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 Трансформация преступности на современном этапе и способы её минимизации

Выполнил: Хамидуллин Салават Айратович
40.05.01 – Правовое обеспечение национальной безопасности, год набора 2017
173 учебная группа

Руководитель:
к.ю.н., доцент, начальник кафедры криминологии и уголовно-исполнительного права КЮИ МВД России
полковник полиции
Шалагин Антон Евгеньевич

Рецензент:
начальник отдела «К» МВД по Республике Татарстан
майор полиции
Афанасьев Артём Игоревич

Дата защиты: «___» _____2022 г. Оценка_____

Казань 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Поступательное развитие науки, техники, наращивание информационно-технологического потенциала на сегодняшний день напрямую влияет на процесс интеграции новых технических решений, позволяющих поддерживать и сопровождать многие сферы жизнедеятельности общества. В связи с этим, научно-технический прогресс диалектически детерминирует изменения в характере трудовой деятельности, формах взаимодействия участников общественного производства, обмена и другой общественно значимой деятельности.

Как известно, научно-техническая революция открыла новые способы и методы управления высокопроизводительными многоотраслевыми технологическими системами, в частности, появились информационно-телекоммуникационные сети, информационные технологии управления и иные виды технологических решений, призванных удовлетворять общественные нужды, в связи с чем, помимо полезных социальных видов взаимодействия общественных институтов, достижения технического прогресса, используются в общественно вредных целях.

Пандемия COVID-19, затронувшая все сферы общественной жизни, дала мощный толчок развитию информационных технологий и разнообразным электронно-цифровым сервисам, дистанционным формам взаимодействия людей. Такая ситуация внесла коррективы в различные формы преступных проявлений, что повлияло на изменения в сферах незаконного оборота наркотиков и оружия, нелегальной миграции, торговли людьми, реализации контрафактной продукции, а также на активность экстремистских, террористических групп, мафиозных организаций[1].

Трансформация преступности представляет собой глобальную проблему в новой цифровой эпохе. Несмотря на снижение уровня насильственной,

[1] Жданов Ю.Н., Кузнецов С.К., Овчинский В.С. COVID-19: преступность, кибербезопасность, общество, полиция. М.: Международные отношения. 2020. С.283.

имущественной, молодежной преступности, отмечается значительный рост киберпреступлений. Так, по данным Главного информационно-аналитического центра МВД России (далее – ГИАЦ МВД РФ) в 2021 году было зарегистрировано 517 722 преступления, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,4% больше, чем за аналогичный период.[1] При этом за последние 5 лет количество преступлений в информационной среде выросло в 25 раз.[2]

Помимо этого, актуальность выбранной темы обусловлена также тем, что состояние киберпреступности в России обострилось в связи с проведением специальной операции на Украине, послужившей катализатором для увеличения информационных атак на правительственные сайты РФ. Согласно данным Лаборатории Касперского, количество кибератак на российские компании в первые месяцы 2022 года выросло в 4 раза, по сравнению с аналогичным периодом прошлого года.[3]

Причины указанного негативного явления разнообразны, среди них можно выделить экономические, правовые и организационно-управленческие, которые в комплексе приводят к увеличению количества совершаемых преступлений в IT-сфере. Изменить положение дел может только стратегическое и тактическое направление развития мер противодействия данному общественно опасному явлению.

Объектом исследования являются общественные отношения, которые складываются при применении норм об уголовной ответственности за преступления с использованием информационно-телекоммуникационных технологий. Предметом исследования является механизм противодействия и предупреждения киберпреступлений.

---

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

[2] Киберпреступность в 2021 году выросла на 25%. – URL: https://pravo.ru/news/232676/ (дата обращения: 15.04.2022).

[3] «Лаборатория Касперского» фиксирует рост сложных кибератак на российские компании. – URL: https://habr.com/ru/news/t/657473/ (дата обращения: 15.04.2022).

Целью исследования выступает комплексный криминологический анализ и выработка мер противодействия киберпреступлениям в РФ. Достижение указанной цели определяет решение следующих задач:

– рассмотреть понятие, признаки и общественную опасность преступности;

– представить анализ количественных и качественных характеристик преступности;

– охарактеризовать сущность и способы оценки латентной преступности;

– проанализировать состояние преступности в Российской Федерации;

– выделить основные тенденции развития преступности в России;

– исследовать основные характеристики киберпреступности в России;

– изучить современные технологии отечественных мер профилактики и противодействия преступности;

– спрогнозировать развитие преступности в России к 2023-2024 годам;

– сделать выводы в рамках проведенного исследования.

В работе применялась совокупность общенаучных и частнонаучных методов: описательный; метод логического осмысления, позволивший последовательно изложить материал; абстрагирование и обобщение, призванные систематизировать факты и дать их толкование; анализ и синтез, обеспечившие достоверность выводов; системный подход, необходимый для раскрытия взаимосвязей между явлениями; статистический метод, использованный для анализа количественных показателей преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Эмпирическими материалами исследования послужили научные статьи, опубликованные в различных изданиях, статистические данные Генеральной прокуратуры Российской Федерации за период с 2017 по 2021 г., а также Главного информационно-аналитического центра МВД России за 2021г., результаты онлайн опроса сотрудников Центра по противодействию экстремизму МВД по Республике Татарстан, интернет-источники, судебная

практика. Апробация и внедрение в практику результатов исследования отражены в Приложении.[1]

В ходе работы использовались труды таких ученых как: Азарова И.В., Арямова А.А., Акутаева Р.М., Галуева В.О., Дегтярева М.О., Долгиева М.М. и многих других.

Структура работы обусловлена поставленными целями и задачами и состоит из введения, трех глав, объединяющих девять параграфов, заключения и списка использованной литературы.

[1] См.: Приложение 1.

ГЛАВА 1. ПРЕСТУПНОСТЬ КАК СОЦИАЛЬНО-НЕГАТИВНОЕ ЯВЛЕНИЕ И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

§1. Понятие, признаки и общественная опасность преступности

Согласно статье 2 Конституции Российской Федерации на государство делегирована обязанность защиты прав и свобод человека и гражданина.[1] Указанное положение свидетельствует о высокой значимости безопасности граждан, проживающих на территории России. В настоящее время безопасность является неотъемлемой частью жизнедеятельности общества и выступает в качестве необходимо обусловленного явления в жизни каждого человека.

Под безопасностью традиционно понимается состояние защищённости от потенциальных угроз, которые могут возникнуть в результате различного рода явлений, одним из которых является преступность. Так, в соответствии с п.42 Указа Президента РФ от 02 июля 2021 года №400 «О Стратегии национальной безопасности Российской Федерации», уровень преступности в России в отдельных социальных сферах остается высоким, в связи с чем вопросы эффективности государственной политики в области противодействия указанному явлению актуализируются, приобретая высокую значимость как для отдельно взятого лица, так и для всего государства в целом.[2]

На сегодняшний день в криминологической доктрине существуют разнообразные подходы к определению понятия «преступность».

С.М. Иншаков под преступностью понимает массовое, статистически устойчивое общественно обусловленное явление, негативную девиацию,

---

[1] Конституция Российской Федерации: принята на всенародном голосовании 12 декабря 1993 г., с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

[2] Указ президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 20.03.2022).

определённую уголовным законом.[1] А.И. Долгова напротив, считает, что преступность – это общественное явление, выражающееся в решении отдельными индивидами отдельно взятых социальных проблем посредством нарушения норм уголовного закона. [2]

О.В. Старков под преступностью понимает явление, подчиняющееся социологическим законам, которое выражает взаимосвязь между преступником и преступлением.[3] По нашему мнению, представленные определения по содержанию являются не полными ввиду нарушения целостности рассматриваемого нами явления как социальной системы, так как в них отсутствуют системные и иные существенные признаки, позволяющие отграничить преступность от иных социальных явлений.

Наиболее точным, по нашему мнению, является следующее определение: «преступность – это исторически обусловленное, изменчивое социально-правовое явление, образующееся из совокупности всех преступлений, совершенных за определенный промежуток времени и в рамках определенной территории, обладающее при этом свойствами социальной системы — саморегуляцией, саморазвитием и обратным воздействием на общество».[4]

В соответствии с данным подходом преступность включает в себя не просто множество преступлений. Их совокупность представляет сложное специфическое системно-структурное образование с многообразными взаимосвязями преступлений и преступников, видовую разнообразность преступлений и самой преступности в целом.

Таким образом, преступность является сложным многообразным социальным явлением, имеющим свои специфические существенные признаки, которые позволяют отграничивать её от иных социальных форм взаимодействия. Так как преступность представляет собой одну из форм социального

---

[1] Иншаков С.М. Криминология: практикум: учебное пособие. М.: ЮнитиДана, 2017. С.92.
[2] Преступность, ее виды и проблемы борьбы / под общ. ред. А. И. Долговой. М., 2011. С. 17.
[3] Криминопенология. Учебное пособие / Старков О.В. М.: Экзамен, 2004. С.37.
[4]Криминология: учебник для академического бакалавриата / Ю. М. Антонян. Москва: Издательство Юрайт, 2019. С.25.

взаимодействия, ей присущи признаки, позволяющие отграничить её от иных форм социальной системы.

Традиционно в криминологической науке выделяют такие существенные признаки преступности, как историческая изменчивость, социальная природа, правовая природа, негативность, системность.

Под исторической изменчивостью преступности следует понимать её диалектически обусловленную связь со временем. Это связано с тем, что на разных этапах общественного развития она формально видоизменяется, приобретая в своем содержании новые качественные состояния. Так, исходя из истории развития человечества – право, как свод общеобязательных формально определённых норм, существовало не всегда. Как отмечает Исаев А.А.: «возникновение права — длительный процесс, который происходил на протяжении многих поколений».[1]

«Понятие преступного связывается с крайними проявлениями зла, преступным считается посягательство на высшее добро... Преступник же — непосредственное воплощение (персонификация) зла», - отмечает А.М. Яковлев.[2] А сторонники психоаналитической, фрейдистской трактовки считают иначе. По мнению исследователей, преступность объясняется нормальными, изначально присущими природе, психике человека агрессивными, низменными подсознательными инстинктами. Сторонники биологической теории обосновывают вечность преступности устойчивыми, не находящимися в непосредственной связи с социумом свойствами личности, передаваемыми из поколения в поколение на генетическом уровне.

По нашему мнению, наиболее точно описывают историческую изменчивость сторонники противоположной позиции, так как существование преступности неразрывно связано с обществом. Мы считаем, что процесс противодействия преступности по своему содержанию сложен, длителен, а само

---

[1] Исаев, А. А. История формирования права и тенденция его развития // Молодой ученый. 2020. № 49 (339). С. 240.

[2] Яковлев А.М. Социология преступности (криминология): Основы общей теории. М.: Содействие новый век, 2001. - URL: http://crimestudy.ru (дата обращения: 24.03.2022).

явление неискоренимо, по крайней мере пока существует социум. Данный процесс вечно протекает на ряду с существующими либо возникающими социальными противоречиями, а также - общественным развитием, развитием научно-технического прогресса, которые так или иначе детерминируют её как явление социальное.

Помимо этого, историческая обусловленность также отражается в её содержании, характере, структуре и уровне на различных этапах общественного развития. Та же особенность в значительной мере свойственна причинам и условиям преступности, а также оценке законодателем круга деяний, признаваемых преступными. Так, поведенческий акт, считавшийся преступным в советский период, на сегодняшний день таковым не является. Например, в советском законодательстве – спекуляция, под которой, в соответствии со ст.154 УК РСФСР, понималась деятельность по скупке и перепродаже товаров, на сегодняшний день является весьма привычным явлением. [1]

Таким образом, историческая изменчивость преступности заключается в её закономерном и неискоренимом характере, возможности вечного существования в обществе. При этом существование преступности возможно только тогда, когда возможно существование общества.

Преступления совершаются представителями общества по отношению к его устоявшимся социальным нормам, против его порядка и отношений, из чего следует, что помимо исторической изменчивости, преступности присуща также социальная обусловленность.

