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

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему Криминогенный потенциал сети Интернет: проблемы предупреждения и противодействия преступлениям в информационной сфере

Выполнил: Самигуллин Нияз Сайдашевич

40.05.02 – Правоохранительная деятельность, год набора 2017
073 учебная группа

Руководитель:
д.п.н., профессор кафедры криминологии и уголовно-исполнительного права
КЮИ МВД России
полковник полиции,
Чанышева Гульнара Габдулхаковна

Рецензент:
начальник отделения раскрытия преступлений, совершенных с использованием информационно-телекоммуникационных технологий
УМВД России по г. Казани
старший лейтенант полиции
Алиев Валех Мубаризович

Дата защиты: "____" _____20___г. Оценка _____

Казань 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. На сегодняшний день наиболее быстро развивающейся является сфера высоких технологий, которая порождает возникновение новых угроз в области телекоммуникаций и сфере цифровых технологий. В связи с чем, следует вывод, что криминогенный потенциал сети Интернет набирает свои обороты, вовлекая в информационную сферу такие виды преступлений, которые ранее совершались только при непосредственном контакте с потенциальной жертвой. Однако, возможности сети Интернет, такие как, возможность сохранить анонимность, скрыть свое местоположение и многие другие значительно расширяют криминальные возможности и потенциал сети Интернет. На наш взгляд, криминогенный потенциал сети Интернет объединяет в себе такие аспекты, как: информационная сфере, сеть Интернет, инновационные технологии и киберпреступления. Следует также отметить, что криминогенный потенциал сети Интернет год за годом лишь возрастает, из чего следует вопросы повышения предупредительной деятельности со стороны государства, в том числе правоохранительных органов, что выступает актуальностью настоящей выпускной квалификационной работы.

Стоит отметить, что количество преступлений, совершенных с использованием информационных технологий, с каждым годом набирает все большие и большие обороты, которые отрицательно сказываются на жизни не только граждан отдельного государства, но и всего мира.

Необходимо обратиться к официальной статистике Министерства внутренних дел Российской Федерации, которая показывает, что за январь–ноябрь 2021 года посредством применения информационно-телекоммуникационных технологий было совершено 157 306 противоправных деяний, а за аналогичный период 2020 года – 814 301. Это свидетельствует о том, что всего лишь за один год доля преступлений, совершаемых с

применением информационно-телекоммуникационных технологий, выросла почти наполовину[1].

Следует отметить, что большое количество преступлений в информационной сфере, связанны с мошенническими действиями. Таким образом, полагаем, что главным аспектом, положенным в основу определения актуальности темы исследования, следует считать наличествующие трудности правоприменительной практики, а также пробелы правового регулирования деятельности подразделений уголовного розыска по организации предупреждения и раскрытия преступлений, совершаемых в информационной сфере. В связи с чем, большое внимание в процессе исследования было уделено мошенничеству, совершаемого посредством информационно-коммуникационных технологий.

Целью настоящей выпускной квалификационной работы является комплексное исследование проблем предупреждения и противодействия преступлениям, совершаемым в информационной сфере посредством информационно-коммуникационных технологий.

Для достижения цели настоящей выпускной квалификационной работы необходимо решить ряд задач:

1. Рассмотреть криминологическую характеристику преступлений в сфере высоких технологий;

2. Изучить сущность и особенности криминогенного потенциала сети интернет;

3. Исследовать криминологическую характеристику личности преступника, совершающего преступления в сети интернет;

4. Проанализировать причины и условия совершения преступлений, способствующие увеличению криминогенного потенциала сети интернет;

5. Рассмотреть меры по предупреждению преступлений, совершаемые в сети интернет;

---

[1] Официальный сайт Министерства внутренних дел РФ. URL: http://mvd.ru/presscenter/statistics/reports/item/804701 (дата обращения: 01.05.2022).

6. Совершенствование мер по предупреждению преступлений, совершаемых в информационной сфере.

Объектом настоящей выпускной квалификационной работы выступают общественные отношения, возникающие в процессе совершения преступлений в информационной сфере посредством информационно-коммуникационных технологий.

Предметом настоящей выпускной квалификационной работы являются наиболее эффективные меры предупреждения преступлений, совершаемые в информационной сфере.

Методологическая основа исследования включает в себя систему идей научного познания, а именно: универсально-металогический диалектический метод и структурно-системный подход; общенаучные (анализ, индукция, дедукция, обобщение) и частнонаучные (уголовно-статистический, изучение нормативно-правовых актов, результаты социологического исследования криминологов) методы познания.

Теоретическую основу исследования составили научные труды и исследования в рассматриваемой нами проблеме по следующим дисциплинам: криминология[1], уголовное право[2], уголовно-процессуальное право[3] и криминалистика[4], оперативно-розыскная деятельность[5] и другие науки.

---

[1] См.: Горшенков Г.Н. Криминология: научные инновации: Монография. – Н. Новгород: Изд-во Волго-Вятской академии государственной службы, 2009. – 212 с.; Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. – Москва. : Академия управления МВД России, 2021. – 244 с.

[2] См.: Фадина, Ю. П. Уголовно – правовая характеристика мошенничества в сети Интернет/ Ю.П. Фадина // Вестник Югорского Государственного университета. – 2017. № 4. – С. 117-121; Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с.

[3] Обеспечение законности в сфере цифровой экономики : учебное пособие для вузов / А. О. Баукин [и др.] ; под редакцией Н. Д. Бут, Ю. А. Тихомирова. — Москва : Издательство Юрайт, 2020. — 250 с.

[4] Васильев, А. А. Электронные носители данных как источники получения криминалистически значимой информации: учебное пособие / А. А. Васильев; К. Е. Демин. – М.: МГОУ, 2009. – 200 с.

[5] Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло; Ун-т прокуратуры Рос. Федерации. – М., 2018. – 184 с.

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

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

Степень научной разработанности проблемы. Различными аспектами исследования преступлений, совершаемые в информационной сфере занимались такие авторы, как: В.И. Авдийский, Ю.М. Антонян, О.Р. Афанасьева, А.Г. Березуцкая, Т.Н. Богданова, Б.В. Борин, А.Н. Варыгин, Ю.В. Гаврилин, А.И. Гайдин, С.В. Горовенко, Н.А. Данилова, А.И. Долгова, Л.А. Доровских, К.Н. Евдокимов, Е.С. Изюмова, Я. Г. Ищук, Т.П. Кесареева, А.А. Комаров, И.А. Кравцов, Д.В. Кузьменко, В. В. Кульков, С.П. Кушниренко, Ю.А. Мерзлов, В.Р. Петушинова, М.А. Простосердов, А.Ю. Решетников, А.В. Ростокинский, А.Н. Саржин, А.Д. Саркисян, С.М. Сергеев, А.П. Симонов, В.Г. Степанов-Егиянц, Е Ю. Титушкина, А.Ю. Тутуков, А.И. Фоменко, А.А. Харламова, Н.Р. Шевко, Н.А. Щеголева, А.Е. Яблонская и др.

Апробация и внедрение в практику результатов исследования. Основные положения исследования были отражены в процессе участия в следующих научно-практических конференциях:

1. Всероссийская научно-практическая конференции на тему: «Актуальные проблемы правоохранительной деятельности по борьбе с

преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий», Казань (КЮИ МВД РФ), 18 мая 2022 года – «Деятельность оперативных подразделений органов внутренних дел по предупреждению мошенничеств, совершаемых посредством информационных технологий»;

2. Всероссийский круглый стол с курсантами и слушателями Казанского юридического института МВД России, проходивший 26 марта 2022 г. – «Способы борьбы с организованной преступностью в сфере высоких технологий».

Структура настоящей выпускной квалификационной работы. Работа состоит из введения, трех глав, включающих шесть параграфов, заключения, списка литературы.

ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КРИМИНОГЕННОГО ПОТЕНЦИАЛА СЕТИ ИНТЕРНЕТ

§1. Криминологическая характеристика преступлений в сфере высоких технологий

Одним из важнейших условий нормальной жизнедеятельности человека и полноценного функционирования общества, в целом, есть постоянная информационная связь с окружающим миром. На современном этапе развития социума и совершенствования информационных технологий человек становится все более зависимым от потока социально значимой информации, которая поступает через сообщения средств массовой информации, средств массовой коммуникации.

В настоящее время, криминогенный потенциал сети Интернет заключается в том, что большинство преступлений совершаются посредством информационного пространства и (или) информационно-телекоммуникационных технологий, что вызывает чрезмерную опасность. К наиболее часто совершаемый преступления в сети Интернет относятся:

1) кибертерроризм;

2) мошенничество;

3) сексторция (сочетание секса и вымогательства) использует нефизические формы принуждения для вымогательства сексуальных услуг у жертвы);

4) наркопреступления;

5) экономическую преступность;

6) незаконный оборот оружия.

По нашему мнению, отдельный интересе криминогенного потенциала сети Интернет выступает совершение мошенничества посредством информационного пространства. Противодействие преступлениям совершаемых посредством сети Интернет является одной из наиболее актуальных проблем, требующее разработки новых форм и методов борьбы с

ними. Как отмечает К.Н. Евдокимов, использование современных информационных технологий в промышленной, торговой, банковской, научной, культурной, образовательной и других сферах общественной жизни детерминировали динамический рост и качественное обновление компьютерной преступности в России, что создает новые угрозы для развития общества и государства[1].

Важными и необходимыми элементами научного обеспечения предупреждения преступности является унификация и легитимизация терминов и определений, заметно сужающие возможность их расширительного толкования, включая и процесс правоприменения.

В научном сообществе криминогенный потенциал сети Интернет сопоставляют с преступления, совершаемые в сфере высоких технологий и киберпреступностью, что вызывает массу противоречий. К примеру, противоречия в трактовке «преступления, совершаемые в сфере высоких технологий» вызваны тем, что сама сфера высоких технологий в современном ее охвате и понимании обширна, к ней относятся традиционные наукоемкие отрасли: информационные технологии, электроника, генная инженерия, робототехника, нанотехнологии и сравнительно недавно появившиеся современные направления: искусственный интеллект, блокчейн[2].

Следует отметить, в научных кругах имеется мнения, касательно определения беспроводной связи. Так, Ю.В. Гаврилин считает беспроводную связь, промышленный интернет, виртуальную и дополненную реальность, искусственный интеллект признанными основными сквозными цифровыми технологиями[3].

---

[1] Евдокимов К. Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. – 2018. – № 2(24). – С. 62-66.

[2] Аносов А.В. Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. – 2018. – Т. 9. – № 2. – С. 111-115.

[3] Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии МВД России. – 2017. – № 4 (44). – С. 45-50.

В современной криминологии понятие «высокие технологии» ассоциируют, как правило, с совершением преступлений в информационно-телекоммуникационной среде с использованием компьютеров или различных средств связи.

Термин «преступления в сфере высоких технологий» ученые рассматривают с разных научных позиций. В свою очередь, Н.Р. Шевко считает, что понятие «преступления, совершаемые с использованием высоких технологий» носит собирательный характер, употребляется в случаях, когда для совершения традиционных в уголовном праве преступлений используются информационные технологии, ответственность за которые предусмотрена статьями различных глав УК РФ: 146, 159.3, 159.6, 187[1].

Считаем, что, понятие «преступления, совершаемые с использованием высоких технологий» и понятие «преступления в сфере компьютерной информации», ответственность за которые предусмотрена в статьях главы 28 УК РФ, имеют существенную разницу. Мнение ряда ученых фактически уравнивает высокие технологии и информационные технологии, в то же время отделяя высокие технологии от сферы компьютерной информации.

Другие авторы, в лице А.И. Фоменко считает, что термин «преступления в сфере высоких технологий» необходимо использовать как самостоятельную уголовно-правовую категорию в российском и международном уголовно-правовом законодательстве, так как введение этой категории преступлений необходимо в целях охраны прав и интересов личности, общества и государства в информационной среде[2].

Некоторые авторы отождествляют преступления в сфере высоких технологий с преступлениями, совершаемыми при помощи

---

[1] Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. – 2016. – Т. 1. – № 1 (1). – С. 13-16.

[2] Фоменко А.И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития // Интеллектуальные ресурсы - региональному развитию. – 2015. – № 1-5. – С.217-222.

телекоммуникационных сетей, включая сеть Интернет. Д.К. Чирков и А.Д. Саркисян относят преступления в сфере высоких технологий к новым видам и способам совершения преступлений, возникшим в результате распространения сети Интернет, информационно-телекоммуникационных сетей[1].

В своем диссертационном исследовании Т.П. Кесарева определяет преступность в сети Интернет как «запрещенные уголовным законом общественно опасные деяния, совершенные путем вхождения в сеть Интернет с использованием средств компьютерной техники, подключенных к сети Интернет», относит ее к сегменту преступлений в сфере высоких технологий[2].

Сегодня в связи с увеличением объема различной информации, размещаемой в сети Интернет, растет численность аудитории интернет-изданий (электронного дайджеста, социальной сети, интернет-блога и т. п.). Это объясняется нарастающей с каждым днем доступностью Интернета и сравнительно низким уровнем цензуры публикуемых сведений. Размещаемая в сети информация при условии ее правильного донесения до аудитории – мощный инструмент формирования общественного мнения относительно какого-либо события в жизни социума в целом или конкретной публичной личности. В целях создания собственного положительного имиджа, дискредитации политических противников или конкурентов в бизнесе те или иные представители политической и бизнес-элиты все чаще на возмездной основе прибегают к услугам так называемых блогеров для организации информационных атак, порой перерастающих в настоящую информационную войну.

---

[1] Чирков Д.К., Саркисян А.Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. – 2017. – № 1 (24). – С. 25-32.

