкт-Петербург, 29 сентября 2021 года. – СПб: ГНИИ «Нацразвитие», 2021. – С. 6-13.

53. Фарахиев Д.М. Коррупция как угроза национальной безопасности: пути противодействия // Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения : Материалы международной научно-практической конференции, Санкт-Петербург, 08 апреля 2022 года / Сост. Н.В. Мячин. – СПб: Санкт-Петербургский университет МВД России, 2022. – С. 462-467.

54. Фарахиев Д.М., Минзянова Д.Ф. Перспективы внедрения информационно-коммуникационных технологий в деятельность оперативных подразделений полиции по противодействию коррупции // Современная наука. 2022. № 1. С. 60-63.

55. Фарахиева Г.Р. Социальная среда как фактор вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов // Вестник Казанского юридического института МВД России. – 2021. – Т. 12. – № 4 (46). – С. 555-560.

56. Харламов, А.А. Проблемные вопросы квалификации мошенничества с использованием платежных карт // Вестник Уральского юридического института МВД России. – 2017. – № 1. – С. 44-47.

57. Шалагин А.Е., Идиятуллов А.Д. Новые тенденции преступности в XXI веке: глобализация, цифровизация, социальный контроль // Modern Science. – 2020. – № 11. – С.131-134.

58. Шалагин А.Е., Идиятуллов А.Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. – 2021. – Т. 12. – № 2(44). – С. 227-235.

59. Шалагин А.Е., Идиятуллов А.Д., Шалагина А.К. Причины девиантного поведения подростков и молодежи // Modern Science. – 2020. – № 12-4. – С. 274-278.

60. Швец А.В., Гайдук В.А. Проблемы и особенности выявления, документирования и правового регулирования киберпреступности в Российской Федерации // Вестник Амурского государственного университета. Серия: Гуманитарные науки. – 2021. – № 94. – С. 17-21.

61. Шишкин А.А. Уголовно-правовая характеристика киберпреступности // Молодежь и наука: шаг к успеху : Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок молодых ученых. В 5-ти томах, Курск, 19-20 марта 2020 года / Отв. ред. А. А. Горохов. – Курск: Юго-Западный государственный университет, 2020. – С. 373-375.

## IV. Эмпирические материалы (материалы судебной практики)

62. Приговор Коминтерновского районного суда г. Воронежа № 1-525/2020 от 24 июля 2020 г. по делу № 1-525/2020. URL: https://sudact.ru/regular/doc/nV1W3qNJLirI/ (дата обращения: 20.09.2022).

63. Приговор Хасавюртовского городского суда № 1-261/2020 от 20 июля 2020 г. по делу № 1-261/2020. URL: https://sudact.ru/regular/doc/SlYwK6TxKKNT/ (дата обращения: 20.09.2022)

64. Приговор Чусовского городского суда № 1-175/2020 от 24 ноября 2020 г. по делу № 1-175/2020. URL: https://sudact.ru/regular/doc/kQeGaLsl08H8/ (дата обращения: 20.09.2022).

## V. Справочная литература

65. Group-IB назвала ключевые тенденции киберпреступлений в период пандемии // Group-IB. URL: https://www.group-ib.ru/media/covid-cybercrime-trends/ (дата обращения: 11.09.2022).

66. Группа Silence-новая угроза для банков. URL: https://www.group-ib.ru/resources/threat-research/silence.html (дата обращения: 10.10.2022).

67. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Официальный сайт Генеральной Прокуратуры. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения 15.09.2022).

68. Организация правоохранительной системы в некоторых федеративных странах мира. URL: https:// komitetgi.ru/upload/iblock/538/538b9dcf40eca849375fa5f15da10d26.pdf (дата обращения: 10.10.2022).

69. «Сбербанк» представил статистику финансовых киберпреступлений. URL: https://tproger.ru/news/sberbank-cyberattack-statistics/ (дата обращение: 10.10.2022).

70. Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 17.09.2022).

71. Стратегические приоритеты сотрудничества в области противодействия киберпреступности в странах Восточного партнерства. URL: https://rm.coe.int/1680300ad3 (дата обращения: 01.10.2022).

72. Судебный департамент при Верховном суде Российской Федерации. URL: http://cdep.ru/ (дата обращения: 10.01.2023).