Вместе с тем, криминология как наука, решая стоящие перед ней задачи, вынуждена исследовать целый ряд «фоновых» для преступности явлений антиобщественного характера. Речь идет о пьянстве, наркомании, проституции, бродяжничестве и тому подобных феноменах, составляющих питательную среду для преступности, но не охватываемых этим понятием.

---

[1] Уголовный кодекс РСФСР от 27 октября 1960 г. - URL: https://base.garant.ru/3983897/055d1b82a84145ca60b96f2b0fee8ae8/ (дата обращения: 23.03.2022).

Следующим рассматриваемым признаком является негативность преступности. Позитивистская и классическая криминологические школы придерживаются общего взгляда на преступность: «преступность - это явление, нарушающее основные ценности и убеждения общества». Эти ценности и убеждения проявляются в виде законов, которые общество принимает. То есть, негативность преступности проявляется в форме закрепленного в отечественном законодательстве закрытого перечня деяний, за совершение которых уголовным законом РФ предусмотрена ответственность. При этом негативный характер проявляется в признаках состава преступления, к которым, в частности, относится общественная опасность поведенческого акта.

Под общественной опасностью следует понимать качественное негативное объективно обусловленное социальное свойство преступления, заключающаяся в причинении существенного вреда объектам, охраняемым уголовным законом. Как справедливо отмечает А.А. Пионтковский: «несмотря на то, что опасность преступного деяния не способна поддаваться «чувственному восприятию», она «объективно существует» и познается рассудком через понимание отрицательного значения данного деяния».[1] Деяния, характеризуемые законодателем как общественно опасные, «разрушают» те или иные общественные отношения, порядок которых структурирован и важен для общества и государства именно в данный момент времени.

Немаловажным признаком преступности также выступает её системный характер. Под системностью понимается рассмотрение преступлений не в каждом отдельно взятом конкретном случае, а в совокупности. Системный подход в криминологии разрабатывается в ряде трудов отечественных криминологов, к которым, в частности, относятся Г. А. Аванесов, Ю. М. Антонян, Ф. Ю. Бердичевский, Ю. Д. Блувштейн, С. Е. Вицин и др. [2]

---

[1] Пионтковский А.А. Курс советского уголовного права. Общая часть. 1: Учение о преступлении по советскому уголовному праву. М., 1961. С.157.

[2] См. напр.: Аванесов Г. А. Теория и методология криминологического прогнозирования. М., 1972; Антонян Ю. М. Системный подход к изучению личности преступника // Советское

Однако системность как характеристика преступности в отечественной криминологии вызывает споры и по сей день. Так, по мнению ряда авторов, преступность, являясь многомерным и сложным диалектически обусловленным явлением, носит системный характер. Как отмечает В.Н. Кудрявцев: «преступность во взаимодействии с влияющими на нее факторами можно рассматривать как сложную систему, статистические процессы в которой образуются на основе разнообразных закономерностей».[1]

Сторонники противоположной позиции считают, что преступность не корректно рассматривать в качестве системного явления, так как ей присущи элементы стихийности, взаимосвязь элементов во многих случаях отсутствуют, не образуя целостной системы.[2] Помимо этого, по мнению учёных, преступность также не является системой в связи с тем, что она сохраняется не в силу своего социально обусловленного характера, а в результате внешних причин и условий на определённом этапе общественного развития. При этом сторонники рассматриваемой позиции признают, что преступности присущи отдельные элементы системы – повторяемость и устойчивость, которые обусловлены тем, что акты общественно опасного поведения возникают в результате влияния сходных причин и условий.

По нашему мнению, преступность следует относить к системе, так как она является процессом, обладающим целостностью взаимосвязанных элементов. Таким образом, резюмируя признаки преступности как явления, то мы приходим к выводу о том, что преступность является социально обусловленным, исторически изменчивым, уголовно-правовым, негативным явлением, проявляющимся в совокупности совершённых общественно опасных деяниях,

---

государство и право. 1974 № 4; Бердичевский Ф. Ю. Взаимодействие органов следствия и дознания как организационная система // Советское государство и право. 1973. № 12; Блувштейн Ю. Д. Криминология и математика. М., 1974; Вицин С. Е. Моделирование в криминологии. М., 1973; он же. Системный подход и преступность. М., 1980 и др.

[1] Кудрявцев В. Н. Проблемы причинности в криминологии // Вопросы философии. М., 1971. № 10. С. 50.

[2] Бородин С. В. Борьба с преступностью: теоретическая модель комплексной программы. М., 1990. С. 129.

совершенных на определенной территории за определенный промежуток времени, а также совокупность лиц, их совершивших на определённой территории за определённый промежуток времени.

Исходя из вышеизложенного следует, что преступность как социально обусловленное явление является закономерным исторически изменчивым, негативным, системным процессом, которое деструктивно воздействует на нормальное функционирование общественных институтов и взаимодействие индивидов в социуме, а также имеет ряд существенных признаков, позволяющих его отграничить от иных форм социального взаимодействия.

§2. Количественные и качественные характеристики преступности

Как было указанно ранее, преступность является социальным явлением, обусловленным состоянием социальной системы. Непрерывность детерминации преступности порождает наибольшие трудности в вытеснении её из жизни общества. В то же время преступность - сравнительно самостоятельное социальное явление, состоящее из количественно-качественных характеристик и подчиняющееся статистическим закономерностям. Выявление и объяснение этих закономерностей составляет главную задачу криминологических исследований преступности.

Рассмотрим количественные и качественные характеристики преступности. Любое явление имеет определенную форму выражения и определённое внутреннее содержание, преступность – не исключение. Под формой преступности подразумевается её внешняя структура, которая состоит из количественных показателей, а под содержанием – её внутренняя структура, которая образуется при совокупности качественных характеристик. Количественные и качественные характеристики преступности в совокупности образуют показатели преступности, которые позволяют оценивать и охарактеризовать состояние преступности на конкретной территории за определённый промежуток времени.

Из этого следует, что показателями преступности с количественной стороны являются определённые символически выраженные величины, позволяющие определить внешнюю сторону рассматриваемого явления, а с качественной стороны они представляют собой её качественную составляющую, позволяющую отражать её признаки и свойства. К количественным показателям преступности относятся состояние (объем), уровень и динамика преступности, к качественным – структура, цена и характер, рассмотрим подробнее.

Количественные показатели, как правило, выражены в числе совершённых преступлений либо в количестве лиц их совершивших. Одним из количественных показателей выступает состояние преступности, которое представляет собой совокупность совершённых преступлений на конкретной территории за определённый промежуток времени, выраженных в абсолютных цифрах. Так, согласно статистическим данным ГИАЦ МВД РФ, с января по ноябрь 2021 года было зарегистрировано 2004,4 тыс. преступлений и выявлено 848,3 тыс. человек, совершивших общественно опасные деяния.[1]

Под уровнем следует понимать индекс или коэффициент преступлений, совершенных на определённой территории за определённый промежуток времени. Данный показатель исчисляется посредством соотношения количества совершённых преступлений и определённого количества населения, проживающего на одной территории (рис.1.1).

$$КП = \frac{П \cdot 100000}{Н}$$

Рис.1.1 Формула вычисления уровня (коэффициента) преступности, где П – количество преступлений, совершенных на конкретной территории, а Н – количество людей, проживающих на данной территории

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

Данная формула также применяется при расчётах коэффициента преступности осуждённых лиц, только количество совершенных преступлений заменяется на количество осуждённых либо лиц, совершивших преступлений (рис.1.2).

$$K_2 = \frac{Л \cdot 100000}{Н}$$

Рис.1.2 Формула вычисления уровня (коэффициента) лиц, совершивших преступление, где Л – количество указанных лиц, проживающих на конкретной территории, а Н – количество людей, проживающих на данной территории

В целях более глубокого и всестороннего анализа преступности применяются дифференцированные коэффициенты по различным уровням: например, коэффициенты, характеризующие распространенность преступлений (преступности) и лиц, их совершивших (судимости) среди различных групп населения (например, с 14 лет и старше).

С помощью коэффициента криминогенной пораженности характеризуют соотношение удельного веса преступников определенной, возрастной или иной социальной группы (по полу, социальному положению, роду занятий и т. п.) в их общем числе к удельному весу этой же группы в общей численности населения. Допустим, удельный вес несовершеннолетних преступников (от 14 до 18 лет) составляет 15 процентов, доля же этой возрастной группы в населении составляет 20 процентов. Коэффициент пораженности определяется одним арифметическим действием: 10:12 = 0,75. Чем больше получается коэффициент пораженности, тем выше, стало быть, криминогенность изучаемой группы.

С помощью коэффициентов можно сравнивать распространенность или интенсивность преступности на разных территориях с разной численностью населения в разные временные периоды.

Под динамикой преступности следует понимать количественный показатель изменения преступности в контексте временной изменчивости её состояния, коэффициента и структуры. Данный показатель измеряется для выявления закономерностей и тенденций развития рассматриваемого негативного явления, который рассчитывается базисным и цепным методами, а также методом укрупнения интервалов.

Под качественными показателями преступности следует понимать её содержательную сторону, отражающую внутреннее выражение рассматриваемого явления, которые вычисляются количественно-статистическими показателями, представляющими собой, в зависимости от конкретного расчёта, абсолютные и обобщающие величины.

Абсолютные величины в свою очередь делятся на численные (число совершённых преступлений) либо на дифференцированные (число лиц, совершивших рецидив) совокупности, а обобщающие – на относительные и средние величины. Относительные величины рассчитываются посредством соотношения показателей (например, количество преступлений на количество населения). Средние величины, напротив, позволяют определить обобщённую характеристику однородной совокупности по конкретному количественному показателю (количество несовершеннолетних, совершивших разбойное нападение).

Под структурой преступности следует понимать соотношение отдельного вида преступлений ко всей группе в целом на конкретной территории за определенный промежуток времени (рис.1.3).

$$СП = \frac{Вп \cdot 100\%}{П}$$

Рис.1.3 Формула по расчёту структуры преступности, где ВП – количество представляющих интерес преступлений, П – общее количество совершенных преступлений

Следует отметить, что в доктрине криминологической науки преступность классифицируются по различным основаниям, так, например, в зависимости от гендерной принадлежности, преступность подразделяется на мужскую и женскую, в зависимости от мотивов – на корыстную, насильственную, должностную и т.д.

Характер преступности – качественный показатель, отражающий отличительные существенные признаки рассматриваемого явления, обусловленные лицами, совершившими преступления, а также территориальными, национально-этническими и региональными особенностями жизни. Данный показатель рассчитывается путём статистического анализа лиц, совершивших преступления, и составления на основе полученных результатов социально-криминологической характеристики преступности. Например, для Республики Татарстан характерны преступления корыстной направленности, организованная преступная деятельность и т.д.[1]

Помимо этого, немаловажным показателем также является её цена. Под ценой преступности понимается наносимый преступлениями имущественный ущерб. Данный показатель измеряется в трёх эквивалентах:

1) вред, причинённый преступлением физическому либо юридическому лицу;

2) косвенные затраты, возникшие в результате материального обеспечения правоохранительных органов, мест лишения свободы;

3) нерегистрируемый вред, выражающийся в негативном воздействии на психику, моральное состояние человека и т.д.[2]

Таким образом, посредством количественных и качественных показателей возможно производить расчёты для определения состояния преступности на определённой территории за конкретный промежуток времени.

---

[1] Криминальный Татарстан: меньше грабежей, больше тяжких преступлений и «кровавый» 2020-й // Сетевое издание «Снег». - URL: https://sntat.ru/news/kriminalnyi-tatarstan-mense-grabezei-bolse-tyazkix-prestuplenii-i-krovavyi-2020-i-5832553 (дата обращения: 15.04.2022).

[2] Криминология: учебник для академического бакалавриата / Ю. М. Антонян. Москва : Издательство Юрайт, 2020. С.65.

Исходя из вышеизложенного следует, что преступность, являясь совокупностью совершенных преступлений на конкретной территории за определённый промежуток времени, имеет количественные и качественные характеристики, позволяющие производить его оценку, необходимую для выстраивания эффективной государственной политики по противодействию и профилактике преступности среди граждан РФ.