[2] Кесареева, Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук : 12.00.08 : Москва, 2002. – 195 с.

Учитывая разнообразные точки зрения на толкование понятия «преступления в сфере высоких технологий», представляется, что проблемы базируются на осмыслении его соответствия нормативно-правовым актам.

На основании вышеизложенного сделаем следующие выводы: нецелесообразно разделять информационные технологии и компьютерную информацию. В примечании к ст. 272 УК РФ под компьютерной информацией понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

В федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» дается определение: «Компьютерная информация – это одна из разнообразных форм представления информации». Законом определено содержание информационных технологий: это «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»[1].

На наш взгляд, компьютерная информация – составляющая информационных технологий, поэтому неоправданно разделять информационные технологии и компьютерную информацию, что значительно сужает их содержание.

Преступления, совершенные с использованием информационно-телекоммуникационных технологий, составляют все большую долю в структуре преступности. В условиях пандемии произошел огромный скачок совершения преступлений в сфере мошенничества (ст.ст. 159-159.6 УК РФ) на 88,4% с 999 до 1 865. Активное использование населением в условиях ограничений современных информационных технологий (в частности, сети

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 02.05.2022).

Интернет) создало благоприятную почву для совершения преступлений против собственности с использованием именно кибертехнологий[1].

Дмитрий Медведев на международном форуме «International Cybersecurity Congress» заявил: «Проблема киберпреступности входит в топ-5 по глобальности и наносимому ущербу среди преступлений, её ставят выше порой даже экологических угроз, терроризма и экстремизма»[2].

Удельный вес составил 17,3%, в том числе рост числа преступлений, совершенных с применением сети Интернет – на 31,9% (с 1 133 до 1 494), компьютерной техники – на 50,5% (с 111 до 167), средств мобильной связи – на 6,7% (с 1 220 до 1 302) по сравнению с прошлым годом. Своеобразным катализатором стала пандемия, которая повлекла «уход в онлайн» многих сфер жизнедеятельности общества.

Раскрываемость данного блока преступлений остается достаточно низкой, поскольку установить личность преступника в сети сложно. Но за 10 месяцев 2021 года очевиден рост раскрываемости до 29,4%, несмотря на общий рост количества преступлений данной группы.

Данный вид мошенничества характеризуется тем, что совершается путем применения в процессе средств мобильной (чаще всего – сотовой) связи; возможностей сети Интернет; компьютерного и иного программируемого оборудования.

Следует отметить, что «согласно последнему исследованию Всероссийского центра изучения общественного мнения (далее – ВЦИОМ), «сталкиваться с противоправными действиями, связанными с сотовой связью

---

[1] Петушинова, В. Р. Криминологическая характеристика преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в Республике Бурятия / В. Р. Петушинова // Вестник науки. – 2022. – Т. 5. – № 1(46). – С. 159-164. – EDN MJYMEU.

[2] Международный конгресс по кибербезопасности. URL: https://icc.moscow/ru/ (дата обращения: 10.04.2022).

и интернет–сервисами» довелось 31% жителей России, то есть трети россиян»[1].

Как справедливо сегодня утверждают криминологи, необходимо полное понимание причин и условий, определяющих развитие данного вида преступлений. Криминологами выдвигались предложения по совершенствованию законодательства в части регулирования деятельности по выявлению ресурсов интернет-сети, содержащих запретную информацию. Они предлагают привлекать к юридической ответственности интернет-провайдеров, которые не ограничивают своим клиентам доступ к подобным ресурсам[2]. Так же есть предложение, что помимо предупреждения преступлений в сети Интернет, заняться урегулированием вопроса в части мобильной связи. Установить санкции для операторов мобильной связи за ненадлежащий контроль своих абонентов, когда любой гражданин может получить сим-карту с индивидуальным номером не на свое имя прямо на улице от лица, просто раздающего их даром.

Ряд научных деятелей в собственных исследованиях отмечают, что большая часть хищений с использованием поддельных банковских карт совершается высокоорганизованными преступными группами, отдельными членами которых являются лица с соответствующим техническим образованием, полученным как самостоятельно, так и в высших учебных заведениях, но всегда отличающиеся высоким уровнем технической подготовки[3]. Представляется, что таким образом проявляется своего рода «разделение труда», при котором в рамках преступной группы одни ее члены

---

[1] Треть россиян стали жертвами интернет–мошенников. URL: https://news.rambler.ru/articles/35808456/?utm_content=rnews&utm_medium=read_more&utm_source=c opylink (дата обращения: 02.05.2022).

[2] Горовенко С.В., Изюмова Е. С. Проблема предупреждений правонарушений в сфере игорного бизнеса в сети Интернет // Вестник Челябинского государственного университета. – 2018. – № 17. – Право. Вып. 43. – С. 25-29.

[3] Данилова Н.А., Кушниренко С.П., Саржин А.Н. Преступления в сфере банковской деятельности как высокотехнологичные преступные посягательства международного характера // Вестник Санкт–Петербургского университета МВД России. – 2018. – № 2. – С. 329–333.

занимаются изготовлением, либо приобретением необходимого оборудования, вторые – устанавливают считывающие устройства на банкоматы (или иные устройства аналогичного назначения), третьи – изготавливают поддельные пластиковые карты, четвертые – наносят полученные данные на фальшивые инструменты платежа, а пятые – обналичивают денежные средства.

Международный характер исследуемого направления преступной деятельности проявляется в том, что участниками схемы незаконной деятельности могут быть граждане нескольких государств, а также участники международных преступных организаций, кроме того, процесс получения данных и изготовления поддельной банковской карты может быть реализован на территории одной страны, а получение денежных средств с нее произведено в другой стране.

В целом, в защите от преступлений, совершаемые в информационном пространстве и (или) сети Интернет, постоянно появляющиеся новые виды противоправных действий ведут за собой и эволюцию методов защиты. Приходится признать при этом, что в настоящее время система профилактики и предупреждения преступлений в анализируемой сфере практически отсутствует, а механизмы привлечения правонарушителей к уголовной ответственности недостаточно отработаны и, как следствие, малоэффективны. Все это приводит к выводу о необходимости разработки методологической основы как профилактики, так и противодействия преступлениям корыстной направленности в сфере систем безналичных расчетов.

§2. Сущность и особенность криминогенного потенциала сети интернет

Рассматривая криминогенный потенциал сети Интернет, следует рассмотреть сущность, свойства и особенности совершения преступления в информационной сфере. Так, совершаемые преступления в информационной сфере и (или) с использованием сети Интернет – это элемент

криминологической, криминалистической и оперативно-розыскной характеристики данного вида преступлений, которым характеризуются места совершения данной формы хищений, время их совершения, а также ряд других факторов и особенностей, прежде всего, условия реализации преступных замыслов.

Из преступлений, совершенных в информационной сфере и (или) с использованием сети Интернет, на современном этапе, большая часть связана с мошенническими действиями, повышающие криминогенный потенциал сети Интернет. Во многом это связано с тем, что на современном этапе присутствует большое количество разнообразных видов преступлений. Как правило, выделение того или иного вида преступления, совершаемого в информационной сфере и (или) с использованием сети Интернет осуществляется в зависимости от схемы, положенной в основу его совершения. Вместе с тем, изменение схемы совершения соответствующим образом сказывается на изменении обстановки его совершения, месте и времени, в рамках которых данные преступные деяния совершаются. Это необходимо учитывать при установлении и соответствующем исследовании такого элемента характеристики того или иного преступления в сети Интернет, как обстановка совершения.

Во многом обстановка совершения преступлений в информационной сфере и (или) с использованием сети Интернет характеризует анонимностью и отсутствием личного контакта между преступником (преступниками) и жертвой (жертвами) преступлений. Так, в случае отсутствия контакта, совершения так называемых бесконтактных преступлений, совершаемых в информационной сфере и (или) с использованием сети Интернет, в том числе мошенничеств, типичные характеристики обстановки преступления, как место и время его совершения практически утрачивают свое криминологическое и оперативно-розыскное значение. Преступники, реализуя бесконтактные противоправные действия, практически не «привязывают» себя к пространственно-временным особенностям и характеристикам. Поэтому,

достаточно сложно говорить о каких-либо тенденциях места и времени совершения данных преступлений. Гораздо большее значение место и время совершения преступлений в информационной сфере и (или) сети Интернет, имеют, когда данные преступления совершаются при личном, непосредственном контакте преступника и жертвы. В данном случае следует привести позицию Д.В. Кузьменко, которая проанализировав существенное количество уголовных дел соответствующей категории, сделала следующие выводы относительно обстановки совершения мошенничеств в сфере высоких технологий. «Время совершения преступления в основном дневное в промежутке от 11 часов до 17 часов. Для утренних часов (с 06 часов до 11 часов) характерно совершение мошенничеств, связанных с медициной и социальной сферой обслуживания. Представленный интервал может меняться в зависимости от способа совершения мошенничества и периода времени совершения самого преступления, такой период может растягиваться на несколько часов и затрагивать как утреннее, так и вечернее время. Местом совершения преступления в большинстве случаев является помещение, в котором проживает пенсионер или инвалид. Зачастую свой преступный умысел мошенник осуществляет, будучи в общественном, шумном месте, где действует фактор отвлечения (шум, посторонние разговоры, суета, высокая плотность людей), например, на рынке или улице. Этот фактор способствует совершению ряда преступных действий, так как сосредоточиться в таком месте затруднительно и явные признаки обмана могут не восприниматься потерпевшим»[1].

Для бесконтактных способов совершения преступлений в информационной сфере и (или) с использованием сети Интернет в плане определения обстановки их совершения особое значение имеют условия,

[1] Кузьменко Д.В. Обстановка совершения преступления, как элемент криминалистической характеристики мошенничеств, совершенных в отношении социально незащищенных категорий граждан // Криминалистика и судебно-экспертная деятельность в условиях современности Материалы IV Международной научно-практической конференции. Краснодарский университет МВД России. – 2016. – С. 258.

создание и обеспечение которых позволяет реализовывать соответствующие преступные замыслы. Например, к таковым условиям при совершении дистанционного мошенничества следует относить:

1. Наличие специальных технических средств;
2. Наличие специальных технологических возможностей.

В первом случае речь идет о тех технических средствах, которые преступники используют в качестве предметов преступных посягательств. Это мобильные телефоны, смартфоны, средства электронных платежей, компьютеры, планшеты и так далее. Особое значение в данном случае имеют электронные платежные системы. Именно посредством них совершается значительная часть мошеннических действий, схем и операций в сфере высоких технологий. В России распространены несколько видов электронных платежных систем, которые очень условно можно классифицировать по трем основным типам[1]:

1. Банковские платежные системы;
2. Платежные системы по переводу электронных денежных средств;
3. Платежные шлюзы.

К первым относятся электронные платежные системы, работающие с обычными банковскими картами (Visa, MasterCard и т. д.). Системы второго типа оперируют с электронными денежными средствами — некой внутренней валютой (титульными знаками), которую нельзя обналичить, но можно свободно переводить на другие счета и использовать в качестве средства оплаты услуг и товаров. Платежные шлюзы представляют собой синергию карточных (банковских) систем и систем электронных денежных средств, предоставляя широкие возможности для взаимной конвертации и способов оплаты товаров и услуг в Интернете, а также обналичивания денежных средств. Стоит отметить, что значительная часть существующих электронных платежных систем относится именно к шлюзам, несмотря на то, что многие из

[1] Симонов А. П. Электронные платежные системы в России [Электронный ресурс]. URL: http://www.crimeres-earch.ru/articles/titunina1207 (дата обращения 15.11.2021)

них выделяют определенный тип платежей как доминирующий[1].

Во втором условии речь идет о конкретных технологиях и возможностях, которые данные технологии предоставляют мошенникам для осуществления своих мошеннических операций в сфере высоких технологий. В данном случае следует упомянуть:

1. Использование персональных данных, расположенных в различных базах, данных. Это могут быть базы данных банков, операторов связи, курьерских служб, социологических организаций, государственных учреждений и так далее. Получение подобных сведений и данных осуществляется посредством налаживания связей в соответствующих организациях – субъектах, обладающих указанными базами. Только за последнее время были зафиксированы ряд фактов информационных утечек подобного характера.

2. Использование массивов информации наподобие «Больших данных».

3. Использование социализированных программ. Это могут быть различные программы, применение которых позволяет решать разные задачи. Например, это сокрытие истинного номера телефона, с которого осуществляется звонок, имитация другого номера телефона, разрыв привязки месторасположения мошенника и осуществления звонка и так далее.

В настоящее время преступники, совершающие преступления в информационной сфере и (или) сети Интернет обладают совершенно специфичными чертами. В целом, систему признаков личности можно представить в следующем виде:

1. Интеллектуальные способности и особенности (адаптированность и гибкость; умение работать с информацией и быстрое реагирование на меняющуюся информацию; умение планировать, обдумывать все до мелочей;

---

[1] Гайдин А.И. Содержание элемента обстановки в механизме мошенничеств, совершаемых с использованием электронных платежных систем // Борьба с преступностью: теория и практика Тезисы докладов VII Международной научно-практической конференции. Редколлегия: Ю.П. Шкаплеров [и др.]. – 2019. – С. 324.

склонность к риску; высокие самоконтроль, самообладание, терпение и др.).

2. Наличие определенных профессиональных знаний в сфере использования и эксплуатации инновационных технологий.

3. Наличие преступного опыта, в том числе в совершении кибепреступлений с использованием инновационных технологий.

4. Организаторские способности.

5. Наличие авторитета в преступной среде (преступный статус).

6. Возраст.

7. Наличие судимости.

8. Факт отбывания (отбытия) наказания в местах лишения свободы.