## *ПРИЛОЖЕНИЕ 1.*

## *Статистические данные о преступности в Российской Федерации*

*1. Количество зарегистрированных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий*

| | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| ***Преступления, совершенные с использованием компьютерных и телекоммуникационных технологий*** | 174 674 | 294 409 | 510 396 | 517 722 | 522 065 |

*1.1. Количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий*

| ***Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий*** | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| компьютерной техники | 18 261 | 28 653 | 27 519 | 29 140 |
| с использованием или применением: расчетных (пластиковых) карт | 34 383 | 190 167 | 165 658 | 127 149 |
| сети "Интернет" | 157 036 | 300 337 | 351 463 | 381 112 |
| средств мобильной связи | 116 154 | 218 739 | 217 552 | 212 963 |

*1.3. Наиболее распространенные преступления, совершаемые посредством информационно-телекоммуникационных технологий*

| ***Наиболее распространенные преступления, совершаемые посредством информационно-телеккомуникационных технологий*** | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| ст. 158 УК РФ | 98 798 | 173 416 | 156 792 | 113 565 |
| ст. 159 УК РФ | 119 903 | 210 493 | 238 560 | 249 984 |
| ст. 159.3 УК РФ | 16 119 | 25 820 | 10 258 | 7 288 |
| ст. 228.1 УК РФ | 24 677 | 47 060 | 51 444 | 62 209 |

## *ПРИЛОЖЕНИЕ 2.*

## *Уровень образования киберпреступников*

| Образование | Доля от общего числа осужденных киберпреступников, в % |
|---|---|
| Высшее, неоконченное высшее | 29,7 |
| Среднее специальное | 37,4 |
| Среднее общее | 26,3 |
| Неполное среднее | 6,3 |

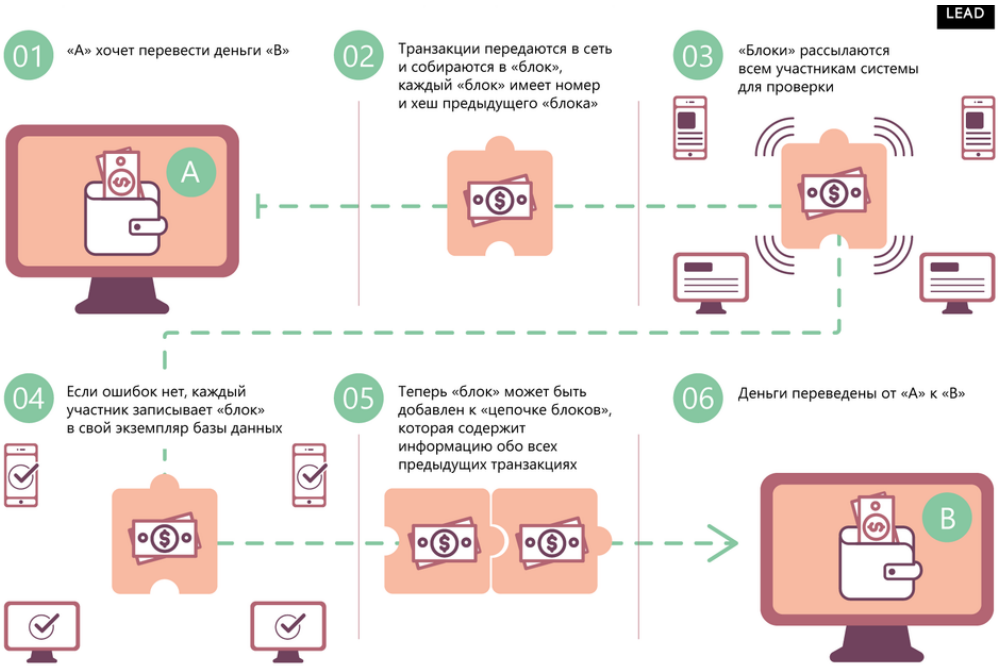
## *ПРИЛОЖЕНИЕ 3.*

## *Уровень занятости киберпреступников*

| Социальный статус | Доля от общего числа осужденных киберпреступников, в % |
|---|---|
| Рабочий | 23,4 |
| Государственный и муниципальный служащий | 1,3 |
| Служащий коммерческой или иной организации | 14,4 |
| Предприниматель | 5,5 |
| Учащийся, студент | 10,2 |
| Нетрудоспособный | 0,8 |
| Сотрудники правоохранительных органов | 0,4 |
| Лица прочих занятий | 1,3 |
| Инвалиды | 0,8 |