§3. Латентная преступность: понятие, виды, способы оценки

Как известно, на сегодняшний день выявляются не все противоправные деяния, совершаемые на территории того или иного региона РФ. Преступность, не зарегистрированная в правоохранительных органах, не попавшая в официальные статистические данные в доктрине криминологической науки определяется как латентная преступность.

Латентная преступность для современной России является одной из наиболее существенных проблем для выработки эффективной уголовной политики, что обусловлено рядом факторов:

1) объём латентной преступности гораздо выше зарегистрированной, особенно в России по сравнению с другими странами;

2) из-за высокой латентности ежегодно происходят колебания состояния преступности;

3) латентность преступности позволяет наиболее полно охватить саму преступность в качестве социального явления, так как она неразрывно с ней связана;

4) данное свойство наиболее наглядно указывает на недостоверность показателей преступности, особенно в России.

Наличие латентной преступности в условиях современности порождает проблему неправильной оценки масштабов преступности, что снижает эффективность проведения программ по профилактике и предупреждению общественно опасных явлений в РФ, а также возможность прогнозирования

развития криминогенной обстановки, что подтверждается исследованиями, проведенными рядом учёных-криминологов.

В результате она выступает катализатором для возникновения у граждан низкого доверия к эффективности деятельности правоохранительных органов по вопросам защиты их прав, свобод и законных интересов.

Помимо этого, латентная преступность создает определённые затруднения в реализации основополагающих принципов уголовно-правовой системы – доступа граждан к правосудию, неотвратимости наказания. Как справедливо отмечает Р.М. Акутаев, что негативное влияние латентной преступности снижает авторитетность уголовного закона, что в результате порождает нигилистическое отношение к нормам права и общественным институтам.[1]

Для выявления показателей латентной преступности необходимо учитывать два фактора, позволяющие отграничить её от учтённой. Первый заключается в её скрытом характере, неизвестность правоохранительным органам информации о совершенном общественно опасном деянии, а второй – в её неучтённости в официальных уголовно-правовых статистических данных. [2]

Из этого следует, что латентная преступность является совокупностью не выявленных на конкретной территории за определенный промежуток времени преступлений, которая в результате не учитывается в официальных уголовно-правовых статистических данных.

Следует отметить, что несмотря на скрытый характер латентной преступности, в криминологической доктрине все же существуют способы её оценки, рассмотрим их. Так, в течение определенного промежутка времени на конкретной территории совершается некоторая совокупность преступлений, называемая фактической преступностью. Однако в учётных показателях содержится лишь часть фактической преступности, регистрируемой государственными органами. Следовательно, для расчёта латентной

---

[1] Акутаев Р.М. Латентная преступность: актуальные проблемы и понятие // Государство и право. 1997. № 12. С.80.

[2] Горяинов К.К., Исиченко А.П., Кондратюк Л.В. Латентная преступность в России: опыт теоретического и прикладного исследования. М., 1994. С.30.

преступности необходимо из фактической вычесть регистрируемую преступность. А для определения коэффициента латентности необходимо найти соотношение между фактической и регистрируемой преступностью.

Таким образом, латентная преступность может быть рассчитана для определения фактического состояния преступности в определенный промежуток времени на конкретной территории, что в результате может позволить минимизировать проявления преступности в целом путём выработки эффективных мер по её предупреждению.

Следует отметить, что по способу формирования существуют различные виды латентной преступности. Так, на сегодняшний день криминологами виды латентной преступности подразделяются по-разному, рассмотрим их подробнее.

По мнению М.М. Черноусова, латентность преступности выражается в следующем:

1) в естественной латентности, под которой понимается отсутствие в правоохранительных органах сведений о совершенном преступлении. В результате оно не будет учтено в официальной статистической отчетности и по нему не будет вынесено итоговое процессуальное решение;

2) в искусственной латентности, под которой понимается отсутствие в статистической отчетности сведений о противоправном деянии, возникшее в результате нарушения правил учета преступлений сотрудниками правоохранительных органов. [1]

Помимо этого, исследователями также выделяется пограничная латентность, под которой понимается неосознание либо непринятие факта совершенного в отношении субъекта преступления общественно опасного деяния.[2]

---

[1] Черноусов М. М. Исследование латентной преступности: теоретические и практические аспекты // Наука, образование и культура. 2018. № 2. С. 31.

[2] Дегтярева, М. О. Классификация и виды латентной преступности на примере Уральского федерального округа // Молодой ученый. 2021. № 5 (347). С. 177.

По мнению ряда отечественных криминологов, указанная классификация ограничена, в связи с тем, что она не охватывает детерминацию латентной преступности.[1] В связи с этим предлагается классифицировать рассматриваемое нами явление в зависимости от причин и условий латентизации преступности, поделив их на:

1) преступления, в которых нет персонафицированного потерпевшего, не заинтересованного в исходе дела;

2) преступления, факт которых известен ограниченному, как правило, виновному кругу лиц;

3) неправильно квалифицированные преступления правоохранительными органами;

4) незаявленные преступления – общественно опасные деяния, о которых потерпевшие не сообщают в компетентные органы;

5) преступления, информация о которых известна правоохранительным органом, но они (ошибочно или сознательно) не оценены ими в установленном уголовно-процессуальном порядке как уголовно наказуемые деяния и оставлены без учета.

6) преступления, по которым принято необоснованное процессуальное решение об отсутствии события или состава преступления.

Таким образом, в криминологии сложились различные точки зрения по классификации латентной преступности, схожие по отдельным признакам и взаимодополняющие друг друга, которые позволяют наиболее полно и всесторонне рассмотреть латентизацию данного социально негативного явления, её детерминацию.

Исходя из вышеизложенного следует, что под латентной преступностью следует понимать совокупность преступлений, ранее известных или

---

[1] См.напр.: Казиев А. З. Проблемы квалификации латентных преступлений // Вестник магистратуры. 2019. № 5-5(92). С. 70; Галуева В. О. Латентная преступность как неотъемлемая составляющая преступности // Общество и право. 2019. № 11. С. 78 и др.

неизвестных правоохранительным органам, которые в силу определённых причин не были учтены в официальной уголовно-правовой статистике.

Подводя итог отметим, что преступность представляет собой негативную девиацию, деструктивную исторически изменчивую социальную систему, которая обладает определённой совокупностью присущих ей существенных признаков, позволяющих отграничивать ее от иных социальных явлений, детерминируемую определённой совокупностью причин и условий и, в некоторых случаях, носящую латентный характер.

ГЛАВА 2. ТРАНСФОРМАЦИЯ ПРЕСТУПНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ

§1. Анализ состояния и тенденций преступности в Российской Федерации

На сегодняшний день во всех странах мира отмечается снижение преступности, в том числе и в Российской Федерации. По нашему мнению, в России снижение уровня преступности обусловлена следующими причинами:

1) в развитии так называемого дополнительного уголовного законодательства (в России: федеральные законы от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»; от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»; от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» и др. Эти законы прямо регулируют общественные отношения, связанные с большой общественной опасностью);

2) трансформация гражданского законодательства: частные общественные отношения интенсивно вытесняются публичными;

3) замещение узкоотраслевой уголовно-правовой специализации межотраслевым подходом;

4) декриминализация ряда статей Уголовного кодекса РФ и другие.

За 2021 год число зарегистрированных преступлений на территории России снизился, по сравнению с аналогичным периодом. Так, в 2021 году было зарегистрировано 2 004 404 преступления, что на 1,9% меньше, чем в 2020 году [1]. (табл. 2.1).

Показатели	Годы			
	2018	2019	2020	2021
Зарегистрировано заявлений (сообщений), млн	-3,3%	1,6%	1,0%	-1,9%

Табл. 2.1. Прирост преступности в России

[1] Статистические данные Генеральной прокуратуры РФ за 2021 г./ Официальный сайт Генеральной прокуратуры РФ. – URL: http://genproc.gov.ru/ (дата обращения: 12.04.2022).

Рост регистрируемых преступлений отмечен в 27 регионах РФ, снижение – в 58 регионах. Наибольшее количество преступлений было зарегистрировано на территориях Тульской области, Ненецкого автономного округа, Республики Ингушетия, Республики Адыгея, Приморского края, Якутии, Краснодарского края, Республики Дагестан, Республики Мордовия и Челябинской области, на которые приходится основная часть всех преступлений.

Четыре преступления (81,0%) из пяти регистрируются в городах и посѐлках городского типа – всего 1,6 млн, почти пятая часть (18,5%) – в сельской местности, где зарегистрировано 371,7 тыс. преступлений, что на 4,8% меньше, чем за январь - декабрь 2020 года.

При этом следует отметить, что ущерб от преступлений (по оконченным и приостановленным уголовным делам) за 2021 год составил 834,5 млрд руб., что на 62,7% больше аналогичного показателя прошлого года. Существенная часть ущерба (92,2%) приходится на преступления, зарегистрированные в городах и посёлках городского типа.

Большая часть зарегистрированных преступлений составляют преступления, связанные с хищением чужого имущества, которые совершены посредством кражи - 733,1 тыс. (-2,4%), мошенничества – 339,6 тыс. (+1,2%), грабежа – 31,5 тыс. (-18,1%), разбоя – 4,4 тыс. (-16,0%). При этом практически каждая 5 кража, грабеж или разбой были сопряжены с незаконным проникновением в жилище, производственное либо иное помещение.

Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с январем - декабрем 2020 года уменьшилось на 5,2% и составило 23,5 тыс. Также уменьшилось (-13,3%) количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств (779 преступлений).

В целом по России удельный вес тяжких и особо тяжких в числе всех зарегистрированных преступлений составляет 27,9%, что выше на 0,3% показателей за аналогичный период. Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с январем - декабрем

2020 года уменьшилось на 5,2% и составило 23,5 тыс. В январе - декабре 2021 года с использованием оружия, боеприпасов, взрывчатых веществ, взрывных или имитирующих их устройств совершено 4,7 тыс. преступлений (-9,1%).

В январе - декабре 2021 года зарегистрировано 2136 преступлений террористического характера (-8,8%) и 1057 преступлений экстремистской направленности (+26,9%).

Снижение числа зарегистрированных преступлений террористического характера, преступлений экстремистской направленности подтверждает действенность российской профилактической антитеррористической системы.

Однако несмотря на общее снижение количества совершаемых преступлений, на практике возникла тенденция по появлению новых форм преступности. Статистические данные и результаты криминологических исследований свидетельствуют о качественных изменениях преступной среды, прежде всего, в силу последствий научно-технической революции, особенно развития информационно-коммуникационных технологий, нарастающего деструктивного влияния со стороны стран, заинтересованных в дестабилизации Российской Федерации, а также сохраняющихся социально-экономических проблем, влияющих на криминализацию современного российского общества.

Особо высокими темпами нарастает киберпреступность, удельный вес которых в 2021 году составил 25,8%, что на 0,8% больше, чем за аналогичный период времени. В информационно-телекоммуникационной сети Интернет (далее – ИТКС Интернет), особенно в его «теневой» части по-прежнему размещены доступные экстремистские, террористические, нарко-, порно- и иные преступные ресурсы. Уровень контроля этого процесса все еще не соответствует его опасности, прежде всего, ввиду нахождения большинства серверов за пределами Российской Федерации и уклонения западных партнеров от сотрудничества на данном треке.

Согласно статистическим данным ГИАЦ МВД РФ, больше половины таких преступлений (55,7%) относится к категориям тяжких и особо тяжких (288,3 тыс.; +7,7%), более двух третей (67,9%) совершается с использованием

ИТКС Интернет (351,5 тыс.; +17,0%), почти половина (42,0%) – средств мобильной связи (217,6 тыс.; -0,5%). Более чем три четвери таких преступлений (78,4%) совершается путем кражи или мошенничества: 406,0 тыс. (-1,1%), почти каждое десятое (9,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 51,4 тыс. (+9,3%).

Следует отметить, что выявляемые в России наркосети организовываются с использованием современных информационных сетей и имеют центры управления за рубежом. Имеются основания для вывода о масштабном проникновении в страну транснациональной наркопреступности[1].