Личность жертвы преступления. В данном случае также следует говорить о специфичном виде личности человека. Преступники ориентируются на конкретных лиц. Ключевой, в данном случае, выступает возможность обмануть человека или, войдя в его доверие, затем злоупотребить. В этой связи, наиболее частыми жертвами преступлений в информационном пространстве становятся пожилые люди, одинокие женщины среднего возраста, лица, желающие получить «выгодный товар по низкой цене», то есть все те, кто обладает повышенным уровнем виктимности своей личности.

Говоря о лицах, как объектах криминологического и оперативно-розыскной характеристики преступлений в сфере высоких технологий, нужно отметить еще две категории лиц.

В первом случае это лица, которые способствовали совершению преступлений в информационной сфере и (или) сети Интернет. Соучастниками могут выступать соисполнители, организаторы, пособники. Наиболее ярким примером в данном случае служит совершение масштабных мошенничеств в сети Интернет на основе так называемых колл-центров. В частности, такие организации могут использоваться для мошеннических действий, связанных с оказанием экстрасенсорных услуг населению. Организаторы подобных учреждений приискивают «непосредственных

исполнителей преступления – «экстрасенсов», «целителей», «ясновидящих» и т. п. (70%); администраторов офиса или салона для принятия звонков и записи клиентов (65%); помощников, доверенных «экстрасенсов» (70%); водителей легковых автомобилей (10%); сотрудников службы безопасности (5%)».

Во втором случае речь идет о лицах, которые обладают некоторыми сведениями, которые могут помочь оперативникам установить механизм совершенного преступления, раскрыть его, задержать преступников. Это свидетели, очевидцы, родственники потерпевших, рядовые члены организованных преступных групп и так далее[1].

Как можно заметить, и обстановка, и личности преступника и жертв информационных преступлений во многом опосредованы видом совершаемых преступлений, схемой, которая лежит в основе данного преступного посягательства. Это необходимо в обязательном порядке учитывать при определении содержания криминологической и оперативно-розыскной характеристики преступлений в сфере высоких технологий, установлении уровней предупреждения и алгоритмов раскрытия преступлений подобной категории.

Как уже было отмечено ранее, наиболее существенным и значимым элементом криминологической и оперативно-розыскной характеристики криминогенного потенциала сети Интернет выступает способ совершения преступлений в информационной сфере и (или) сети Интернет. Содержание способа определяет конкретный механизм преступной деятельности данного вида, все остальные элементы его криминологической и оперативно-розыскной характеристики. Естественным образом, в зависимости от способа определяются организационные механизмы противодействия преступлениям в информационной сфере и (или) сети Интернет. Сложность определения способов совершения преступлений исследуемой категории во многом

[1] Нугаева Э.Д. О способе мошенничества, совершенного под предлогом оказания квалифицированной платной парапсихологической помощи при непосредственном контакте подозреваемого с потерпевшим // Научный портал МВД России. – 2017. – № 3 (39). – С. 38.

связана с их многообразием и практической невозможностью систематизации и группировки. В частности, следует на отдельной основе говорить о способах совершения:

1) «телефонного» мошенничества, мошенничества в сети Интернет, мошенничества в различных экономических сферах, мошенничества при использовании личного контакта, мошенничества при использовании банковских карт, платежных устройств и систем и так далее;

2) незаконного сбыта наркотических средств, психотропных веществ или их аналогов посредством сети Интернет; вовлечения несовершеннолетних в наркопреступность[1];

3) компьютерных преступлений: изъятие средств компьютерной техники; неправомерный доступ к компьютерной информации; изготовление или распространение вредоносных программ; перехват информации и др.;

4) терроризма и экстремизма в сети Интернет, в том числе посредством Telegram-каналов: финансирование, получение запрещенных предметов, изъятые из гражданского оборот и др.

Так, к примеру, Г.Р. Фарахиева приходит к выводу, что информационное пространство является одним из наиболее распространенных способов вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов[2]. Также автор, рассматривая социальную обусловленность вовлечения несовершеннолетних в незаконный

---

[1] См.: Фарахиева, Г. Р. Влияние интернет-пространства на процессы вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Саратовской государственной юридической академии. – 2021. – № 5(142). – С. 182-191. – DOI 10.24412/2227-7315-2021-5-182-191. – EDN ZEXJCB; Фарахиева, Г. Р. Социальная среда как фактор вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Казанского юридического института МВД России. – 2021. – Т. 12. – № 4(46). – С. 555-560. – DOI 10.37973/KUI.2021.25.81.016. – EDN BFGQFN.

[2] Фарахиева, Г. Р. Влияние интернет-пространства на процессы вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Саратовской государственной юридической академии. – 2021. – № 5(142). – С. 182-191. – DOI 10.24412/2227-7315-2021-5-182-191. – EDN ZEXJCB.

оборот наркотических средств, приходит к выводу, что: «именно информационно-социальная среда оказывает существенное влияние на несовершеннолетних в контексте их вовлечения»[1].

В свою очередь Н.В. Рябко, рассматривая проблемы борьбы с трансграничным оборотом порнографии, пишет, что сегодня трансграничный оборот порнографических материалов в отличие от прошлого века глобально изменился путем отказа распространителей этой продукции от фактического перемещения этих материалов через границы государств, перейдя в основном к их распространению в сети Интернет[2].

Стремительное развитие информационно-телекоммуникационных технологий поставило еще один важный вопрос виктимологического толка. Речь идет о технологиях, с помощью которых может создаваться в том числе и так называемая виртуальная детская порнография. Это технология создания фото- и видеоизображений людей без использования их реальных образов, т.е. комбинация миллионов компьютерных пикселей, созданных опытным художником. Вторая технология именуется морфингом – это когда фото- или видеоизображение реального человека может быть изменено путем заполнения пробелов между различными объектами для получения комбинированного изображения.

Противодействие распространению детской порнографии в сети Интернет – это безусловно и преимущественно обязанность отдельных государств. Но не менее важным аспектом в этой работе является помощь неправительственных некоммерческих организаций. Техническое решение данной проблемы имеет научную основу. Одними из первых этим вопросом заинтересовались ученые из Канады и Чили. В своем исследовании они

---

[1] Фарахиева, Г. Р. Социальная среда как фактор вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Казанского юридического института МВД России. – 2021. – Т. 12. – № 4(46). – С. 555-560. – DOI 10.37973/KUI.2021.25.81.016. – EDN BFGQFN.

[2] Рябко, Н. В. Современные проблемы борьбы с трансграничным оборотом порнографии / Н. В. Рябко, Е. А. Миллерова // Юристъ-Правоведъ. – 2020. – № 1(92). – С. 80-85. – EDN FDUXEN.

подробно описывают сущность предлагаемого ими технологического подхода к борьбе с детской порнографией в сети Интернет[1].

Также предлагаем рассмотреть способы совершения мошенничеств посредством информационной сферы и (или) совершенных посредством сети Интернет, которые наиболее распространены на сегодняшний день, и наносят наиболее существенный ущерб охраняемым законом общественным интересам, одновременно, являясь наиболее сложными с точки зрения организации своего раскрытия, в том числе в связи с высокой степенью латентности. Таковыми видами мошенничеств являются мошенничества с использованием средств сотовой (мобильной) связи, мошенничества в сети Интернет, а также мошенничества с платежными системами и всеми возможными ее элементами (устройствами, карточками и так далее).

Наиболее распространенными видами «телефонных мошенничеств» являются:

1. «Счастливый выигрыш». Мошенник путем набора различных абонентских номеров звонит (отправляет SMS или MMS) на мобильный телефон (на стационарный телефон) потерпевшему, представляется сотрудником радио, торговой фирмы, банка или иной организации, сообщает о «счастливом выигрыше» (крупной денежной суммы, автомобиля, бытовой техники, туристической поездки). Наряду с поздравлениями, как бы вскользь, мошенник указывает на необходимость соблюсти небольшую формальность - оплатить налог за «выигранный» приз (деньги за его доставку в адрес проживания победителя и т.п.), указывает абонентский номер мобильного телефона (либо номер счета в коммерческом банке), на который необходимо сделать перевод денежных средств;

2. «Родственник попал в беду». Суть способа заключается в том, что злоумышленники звонят жертвам и сообщают о том, что их родственник

[1] Cyber Child Pornography: a Review Paper of Social and Legal Issues and Remedies - and a Proposed Technological Solution / B.H. Shell, M.V. Martin, P.C.K. Hung, L. Rueda // Aggression and Violent Behavior. - 2007. - Vol. 12, № 1. - P. 45-63.

якобы попал в неприятную ситуацию (попал в ДТП, где виноват он, совершил преступление, иное противоправное деяние). Однако, имеется возможность решить вопрос посредством дачи взятки. Часто преступники представляются самими родственниками или же сотрудниками правоохранительных органов, которым необходимо дать взятку;

3. «Ложная блокировка счета». Мошенник звонит (либо отправляет SMS) на мобильные телефоны потенциальных жертв, представляясь сотрудником банка или сотовой компании, сообщает информацию о том, что их банковская карта или счет мобильного телефона заблокирован в результате преступного посягательства, а затем предлагает набрать комбинацию цифр (при этом, как правило, для того чтобы не вызывать подозрение диктуют по две цифры) на банкомате или сотовом телефоне для разблокировки, в результате чего денежные средства перечисляются на счет мошенника или его соучастника;

4. «Компенсация за недоброкачественный товар». Мошенники, используя доступ к соответствующим базам данных торговых площадок, магазинов, сайтов, выявляют лиц, которые недавно приобрели тот или иной товар, чаще всего, бытовую технику. Далее, мошенник звонит жертве, представляется соответствующим образом (например, представитель общественной организации, правоохранительного органа, контрольного органа) и заявляет о том, что во всей линейке товаров (в которую входит и приобретенный жертвой) обнаружены несущественные недостатки, которые не влияя на работу продукции, тем не менее, воздействуют соответствующим образом на его качество. В связи с этим необходимо вернуть часть средств покупателю. Далее действует схема выявления счета, на который необходимо вернуть денежные средства, установление его реквизитов и реализация последующих действий по переводу денежных средств;

5. «Объявления ловушки». Мошенник звонит по объявлению о продаже (сотового телефона, автомобиля, дачи и т.п.), размещенному на одном из интернет-сайтов и соглашается приобрести товар.

Таким образом, рассмотрев разновидность преступлений, совершаемых в информационной сфере и (или) сети Интернет следует вывод, что криминогенный потенциал получает все большее развитие. Наибольшее распространение получили различных торговых площадках (DarkNet, HYDRA, Telegram-каналы и др.), в том числе предоставляющих услуги по размещению объявлений (Авито, Юла, ВК-Объявления) и др. Помимо прочего, в сети Интернет распространены такие схемы, как «проведение конкурсов», «розыгрышей», «опросов», «благотворительных акций» и так далее.

Оценка способов совершения преступлений в информационной сфере и (или) сети Интернет представляется достаточно сложным процессом, реализация которого затруднена множеством способов, схем и механизмов совершения преступлений. На наш взгляд, учитывая, в первую очередь прикладной характер настоящего исследования, необходимо рассмотреть способы совершения информационных преступлений, виды которых наиболее распространены на сегодняшний день, которые наносят наиболее существенный ущерб охраняемым законом общественным интересам, одновременно, являясь наиболее сложными.

§3. Криминологическая характеристика личности преступника, совершающего преступления в сети интернет

Изучение личности преступника считается одним из самых сложных аспектов криминологии. Достижение целей предупреждения отдельных видов преступлений, и в частности хищений с использованием служебного положения, возможно только при внимательном, тщательном изучении личности преступника учеными и правоприменителями. Личность занимает ведущую позицию в механизме противоправного поведения, именно она признается первопричиной совершения преступления, подталкивающей на него. Обладая определенными особенностями, она формирует

предрасположенность к нарушению уголовного закона. «Именно на корректировку особенностей личности должен быть направлен основной и сконцентрированный удар предупредительного воздействия»[1].

Успешное предупреждение преступлений возможно лишь в том случае, если внимание будет сконцентрировано на личности преступника, поскольку именно личность – носитель причин их совершения. Личность преступника – основное и важнейшее звено всего механизма преступного поведения. Те её особенности, которые порождают такое поведение, должны быть непосредственным объектом предупредительного воздействия. Поэтому проблема личности преступника относится к числу ведущих и вместе с тем наиболее сложных проблем криминологии.

В своих трудах, Ю.М. Антонян определяет личность преступника как «совокупность психологических социально значимых негативных свойств психики человека, развившихся в процессе многообразных и систематических взаимодействий с другими людьми»[2].

В работах ряда отечественных ученых сделан вывод, что характер и нравственное формирование личности играют главную роль в генезисе преступного поведения. Не биологические свойства человека, не кратковременное, в том числе и случайное, воздействие внешней ситуации, а весь жизненный путь индивидуума в конечном счете определяет содержание подавляющего большинства его поступков.

Криминологический портрет лиц, совершивших преступления в информационной сфере и (или) сети Интернет, как, в общем, так и в частности, может быть составлен на основе четырех групп признаков:

---

[1] Кравцов И.А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально– Черноземного региона // Вестник ВИ МВД России. – 2021. – № 3. – С. 99.

[2] Антонян Ю.М. Личность преступника. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. – 4-е изд., перераб. и доп. – М.: Норма, 2019. – 912 с.

– социально-демографические, к числу которых относятся: пол, возраст, уровень образования, занятость и др.;

– социально-ролевые: гражданство, профессия, семейное положение;

– уголовно-правовые, к ним относятся: особый служебный статус, обусловливающий совершение мошенничества, наличие судимости;

– нравственно-психологические качества, характеризующие мотивационный фон преступного поведения.