## *ПРИЛОЖЕНИЕ 4.*

## *Принцип работы технологии blockchain*




*Для того, чтобы осуществить перевод денежных средств от пользователя А – пользователю В, необходимо внести в систему blockchain новый блок, содержащий hash предыдущего блока и новый, который характерен только для данного пользователя. Поскольку технология blockchain не имеет единого сервера, а поддерживает работу на базе масштабного числа персональных компьютеров пользователей. Каждый уже имеющийся в общей цепочке блок отправляется всем пользователям системы вместе с новым для согласованности друг с другом и для проверки конечного результата. Если ошибок не обнаружено, каждому пользователю добавляется новый блок в свою тестовую базу данных. После успешного прохождения проверки и реализации вышеуказанных механизмов новый блок, внесенный пользователем А., может быть добавлен в «цепочку блоков», содержащую информацию обо всех предыдущих транзакциях. Итоговым положительным результатом является перевод денежных средств от пользователя А. к пользователю В.*

# ОТЗЫВ

о работе обучающегося 082 учебной группы
очной формы обучения, 2018 года набора,
по специальности 40.05.02 –Правоохранительная деятельность
Осипова Никиты Алексеевича
в период подготовки дипломной работы
на тему «Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по Республике Татарстан)»

Тема дипломной работы Осипова Н.А. «Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по Республике Татарстан)» была выбрана из списка, предложенного кафедрой, и не лишена актуальности. Число киберпреступлений увеличивается прямо пропорционально числу пользователей информационного пространства. Так, согласно статистическим данным за последние пять лет, следует, что в 2018 году было зарегистрировано 174 674, в 2019 году – 294 409, в 2020 году – 510 396, в 2021 году – 517 722, в году 2022 – 522 065 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. На основе представленных данных, за последние несколько лет преступления, совершенные с использованием компьютерных и телекоммуникационных технологий, увеличились практически в два раза.

В соответствии с выбранной темой автор, совместно с научным руководителем разработал план исследования, который имеет логическую структуру и последовательно раскрывает исследуемую проблему, кроме того Осиповым Н.А. были сформулированы цель и задачи, объект и предмет исследования. Определены методы исследования.

Инициативность слушателя Осипова Н.А. в выборе методов исследования, постановки цели и задач, способах описания результатов исследования на удовлетворительном уровне. Контакты с научным руководителем, необходимые для научно-методического обеспечения работы, поддерживал в соответствии с имеющимися потребностями. В выполнении структурных элементов работы в установленные научным руководителем сроки показал удовлетворительную пунктуальность. Работа по устранению выявленных замечаний и недостатков проводилась своевременно, но с не достаточной степенью внимательности и ответственности. В процессе работы над исследовательской частью Осипов Н.А. показал умения анализа статистических данных, работы с материалами судебной и следственной

практики, а также пользования научной литературой и применения их в исследовании.

В ходе написания дипломной работы слушатель Осипов Н.А. продемонстрировал способности: самостоятельно формулировать результаты исследования, владеть компьютерными методами сбора и обработки информации, используемой в сфере профессиональной деятельности, работы с компьютерными программами, информационно-справочными ресурсами, работы в системе Интернет.

Структура исследования построена с учетом характера темы, а также степени научной разработанности затрагиваемых в ней проблем. Дипломная работа состоит из введения, заключения, трех глав, поделенных на девять параграфов, списка использованной литературы.

Уровень оригинальности и оформление исследования соответствуют предъявляемым требованиям.

Дипломная работа слушателя Осипова Н.И. на тему: «Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по Республике Татарстан)» является оконченным научным исследованием, может быть рекомендована к публичной защите и заслуживает положительной оценки.

Руководитель:

доцент кафедры криминологии и
уголовно-исполнительного права
КЮИ МВД России, к.ю.н.
подполковник полиции А.М. Хафизова

Подпись А.М. Хафизовой
УДОСТОВЕРЯЕТСЯ
ОД и РКЮИ МВД России

«27» 04 2023 г.

С отзывом ознакомлен Н.А. Осипов

«27» 04 2023 г.

**РЕЦЕНЗИЯ**

на дипломную работу
обучающегося 082 учебной группы
очной формы обучения, 2018 года набора,
по специальности 40.05.02 – Правоохранительная деятельность

Осипова Никиты Алексеевича
на тему «Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по Республике Татарстан)»

В современном мире развитие высоких технологий тесно взаимосвязано с потребностями человека, ведь их создание позволило обеспечить доступность и автоматизированость в различных сферах жизнедеятельности общества. Но есть лица, которые используют их во вред - киберпреступники

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Опасность заключается в том, что киберпреступления, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем, – это несанкционированный доступ незаконный перехват и противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных или систем, а также кибертерроризм.