С января по декабрь 2021 года зарегистрировано 35 051 преступление коррупционной направленности, что на 13,8% больше, чем за аналогичный период. При этом отмечается рост преступлений, связанных со взяточничеством (+27,8%) и с коммерческим подкупом (+0,9 %), что является следствием возросшей активности органов внутренних дел, прежде всего, полиции.

В январе - декабре 2021 года зарегистрировано 20,3 тыс. экологических преступлений, что на 10,5% меньше, чем за аналогичный период прошлого года, что говорит об их высокой латентности.

По сравнению с январем - декабрем 2020 года на 11,6% увеличилось число преступлений экономической направленности, выявленных правоохранительными органами. Всего выявлено 117,7 тыс. преступлений данной категории, удельный вес этих преступлений в общем числе зарегистрированных составил 5,9%. Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 641,9 млрд руб.

В январе - декабре 2021 года выявлено 179,7 тыс. преступлений, связанных с незаконным оборотом наркотиков, что на 5,4% меньше, чем за аналогичный период прошлого года. Уменьшение общего количества зарегистрированных преступлений в сфере незаконного оборота наркотиков, а также совершенных в

[1] Статистические данные Генеральной прокуратуры РФ за 2021 г./ Официальный сайт Генеральной прокуратуры РФ. - URL: http://genproc.gov.ru/ (дата обращения: 12.04.2022).

состоянии алкогольного, наркотического и токсического опьянения свидетельствует об успешности принимаемых на протяжении последних лет мер по усилению контроля и профилактики на данном направлении, а также о вероятности переориентации части мировых наркопотоков (прежде всего, следующих из Афганистана) в обход России.

Так, в соответствии со Стратегией государственной антинаркотической политики Российской Федерации до 2030 года[1], с 2020 по 2022 год:

1) реализован комплекс организационных мер, обеспечивших совершенствование и оптимизацию государственного управления в сфере контроля за оборотом наркотиков, а также в области противодействия их незаконному обороту;

2) сформирована и функционирует государственная система мониторинга наркоситуации, обеспечивающая постоянное наблюдение за ее развитием;

3) реализован комплекс мер по пресечению незаконного распространения наркотиков;

4) обеспечена реализация мероприятий в рамках формирования системы защиты территории Российской Федерации от незаконного перемещения наркотиков через государственную границу Российской Федерации, что позволило пресечь более 16 тыс. фактов контрабанды наркотиков;

5) сформированы механизмы раннего выявления незаконного потребления наркотиков;

6) реализован комплекс правовых, организационных и экономических мер, направленных на повышение доступности и качества оказания наркологической помощи населению Российской Федерации;

7) получило дальнейшее развитие законодательство в сфере контроля за оборотом наркотиков, а также в области противодействия их незаконному обороту.

---

[1] Указ Президента РФ от 23.11.2020 №733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года». – URL: http://www.consultant.ru/document/cons_doc_LAW_368501/ (дата обращения: 20.03.2022).

Одной из превентивных мер государства направленных против изготовления и сбыта наркотических средств и психотропных веществ является утверждение Президентом РФ указа «О Стратегии государственной антинаркотической политики РФ на период до 2030 года», согласно которого Президент Российской Федерации перед государственным антинаркотическим комитетом поставил задачу в 6-ти месячный срок утвердить план мероприятий антинаркотической политики на период до 2030 г., направленных на повышение уровня контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров в целях обеспечения государственной и общественной безопасности.

О сохраняющейся и даже нарастающей активности организованной преступности в 2021 г. свидетельствуют рост на 26,5% преступлений, причём их удельный вес в общем числе расследованных преступлений этих категорий возрос с 7,8% в январе - декабре 2020 года до 9,3%.

Подтверждаются ранее сделанные выводы о нарастающей профессионализации преступной среды, недостаточном уровне профилактики рецидивной преступности и неэффективности пенитенциарной системы.

Однако ситуации с совершением преступлений организованными преступными группами в регионах складывается по-разному. Так, согласно докладу П.Ю. Серова, на сегодняшний день в Республике Татарстан система мер по противодействию организованной преступности отлажена, она эффективно справляется с поставленными перед правоохранителями задачами. По мнению автора, в настоящее время в Татарстане отсутствует та криминогенная среда, которая была в 90-х годах XX века, с начала 2000-х годов количество организованных преступных групп и сообществ сократилось на 40%, а число членов организованных преступных формирований в 2,5 раза.

Рассматривая динамику различных видов преступлений, необходимо установить, кто совершает подобные деяния, какие слои населения наиболее уязвимы перед соблазном нарушить закон.

В 2021 году в числе лиц, совершивших преступления, уменьшилось на 0,5%, однако удельный вес безработных (64,1%), совершивших преступление увеличился сна 0,2%, как и число ранее судимых лиц (30,1%).

Больше половины (60,0%) расследованных преступлений совершено лицами, ранее совершавшими преступления, каждое четвѐртое (28,1%) – в состоянии алкогольного опьянения, каждое тридцать второе (3,1%) – несовершеннолетними или при их соучастии.

Иностранными гражданами и лицами без гражданства на территории Российской Федерации совершено 36,4 тыс. преступлений, что на 5,9% больше, чем за январь - декабрь 2020 года, в том числе гражданами государств-участников СНГ – 28,5 тыс. преступлений, их удельный вес составил 78,3%.[1] Сокращение общего количества преступлений, совершенных иностранцами и лицами без гражданства, свидетельствует о повышении эффективности миграционного контроля после возложения данной функции на МВД России, а также об успешности реализации ведомственной подсистемы приоритетной программы «Реформа контрольной и надзорной деятельности».

Последовательное снижение в числе лиц, совершивших преступления, доли несовершеннолетних, компенсируется ростом и высоким удельным весом несовершеннолетних, совершивших преступления в соучастии.

Таким образом, анализ состояния преступности в 2021 году позволяет сделать вывод о том, что в настоящее время преобладает тенденция по увеличению количества преступлений в сфере собственности и совершенные с использованием информационно-телекоммуникационных технологий, в том числе с использованием ИТКС Интернет. При этом, по нашему мнению, количество подобного рода деяний со временем будет только нарастать.

Подведя итог, можно сформулировать наиболее значимые черты и особенности, присущие современной преступности. Это — организованность,

---

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

нарастающая транснационализация, особенно в сфере киберпреступности и незаконном обороте наркотических средств и психотропных веществ, увеличение числа тяжких и особо тяжких преступлений, появление новых форм подростковой преступности, а также иных социально-негативных явлений.

§2. Особенности трансформации преступности в XXI веке

История развития общества неразрывно связана с развитием научно-технического прогресса, который выступает необходимым условием для развития общественных отношений. В частности, на сегодняшний день жизнь человека невозможно представить без мобильных гаджетов, персональных компьютеров и иных информационных-телекоммуникационных устройств, так как, значительно упростив жизнь, они плотно вошли в различные сферы жизнедеятельности общества.

Однако использование технологических решений в обыденной жизни используется не только в общественно полезных, но и в преступных целях. Особую общественную опасность вызывает рост преступности в телекоммуникационной ИТКС Интернет. По данным ГИАЦ МВД России в 2021 году было зарегистрировано 517 722 преступления, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,4% больше, чем за аналогичный период.[1] При этом за последние 5 лет количество преступлений в информационной среде выросло в 25 раз.[2]

Таким образом, преступность с использованием информационно-телекоммуникационных технологий неуклонно растет, приобретая новое качественное состояние.

---

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

[2] Киберпреступность в 2021 году выросла на 25%. - URL: https://pravo.ru/news/232676/ (дата обращения: 15.04.2022).

Особый интерес представляет преступность в теневой сети Darknet. По мнению А.А. Мазура, под сетью Darknet следует понимать сетевой ресурс, соединения которого устанавливается лишь между доверенными пирами, с использованием нестандартных протоколов и портов, что по сравнению с иными видами сетевых ресурсов делает его наиболее скрытым. В Darknet используются домены, на которые возможно зайти только со специального программного обеспечения, такого как, например, Tor.[1]

Согласно исследованию Р.И. Дремлюги было выяснено, что в данной сети реализуются оружие, наркотические средства, детская порнография, поддельные денежные средства, краденое имущество и иные виды вещей, оборот которых запрещен на территории Российской Федерации. Расчеты по сделкам в ней производится при помощи цифровой валюты, которая позволяет сторонам сделок также оставаться анонимными.[2] Таким образом, совокупность преступлений, совершенных с использованием сетевого ресурса Darknet и криптовалюты носит высокий уровень латентности.

Одной из глобальных проблем в современном мире остается наркомания, которая затрагивает большинство стран мира, создавая угрозу физическому и психическому здоровью граждан. За последние десять лет наркомания привела к значительному увеличению количества госпитализаций вследствие психических и поведенческих расстройств. В целях распространения наркотических средств нередко используются криптовалюты и зашифрованные каналы связи (Telegram, Wickr, Signal и др.). Торговля наркотиками нередко связана с иными формами преступности, такими как отмывание денежных средств, полученных преступным путем, коррупция, терроризм.[3]

---

[1] Мазур А. А. Актуальные проблемы предупреждения преступности в сети Даркнет // Вестник Российского института кооперации. 2018. № 3. С. 125.

[2] Дремлюга, Р. И. Преступный мир Darknet /Р. И. Дремлюга// Юридическая наука и практика. Владивосток. 2018. № 1. С. 55.

[3] Шалагин А.Е., Идиятуллов А.Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2 (44). С.230.

Также трансформируется организованная и профессиональная преступность. Согласно статистике ГИАЦ МВД России, в 2021 году было зарегистрировано 634 преступления, совершенных в составе организованной группы либо преступным сообществом (+47,8%). Приведённая статистика указывает на распространённость данной общественно опасной организованности лиц, совершающих преступные деяния.[1]

Если ранее в 80-90-е годы прошлого века, происходило сращивание организованных преступных групп (ОПГ), совершающих общеуголовные преступления, и преступных сообществ, специализирующихся на преступлениях экономической направленности, то на сегодняшний день она постепенно перемещается в киберпространство.

В связи с этим ИТКС Интернет представляет повышенный криминогенный интерес для организованных преступных групп и сообществ, так как позволяет упростить совершение общественно опасных деяний, а также внедрятся в другие страны, приобретая качество транснациональности.

Трансформация профессиональной преступности детерминируется возросшей значимостью вовлечения в ряды преступных группировок высококвалифицированный специалистов и экспертов в области прикладного применения информационно-телекоммуникационных технологий. Помимо этого, в зависимости от конкретной преступной специализации, также возрастает значимость таких специалистов, как юристы, экономисты, медики, фармацевты, химики, биогенетики.

Таким образом, вся внутренняя структура организованной преступности постепенно трансформируется в кибер-организованные преступные группы и сообщества, поле деятельности которых охватывает все сферы современных способов совершения преступлений, в том числе кибератаки на критически важную государственную инфраструктуру, активизация преступной

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

деятельности в теневой сети Darknet, использование криптовалюты, токенов в механизме онлайн-преступлений, кража персональных данных и шантаж, киберторговля людьми и онлайн-секс индустрия, кибернаркотрафик и т.д.

Значительное место в современной структуре преступности занимают преступления против половой неприкосновенности и половой свободы личности. Согласно совместному отчету Интерпола и международной организации по борьбе с детской проституцией и торговлей людьми ECPAT (End Child Prostitution and Trafficking), 84% изображений CSAM-контента содержат откровенные сексуальные сцены, 52% лиц, задействованных в порнографических фильмах (видеосюжетах), не достигли совершеннолетия. В некоторых странах (Таиланд, Филиппины, Бразилия, Колумбия) развита сексиндустрия (секстуризм), в том числе с привлечением детей и подростков. Согласно данным Независимого агентства по расследованию случаев сексуального насилия над детьми (IICSA), в группе риска находятся девочки в возрасте от 11 до 17 лет.[1]

Также следует отметить, что в условиях пандемии появились новые схемы преступной деятельности:

1) незаконные компенсации (несуществующие социальные выплаты);

2) поддельные сайты по продаже масок и антисептических средств;

3) несуществующие приглашения из поликлиник для прохождения медицинского обследования;

4) призывы пожертвовать свои деньги на псевдоблаготворительные цели;

5) реализация поддельных лекарственных средств и БАДов;

6) хакерские атаки на государственные и муниципальные учреждения;

7) незаконная реализация сертификатов о вакцинации от вируса Covid-19 и др.