В основе социально–демографической характеристики личности современного преступника, совершающего преступления в информационной сфере и (или) сети Интернет лежат: пол, возраст, социальное положение и др. Взятые в совокупности, они указывают на наличие определенных отклонений в системе социализации преступников и служат информационной основой для общесоциальной и специально–криминологической профилактики хищений.

Пол. По данным изученных автором материалов, большинство преступлений против собственности, в том числе и мошенничество, в частности, совершенные в информационной сфере и (или) сети Интернет, совершается лицами мужского пола. Однако, рассматривая статистические данные в динамике, следует отметить повышение (хоть и незначительное) относительной доли женщин.

Результаты статистических исследований 2011 и 2021 годов были практически неизменны (мужчины – 98,2% и 97,2%, женщины – 1,8% и 2,8% соответственно)[1], однако соотношение мужчин и женщин в 2021 году составило 91,1% и 8,9% соответственно. Несмотря на то, что относительная численность женщин выросла втрое, разница на 6,1% (прирост в диапазоне 2011–2021 годов) за 10 лет может считаться незначительной.

Кроме того, анализируя изменение соотношения численности мужчин и женщин в сфере IT (как на соответствующих должностях, так и на

[1] Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 02.05.2022).

соответствующих направлениях подготовки специалистов), следует отметить, что в 2021 году доля женщин составляет около 10%[12], в то время как в 2020 году этот показатель был на отметке 4,1%. Таким образом, можно говорить об определенном уровне корреляции между данными показателями.

Возраст. По данным исследования, проведенного по 2011 году, распределение преступников по возрасту выглядело следующим образом: до 18 лет – 29,9%; от 18 до 24 лет – 60,4%; старше 24 лет – 9,7%. При этом самому младшему было 12 лет, самому старшему – 45. Средний возраст преступника составлял около 20–ти лет.

По сравнению с исследованиями 2021 года доля преступников группы от 18 до 24 практически не изменилась (65,8%), зато процент преступников, не достигших 18 лет, заметно вырос (12,8% в 2021году)[3].

Рассматривая актуальные данные, следует отметить, что возрастная группа от 18 до 24 лет по–прежнему остается самой многочисленной. Численность же двух оставшихся групп можно условно считать равными. Подобное изменение (в сравнении с данными более ранних исследований), по мнению автора, можно считать закономерным, поскольку минимальный разрыв между исследованиями составляет 10 лет. Сравнивая данные, полученные в 2021 году, с данными 2021 года, можно отметить, что категории «до 18 лет» и «старше 24 лет» различаются на 0,2%. Снижение же относительной доли лиц от 18 до 24 лет не говорит о сокращении абсолютного значения данной категории. В рамках статистических данных всех периодов следует сделать вывод о том, что данная категория была и остается самой многочисленной.

1

2 На основании статьи «Исследование рынка труда и обзора заработных плат. Россия. 2021» (Исследование проведено компанией Антал). URL: https://antalrussia.ru/upload/medialibrary/d54/antal_issledovanie–rynka–truda–i–obzor–zarplat–2018_rus_2.pdf (дата обращения: 02.05.2022).

3 Дремлюга Р. И. Международно–правовое регулирование сотрудничества в сфере борьбы с интернет– преступностью // Библиотека криминалиста. – 2018. – № 5(10). – С. 339–346.

Объяснение данного факта в действительности весьма простое – в этот возрастной диапазон входят лица, только вступающие в сознательную взрослую жизнь. Это студенты высших и средних специальных учебных заведений и не поступившие на дальнейшее обучение выпускники школ. С точки зрения психологии в современном мире у данной возрастной группы порог социальной ответственности достаточно низок, а понятие «преступление» но в большей степени романтическую окраску. К тому же уровень собственных доходов у лиц данной возрастной группы зачастую минимален, и если лица, не достигшие 18-летнего возраста и фактически, и психологически находятся в зависимости от уровня доходов своих родителей, то рассматриваемая категория лиц зачастую испытывает психологический дискомфорт, обусловленный как сравнением себя с более успешными сверстниками в рамках внутреннего диалога, так и ввиду фактического отсутствия возможности повышения своего социального статуса за счет улучшения материального благосостояния законными методами.

Образование. Совершающий деяние данного вида преступник всегда технически подготовлен и обладает комплексом программно-аппаратных методов и навыков, позволяющих не просто облегчить, но и обеспечить сам факт совершения преступления.

Также необходимо отметить, что лица, совершающие преступления в информационной сфере и (или) сети Интернет, а также с использованием современных технологий, обладают более высоким интеллектуальным уровнем, чем преступники в других сферах. В данном случае речь идет не только об образовании в классическом его понимании, но и о стремлении к саморазвитию, которое предопределяет, по сути, процесс выявления в существующих системах (как компьютерных, так и социальных) брешей, позволяющих злоумышленникам улучшить свое материальное положение незаконным путем.

Полученная нами в ходе статистического анализа, проведенного автором за период времени с 2011 по 2021 гг., общая картина распределения

преступников по уровню образования имела следующий вид: 34% – среднее образование, 27% – среднее специальное образование (из них 72% – образование в сфере информатики и инфокоммуникаций), 39% – высшее образование (из них высшее техническое образование – 37%, экономические специальности – 52%)[1].

Такое статистическое распределение убедительно опровергает распространенное мнение о том, что совершить преступление с использованием компьютерной техники могут только лица, имеющие фундаментальное образование и глубокие знания особенностей функционирования средств компьютерной техники. Как показывает статистика, значительная доля лиц, совершивших рассматриваемые преступления, не имели профильного образования по специальностям технической направленности. Представляется, что данное обстоятельство связано с тем, что нередко для реализации того или иного способа совершения преступления достаточно навыков владения персональным компьютером на уровне пользователя, что в наше время весьма распространено. Навыки работы с компьютером на уровне пользователя приобретаются еще в средней школе, к тому же многим доступны различные самоучители работы на компьютере, курсы компьютерной грамотности и иные источники знаний.

Трудовая занятость. Одним из связующих звеньев между отдельной личностью и обществом является трудовая деятельность, в процессе которой человек ощущает на себе воздействие соответствующей социальной среды и сам, в свою очередь, влияет на нее.

Рассматривая данные о преступлениях прошлых лет по преступлениям, совершенные посредством информационно-телекоммуникационных технологий, нами были установлено, что постоянное место работы в 2020 году было лишь у 31,3% (33% – по данным исследований 2011 года), лишь у 13,9% из выявленных лиц работа была связана с IT–индустрией. По

[1] Состояние преступности в России за 2011-2021 гг. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 24.05.2022).

актуализированным данным, за 2021 год постоянное место работы имели более 60%, случайные заработки имели лишь 8% лиц[1].

Следует отметить, что столь высокий рост показателя трудовой занятости (постоянное место работы) не опровергает идею активной трансформации рассматриваемой категории преступлений в одну из форм профессиональной преступности. По признанию опрошенных лиц, наличие постоянного места работы предполагает, с их точки зрения, некоторую систему «социальной маскировки»: в понимании мошенника социальная интеграция является показателем отсутствия социальной девиации, что, в свою очередь, должно усыпить бдительность правоохранителей.

На рассматриваемый контингент преступников распространяется общий статистический закон: по мере увеличения возраста преступников увеличивается количество лиц, состоящих в браке и имеющих детей. Это говорит о достаточно высоком уровне социализации мошенников и отсутствии таких изолирующих факторов, как жесткие правила воровской субкультуры[2].

Таким образом, следует отметить, что основная отличительная черта личности преступника, совершающего преступления в сети Интернет от любого другого преступника является тот факт, что преступников может быть любой человек, начиная от несовершеннолетнего, заканчивая пенсионером. Следует принимать во внимание, что информационная сфера и сеть Интернет предоставляют пользователям конфиденциальность, раскрепощенность и иллюзию безнаказанности. Согласно изученным материалам уголовных дел и судебно-следственной практики, мы пришли к выводу, что в большинстве случаев, преступники, совершающие преступления в информационной сфере обладают высоким уровнем интеллектуальных способностей.

---

[1] Дремлюга Р. И. Интернет–преступность. – Владивосток: изд-во Дальневосточного университета, 2022. – 240 с.

[2] Мерзлов Ю. А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2019. – № 4(7). – С. 56–61.

ГЛАВА 2. ДЕТЕРМИНАНТЫ ПРЕСТУПЛЕНИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ

§1. Причины и условия совершения преступлений, способствующие увеличению криминогенного потенциала сети Интернет

В целях анализа преступлений в информационном пространстве, сети Интернет и в сфере компьютерной информации и определения мер противодействия им, необходимо полное понимание причин и условий, детерминирующих развитие исследуемой категории преступлений в российском государстве.

По мнению А. И. Долговой, изменения социальной среды, связанные с компьютеризацией общества, характеризуются следующими криминологически значимыми обстоятельствами[1]:

1) повсеместное и всестороннее внедрение новых технологий привело к техническому оснащению отдельных преступников и организованных преступных групп;

2) появились новые технологии совершения преступлений. Многие «традиционные» преступления стало невозможно совершать или масштабно, или без риска быстрого разоблачения, если не использовать высокие технологии. Поэтому, например, все большее распространение получают мошеннические действия, связанные с системой электронного безналичного денежного обращения;

3) формирование информационного пространства, основанного на использовании ЭВМ, систем ЭВМ и сетей ЭВМ, а также взаимосвязанные с этим процессы зарождения и развития общественных отношений в сфере компьютерной информации стали основой возникновения новых видов преступной деятельности.

---

[1] Долгова, А. И. Криминология : кр. учеб. курс / А.И. Долгова. – 4-е изд., перераб. и доп. – Москва : Норма : ИНФРА-М, 2019. – 368 с.

Богданова Т.Н. в своей работе приводит мнение В. Д. Курушина и В. А. Минаева которые выделяют причины компьютерной преступности, как элемента криминогенного потенциала сети Интернет[1]:

1. Уязвимость и взаимозависимость компьютерных систем;

2. Несовершенство социальных, юридических и политических структур, уровень развития которых значительно отстает от уровня развития компьютерных и телекоммуникационных технологий;

3. Возрастающая зависимость современных технологий от компьютерных систем и средств телесвязи;

4. Важность проблемы для развитых и развивающихся стран. В целях ликвидации технологического отставания развивающимся странам следует сосредоточить свои усилия на внедрении высоких технологий в свою экономику, хотя такое внедрение неизбежно связано с огромными материальными затратами на первоначальном этапе и потенциальной уязвимостью;

5. Несовершенство уголовного законодательства, связанное либо с отсутствием соответствующих составов преступлений, либо со сложностью толкования и применения норм, что ограничивает действия правоохранительных органов;

6. Несогласованность существующих законов как на международном, так и на национальном уровнях;

7. Неэффективность гражданского законодательства, которое должно дополнять уголовные санкции;

8. Обслуживающие организации, поставщики и персонал в компьютерной и телекоммуникационной промышленности далеко не всегда проникнуты чувством ответственности перед покупателями и пользователями;

[1] Богданова Т.Н. Причины и условия совершения преступлений в сфере компьютерной информации // Вестник ЧелГУ. – 2019. – №11 (302). – С.64-67

9. Система международных стандартов в области компьютерной техники, связи и информационной безопасности не успевает за требованиями времени;

10. Пользователи систем передачи и обработки данных как в частном, так и в государственном секторах не проявляют должной бдительности при обеспечении информационной безопасности;

11. При реализации новых технологических достижений не всегда соблюдаются права личности, допускаются нарушения этических и правовых концепций.

Следует признать, что во многих случаях криминогенный потенциал сети Интернет имеет законный характер. Между тем нередко информационное пространство превращается в место воплощения преступных посягательств. При этом как справедливо отмечает Т.П. Кесареева, «наиболее организованная и общественно опасная часть преступности в сети Интернет не попадает в поле зрения правоохранительных органов, поэтому реальные показатели этой преступности существенно отличаются от данных, полученных в результате изучения статистики и уголовных дел»[1].

Среди причин и условий развития преступности в информационной сфере и (или) сети Интернет следует выделить высокую степень сокрытия данных преступлений, создающую трудности в их расследовании. Латентность рассматриваемого вида преступности обусловливается сложностью выявления исследуемой категории преступлений, подозрительностью потерпевшей стороны к правоохранительным органам и ее стремление сохранить репутацию[2].

Существует точка зрения, согласно которой, к числу причин и условий, способствующих совершению преступлений посредством информационного пространства, в том числе в сети Интернет, предлагают относить нарушение

---

[1] Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис... канд. юрид. наук. М., 2002.

[2] Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2019. – № 24. – С. 43-46.

установленных сроков хранения копий программ и компьютерной информации, либо полное их отсутствие[1].

Кроме того, необходимо отметить, что в доктрине существует достаточно интересная точка зрения, согласно которой в качестве причины и условия совершения преступлений в информационной сфере и (или) сети Интернет указываются низкий уровень социального и информационного развития общества в России[2]. Пожалуй, отчасти мы согласны с данным мнением, поскольку на сегодняшний день в нашей стране действительно слаборазвит информационный потенциал.