Заявленная тема автором отражена в полном объеме. При этом, в основе раскрытия темы автор использовал статистические данные ГИАЦ МВД России, статистические данные от сотрудников отдела «К» МВД по РТ (ОБК МВД по РТ), проведенние анкетирования сотрудников, которые занимаются раскрытием преступлений в сфере IT-технологий и сети «Интернет», а также открытую статистику, благодаря чему смог передается полнота состояния преступности данной в сфере. Раскрывая вопросы дипломной работы, удалось отразить различные точки зрения на решение поставленных задач, обозначить свое мнение, подкрепленное совокупность аргументов, что дает основание считать работу выполненной на достаточно высоком теоретическом и практическом уровне.

Структура работы логична и соответствует плану-графика выполнения выпускной квалификационной работы, и состоит из введения, трех глав, девяти параграфов, заключения и списка литературы. Материал оформлен правильно, изложен последовательно, систематично и доступно. Главы раскрывают содержание темы, по ходу работы цели исследования становятся достигнуты.

Список литературы по данному вопросу достаточно полный, отражает современное состояние исследуемой проблемы. Дипломная работа говорит о том, что слушатель хорошо владеет учебными и нормативными материалами.

В целом, выпускная квалификационная работа слушателя Осипова Н.А. выполнена на достаточном уровне, показывающий самостоятельный и творческий подход к исследованию проблемы.

Достоинствами работы является четкость позиции автора при решении выявленных проблем, отличная практическая значимость, обоснованность выводов и польза предложений. Стоит отметить, что при написании работы использовались научные термины и профессиональный сленг, при этом данные понятия объясняются доступным для понимания языком.

Таким образом, с учетом изложенного, полагал бы необходимым сделать следующий вывод по выпускной квалификационной работе Осипова Н.А.: работа имеет исследовательский характер, хорошо изложенную теоретическую часть, логичное и последовательное изложение материала с соответствующими выводами и обоснованными предложениями. В ней автор показывает свое знание вопросов рассматриваемой им темы и действующего российского законодательства, свое умение ориентироваться в источниках права и применения его при изложении материала, а также владение современными методами исследования.

С учетом изложенного, полагал бы необходимым рекомендовать выпускную квалификационную работу Осипова Н.А по теме «Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по РТ)».

Рецензент
Заместитель начальника ОП №3 «Зареченский»
УМВД России по г. Казани
подполковник полиции Р.Р. Казаков
«24» апреля 2023 г.

С рецензией ознакомлен Н.А. Осипов
«24» апреля 2023 г.

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Казанский юридический институт МВД России

# СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

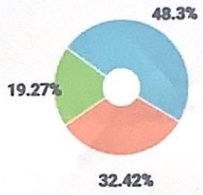
**ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ**

**Автор работы:** Осипов Никита Алексеевич
**Самоцитирование рассчитано для:** Осипов Никита Алексеевич
**Название работы:** Криминологическая характеристика и предупреждение киберпреступности (по материалам МВД по РТ)
**Тип работы:** Дипломная работа
**Подразделение:**

## РЕЗУЛЬТАТЫ

| | |
|---|---|
| СОВПАДЕНИЯ | 32.42% |
| ОРИГИНАЛЬНОСТЬ | 48.3% |
| ЦИТИРОВАНИЯ | 19.27% |
| САМОЦИТИРОВАНИЯ | 0% |

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 27.04.2023




**Модули поиска:** ИПС Адилет; Библиография; Сводная коллекция ЭБС; Интернет Плюс; Сводная коллекция РГБ; Цитирование; Переводные заимствования (RuEn); Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по Интернету (EnRu); Переводные заимствования издательства Wiley (RuEn); eLIBRARY.RU; СПС ГАРАНТ: аналитика; СПС ГАРАНТ: нормативно-правовая документация; Модуль поиска "КЮИ МВД РФ"; Медицина; Сводная коллекция вузов МВД; Диссертации НББ; Перефразирования по eLIBRARY.RU; Перефразирования по СПС ГАРАНТ: аналитика; Перефразирования по Интернету; Патенты СССР, РФ, СНГ; Коллекция СМИ; Шаблонные фразы; Кольцо вузов; Издательство Wiley

**Работу проверил:** Хафизова Альбина Мансуровна

ФИО проверяющего

**Дата подписи:** 27.04.2023

Подпись проверяющего

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

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