---

[1] Шалагин А.Е., Идиятуллов А.Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. 2021. Т. 12. № 2 (44). С. 231.

Исходя из изложенного следует, что в изменения в социально-экономических и общественных отношениях вызвали качественную трансформацию преступности, которая характеризуется высоколатентными противоправными деяниями в сфере информационных технологий, распространением влияния транснациональных преступных сообществ, появлением новых форм мошеннических действий, распространением деструктивных идей среди молодёжи. Происходит стирание границ (различий) между реальностью и виртуальностью, миром вещей и информации, деятельностью онлайн и оффлайн, социальной средой и киберпространством, что, в результате, порождает новые формы преступности в России.

§3. Киберпреступность как угроза национальной безопасности

На сегодняшний день особый интерес представляет киберпреступность, так как ежегодно она вычленяется из совокупности зарегистрированных преступлений высокими темпами роста, по сравнению с иными видами преступных деяний.

Как было отмечено начальником Главного организационно-аналитического управления Генеральной прокуратуры Российской Федерации А.Ю. Некрасов: «Ситуация с киберпреступностью и кражей денег у населения по телефону с каждым годом лишь ухудшается – власти уже официально признают ее национальной проблемой. Злоумышленники действуют на опережение и находятся на несколько шагов впереди тех, кто им противодействует: законодательство не поспевает за новыми угрозами в сфере высоких технологий и схемами краж денег «сотрудниками безопасности банка»».[1]

[1] Арапов В.В., Заруцкая Н.А. Почему киберпреступления – угроза национальной безопасности. – URL:https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti (дата обращения: 15.04.2022).

Таким образом, масштабы киберпреступности достигли таких размеров, что позволяют называть их угрозой национальной безопасности.

Как отмечается в Доктрине информационной безопасности, на сегодняшний день возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.[1]

В связи с этим возникает интерес к киберпреступности как к социально-негативному явлению XXI века и одной из наиболее актуальных угроз национальной безопасности России, рассмотрим подробнее способы совершения киберпреступлений.

Данная угроза актуальна не только для России, но и для всего мирового сообщества. По статистике, каждую секунду в мире совершается около 18 попыток совершения противоправного деяния в IT-сфере, и около 40 % из них - удачные. По данным многих аналитических компаний около 2/3 пользователей Интернета хотя бы раз становились жертвами киберпреступников (в некоторых случаях жертва даже не подозревает о совершенном в ее отношении преступлении). Мировой ущерб от киберпреступлений исчисляется миллиардами. Только за 2018 год мировая экономика потеряла около 400 млрд долларов в связи с активной деятельностью киберпреступников.[2]

Следует отметить, что наибольшее распространение киберпреступность получила в сфере совершения преступлений против собственности в форме кражи и мошенничества с использованием банковских карт. Криминогенный

---

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL:https://base.garant.ru/71556224/ (дата обращения: 20.03.2022).

[2] Итоги исследования: Киберпреступность в России и мире. - URL: https://rb.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/ (дата обращения: 11.04.2022).

интерес к данной сфере преступной деятельности обусловлен многими факторами, одним из которых, к примеру, является утечка баз данных, в которых хранятся персональные данные, а также коммерческая, профессиональная, врачебная и иная охраняемая законом тайна, заполучив которую злоумышленник может нанести материальный вред охраняемым законом интересам, начиная от простого хищения чужого имущества, заканчивая – приостановлением деятельности крупных предприятий.

Цифровые преступления, по своей сути, малоизучены и имеют высокий уровень латентности, что обусловлено, с одной стороны «отсутствием современной методической базы исследования этого вида деяний, недостаточными знаниями IT-технологий, изменением способов совершения преступлений и пр. Действительно, в настоящее время, преступления могут совершаться в виртуальной среде, не выходя из своего дома или офиса и сохраняя анонимность».[1] Помимо этого, основные затруднения в раскрываемости киберпреступлений также заключаются в практической невозможности своевременного выявления подобного рода деяний ввиду того, что абсолютное большинство таких действий совершается в информационной среде, которая на данный момент не является полностью подконтрольной компетентным органам власти.

Особую тревогу вызывают хакинг, кардинг и современный фишинг. Чаще всего объектами хакерских атак становится промышленность, в 28,9 % случаев, и правительственные учреждения, в 25 % случаев.[2] Этот показатель свидетельствует о том, что преступные формирования сегодня стремятся владеть всей информацией о развитии новых технологий, их внедрении в промышленность, о принятии новых законов и иных нормативных актах, а также получать информацию о деятельности правительства.

---

[1] Конев Д.А. Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: постановка проблемы: автореф. дис. ... канд. юрид. наук. М., 2020. С.25.
[2] Там же.

Особенно остро ощущается проблема распространения фишинговых атак, содержащих вредоносные файлы, например, с использованием шифровальщиков данных, способных зашифровать всю информацию, содержащуюся на информационных носителях той либо иной организации. Чаще всего мишенью являются объекты критической информационной инфраструктуры (банки, атомные предприятия, объекты здравоохранения, электроснабжения, военные объекты и госструктуры).

Анализ типов атак, проведенный Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка позволяет сделать вывод о том, что на территории Российской Федерации в 2020 года был зафиксирован рост числа кибератак на различные сервисы дистанционного обслуживания, что связано с неблагоприятной эпидемиологической ситуацией в стране. Основная причина такого роста – введение большинством организаций кредитно-финансовой сферы режима удаленной работы. Многие граждане находились дома (на самоизоляции) и активно использовали банковские приложения для оплаты различных услуг – этому способствовало временное закрытие филиалов банков, МФО, введение штрафов за нарушение требований самоизоляции.[1]

В период борьбы с COVID-19 Банк России зафиксировал (в сравнении с аналогичным периодом прошлого года):

• значительный рост количества фишинговых рассылок;

• появление новых видов вредоносного программного обеспечения;

• активизацию хакерских группировок.

Злоумышленники переориентировали свою деятельность на использование программ-шпионов с целью осуществления удаленного доступа к информационным системам организаций и последующего получения данных компаний для извлечения материальной выгоды.

---

[1] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов// Официальный сайт Центрального Банка России. – URL: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения: 15.04.2022).

Прежде всего это связано с тем, что большинство организаций перешли на удаленный режим работы. Так, в 2020 году по сравнению с 2019 годом был зафиксирован двукратный рост использования шпионских программ.

Данные Центра мониторинга и реагирования на кибератаки Solar JSOC за «период январь–ноябрь 2020 г. зафиксировано более 200 профессиональных хакерских атак на российские компании, что в двое больше, чем за весь 2019 год, обращает внимание издание. При этом 30 атак совершили хакерские группировки наиболее высокого уровня».[1]

Основой этих преступлений является социальная инженерия – обман, который провоцирует пользователей на совершение последовательных действий, которые способствуют активизации вредоносного программного обеспечения. Опасность ее применения заключается в том, что от ее методов пока нет защиты, так как воздействие идёт не на программный продукт, а на психику человека.

В настоящее время также активно распространён киберэкстремизм (кибертерроризм). Данные явления представляют повышенную общественную опасность, угрожающую состоянию защищённости личности, общества и государства. Так, согласно статистическим данным, в 2021 году зарегистрировано 2136 преступлений террористического характера (-8,8%) и 1057 преступлений экстремистской направленности (+26,9%), что говорит о тенденциях роста и актуализации рассматриваемой нами проблемы.[2]

Несмотря на незначительное количество преступлений экстремистской направленности, по сравнению с общим показателем преступности, каждое такое преступление способно вызвать повышенный общественный резонанс и дестабилизировать внутриполитическую и социальную обстановку, как в отдельном регионе, так и по всей стране.

---

[1] Обзор: Эксперты выявили скачок числа кибератак на стратегические предприятия РФ. - URL: https://www.interfax.ru/russia/739380 (дата обращения: 15.04.2022).

[2] Статистические данные Генеральной прокуратуры РФ за 2021 г./ Официальный сайт Генеральной прокуратуры РФ.- URL: http://genproc.gov.ru/ (дата обращения: 12.04.2022).

Как отметил Президент РФ на расширенной коллегии МВД России, «серьёзной угрозой национальной безопасности остаётся экстремизм. В прошлом году сотрудниками органов внутренних дел выявлено 500 преступлений экстремистской направленности, или 60 процентов от общего количества зарегистрированных».[1] При этом особую опасность представляет распространение экстремистских идей и публичных призывов к экстремистской деятельности в ИТКС Интернет, так как доступ к такой информации предоставляется широкому кругу лиц.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.[2]

Так, согласно статистическим данным, большинство преступных проявлений экстремизма связаны с публичными призывами к осуществлению экстремистской деятельности (+34,9 %, 367 ед.), значительная часть из которых совершена с использованием ИТКС Интернет (339 ед.).[3]

Это обусловлено тем, что использование новейших цифровых технологий повышает не только эффективность преступной деятельности экстремистов и террористов, позволяя обеспечить «анонимность» их финансирования, но и дает возможность объединять широкий круг разобщенных пользователей

---

[1] Расширенное заседание коллегии МВД России // Официальный сайт Президента России . - URL: http://www.kremlin.ru/catalog/persons/310/events/65090 (дата обращения: 12.04.2022).

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». - URL: https://base.garant.ru/71556224/ (дата обращения: 20.03.2022).

[3] Статистические данные Генеральной прокуратуры РФ за 2021 г./ Официальный сайт Генеральной прокуратуры РФ. - URL: http://genproc.gov.ru/ (дата обращения: 12.04.2022).

информационно-телекоммуникационных сетей, находящихся в разных точках мира.

При этом повышенную общественную опасность, как отмечается в Указе Президента РФ от 29 мая 2020 г. № 344, представляет вовлечение молодёжи, так как, в силу социально-демографических, психологических и иных особенностей она более восприимчива к деструктивной информации пропагандистского характера.[1]

В настоящее время в ИТКС Интернет отмечается негативное влияние на несовершеннолетних появление и развитие неформальных объединений, популяризирующих идеи терроризма и экстремизма, пропагандирующих культуру насилия, потребления наркотиков и сильнодействующих веществ. При этом особый интерес представляет распространение идеи скуллшутинга в мессенджерах и социальных сетях. Так, на сегодняшний день превалирует тенденция по смешению деструктивных идеологий и появлению новых качественно отличающихся форм киберэктремизма (кибертерроризма), что подтверждается опросом сотрудников отделения по борьбе с IT-преступлениями Центра по противодействию экстремизму МВД по Республике Татарстан.[2] 25.01.2022 г. был проведен опрос фокус-группы в форме анкетирования, в рамках которого были поставлены следующие вопросы:

1. Какие деструктивные идеи на сегодняшний день наиболее распространены в сети Интернет?

2. Прослеживаются ли тенденции по качественному изменению деструктивных идей в сети Интернет? Если да, то какие?

3. Посредством каких информационных ресурсов производится вовлечение в деструктивные идеологии?

4. Какие возрастные категории больше всего подвержены деструктивному влиянию?

---

[1] Указ Президента РФ от 29.05.2020 №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. 01.06.2020. № 22. Ст. 3475.

[2] См.: Приложение 2.

По результатам опроса установлено, что наиболее распространенными выступают идеи скуллшутинга (98% респондентов), распространяемых чаще всего в мессенджерах (57,1%), чем в социальных сетях (42,9%). Это обусловлено тем, что в мессенджерах, как правило, применяются криптографические методы шифрования информации, позволяющие повысить анонимность лица в ИТКС Интернет.[1]

При этом отмечается факт того, что наиболее подверженными вовлечению в деструктивные идеи выступают несовершеннолетние лица (65,4% респондентов), так как, в силу социально-демографических, психологических и иных особенностей она более восприимчива к деструктивной информации пропагандистского характера.