Отдельно следует отметить проблему некомпетентности органов по борьбе с криминогенным потенциалом сети Интернет. Большинство уголовных дел рассматриваемого вида прекращаются на стадии предварительного следствия, нередки случаи, когда дело вообще не возбуждают, причина тому – недостаточная подготовка сотрудников правоохранительных органов, отсутствие у них специальных знаний и необходимых навыков в области информационно-телекоммуникационных технологий. На федеральном уровне сформировано Управление «К» МВД России (в задачу которого входит противодействие преступлениям в сфере компьютерной информации), при многих УВД, ГУВД и МВД РФ созданы отделы по борьбе с преступлениями в сфере высоких технологий, но проблема нехватки высококвалифицированных кадров, особенно на региональном уровне, остается по-прежнему острой. Такие отделы, чаще всего, укомплектованы сотрудниками, обладающими оперативным опытом в части борьбы с экономическими преступлениями, связанными с раскрытием преступлений в сфере нарушения авторских и смежных прав, изъятием контрафактной продукции, но не имеющими знаний и навыков по раскрытию

---

[1] Ищук Я. Г. Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. – Москва. : Академия управления МВД России, 2021. – 244 с.

[2] Решетников, А. Ю. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А. Ю. Решетников, О. Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2018. – 168 с.

преступлений, которые совершаются в информационной сфере и (или) сети Интернет. А без дополнительной подготовки специалистов по техническим аспектам информационной преступности эффективная борьба с ней будет равно нулю.

В этой связи представляется необходимым осуществлять профессиональную подготовку и переподготовку сотрудников правоохранительных органов, непосредственно связанных с расследованием преступлений, совершаемых в информационной сфере и (или) сети Интернет; в основных образовательных программах высших учебных заведений системы МВД России предусмотреть углубленное изучение теории и практики расследования компьютерных инцидентов, а также специфики использования инновационных технологий при совершении преступных действий[1].

Основываясь на результатах анализа статистических данных Главного информационно-аналитического центра Министерства внутренних дел России, судебно-следственной практики, а также специализированной литературы, можно выделить основные детерминанты преступности в информационной сфере и (или) сети Интернет:

1) информационно-технологическое оборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных;

2) реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием инновационных технологий;

3) низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности;

4) ненадлежащее отношение к вопросу обеспечения информационной безопасности;

---

[1] Тутуков А.Ю. Основные детерминанты компьютерной преступности в российской Федерации // Пробелы в российском законодательстве. – 2018. – №3. – С. 82-84.

5) низкий уровень программно-технических средств защиты информации;

6) небрежность в обеспечении конфиденциальности информации[1].

Таким образом, следует вывод, что рассмотренный перечень факторов, детерминирующих преступления в информационной сфере и (или) сети Интернет не является исчерпывающим, поскольку постоянное развитие информационно-коммуникационных технологий в современном обществе будет порождать все новые причины и условия совершения преступлений в сети Интернет.

Рассмотрим также детерминанты преступлений в сфере незаконного оборота наркотических средств, психотропных веществ или их аналогов. Так, общесоциальные детерминанты наркопреступности в сети Интернет связаны с социальными процессами, происходящими в обществе в целом (прежде всего макроэкономическими процессами) и отражающимися на образе жизни целых макрогрупп (возрастных, национальных, профессиональных и т.д.). А.В. Шеслер, В.Б. Вехов, А.С. Овчинский отмечают, что деформации, возникшие в образе жизни этих групп, способны оказывать криминогенное воздействие на личность в следующих направлениях: 1) являться источником конфликтов; 2) вызывать отклонения от одобряемых обществом ценностей; 3) ослаблять позитивный социальный контроль; 4) затруднять реализацию законных возможностей личности.

Специфика этих процессов применительно к наркопреступности в сети Интернет имеет много общего с групповой преступностью в целом, и как верно отмечает А.В. Шеслер состоит, во-первых, в том, что они порождают социальную базу этой преступности, то есть группы людей, оказавшихся из-за социально-экономического кризиса невостребованными в позитивных сферах жизнедеятельности общества и вынужденных приобщаться к

---

[1] Криминология и предупреждение преступлений : учебник для среднего профессионального образования / В. И. Авдийский [и др.] ; под редакцией В. И. Авдийского, Л. А. Букалеровой. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2021. – 301 с.

криминальной деятельности уже существующих преступных групп или объединяться в такие группы для адаптации к усложнившимся условиям через девиантное поведение[1].

Детерминанты мошеннических действий, совершаемых посредством информационной сфере или с использование сети Интернет – это совокупность причин и условий, характерных лишь для рассматриваемого вида преступлений[2]. При рассмотрении мошенничества, совершаемого с информационной сфере и (или) в сети Интернет, следует отметить такие стабильно сохраняющиеся детерминанты, как[3]:

– небрежность и неосведомленность держателей карт;

– соучастие в преступлениях инсайдеров;

– трансграничность преступлений;

– появление новых угроз в связи изменениями, как в технологии карточной индустрии, так и с развитием общества в целом;

– развитие высокотехнологичных форм преступления, требующих специальных знаний;

– повышение уровня угроз со стороны традиционной преступности.

---

[1] Гуминский, М. Н. Характеристика причин и условий совершения преступлений в сфере незаконного оборота наркотиков с использованием компьютерных технологий / М. Н. Гуминский // Актуальные проблемы правового регулирования международных отношений : Сборник научных статей / Витебский государственный университет им. П.М. Машерова; ответственный редактор В.С. Елисеев. – Витебск : Витебский государственный университет им. П.М. Машерова, 2019. – С. 168-170. – EDN KHPHPK.

[2] Варыгин, А. Н. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А. Н. Варыгин, В. Г. Громов, О. В. Шляпникова ; под редакцией А. Н. Варыгина. – 2-е изд. – Москва : Издательство Юрайт, 2019. – 165 с.

[3] Березуцкая А. Г., Яблонская А. Е. Современные проблемы безопасности пластиковых карт в платежной системе России // ЭПП. 2018. № 3. – С.195–202.

ГЛАВА 3. МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ ИНФОРМАЦИОННОЙ СФЕРЫ, КАК НЕОТЪЕМЛЕМЫЙ ЭЛЕМЕНТ МИНИМИЗАЦИИ КРИМИНОГЕННОГО ПОТЕНЦИАЛА СЕТИ ИНТЕРНЕТ

§1. Предупреждение преступлений, совершаемых в сети Интернет

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.

Обеспечение своевременности и эффективности 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 общесоциального и специального мер предупреждения исследуемой категории преступлений[1].

В реальной действительности предупреждение преступлений, совершаемых в информационной сфере и (или) сети Интернет представляет собой сложную систему, состоящую из отдельных элементов деятельности разнообразного характера, целью которой служит оказание воздействия на причины и условия, способствующие совершению преступлений, а также на лиц, их совершающих[2]. Деятельность по предупреждению преступлений, совершаемых в информационной сфере и (или) сети Интернет носит многоуровневый характер, поскольку помимо масштабных, долговременных,

---

[1] Кульков, В. В. Расследование и предупреждение преступлений. Руководство для следователей и дознавателей : практическое пособие / В. В. Кульков, П. В. Ракчеева ; под редакцией В. В. Кулькова. – Москва : Издательство Юрайт, 2017. – 288 с.

[2] Титушкина Е. Ю. К вопросу о криминологических терминах. // Российский следователь. – 2019. – №21. – С. 23-25.

перспективных мер, таких как постановка стратегических задач по борьбе с преступностью, нормативного, организационного и ресурсного обеспечения, необходимым является разработка и принятие мер более узкого, конкретного характера, имеющих прикладное значение и рассчитанных на достижение менее крупных, но не менее значимых целей.

Одной из главных причин положительной результативности преступных деяний в информационной сфере и (или) сети Интернет являются средства анонимизации и их доступность. В этой связи следует в том же ключе проводить профилактические мероприятия с населением для повышения грамотности в информационно-телекоммуникационной сфере, чтобы преступникам было сложнее обманывать граждан[1].

Сложность и проблемность раскрытия преступлений, совершенных в информационной сфере и (или) сети Интернет заключаются в следующем:

1) анонимность и конфиденциальность преступников является одной из важнейших и серьёзных проблем;

2) получение информации, запрошенной правоохранительными органами у банковских организаций, операторов мобильной связи и установление IP-адресов является долгим процессом и не приносит большой пользы, так как все счета, телефонные номера регистрируются на третьих лиц;

3) появление все новых способов совершения преступлений в информационной сфере и (или) сети Интернет; в связи с этим не успевают создаваться методики для раскрытия данных преступлений;

4) нестабильная эпидемиологическая ситуация в государстве, где большинство организаций и учреждений перешли на дистанционную работу,

[1] Криминология и предупреждение преступлений: преступность несовершеннолетних : учебное пособие для среднего профессионального образования / А. В. Ростокинский [и др.] ; под редакцией А. В. Ростокинского, Р. С. Данелян. – 2-е изд. – Москва : Издательство Юрайт, 2020. – 220 с.

количество пользователей интернета увеличилось, как и количество кибератак со стороны злоумышленников[1].

Необходимо повышать профессионализм в сфере информационных технологий, ведь большое количество преступлений переходит в дистанционный режим. В связи с чем, следует улучшать методы обучения в образовательной системе России, готовить специалистов с техническим образованием.

Также считается целесообразным проводить занятия с действующими сотрудниками органов внутренних дел, обучать их работе с существующим комплексом IT-технологий, представляя информацию о том, как работает то или иное программное обеспечение, его особенности, слабые и сильные места конкретного софта на практике[2].

Проблема роста преступности, совершаемой в информационной сфере и (или) сети Интернет, причиняющей огромный вред общественным отношениям, требует от государства выработки принципиально новых подходов для борьбы с данным явлением. Полагаю, необходимым ускорить разработку и внедрение передовых методик выявления и раскрытия преступлений, совершенных информационной сфере и (или) сети Интернет, ужесточить уголовное наказание за совершение преступлений в сфере информационных технологий, осуществлять просвещение населения относительно безопасного поведения при использовании информационно-телекоммуникационных средств[3].

---

[1] Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2021. – №1 (89). – С. 167-171.

[2] Афанасьева, О. Р. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. – Москва : Издательство Юрайт, 2022. – 360 с.

[3] Дук Ю.И. Пандемия и криминализация населения // Аиатско-Тихоокеанский регион: экономика, политика и право – 2021 – т23. – №3 – 200 с.

В свою очередь, следует обновить методы и меры практического воздействия на преступления в сфере информационно-телекоммуникационных технологий.

В заключение отметим, что меры предупреждения действенны в области уголовно наказуемых деяний, совершаемых с использованием информационно-телекоммуникационных технологий или в информационной сфере и (или) сети Интернет. Важность постоянного осуществления мер предупреждения, а также их совершенствования в части рассматриваемой нами преступности, не поддается сомнению. Криминогенный потенциал сети Интернет характеризуется прежде всего тем, что в последнее время увеличивается число мошенничества. Так, мошенничества в информационно-телекоммуникационной среде стали глобальной проблемой для всего человечества, миллиарды долларов в год похищаются бесследно различными способами, поэтому следует серьезно подходить к институту мер предупреждения преступности в части его развития, совершенствования и работоспособности.

Необходимо принимать во внимание, что, совершая преступления в информационном пространстве, повышается уровень латентности. Путями преодоления латентности преступлений в информационной сфере и (или) сети Интернет можно назвать следующие:

– использование социологических методов и приемов выявления и измерения латентной преступности: массовый опрос населения, анкетирование, экспертные оценки, контент-анализ материалов средств массовой информации;

– преодоление правового нигилизма руководителей учреждений, предприятий, организаций и отдельных граждан путем освещения проблем информационной преступности в средствах массовой информации;

– повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов.

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 информационной сфере и (или) сети Интернет 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 средства и информационно-телекоммуникационных систем.

2. Совершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями в информационной сфере и (или) сети Интернет (научно-методическое обеспечение).

К отдельным направлениям совершенствования научно-методического обеспечения противодействия высокотехнологичной информационной преступности относятся:

---

[1] Борин Б. В., Ищук Я. Г. Понятие оперативно-розыскной профилактики преступлений // Пробелы в российском законодательстве. – 2017. – №3. – С. 381-386.

– унификация и легитимизация терминов и определений, связанных с данным направлением деятельности. Так, само понятие «криминогенный потенциал сети Интернет»; «преступления, совершаемые в информационной сфере и (или) сети Интернет» включает в себя не только преступления, предусмотренные статьями Особенной части УК РФ, но и те, где информационно-телекоммуникационные сети или компьютерная информация выступают в качестве средства или орудия совершения преступного деяния[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 и т. д. предустанавливать в свою 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 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.).

– обеспечение своевременности реагирования законодательства на изменяющиеся условия функционирования систем защиты информации и

[1] Харламова А. А. Проблемные вопросы квалификации мошенничества с использованием платежных карт // Вестник Уральского юридического института МВД России. – 2017. – № 1. 9. – С. 44-47.

информационных ресурсов. При этом для решения задач совершенствования нормативного правового обеспечения деятельности по предупреждению высокотехнологичной преступности полезно обращаться к зарубежной практике правового регулирования данной деятельности, в частности опыта Китайской народной республики по созданию «Золотого щита». Кроме того для предупреждения совершения компьютерных преступлений в сети Интернет, представляется возможным в Федеральном законе «Об информации, информационных 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).

3. Принятие организационно-управленческих мер предупреждения высокотехнологичных информационных преступлений. Данное направление характеризуется комплексом мер, направленных на совершенствование практической деятельности субъектов предупреждения преступлений информационной сфере и (или) сети Интернет.

В настоящее время наиболее инновационным средством предупреждения преступлений в информационной сфере и (или) сети Интернет является формирование и внедрение специализированного приложения с использование искусственных технологий, позволяющих блокировать сообщения и звонки мошенников в сфере информационного пространства. Рассмотрим опыт зарубежных страх. 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

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 02.05.2022).

пользуются мошенники. Используя этот опыт, можно повысить эффективность превенции дистанционного хищения 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.