Среди существенных причин распространения экстремизма среди молодёжи выступают проблемы в семье, реальные жизненные проблемы, которые оставляют неизгладимый след в психике, особенно у подростков. В частности, неудовлетворённость материальной стороной жизни, утрата ценностных ориентиров являются одними из наиболее частых причин вовлеченности в деструктивные идеи. В связи с этим именно молодёжь является наиболее подверженной деструктивной обработке, так как, в связи с отсутствием жизненного опыта, она не способна критически подходить к информационным потокам.

Помимо этого, одной из существенных причин выступают психологические травмы, являющиеся следствием психотравмирующих событий, воздействия стрессовых или фрустрационных факторов. Переживание травмы приводит к депрессии, побуждает, при дефиците родительской поддержки и сложностях в коммуникациях со сверстниками, к поиску альтернативной самореализации в социальных сетях, ослабляет иммунитет к деструктивному воздействию. В ряде случаев выбираются агрессивные или

[1] См.: Приложение 3.

аутоагрессивные способы преодоления жизненных трудностей, предлагаемые экстремистскими идеями.

В числе указанных негативных факторов часто встречаются различные нарушения воспитания в семьях, которые внешне считаются благополучными. Однако в каждой второй такой семье родители привлекались к административной, реже уголовной ответственности за побои, домашнее насилие, дебоширство, в том числе связанные с употреблением наркотиков или алкоголя.

Однако данное условие не присуще к представителям радикального ислама, преследующих цель установить «джихад», так как, в основном, данные лица воспитываются в полных семьях, где почитаются ценности и догматы традиционного ислама. Например, случай совершения нападения подростка на отдел полиции в г. Кукмор. Согласно материалам проверки, подросток, находясь возле парковки отдела внутренних дел, бросил в сторону здания два «коктейля Молотова» и выкрикивал лозунги: «Аллах Акбар, я вас всех убью», после чего напал на двух сотрудников полиции с ножом и, в результате, был ликвидирован. Перед своим нападением подросток записал видео обращение, в котором он призывал «братьев-мусульман» к джихаду.[1] Данное происшествие, помимо распространения деструктивной идеологии, направленной на разжигание розни и ненависти, также является ярким примером перехода от простых слов к акциям прямого действия, что обуславливает повышенную общественную опасность подобного рода деяний.

Таким образом, ввиду семейно-бытовых проблем, психотравмирующих ситуаций и иных детерминант, обуславливающих распространение экстремизма, молодёжь является наиболее подверженной к вовлечению в деструктивные идеи посредством ИТКС Интернет, так как для лиц, пропагандирующих радикальные

[1] Подросток в Кукморе напал на отдел полиции – его застрелили // Деловая информационная газета «Бизнес Онлайн». - URL: https://yandex.ru/turbo/business-gazeta.ru/s/news/486484 (дата обращения: 05.04.2022).

взгляды, они являются наиболее уязвимой мишенью для реализации их преступных замыслов.

Также респондентами отмечается тенденция по смешению деструктивных идеологий между собой (колумбайна с правым радикализмом, псевдоислама с суицидально-направленными идеями и т.д.) и созданию качественно новых деструктивных явлений. Так, например, мессенджере «Telegram» в 2021 году существовали каналы и чаты, распространяющие идеи скуллшутинга, в которых, как правило, состояли приверженцы националистических взглядов, пропагандирующих культ насилия, ксенофобии, нетерпимости к другим нациям.

Таким образом, распространение преступности в сфере цифровых технологий и в отношении их непосредственно, «настолько велико, что еще раз подтверждает необходимость самого серьезного внимания со стороны государства к этой проблеме и взвешенного принятия решений по предупреждению правонарушений и преступлений в названной сфере».[1]

Исходя из вышеизложенного следует, что киберпреступность с каждым днём становится все более совершенной в результате возникновения новых методов и способов совершения преступных деяний с использованием информационных технологий, что предполагает серьёзный правовой и прикладной поиск методов и средств, обеспечивающих эффективное противодействие им.

Подводя итог отметим, что активное развитие научно-технического прогресса детерминирует новые способы совершения преступных деяний с использованием информационных технологий, ИТКС Интернет, а также совершённых в сфере компьютерной информации, что в результате приводит к активному росту преступлений в информационной среде, со временем приобретая высокий уровень угрозы для национальной безопасности России, в

[1] Смольянинов Е.С. Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий / Е.С. Смольянинов, М.Ю. Воронин // Вестник РГГУ. Серия «Экономика. Управление. Право». 2018. № 3 (13). С. 136.

связи с чем остаются актуальными вопросы обеспечения эффективной работы правоохранительных органов по минимизации информационных рисков.

ГЛАВА 3. ПРЕДУПРЕЖДЕНИЕ И ПРОГНОЗИРОВАНИЕ ПРЕСТУПНОСТИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

§1. Современные технологии профилактики и предотвращения преступлений

Одним из наиболее приоритетных направлений криминологической науки выступает предупреждение преступности. Изучение криминологической характеристики преступности, особенностей личности лиц, совершающих преступления, а также факторов, детерминирующих преступное поведение, осуществляется с целью формирования комплексных мер предупредительного характера.

Как справедливо указывает Р.В. Авдеев, «предупреждение преступности должно иметь приоритет перед карательной политикой».[1]

Предупреждение преступлений и административных правонарушений в первую очередь направлено на детерминирующие свойства конкретного криминогенного фактора, который может поспособствовать развитию антиобщественного поведения.

При этом несмотря на то, что криминология является наукой о преступности, из поля своего научного зрения она не вправе упускать административные правонарушения. Изучение данных проступков и их тенденций должно осуществляться по следующим причинам:[2]

1) существует целый ряд административных правонарушений, смежных с преступлениями (мелкое хищение, незаконное хранение наркотических средств и др.). Данные правонарушения отличаются от преступлений лишь по отдельным

---

[1] Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. – Москва. : Академия управления МВД России, 2021. – URL: https://coollib.com/b/536932-t-v-pinkevich-tsifrovaya-kriminologiya/read (дата обращения: 20.04.2022).

[2] Предупреждение преступлений и административных правонарушений органами внутренних дел: учебное пособие / под общей редакцией Ф.К. Зиннурова. Казань: КЮИ МВД России, 2022. С.3.

признакам объективной стороны их состава, в остальном же они сходны с преступлениями.

2) Уголовный Кодекс Российской Федерации (далее – УК РФ) содержит ряд преступлений, которые содержат административную преюдицию, то есть привлечение к уголовной ответственности за них осуществляется при повторном совершении после привлечения к административной ответственности (мелкая кража, побои и др.).

3) многие лица, совершающие преступления, склонны и к совершению административных правонарушений (мелкому хулиганству, распитию алкогольной продукции в запрещенных местах и т.п.). Поэтому для комплексного понимания личностных факторов, детерминирующих преступное поведение, важно изучать и соответствующие административные правонарушения в их статике и динамике.

В связи с этим изучение проблем предупреждения преступлений в комплексе с административными правонарушениями представляет собой наиболее эффективный путь противодействия данным антиобщественным явлениям.

Система предупреждения преступлений и административных правонарушений представляет собой сложную, взаимосвязанную схему, включающую органы государственной и муниципальной власти, их должностных лиц, а также юридических лиц, общественных объединений и граждан, взаимодействующих между собой и взаимодополняющих друг друга, воздействующих на факторы, детерминирующие антиобщественное поведение, с целью его сокращения, сдерживания и искоренения.

Данная система включает большое количество субъектов, осуществляющих свои полномочия на различных уровнях – уровне всего общества и государства (Президент, Правительство, Федеральное Собрание, общественные объединения всероссийского масштаба деятельности), на уровне субъектов Федерации – органы государственной власти субъектов и общественные объединения на регионального характера, на муниципальном

уровне – органы местного самоуправления и муниципальные общественные объединения, а также отдельные юридические лица и граждане.

В криминологической науке субъекты профилактики делятся на общие и специализированные.

К первой группе можно отнести, например, Президента, Правительство, Федеральное Собрание и другие органы власти, к компетенции которых отнесены многочисленные вопросы управления общего характера. Данная группа субъектов непосредственно не осуществляет деятельность по предупреждению преступлений и административных правонарушений, однако, именно, они определяют общую стратегию противодействия антиобщественным явлениям.

К специализированным субъектам относятся органы власти, общественные объединения и юридические лица, в компетенцию которых входит осуществление непосредственной деятельности по предупреждению антиобщественного поведения.

К данным субъектам относятся: органы и должностные лица Министерства внутренних дел, Федеральной службы безопасности, Федеральной службы исполнения наказаний, Федеральной таможенной службы, прокуратуры, добровольные народные дружины, казачьи общества, частные детективные и охранные предприятия.

Все указанные субъекты имеют свои полномочия, круг установленных задач и сферу деятельности. Выполняя свои обязанности, органы и должностные лица активно взаимодействуют друг с другом, обмениваются при необходимости значимой информацией, оказывают другу содействие в проведении правоохранительных мероприятий, обеспечивая комплексность и системность в сфере предупреждения и пресечения преступлений и административных правонарушений, в частности:

– ФСБ России выполняет задачи по контрразведке, борьбе с терроризмом, преступностью, обеспечению информационной безопасности и др.

– Федеральная служба исполнения наказаний, среди прочего, обеспечивает правопорядок и законность в системе учреждений, исполняющих уголовные наказания.

– Федеральная таможенная служба осуществляет деятельность по обеспечению законности перемещения товаров через таможенную границу, предупреждению и пресечению преступлений и административных правонарушений в таможенной сфере.

– Органы прокуратуры активно включены в деятельность по предупреждению преступлений и административных правонарушений путем реализации надзорных и координационных полномочий.

– Добровольные народные дружины и казачьи общества участвуют в предупредительной деятельности путем содействия правоохранительным органам и участия в охране общественного порядка, пресечении преступлений и административных правонарушений и др.

– Частные охранные предприятия осуществляют деятельность по охране жизни и здоровья граждан, собственности физических и юридических лиц, обеспечивают пропускной режим и охрану общественных мероприятий и т.д.

Особое место в данной системе занимают органы и должностные лица Министерства внутренних дел России, на которые возложен широкий круг полномочий по противодействию преступности и административным правонарушениям.

Органы внутренних дел и их должностные лица наделяются значительными полномочиями, связанными с предупреждением, выявлением, раскрытием и пресечением как преступлений, так и административных правонарушений, обеспечивают защиту жизни, здоровья, собственности, прав и свобод физических и юридических лиц, общественный порядок и общественную безопасность.

На основании изложенного можно сделать вывод о том, что деятельность субъектов профилактики по предупреждению преступлений и

административных правонарушений является одним из ведущих криминологически значимых направлений, состоящем в воздействии на детерминанты преступности, провоцирующие и способствующие совершению и распространению антисоциальных явлений.

Как было указанно ранее, преступность постепенно изменяется, приобретая новые качественные характеристики. При этом особый интерес представляют преступления и административные правонарушения, совершенные в ИТКС Интернет, в связи с чем возрастает потребность в эффективных способах и методах профилактики данных антиобщественных явлений. Рассмотрим существующие способы профилактики преступлений и административных правонарушений, совершаемых с использованием ИТКС Интернет.

Компьютерные технологии являются неотъемлемой частью жизни современного общества. В очередном отчете Digital 2020, отражающем результаты ежегодного глобального исследования, проводимого агентством We Are Social1 и платформой Hootsuite, содержатся следующие сведения:

– количество интернет-пользователей в мире в январе 2020 года составляло 4,54 млрд, а в июле 2020 уже 4,57 млрд;

– в январе 2020 года в мире насчитывалось 3,80 млрд пользователей социальных сетей, в июле – 3,96 млрд;

– более 5,19 млрд человек пользуются мобильными телефонами – прирост на 124 млн (2,4 %) за последний год.

В России количество интернет-пользователей, по данным Digital 2020, составило 118 млн (81 %), а численность аудитории социальных сетей на начало 2020 года достигла 70 млн пользователей, что составляет 48 % от всего населения страны. [1]

[1] Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite. – URL: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite (дата обращения: 20.04.2022).

Очевидно, что неограниченность просторов сети Интернет, огромное количество пользователей, среди которых много тех, кто не боится нарушать законы, возможность обеспечения анонимности (особенно при использовании Darknet), привело к тому, что, несмотря на достаточно жесткое и межправительственное противодействие киберпреступлениям, наблюдается значительный рост данных деяний из года в год.

Криминологическая ситуация в России продолжает быть сложной, поэтому предупреждению преступлений уделяется особое внимание. Государством принимаются необходимые меры по изменению сложившейся ситуации и снижению напряженности в этой сфере. В связи с этим, на федеральном уровне принят ряд документов, который определяет основные принципы, задачи и цели предупреждения преступлений, как в целом, так и отдельных ее видов.[1] Это дает основание считать, что правовая основа предупреждения преступлений создана и действует единая государственная система их предупреждения.

Целью деятельности, направленной на предупреждение преступлений, совершаемых в сфере цифровых технологий, является снижение уровня этих преступлений, а также защита личности, общества и государства от преступных посягательств. Основная задача предупреждения преступлений, совершаемых в сфере цифровых технологий, заключается в выявлении, устранении и нейтрализации причин и условий, способствующих совершению названных преступлений и предотвращении готовящихся преступлений. Практическая реализация целей, задач и принципов предупреждения преступлений зависит от правоприменительной деятельности. Объектом предупредительной деятельности выступает система причин и условий, способствующих совершению преступлений, что дает основание рассматривать предупредительную деятельность как целенаправленную деятельность

[1] См.напр: Концепция общественной безопасности в Российской Федерации (утв. Президентом Российской Федерации. 14 ноября 2013 г. № Пр-2685); Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.) и др.

государства, общества, физических и юридических лиц, направленную на недопущение их совершения путем выявления, анализа, устранения или нейтрализации причин преступлений, условий, способствующих их совершению, оказания предупредительного воздействия на лиц с противоправным поведением.[1]

Необходимо отметить, что понятие предупреждения преступности является родовым понятием по отношению к понятиям: профилактика предотвращение и пресечение преступлений. По мнению ряда авторов, эти понятия идентичны. При этом, профилактика преступлений – это предупредительная деятельность, направленная на устранение, ослабление, нейтрализацию криминогенных факторов, детерминирующих преступление; недопущение совершения преступления лицом, ведущим антиобщественный образ жизни; разъяснение гражданам их прав и обязанностей, способов защиты себя, своего имущества от преступных посягательств. Под предотвращением преступлений понимается деятельность, направленная на недопущение замышляемых или подготавливаемых преступлений. На этой стадии формирования замысла преступного поведения путем проведения оперативно-розыскных мероприятий: выявляются лица, от которых по их негативному поведению можно ожидать совершений правонарушений (преступлений); устраняются условия, которые способствуют реализации подобных мыслей.

Предупреждение преступлений, совершаемых в сфере цифровых технологий, требует весьма серьезных усилий государства и общества и может быть успешным только на основе использования широкого комплекса общесоциальных и специальных предупредительных мер. Необходимой предпосылкой эффективности деятельности по предупреждению преступлений, совершаемых в сфере цифровых технологий является ее социальная и

[1] Федеральный закон от 23 июня 2016 года №182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ. 27.06.2016. № 26 (ч.1). Ст. 3851.

экономическая обоснованность. Вместе с тем предупредительная деятельность должна отвечать не только требованиям эффективности, но и системности.

Системный подход к разработке и осуществлению мер предупреждения цифровых преступлений включает действия различных звеньев предупредительной деятельности, дифференцированных по масштабу, функциям, свойствам и в то же время взаимодействующих в решении задач предупредительного характера. Речь должна идти о всесторонности воздействия взаимосвязанного комплекса экономических, политических, социальных, правовых, идеологических и иных мер воздействия на причинный комплекс цифровой преступности.

В теории криминологии предлагается рассматривать систему предупредительного воздействия на преступность в четырех уровнях предупредительно-профилактической деятельности:

1) общесоциальное предупреждение, которое имеет целью устранение, нейтрализацию, ослабление всего комплекса криминогенных факторов; предупреждение самой возможности формирования антиобщественной направленности личности;

2) криминологическая профилактика, включающая устранение, нейтрализацию или ослабление неблагоприятных факторов социализации; пресечение начавшегося процесса криминогенной деформации личности; недопущение перехода на преступный путь лиц с явной антиобщественной направленностью; исключение рецидива со стороны лиц, уже совершивших преступления;

3) охранительное предупреждение преступлений удержание неустойчивых лиц от совершения преступлений; создание внешних, объективных препятствий, делающих невозможным или же затрудняющим совершение преступлений; обнаружение и пресечение подготавливаемых и начатых преступлений;

4) уголовно-правовое предупреждение, которое обеспечивает: механизмы общей и частной превенции с помощью устрашения уголовной ответственностью и практикой ее осуществления; лишение лица с помощью

изоляции физической возможности совершать преступления; исправительное и воспитательное воздействие в ходе отбывания наказания.[1]

Построение системы предупредительно-профилактической деятельности можно считать оправданной, потому что она включает все этапы предупредительного воздействия. Следует признать, что в криминологической литературе предлагаются различные классификации предупредительных мер. Известно, что классификация мер предупреждения как прием научного исследования подчиняется строгим требованиям. Она должна, в частности, охватывать все меры, которые осуществляются субъектами предупредительной деятельности, обеспечить их исполнение и облегчить их применение, создавать теоретическую основу совершенствования методики их проведения, определить этапы проведения и т.п. Но все это возможно осуществить только при построении классификационных систем, основанных на различных критериях, а поскольку существует различные классификации предупредительной деятельности, остановимся на классификации предупреждения преступлений по уровню: общесоциальные и специально-криминологические предупреждение.

При этом общесоциальное предупреждение включает в себя совершенствование экономических, социальных, духовных, политических отношений в обществе; выявление и устранение диспропорций в них; криминологическая экспертиза; экспертные исследования, укрепление законности, социальная защита населения. На этом уровне наиболее эффективным является разработка социальных программ по отдельным проблемам криминогенного характера.

Основой общесоциального уровня предупредительной деятельности названных преступлений должны стать результаты проведенного мониторинга современного состояния цифровой преступности, при этом должны учитываться не только показатели зарегистрированных преступлений, совершенных в сфере цифровых технологий, но и реальное состояние с учетом ее латентной части,

[1] Криминология: учеб. / Под ред. В.Н. Кудрявцева, В.Е. Эминова. М.: Норма: Инфра-М, 2010. С.265.

причинного комплекса, судебно-следственной практики по данной категории дел, механизма привлечения к уголовной ответственности и его реализация в целом, социально политической и экономической ситуации, сложившейся на момент подготовки мер предупредительного воздействия, результаты криминологического прогноза на краткосрочный и среднесрочный периоды, и другие составляющие, которые позволят правильно и в полном объеме учесть все необходимые особенности современных криминологических угроз с целью определения направления предупредительного воздействия.

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

Социально-политические меры предупреждения преступлений, совершаемых в сфере цифровых технологий являются основными при осуществлении названной деятельности, так как государственная уголовная политика во «многом зависит от укрепления роли государственной власти, рационализации подходов к выработке решений в формировании уголовной политики, от создания условий для эффективной работы механизмов, основанных на саморегулировании и препятствующих развитию дестабилизирующих факторов».[1] Важным направлением в данном случае должны стать меры, направленные на стабилизацию политической ситуации в России; укрепление и повышение авторитета политической власти; создание законодательной базы по охране цифровых технологий и защиты, но базы правовой защищенности российских граждан; выработка стратегии и тактики уголовной политики, а также политики идеологического воздействия.

[1] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т.В. Пинкевич. Москва: Юрлитформ, 2020. С.231.

Особое внимание следует уделить и нормативным предписаниям, регламентирующим противодействие цифровой преступности, в соответствии с международно-правовыми стандартами и международными обязательствами России; заключение и ратификация международных Конвенций, межгосударственных договоров и соглашений по вопросам противодействия цифровой преступности.

Организационно-управленческие меры предупреждения преступлений, совершаемых в сфере цифровых технологий призваны способствовать организации предупредительной деятельности, принятию стратегических решений по обеспечению охранительными, контрольными и надзорными функциями органов и учреждений за сферой цифровых технологий, определить их взаимодействие по защите цифровых технологий от преступных посягательств и пр.

Предупреждение названного вида преступлений зависит от профессионализма субъектов предупредительной деятельности в сфере IT-технологий. В связи с этим необходима подготовка и переквалификация сотрудников правоохранительных органов, необходимо укрепление подразделений, которые непосредственно осуществляют мероприятия по противодействию преступлениям в сфере цифровых технологий.

Помимо этого, эффективность предупреждения преступлений в сфере цифровых технологий зависит, прежде всего, от основ ее организации, которая включает деятельность по формированию самой системы предупреждения преступлений и обеспечению процесса ее функционирования. Она может быть успешной только при комплексном воздействии на причины и условия, способствующие совершению цифровой преступности. С этим нельзя не согласиться, так как преступность – явление, обладающее разноуровневыми характеристиками и детерминированная факторами социального, социально-психологического и индивидуально-психологического порядка, требующее для своего изучения использование комплексного подхода.

Комплексный подход к воздействию на причинный комплекс цифровой преступности обеспечит достижение ощутимого предупредительного эффекта при условии проведения целой системы мер, рассчитанных на длительный период, учитывающих особенности криминологической обстановки.

Совокупность наиболее существенных конкретных требований, соблюдение которых в различном сочетании может обеспечить комплексный подход к предупреждению названного вида преступности, характеризуется сочетанием: общесоциального и специального предупреждения; мер общей и индивидуальной профилактики, охватом всех основных сфер жизнедеятельности и институтов социализации гражданина, использованием взаимосвязанных и взаимообусловленных мер экономического, идеологического, культурного, правового, организационно-управленческого характера, взаимодействием и координацией деятельности всех субъектов профилактики, охватом совокупности объектов, требующих профилактического воздействия на совокупность причин и условий, способствующих совершению цифровых преступлений.

Обеспечение комплексного подхода в предупредительной деятельности зависит от выбора направлений и мер предупредительного воздействия. К таковым можно отнести:

– вовлечение всей системы субъектов предупреждения преступности и средств, направленных на снижение негативных явлений, влияющих на рост цифровой преступности;

– взаимодействие и активизация государственных и общественных органов и организаций в сфере предупреждения цифровой преступности;

– использование форм и методов предупреждения цифровой преступности, основанных на результатах научных исследований и внедренных в практическую деятельность правоохранительных органов;

– разработка и реализация федеральных и региональных программ предупреждения цифровой преступности.

Подготовка таких программ должна осуществляться с учетом:

– результатов проведенного мониторинга состояния защищенности населения;

– определения степени его криминологической безопасности, выступающей составной частью общей системы национальной безопасности России;

– изучения и определения криминологических угроз и рисков, которые позволят определить «как будет меняться структура преступности, какие будут появляться новые формы организации преступных сообществ, как изменяется преступное поведение под воздействием технологий новой технологической революции и т. п.». [1]

Более того, основой такой работы должны стать результаты работы с использованием методов и программ искусственного интеллекта и анализа больших данных. Такая подготовка должна вестись совершенно на новом уровне, строго выверенных научных данных, к разработке которых следует привлечь квалифицированных сотрудников научных центров страны в сфере IT-технологий, ученых, представляющих различные отрасли знаний – экономики, право, управление, социологию, практических работников и др.;

– привлечение современных специалистов, имеющих определенные знания в названной сфере. Но самое главное необходима подготовка организационных антикриминальных инструментов, в их числе:

а) разработка новой системы профессионального образовательного процесса, направленного на обучение будущих специалистов правоохранительной деятельности и повышение квалификации действующего правоохранительного сообщества способам, методам, приемам и формам выявления, раскрытия и расследования преступлений, совершаемых в сфере цифровых технологий;

б) внесение изменений в учебные программы подготовки и повышения квалификации сотрудников правоохранительных органов;

---

[1] Овчинский В. С. Как изучать организованную преступность в XXI веке. - URL: https://izborsk-club.ru/15222 (дата обращения: 30.03.2022).