Если рассматривать предупреждение преступлениям в сфере незаконного оборота наркотических средств, совершающиеся посредством информационной сферы и (или) сети Интернет, то нами предлагаются следующие меры:

1. 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)[1].

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 и др.

Деятельность данного Центра должна быть направлена на совершенствование механизма предупреждения преступлений в сфере

[1] Организация правоохранительной системы в некоторых федеративных странах мира. URL: https:// komitetgi.ru/upload/iblock/538/538b9dcf40eca849375fa5f15da10d26.pdf (дата обращения: 25.05.2022).

незаконного оборота наркотических средств в интернет-пространстве посредством разработанной многофункциональной инновационной многоязычной Web-платформы.

2. На федеральном уровне:

2.1. На базе Федеральной службы по финансовому мониторингу (далее – Росфинмониторинг) сформировать Федеральный центр антинаркотического мониторинга информационных платформ (далее – ФЦАМ), предоставить техническую возможность и инфраструктуру для сотрудников ФЦАМ и наделить их полномочиями по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере незаконного оборота наркотических средств в интернет-пространстве; по блокировке подозрительных сайтов, по представлению Центра на основе их базы данных и др. На наш взгляд, функционирование ФЦАМ отразится на современной цифровой (инновационной) антинаркотической сфере, которая откроет перед пользователями интернет-пространства новые перспективы.

2.2. Сформировать специализированное аналитическое подразделение в ФЦАМ с внедрением в него искусственного интеллекта и технологий блокчейн в целях накопления больших данных о наркотических средствах в Интернет-пространстве «Big Data DIS»[1].

На наш взгляд, в процессе раскрытия, расследования и предупреждения преступлений в сфере незаконного оборота наркотических средств в интернет-пространстве необходимо в первую очередь наладить эффективное взаимодействие между органами исполнительной власти: Министерством внутренних дел Российской Федерации, Федеральной службой безопасности Российской Федерации, Роскомнадзором, Росфинмониторингом, а также Прокуратурой Российской Федерации. На расширенном заседании коллегии МВД России остроту этой проблемы обозначил Президент Российской

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

Федерации В.В. Путин: «Нужно самым серьёзным образом совершенствовать порядок взаимодействия МВД с финансовыми организациями, операторами связи и другими структурами, работающими в цифровом пространстве и в области телекоммуникаций. В целом для укрепления кибербезопасности требуется более скоординированная работа правоохранительных органов, соответствующих государственных ведомств и регуляторов, экспертного сообщества и бизнеса»[1].

Таким образом, следует вывод, что введение биометрических параметров населения может стать отправной точкой для новых схем мошенничеств в сфере высоких технологий (к примеру, могут быть использованы программы, позволяющие в точности копировать голоса любой жертвы или их родственников). Во многих программах имеется функция, позволяющая менять голос, и их использование не требует особых навыков. В целях противодействия таким преступлениям следует установить уголовную ответственность за данную категорию преступлений на законодательном уровне.

§2. Совершенствование мер по профилактике преступлений, совершаемых в информационной сфере

Профилактическая деятельность является основополагающей частью деятельностью субъектов профилактики, поскольку от эффективности профилактики преступлений в информационной сфере и (или) сети Интернет зависит нормальная и обыденная жизнедеятельность общества и государства в целом.

Основным субъектом профилактики преступлений в информационной сфере и (или) сети Интернет являются органы внутренних дел. Большой приоритет при этом получают сотрудники уголовного розыска и иных

[1] Расширенное заседание коллегии МВД России. 17 февраля 2022 года. URL: http://kremlin.ru/ events/president/news/67795 (дата обращения: 20.05.2022).

оперативных подразделений МВД России. Таким образом, организационное обеспечение является ключевым элементом механизма реализации требований законодательства по внедрению и использованию криминалистических средств и рекомендаций в процессе раскрытия и расследования киберпреступлений. Традиционно оно предполагает комплексный подход к исследованию соответствующих потребностей, научно-технического и материального потенциала их удовлетворения, реализации и использования.

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 преступлений в информационной сфере и (или) сети Интернет, разработка алгоритма действий в случае вероятного информационного преступления, 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. В связи с чем предлагаем следующее:

Во-первых, 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 позволит обеспечить комплектование правоохранительных органов компетентными и профессиональными сотрудниками. Частью данной системы являются проводимые на регулярной основе курсы повышения квалификации, стажировки в практических органах, обмен опытом, семинары и круглые столы для сотрудников и профессорско-преподавательского состава

ВУЗов в государственных образовательных учреждениях, а также российских компаниях, занимающихся информационной безопасностью[1].

Во-вторых, переход от преимущественно территориального принципа работы правоохранительных органов в сфере профилактики 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.

В-третьих, совершенствование информационно-аналитического обеспечения деятельности по противодействию преступлениям, совершаемых в информационной сфере и (или) сети. 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.

Виктимологическая профилактика также является основным направлением деятельности субъектов профилактики. В данном направлении целесообразно сформировать алгоритм действий, направленных на выполнение определенных (поочередных) действий (к примеру, как себя вести, когда разговариваешь с Интернет преступниками; как распознать Интернет преступника; куда можно обратиться и т.д.), как для наиболее виктимных категорий граждан, так и для других.

В качестве субъектов осуществления виктимологической профилактики преступлений в сфере высоких технологий выступают государство в лице правоохранительных органов, общественные организации и иные

---

[1] Шевко Н. Р. Проблемы подготовки специалистов по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России // Вестник Казанского юридического института МВД России. – 2017. – № 1 (27). – С. 87-89.

негосударственные структуры. Виктимологическая профилактика преступлений данного вида охватывает различные формы поведения, являющиеся закономерным результатом разных вариантов виктимности: легкомысленность поведения, излишнее любопытство, пользовательская небрежность, незнание элементарных мер защиты, возрастные и интеллектуальные особенности и др. Механизмами регулирования виктимологической защиты являются не только нормы права, но и иные социальные регуляторы: морально-нравственные, корпоративные и этические правила поведения. Необходимо подчеркнуть, что обеспечение эффективности виктимологической профилактики в целях предотвращения или минимизации последствий высокотехнологичной преступности невозможно без активного участия социума.

А.А. Комаров предлагает осуществлять виктимологическую профилактику преступлений в глобальной сети по следующим основным направлениям:

а) повышение эффективности информационной безопасности, совершенствование программно-технических средств защиты компьютерной информации;

б) противодействие распространению спама по электронной почте;

в) использование возможностей Интернета для предупреждения высокотехнологичных преступлений (для этого необходимо создать централизованный информационный ресурс, посвященный вопросам противодействия мошенничеству в глобальной сети, обладающий государственной поддержкой и обратной связью с правоохранительными органами)[1].

Виктимологическую профилактику преступлений в сфере информационных технологий требуется организовывать с учетом виктимности различных групп населения. Следует учитывать различные

[1] Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: Дис. … канд. юрид. н. Пятигорск, 2011. 262 с. EDN: UATITN

аспекты обеспечения данного вида деятельности, а она сама должна быть ориентирована на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве, основываться на доступных для населения или работников-неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

Таким образом, своевременная разработка и комплексное использование мер профилактики преступлений в информационной сфере и (или) сети Интернет способствует значительному повышению уровня информационной безопасности России и эффективности борьбы с противоправными деяниями в данной сфере. При этом следует учитывать, что предложенные профилактические 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.

ЗАКЛЮЧЕНИЕ

Согласно статистическим данным, за 2021 г. было зарегистрировано 517 722 преступления, совершенных посредством информационно-телекоммуникационных технологий. Криминогенный потенциал сети Интернет как правило обусловлен тем, что большинство преступлений, которые совершаются посредством сети Интернет – это мошенничество; наркопреступления и кибертерроризм.

Криминологическая характеристика преступлений в информационной сфере и (или) сети Интернет содержит в себе ряд элементов. Так, первый элемент – обстановка совершения преступлений. Обстановка совершения преступления – это элемент криминологической, криминалистической и оперативно-розыскной характеристики данного вида преступлений, которым характеризуются места совершения данной формы хищений, время их совершения, а также ряд других факторов и особенностей, прежде всего, условия реализации преступных замыслов.

Из преступлений, совершенных в информационной сфере и (или) с использованием сети Интернет, на современном этапе, большая часть связана с мошенническими действиями, повышающие криминогенный потенциал сети Интернет. Во многом это связано с тем, что на современном этапе наличествует большое количество разнообразных видов мошенничеств.

Для бесконтактных способов совершения преступлений в информационной сфере и (или) с использованием сети Интернет в плане определения обстановки их совершения особое значение имеют условия, создание и обеспечение которых позволяет реализовывать соответствующие преступные замыслы. Например, к таковым условиям при совершении дистанционного мошенничества следует относить:

1. Наличие специальных технических средств;
2. Наличие специальных технологических возможностей.

В первом случае речь идет о тех технических средствах, которые

преступники используют в качестве предметов преступных посягательств. Это мобильные телефоны, смартфоны, средства электронных платежей, компьютеры, планшеты и так далее. Особое значение в данном случае имеют электронные платежные системы. Именно посредством них совершается значительная часть мошеннических действий, схем и операций в сфере высоких технологий.

Во втором условии речь идет о конкретных технологиях и возможностях, которые данные технологии предоставляют мошенникам для осуществления своих мошеннических операций в сфере высоких технологий. В данном случае следует упомянуть: 1. Использование персональных данных, расположенных в различных базах, данных; 2. Использование массивов информации наподобие «Больших данных»; 3. Использование социализированных программ.

Второй элемент – личность преступника, личность жертвы. В данном случае также следует говорить о специфичном виде личности человека. Преступники ориентируются на конкретных лиц. Ключевой, в случае с мошенничеством, выступает возможность обмануть человека или, войдя в его доверие, затем злоупотребить. В случае с незаконным оборотом наркотических средств речь идет о преступлении без жертв.

В процессе исследования, мы выделили ряд особенностей личности преступника, разделив их по определенным группам. Так, первая группа – это половая принадлежность. Согласно исследованию материалов уголовных дел, правоприменительной и следственно-судебной практик следует, что в большинстве случаев преступниками, которые совершают преступления в информационной среде, являются лица мужского пола (79%). Как правило, в 76% случаев преступники обладают высокими навыками использования инновационных технологий и имеются достаточно высокие интеллектуальные способности. Образовательный уровень преступников также является одной из групп характеристики преступников. Так, согласно анализу, следует вывод, что преступник имеется высокий уровень информационно-программно-

аппаратного обеспечения; профессиональных навыков в информационном пространстве.

Следующей группой является возрастной критерий преступников. Согласно исследованию материалов уголовных дел, правоприменительной и следственно-судебной практик следует, что преступников является:

1) лицо, недостригшее возраста 18 лет – в 26%;

2) лицо, в возрасте от 18 до 25 лет – в 52%;

3) лицо, в возрасте от 25 до 40 лет – в 15%;

4) лицо, старше 40 лет – 7%.

Следующей группой является семейное положение преступников. Согласно статистическим данным и изученным материалам уголовных дел следует, что в около 30% случаев, лица в браке не состояли; около 20% преступников находились в разводе, остальная часть преступников состояли в браке официально, из них 20 % имели сожителей. Более половины имели детей.

Наиболее частыми жертвами информационных преступников становятся пожилые люди, одинокие женщины среднего возраста, лица, желающие получить «выгодный товар по низкой цене», то есть все те, кто обладает повышенным уровнем виктимности своей личности.

Таким образом, рассмотрев разновидность преступлений, совершаемых в информационной сфере и (или) сети Интернет следует вывод, что криминогенный потенциал получает все большее развитие. Наибольшее распространение получили различных торговых площадках (DarkNet, HYDRA, Telegram-каналы и др.), в том числе предоставляющих услуги по размещению объявлений (Авито, Юла, ВК-Объявления) и др. Помимо прочего, в сети Интернет распространены такие схемы, как «проведение конкурсов», «розыгрышей», «опросов», «благотворительных акций» и так далее.

Оценка способов совершения преступлений в информационной сфере и (или) сети Интернет представляется достаточно сложным процессом,

реализация которого затруднена множеством способов, схем и механизмов совершения преступлений. На наш взгляд, учитывая, в первую очередь прикладной характер настоящего исследования, необходимо рассмотреть способы совершения информационных преступлений, виды которых наиболее распространены на сегодняшний день, которые наносят наиболее существенный ущерб охраняемым законом общественным интересам, одновременно, являясь наиболее сложными с точки зрения организации своего раскрытия, в том числе в связи с высокой степенью латентности.

Третий элемент – детерминанты (причины и условия) преступления.

1. Экономические детерминанты. Экономические детерминанты прежде всего связанны с нестабильностью экономики страны, высокой инфляцией и безработицей. Одним из основных экономических детерминантов преступлений в информационном пространстве выступает экономический кризис. Также в данному блоку следует относить следующие детерминанты: развитие теневой экономики; невозможность благотворения нужд населения в силу их экономических возможностей; существование класса весьма богатых граждан и организаций, которые могут позволить себе потратить часть денег на взяточничество.

2. Политические детерминанты. Политические детерминанты, содействующие совершению преступлений в информационном пространстве, также занимают высокое место в современном обществе. К данному блоку детерминантов следует относить: нехватка политической культуры; отдаление общества и населения от государственного аппарата; не укоренившиеся демократические политические традиции; бюрократизация административного аппарата; несформированность институтов гражданского общества; наличие неустойчивой уголовной политики и политического режима в государстве; отсутствие или нехватка прозрачности системы принятия политических решений.

3. Правовые детерминанты. К данному блоку, в процессе исследования мы отнести следующие детерминанты: несовершенство законодательной базы

в сфере киберпреступности; многочисленные лазейки в налоговом законодательстве для общества; низкий уровень раскрытия преступлений в информационном пространстве и др.

4. Нравственно- и социально-психологические детерминанты. К данному блоку детерминантов мы отнести следующее: деформирование морального сознания некоторых граждан в сторону наживы, извлечения выгоды любыми способами.

На наш взгляд, большое значения в области причин, способствующие совершению преступлений в информационной сфере является возможность сохранения конфиденциальности, посредством использования программ, позволяющие шифровать IP-адреса.

Четвертый элемент – меры предупреждения и профилактики. В юридической литературе высказывается большое количество мнений относительно того, каким образом необходимо исследовать процесс предупреждения и раскрытия преступлений, совершаемых посредством средств сотовой связи, информационно-телекоммуникационной сети Интернет, а также при использовании банковских средств платежа (банковских карт). Исследовав множество подобных мнений, можно прийти к выводу о трех основных подходах, а именно:

1. Ситуационный подход, предполагающий постановку во главу угла конкретную оперативно-тактическую ситуацию совершения преступлений и, соответственно, действия, предпринимаемые оперативниками в зависимости от содержания каждой из ситуаций;

2. Алгоритмический, предполагающий представление деятельности по раскрытию в виде выверенного и поэтапного процесса, подразделяемого на соответствующие стадии, где первой стадией будет получение информации о совершенном преступлении, а заключительной стадией – оперативное сопровождение расследования уголовного дела вплоть до передачи дела в суд;

3. Видовой, предполагающий определение особенностей тактики предупреждения и раскрытия преступлений в информационной сфере в зависимости от способов и схем совершаемого преступного деяния.

Первоначальные действия оперуполномоченных по предупреждению и раскрытию преступлений в информационной сфере и (или) сети Интернет зависят от конкретной оперативно-тактической ситуации (первый подход). Практика показывает, что основополагающим основанием в данном случае выступает источник получения первоначальной информации, на основании которой стало известно о факте совершения деяния, содержащего признаки информационного преступления. В этой связи, можем говорить о трех основных оперативно-тактических ситуациях совершения информационного преступления, а именно:

1. Обращение потерпевшего (его близких лиц, представителей) с заявлением в территориальный орган внутренних дел по факту совершения в отношении него противоправных действий в сети Интернет;

2. Поступление информации о противоправных действиях в сети Интернет из иных источников (прежде всего, правоохранительных и контролирующих органов, а также банковских учреждений операторов сотовой связи);

3. Оперативный поиск сотрудников подразделений уголовного розыска, инициативное и самостоятельное выявление фактов, свидетельствующих о совершении киберпреступности.

Предупреждение и профилактика преступлений в сфере информационных технологий на сегодняшний день является одним из основных направлений деятельности правоохранительных органов по противодействию данному виду преступности и выявлению лиц, их совершивших.

Социальная опасность рассматриваемой проблемы настолько существенна, что к ее разрешению присоединилось множество неправительственных международных организаций. Причем они не только

осуществляют наблюдение и гражданский надзор, но и предпринимают реальные меры по борьбе с порнографией (детской, как правило).

На международном уровне (в рамках ООН, Совета Европы) принят ряд документов, направленных на защиту детей от сексуальной эксплуатации и противодействие распространению детской порнографии в сети Интернет. Достаточно ли этого? На сегодняшний день может быть. Поскольку интернет-технологии постоянно развиваются, вопрос правового обеспечения безопасности детей должен всегда находиться на контроле. По нашему мнению, одно из наиболее слабых мест в противодействии распространению детской порнографии в сети Интернет – в недостаточной мере отлаженное взаимодействие между государствами. В свете глобализационных процессов в мире, а также с учетом того, что Интернет не имеет границ, считаем, что основные усилия государств должны быть направлены на активизацию сотрудничества (в том числе под эгидой международных организаций, в первую очередь Интерпола) в противодействии деяниям, связанным с сексуальной эксплуатацией детей, и координацию своих действий в этой сфере.

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-коммуникационные технологии. 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 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.

В целях эффективности предупредительной деятельности в области информационного пространства, необходимо отталкиваться от вышеуказанных элементов криминологической характеристики. Так как информационные технологии, существующие на данный момент, позволяют как скрывать местоположение, так и использовать данные других, то, по

нашему мнению, следует предпринимать следующие шаги в борьбе с наркопреступностью.

1. На международном уровне:

1.1. Наладить взаимодействие между правоохранительными органами России и зарубежных стран в области борьбы с преступностью 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)[1].

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 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.

2. На федеральном уровне:

2.1. На базе Федеральной службы по финансовому мониторингу (далее – Росфинмониторинг) сформировать Федеральный центр антинаркотического мониторинга информационных платформ (далее – ФЦАМ), предоставить техническую возможность и инфраструктуру для сотрудников ФЦАМ и

[1] Организация правоохранительной системы в некоторых федеративных странах мира. URL: https:// komitetgi.ru/upload/iblock/538/538b9dcf40eca849375fa5f15da10d26.pdf (дата обращения: 25.05.2022).

наделить их полномочиями по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере незаконного оборота наркотических средств в интернет-пространстве; по блокировке подозрительных сайтов, по представлению Центра на основе их базы данных и др. На наш взгляд, функционирование ФЦАМ отразится на современной цифровой (инновационной) антинаркотической сфере, которая откроет перед пользователями интернет-пространства новые перспективы.

2.2. Сформировать специализированное аналитическое подразделение в ФЦАМ с внедрением в него искусственного интеллекта и технологий блокчейн в целях накопления больших данных о наркотических средствах и других видах преступлений, совершаемые в Интернет-пространстве «Big Data DIS».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

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

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, N 0001202007040001 (дата обращения: 25.03.2022).

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 N 63-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 N 174-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Российская газета, N 165, 29.07.2006.

5. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 01.07.2010 N 143-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

6. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации и Федеральный закон «О прокуратуре Российской Федерации»: Федеральный закон от 05.06.2007 № 87-ФЗ (ред. от 22.12.2014) // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

7. О почтовой связи: Федеральный закон от 17 июля 1999 г. № 176-ФЗ // Ведомости Федерального Собрания, N 25, 01.09.1999.

8. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ // Ведомости Федерального Собрания РФ, N 25, 01.09.2003.

9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 02.05.2022).

10. О порядке оказания услуг телефонной связи: Постановление Правительства РФ от 09.12.2014 N 1342 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

11. О порядке оказания услуг телефонной связи: Постановление Правительства РФ от 09.12.2014 N 1342 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

12. О порядке оказания услуг телефонной связи: Постановление Правительства РФ от 9 декабря 2014 г. № 1342 (ред. от 25.10.2017) // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

13. Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия: Приказ Генпрокуратуры России от 17.09.2021 N 544 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

14. Об установлении объема и пределов процессуальных полномочий руководителей следственных органов (следственных подразделений) системы Следственного комитета Российской Федерации: Приказ Следственного комитета РФ от 15.01.2011 N 5 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

15. О практике рассмотрения судами жалоб в порядке статьи 125 Уголовно-процессуального кодекса Российской Федерации: Постановление Пленума Верховного Суда Российской Федерации от 10 февраля 2009 г. № 1 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

16. О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): Постановление Пленума Верховного Суда РФ

от 01.06.2017 N 19 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.03.2022).

II. Монографии, учебники, учебные пособия:

17. Антонян Ю.М. Личность преступника. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. – 4-е изд., перераб. и доп. – М.: Норма, 2019. – 912 с.

18. Афанасьева, О. Р. Криминология и предупреждение преступлений : учебник и практикум для среднего профессионального образования / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. – Москва : Издательство Юрайт, 2022. – 360 с.

19. Варыгин, А. Н. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А. Н. Варыгин, В. Г. Громов, О. В. Шляпникова ; под редакцией А. Н. Варыгина. – 2-е изд. – Москва : Издательство Юрайт, 2019. – 165 с.

20. Долгова, А. И. Криминология : кр. учеб. курс / А.И. Долгова. – 4-е изд., перераб. и доп. – Москва : Норма : ИНФРА-М, 2019. – 368 с.

21. Дремлюга Р. И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2022. 240 с.

22. Криминология и предупреждение преступлений : учебник для среднего профессионального образования / В. И. Авдийский [и др.] ; под редакцией В. И. Авдийского, Л. А. Букалеровой. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2021. – 301 с.

23. Криминология и предупреждение преступлений: преступность несовершеннолетних : учебное пособие для среднего профессионального образования / А. В. Ростокинский [и др.] ; под редакцией А. В. Ростокинского, Р. С. Данелян. – 2-е изд. – Москва : Издательство Юрайт, 2020. – 220 с.

24. Кульков, В. В. Расследование и предупреждение преступлений. Руководство для следователей и дознавателей : практическое пособие / В. В.

Кульков, П. В. Ракчеева ; под редакцией В. В. Кулькова. – Москва : Издательство Юрайт, 2017. – 288 с.

25. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук. – М., 2016. – С. 54.

26. Решетников, А. Ю. Криминология и предупреждение преступлений : учебное пособие для среднего профессионального образования / А. Ю. Решетников, О. Р. Афанасьева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2018. – 168 с.

III. Статьи, научные публикации:

27. Аносов А.В. Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. – 2018. – Т. 9. – № 2. – С. 111-115.

28. Березуцкая А. Г., Яблонская А. Е. Современные проблемы безопасности пластиковых карт в платежной системе России // ЭПП. 2018. № 3. – С.195–202.

29. Богданова Т.Н. Причины и условия совершения преступлений в сфере компьютерной информации // Вестник ЧелГУ. – 2019. – №11 (302). – С.64-67

30. Борин Б. В., Ищук Я. Г. Понятие оперативно-розыскной профилактики преступлений // Пробелы в российском законодательстве. – 2017. – №3. – С. 381-386.

31. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии МВД России. – 2017. – № 4 (44). – С. 45-50.

32. Гайдин А.И. Содержание элемента обстановки в механизме мошенничеств, совершаемых с использованием электронных платежных систем // Борьба с преступностью: теория и практика Тезисы докладов VII

Международной научно-практической конференции. Редколлегия: Ю.П. Шкаплеров [и др.]. – 2019. – С. 324.

33. Горовенко С.В., Изюмова Е. С. Проблема предупреждений правонарушений в сфере игорного бизнеса в сети Интернет // Вестник Челябинского государственного университета. – 2018. – № 17. – Право. Вып. 43. – С. 25-29.

34. Данилова Н.А., Кушниренко С.П., Саржин А.Н. Преступления в сфере банковской деятельности как высокотехнологичные преступные посягательства международного характера // Вестник Санкт–Петербургского университета МВД России. – 2018. – № 2. – С. 329–333.

35. Доровских Л.А. Преступления в сфере высоких технологий // Кибер-преступность. – 2018. – № 4 (28). – С. 240-243.

36. Дремлюга Р. И. Международно–правовое регулирование сотрудничества в сфере борьбы с интернет– преступностью // Библиотека криминалиста. – 2018. – № 5(10). – С. 339–346.

37. Дук Ю.И. Пандемия и криминализация населения // Аиатско-Тихоокеанский регион: экономика, политика и право – 2021 – т23. – №3 – 200 с.

38. Евдокимов К. Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. – 2018. – № 2(24). – С. 62-66.

39. Комаров А.А. О критериях общественной опасности, преступлений в сфере высоких технологий // Актуальные вопросы права, экономики и управления: сб. статей IX междунар. науч.-практич. конф. – Пенза, 2017. – С. 243-245.

40. Кравцов И.А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально–Черноземного региона // Вестник ВИ МВД России. – 2021. – № 3. – С. 99.

41. Кузьменко Д.В. Обстановка совершения преступления, как элемент криминалистической характеристики мошенничеств, совершенных в отношении социально незащищенных категорий граждан // Криминалистика и судебно-экспертная деятельность в условиях современности Материалы IV Международной научно-практической конференции. Краснодарский университет МВД России. – 2016. – С. 258.

42. Мерзлов Ю. А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2019. – № 4(7). – С. 56–61.

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

44. Нугаева Э.Д. О способе мошенничества, совершенного под предлогом оказания квалифицированной платной парапсихологической помощи при непосредственном контакте подозреваемого с потерпевшим // Научный портал МВД России. – 2017. – № 3 (39). – С. 38.

45. Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2021. – №1 (89). – С. 167-171.

46. Петушинова, В. Р. Криминологическая характеристика преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в Республике Бурятия / В. Р. Петушинова // Вестник науки. – 2022. – Т. 5. – № 1(46). – С. 159-164. – EDN MJYMEU.

47. 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). 7. – С. 137-140.

48. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2019. – № 24. – С. 43-46.

49. Титушкина Е. Ю. К вопросу о криминологических терминах. // Российский следователь. – 2019. – №21. – С. 23-25.

50. Тутуков А.Ю. Основные детерминанты компьютерной преступности в российской Федерации // Пробелы в российском законодательстве. – 2018. – №3. – С. 82-84

51. Фарахиев, Д. М. Технология blockchain как высокотехнологичное (инновационное) средство противодействия коррупции / Д. М. Фарахиев // Современность в творчестве начинающего исследователя : Материалы научно-практической конференции молодых ученых, Иркутск, 25 марта 2022 года. – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2022. – С. 264-269. – EDN OPVGYV.

52. Фарахиева, Г. Р. Влияние интернет-пространства на процессы вовлечениянесовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Саратовской государственной юридической академии. – 2021. – № 5(142). – С. 182-191. – DOI 10.24412/2227-7315-2021-5-182-191. – EDN ZEXJCB.

53. Фарахиева, Г. Р. Социальная среда как фактор вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов / Г. Р. Фарахиева // Вестник Казанского юридического института МВД России. – 2021. – Т. 12. – № 4(46). – С. 555-560. – DOI 10.37973/KUI.2021.25.81.016. – EDN BFGQFN.

54. Фоменко А.И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития // Интеллектуальные ресурсы - региональному развитию. – 2015. – № 1-5. – С.217-222.

55. Харламова А. А. Проблемные вопросы квалификации мошенничества с использованием платежных карт // Вестник Уральского юридического института МВД России. – 2017. – № 1. 9. – С. 44-47.

56. Чирков Д.К., Саркисян А.Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. – 2017. – № 1 (24). – С. 25-32.

57. Шевко Н. Р. Проблемы подготовки специалистов по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России // Вестник Казанского юридического института МВД России. – 2017. – № 1 (27). – С. 87-89.

58. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. – 2016. – Т. 1. – № 1 (1). – С. 13-16.

59. Щеголева Н.А. Право на участие в управлении делами государства: понятие и ограничения // Среднерусский вестник общественных наук. – 2021. – № 3. – С. 114-116.

IV. Иные источники:

60. Международный конгресс по кибербезопасности. URL: https://icc.moscow/ru/ (дата обращения: 10.04.2022).

61. На основании статьи «Исследование рынка труда и обзора заработных плат. Россия. 2021». (Исследование проведено компанией Антал). URL: https://antalrussia.ru/upload/medialibrary/d54/antal_issledovanie–rynka–truda–i–obzor–zarplat–2018_rus_2.pdf (дата обращения: 02.05.2022).

62. Официальный сайт Министерства внутренних дел РФ. URL: http://mvd.ru/ presscenter/statistics/reports/item/804701 (дата обращения: 01.05.2022).

63. Симонов А. П. Электронные платежные системы в России

[Электронный ресурс]. URL: http://www.crimeres-earch.ru/articles/titunina1207 (дата обращения 15.11.2021)

64. Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 02.05.2022).

65. Треть россиян стали жертвами интернет–мошенников. URL: https://news.rambler.ru/articles/35808456/?utm_content=rnews&utm_medium=read_more&utm_source=c opylink (дата обращения: 02.05.2022).

РЕЦЕНЗИЯ

на выпускную квалификационную работу

обучающегося 073 учебной группы, очной формы обучения, 2017 года набора, по специальности 40.05.02 – Правоохранительная деятельность

Самигуллина Нияза Сайдашевича

на тему «Криминогенный потенциал сети Интернет: проблемы предупреждения и противодействия преступлениям в информационной сфере»

Тема выпускной квалификационной работы представляется достаточно актуальной, поскольку криминогенный потенциал сети Интернет набирает свои обороты, вовлекая в информационную сферу такие виды преступлений, которые ранее совершались только при непосредственном контакте с потенциальной жертвой. Следует также отметить, что криминогенный потенциал сети Интернет год за годом лишь возрастает, из чего следует вопросы повышения предупредительной деятельности со стороны государства, в том числе правоохранительных органов, что выступает актуальностью настоящей выпускной квалификационной работы.

Представленная на рецензирование выпускная квалификационная работа состоит из введения, трех глав, объединяющие шесть параграфов, заключения, перечня использованной литературы.

Содержание работы полностью раскрывает заявленную тему.

Во введении автор достаточно обосновывает актуальность темы, теоретическую и практическую значимость исследования. Раскрывается цель работы, ставятся задачи, верная постановка которых позволила структурно наиболее полно раскрыть их и достигнуть цели исследования в основной части работы. Данная часть исследования обосновывает её научно-методическую основу.

Основная часть работы раскрывает заявленную тему. Можно утверждать, что в ней автору удалось отразить как имеющиеся взгляды специалистов в сфере исследуемой темы, так и достаточно успешно выработать авторские положение. При этом теоретические аспекты, касающиеся, уголовно-правовой и криминологической характеристики преступлений, связанных с криминогенным потенциалом сети Интернет.

В первой главе «Криминологическая характеристика криминогенного потенциала сети интернет» автором с опорой на фундаментальные научные труды разъясняется основные виды преступлений, совершаемые в информационной среде. Изучены сущность и особенность криминогенного потенциала сети интернет, исследованы объективные, субъективные и квалифицирующие признаки составов преступлений. А также, изучилась криминологическая характеристика личности, совершающего преступления в сети интернет.

Во второй главе «Детерминанты преступлений в информационной среде» автором, с опорой на статистические и эмпирические данные, судебную практику и научную литературу, выявлены основные детерминанты, определяющие причины и условия, связанные с потенциалом сети интернет. А также, изучается криминологическая характеристика личности преступника, совершающего преступления в сети Интернет.

В третьей главе «Меры по предупреждению преступлений, совершаемых посредством информационной сферы, как неотъемлемый элемент минимизации криминогенного потенциала сети Интернет» автором, с опорой на зарубежный опыт, фундаментальные научные труды, выработаны авторские определения сущности, цели и задач предупреждения преступлений, сопряженных с преступлениями, совершаемыми в сети Интернет предложены пути преодоления латентности преступлений в информационной сфере и (или) сети Интернет; выявлены основные проблемные вопросы, связанные с данным видом деятельности; изучены предложения различных авторов, связанные с улучшением предупреждения и

профилактики преступлений, сопряженных, сформулированы научно обоснованные предложения законодательного и организационного характера по улучшению деятельности по предупреждению и профилактике преступлений, преступлений в информационной сфере и (или) сети Интернет. В заключении излагаются основные результаты работы и выводы автора.

Автор умело использовал различные виды источников, умело сочетая научную и справочную литературу, которая нашла своё отражение не только в основной части исследования в виде сносок, но и в перечне использованной литературы. В работе все законодательные источники использованы с учетом их последних изменений, реализованы результаты диссертационных исследований, специальной научной литературы. Список литературы по исследуемому вопросу достаточно полный, отражает современное состояние исследуемой проблемы.

Результаты проведённого слушателем Самигуллиным Н.С. исследования свидетельствуют о высокой способности к самостоятельной научно-исследовательской работе, умение изучать и анализировать нормативную и специальную литературу, делать необходимые выводы.

Среди основных положительных черт работы следует отметить широкий круг источников, использованных в ходе исследования, проведение самостоятельного анализа имеющихся проблем в деятельности по предупреждению преступлений в информационной сфере и (или) сети Интернет, отечественной судебной практики и официальной статистики, а также достаточно интересные положения и выводы, которые могут быть использованы в практической деятельности в случае их внедрения в работу соответствующих органов посредством законодательных и организационных техник. Работа имеет чёткую логическую структуру, написана на достаточно высоком научно-методическом уровне. Кроме того, по ряду вопросов и проблем, обозначенных в ходе исследования, автором выработана собственная позиция, заслуживающая внимания.

В целом представленная Самигуллиным Н.С. выпускная квалификационная работа на тему «Криминогенный потенциал сети Интернет: проблемы предупреждения и противодействия преступлениям в информационной сфере» соответствует требованиям, предъявляемым к выпускным квалификационным работам, представляет собой законченное самостоятельное исследование, может быть рекомендована к публичной защите, и заслуживает оценку «отлично».

Рекомендую выпускную квалификационную работу Самигуллина Н.С. к защите в Казанском юридическом институте МВД России.

Рецензент:

Начальник отделения раскрытия
преступлений, совершенных с использованием
информационно-телекоммуникационных технологий
УМВД России по г. Казани
старший лейтенант полиции Алиев В.М.

«12» мая 2022г.

С рецензией ознакомлен Самигуллин Н.С.
12 мая 2022г

ОТЗЫВ

о работе обучающегося 073 учебной группы очной формы обучения, 2017 года набора, по специальности 40.05.02 Правоохранительная деятельность Самигуллина Нияза Сайдашевича
в период подготовки выпускной квалификационной работы
на тему «Криминогенный потенциал сети Интернет: проблемы предупреждения и противодействия преступлениям в информационной сфере»

Представленная выпускная квалификационная работа посвящена исследованиюкриминогенного потенциала сети Интернет и проблем предупреждения и противодействия преступлениям в информационной сфере. Слушатель Самигуллин Н.С.при выборе темы исследования руководствовался своими научными и профессиональными интересами.

Слушатель Самигуллин Н.С. четко сформулировал цель исследования и поставил задачи, необходимые для реализации цели работы и ее достижения. Логичность и корректность сформулированных задач и цели в свою очередь, сформировали логически четкую и последовательную, структуру работы.

Разработка плана исследования проводилась самостоятельно, но при этом, автор учел все предложения научного руководителя, что, несомненно, сказалось на логичности и структуре плана исследования.

Актуальность темы исследования не вызывает сомнения и четко сформулирована, что позволяет судить о способности автора грамотно и четко формулировать основную мысль и важность данной работы.Автор показал высокую степень владения методами системного анализа.

Несомненным достоинством данного исследования является вдумчивый анализ исследуемой проблемы, чем автор продемонстрировал хорошие навыки исследователя. Автором была проделана большая работа по сбору и анализу эмпирического материала, что также является достоинством данного исследования. Автор всесторонне постарался изучить проблему криминогенного потенциала сети Интернет, что представляет как научный так и практический интерес для правоохранительных органов.

После каждой главы автор сформулировал выводы, которые обоснованы и позволяют нам судить о достижении задач исследования.

В заключение своей дипломной работы автором сформулированы выводы и предложения по проведённому научно-практическому исследованию в рамках данной выпускной квалификационной работы. В течение всего периода выполнения исследования, слушатель Самигуллин Н.С. строго соблюдал все требования и представлял все этапы выполнения работы четко и в срок, что указывает на несомненную способность рационально планировать время последовательность работ при исполнении поставленной задачи.

Все указанные научным руководителем замечания и недостатки устранялись в установленные сроки. Слушатель Самигуллин Н.С. проявлял дисциплинированность и пунктуальность. Что, разумеется, сказалось положительно на результатах исследования.

Представленная выпускная квалификационная работа посвящена исследованию вопросов криминогенного потенциала сети Интернет. Данная актуальная проблема рассмотрена насколько это возможно в рамках выпускной квалификационной работы, последовательно, всесторонне и полно.

В содержании работы последовательно раскрываются вопросы, касающиеся характеристики преступлений, совершаемых в сети Интернет; а также практические аспекты предупреждения данных преступлений.

Автор изучил и проанализировал как специальную, научную литературу, так и следственную, судебную практику.

В заключение своей дипломной работы автором сформулированы выводы и предложения по проведённому научно-практическому исследованию в рамках данной выпускной квалификационной работы.

Слушателем Самигуллиным Н.С. был проанализирован большой объем теоретического материала, для написания работы использованы научные труды отечественных и зарубежных авторов, проблема раскрыта всесторонне, с разных точек зрения. Весь собранный материал изложен четко, последовательно, с соблюдением внутренней логики повествования. Практическое исследование проведено на высоком методологическом и теоретическом уровнях. Прослеживается тщательная и глубокая проработка каждого вопроса, что является итогом долгого научного исследования данной темы.

Таким образом, содержание данного дипломного исследования полностью соответствует первоначальному заданию и отвечает всем необходимым требованиям.

Оригинальность текста исследования 41,51%, цитирование 25,78% Структурно работа раскрывает основные аспекты темы. После каждой главы имеются выводы, которые подводят итог вышесказанному. В качестве недостатка данной работы можно отметить недостаточное исследование диссертационных исследований и монографий рассматриваемой темы, но указанный недостаток не является значительным, и не оказывает влияния на качество представленной работы.

Выбранная проблематика раскрыта полно и всесторонне, цель достигнута, задачи решены, выводы правильны и обоснованы, выработанные рекомендации и предложения имеют некоторую практическую значимость, и их реализация возможно, будет способствовать совершенствованию минимизации криминогенному потенциалу сети Интернет.

Основные положения выпускной квалификационной работы докладывались на Всероссийском научно-практический семинаре «Дистанционные хищения и кибербезопасность».

Исходя из вышеизложенного, полагаем, что представленная выпускная

квалификационная работа слушателя Самигуллина Нияза Сайдашевича рекомендуется к защите и заслуживает оценки «отлично».

Научный руководитель
Профессор кафедры криминологии и уголовно-исполнительного права
доктор педагогических наук, профессор
полковник полиции _____ Чанышева Г.Г.
(подпись) (инициалы, фамилия)

Подпись Чанышевой Г.Г.
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

«20» мая 2022 г.

С отзывом ознакомлен _____ «20» мая 2022 г.
ФИО, расшифровка

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Казанский юридический институт МВД России

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

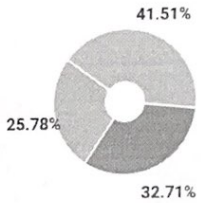
ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Самигуллин Нияз Сайдашевич
Самоцитирование рассчитано для: Самигуллин Нияз Сайдашевич
Название работы: Н. Самигуллин Криминогенный потенциал сети Интернет
Тип работы: Выпускная квалификационная работа
Подразделение: кафедра криминологии и уголовно-исплнительного права

РЕЗУЛЬТАТЫ

ЗАИМСТВОВАНИЯ	32.71%
ОРИГИНАЛЬНОСТЬ	41.51%
ЦИТИРОВАНИЯ	25.78%
САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 21.06.2022



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; Модуль поиска "КЮИ МВД РФ"; Медицина; Сводная коллекция вузов МВД; Диссертации НББ; Перефразирования по eLIBRARY.RU; Перефразирования по Интернету; Патенты СССР, РФ, СНГ; Коллекция СМИ; Шаблонные фразы; Кольцо вузов; Издательство Wiley

Работу проверил: Чанышева Гульнара Габдулхаковна

ФИО проверяющего

Дата подписи: 21.06.2022

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.