в) разработка методических рекомендаций по противодействию современным вызовам преступности;

г) техническая оснащенность правоохранительных органов новейшими технологиями цифрового мира; – учитывая предшествующий опыт, когда граждане, да и юридические лица, не имея достаточных знаний в той или иной сфере, теряли свою собственность, становились банкротами и т. д., созрела необходимость правовой пропаганды и обучения граждан правовым основам цифрового права.

При мероприятиях по предупреждению цифровой преступности необходимо проводить мониторинг с целью получения сведений об уровне электронной торговли, о количестве интернет-магазинов, осуществляющих электронную торговлю, оборот электронной торговли, количество пользователей компьютерами и имеющих доступ к сети Интернет, уровень компьютерных навыков населения; объем инвестиций в телекоммуникации и др. С целью прогнозирования цифровой преступности особое внимание следует уделять электронному маркетингу, электронному банкингу и электронным страховым услугам.

Субъектами предупреждения цифровой преступности являются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, действующие в пределах своей компетенции как непосредственно, так и через подведомственные им структуры. В предупреждении данного вида преступлений важная роль принадлежит различным государственным и негосударственным структурам, выполняющим функции по обеспечению цифровой безопасности. Ряд таких структур создан законодательными актами, принятыми в Российской Федерации в последние годы.

Участвовать в профилактике могут как отдельные лица, так и общественные объединения, и иные организации, которые целенаправленно осуществляют на различных уровнях и в различных масштабах профилактическую деятельность, наделенные, в связи с этим определенными

правами и обязанностями и несут ответственность за их реализацию в рамках ч. 1, 7, ст. 10, ст. 13, ч. 1 ст. 17 Федерального закона от 23 июня 2016 г. №182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации».[1]

По нашему мнению, привлечение молодёжных лидеров, некоммерческих организаций, ассоциаций, объединений и иных общественных организаций является эффективным способом профилактики противоправных деяний в ИТКС Интернет. Так, в настоящее время в ряде субъектов Российской Федерации работают, например, кибердружины, которые осуществляют мониторинг информационно-телекоммуникационной сети «Интернет» и при обнаружении распространения противоправного контента, в частности, так называемого «трэш-контента» (фото- видеоизображения, с элементами насилия), распространения наркотических веществ, детской порнографии и пр., передают информацию в правоохранительные органы. В 2016 в Республике Татарстан было создано региональное отделение молодежного общественного движения «Кибердружина» (далее – кибердружина РТ), образованное Лигой безопасного интернета, в функции которого входит мониторинг ИТКС Интернет на предмет противоправной информации.

Помимо этого, в Республике Татарстан также существует институт молодёжных помощников руководителя Аппарата антитеррористической комиссии в Республике Татарстан (далее – молодёжные помощники АТК в РТ), занимающийся вопросами общей и специализированной профилактики деструктивных явлений среди молодёжи. Одним из основных направлений деятельности данного института молодёжного участия в деятельности органов государственной власти заключается в мониторинге социальных сетей, мессенджеров и иных информационных ресурсов на предмет противоправного контента экстремистской, террористической либо суицидальной

[1] Федеральный закон от 23 июня 2016 года №182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ. 27.06.2016. № 26 (ч.1). Ст. 3851.

направленности, способного навредить нормальному контента, данная информация в рамках обращения передается в правоохранительные органы либо направляется на блокировку доменного имени в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций России (далее – Роскомнадзор).

Так, с сентября по декабрь 2021 года молодёжными помощниками руководителя Аппарата АТК в РТ было выявлено более 95 информационных источников противоправной направленности с изображением нацистской символики или символики, сходной с ней до степени смешения, суицидального, колумбайн контента, которые были направлены в компетентные надзирающие и правоохранительные органы.

По нашему мнению, для наиболее эффективной предупредительной деятельности необходимо сократить дистанцию между правоохранительными органами и общественными организациями, выработать эффективную систему сотрудничества и непосредственного взаимодействия, что, в последствии, позволит выработать наиболее эффективный превентивный механизм предупреждения преступлений и административных правонарушений в ИТКС Интернет. Таким образом, в настоящее время существует ряд серьезных проблем, способствующих развитию преступности в информационной среде, которые требуют незамедлительного разрешения.

Исходя из изложенного следует, что одним из наиболее приоритетных направлений криминологической науки выступает предупреждение преступности, так как изучение криминологической характеристики преступности, особенностей личности лиц, совершающих преступления, а также факторов, детерминирующих преступное поведение, осуществляется с целью формирования комплексных мер предупредительного характера. А также о том, что на сегодняшний день существует ряд проблемных вопросов предупреждения преступлений и административных правонарушений в ИТКС Интернет, требующих незамедлительного разрешения со стороны компетентных органов.

§2. Прогнозирование и планирование в сфере предупреждения преступлений

В повседневной жизни мы часто прогнозируем развитие тех или иных социальных, экономических, политических, семейно-бытовых процессов. Прогнозирование и планирование - одно из приоритетных направлений в деятельности по предупреждению и минимизации преступности.

По мнению В.В. Лунеева, криминологическое прогнозирование представляет собой научное предсказание основных изменений (тенденций) развития преступности или вероятности совершения уголовно-наказуемых деяний конкретными лицами в обозримом будущем, базирующееся на исследованиях, проводимых научными и практическими сотрудниками.[1]

Криминологическое прогнозирование основывается на знании тенденций преступности, а также на разнообразных и взаимосвязанных процессах, оказывающих непосредственное влияние на криминальную и антиобщественную среду. Анализ количественных и качественных характеристик преступности в прошлом и настоящем позволяет установить общие закономерности развития этого социально-негативного (общественно-опасного) явления в будущем.

Для составления криминологического прогноза необходимо обращение к множеству нормативных правовых актов, статистической информации, результатам оперативно-служебной деятельности правоохранительных органов, материалам контрольно-ревизионных проверок, научным, учебно-методическим, справочным источникам. Криминологическое прогнозирование должно отвечать требованиям достоверности, обоснованности, согласованности, системности, достаточности, своевременности, непрерывности.

Анализ состояния, структуры, динамики, иных показателей преступности позволяет оценить масштабы этого явления, уровень угрозы конкретным общественным отношениям. Результаты такой деятельности позволяют

---

[1] Лунеев В.В. Курс мировой и российской криминологии. Общая часть: учебник. М.: Юрайт, 2011. С.801.

определить взаимосвязь преступности с иными социально-негативными явлениями (алкоголизмом, наркоманией, проституцией, безнадзорностью, экстремистскими взглядами и т.д.). Они способствуют выработке новых форм и методов противодействия преступности, а также повышению эффективности правоприменительной практики.[1]

Деятельность по прогнозированию преступности направлена на решение следующих задач:

а) установление общих показателей, характеризующих изменение преступности в перспективе;

б) сбор информации, представляющей существенное значение для разработки комплексных планов;

в) выработка тактики и стратегии противодействия преступности;

г) выявление (устранение) причин и условий преступности;

д) профилактическое воздействие на противоправное (асоциальное) поведение;

е) выполнение криминологических исследований, направленных на профилактику преступности.

К этапам криминологического прогнозирования относятся: 1) сбор необходимой информации; 2) обработка и анализ информации; 3) разработка вариантов (сценариев); 4) оценка и уточнение полученных данных; 5) корректировка прогноза. Прогнозирование преступного (антиобщественного) поведения возможно проводить в предкриминальной, преступной, постпреступной ситуациях.[2]

Криминологические прогнозы по масштабу распространения можно разделить на: мировые, общероссийские, региональные, местные, локальные. В

---

[1] Шалагин А.Е. Предупреждение социально-негативных явлений, представляющих угрозу здоровью населения и общественной нравственности // Вестник экономики, права и социологии. 2015. № 2. С. 15.

[2] Криминология: учеб. / Под ред. В.Н. Кудрявцева, В.Е. Эминова. М.: Норма: Инфра-М, 2010. С.270.

зависимости от роли прогнозов в решении задач по предупреждению преступности они делятся на: оперативные, тактические, стратегические. По временному признаку их можно классифицировать на: краткосрочные (до 1 года); среднесрочные (от 1 года до 5 лет); долгосрочные (5-10 лет); дальнесрочные (свыше 10 лет).[1]

К методам криминологического прогнозирования, получившим распространение на практике, относятся:

1) экстраполяция - суть заключается в изучении истории прогнозируемого объекта и перенесении закономерностей его развития в прошлом и настоящем на будущее;

2) моделирование - создание упрощенного образа прогнозируемого объекта, отражающего его существенные свойства (график, диаграмма, формула, схема, таблица и т.п.);

3) экспертная оценка - заключается в обобщении мнений специалистов, основывающихся на большом практическом опыте в сфере правоохранительной деятельности;

4) системный анализ - предусматривает обязательный учет взаимосвязи преступности и ее причин с другими социальными, экономическими, политическими, демографическими и иными факторами.[2]

Криминологическое прогнозирование предшествует составлению перспективного плана по противодействию преступности. Прогнозируется и сам процесс выполнения плана, ожидаемые результаты. Криминологическое планирование представляет собой элемент социального управления, выражающийся в определении субъектов и объектов предупреждения преступности, поиске наиболее эффективных средств и методов противодействия криминальной среде.

---

[1] Иншаков С.М. Криминология: практикум: учебное пособие. М.: ЮнитиДана, 2017. С.98.

[2] Демидов В.Н., Сафиуллин Н.Х. Криминологическое прогнозирование: современное состояние и перспективы: учеб. пособие. - Казань: КЮИ МВД России, 2000. С.58.

Таким образом, криминологическое прогнозирование необходимо для разработки эффективного плана по борьбе с преступностью, что в первую обусловлено его опережающим характером. Перспективные оценки возможных вариантов преступности позволяют достичь точности и своевременности в определении целей и задач борьбы с ней, их соотношений и приоритетов, установить объемы и интенсивность мер профилактики и уголовно-правового воздействия.

По результатам сравнительного количественно-качественного анализа состояния преступности за последние 5 лет, а текущей геополитической ситуации, позволяет выделить тенденции развития преступности к 2023-2024 годам. По нашему мнению, в прогнозируемом периоде будет отмечен значительный рост киберпреступлений, а также преступлений террористического характера и экстремистской направленности.

Преступления террористического характера, экстремистской направленности. В 2021 году число зарегистрированных преступлений террористического характера уменьшилось на 8,8 %. [1]

На снижение числа преступлений террористического характера повлияло:

– создание в Российской Федерации действенной системы раннего предупреждения и пресечения преступлений террористического характера, в том числе государственной системы предупреждения, пресечения ядерного терроризма и ликвидации его возможных последствий;

– организация эффективного межведомственного и международного взаимодействия на данном направлении;

– реализация органами внутренних дел мероприятий, предусмотренных Федеральным законом «О противодействии экстремистской деятельности», Стратегией противодействия экстремизму в Российской Федерации до 2025 года, Стратегией национальной безопасности Российской

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

Федерации, Стратегией государственной национальной политики Российской Федерации на период до 2025 года, Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы, а также Комплексным планом противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы;

– последовательное усиление ответственности за любые проявления террористической активности и экстремистскую деятельность, а также постоянное совершенствование правоприменительной практики;

– проведение на системной основе мероприятий по противодействию пропагандистской деятельности иностранных государств, международных правительственных и неправительственных организаций, направленных на стимулирование сепаратизма, дестабилизацию общественно-политической обстановки в стране, возбуждение ненависти и вражды;

– обеспечение снижения криминогенного потенциала, связанного с перекрытием каналов нелегальной миграции и сокращением трудовой

– миграции из стран СНГ, произошедшим в результате изменений в законодательстве (ужесточение порядка въезда трудовых мигрантов, профессиональных требований к лицам и порядку получения разрешения на трудовую деятельность)[1].

Продолжился рост регистрации таких преступлений, как содействие террористической деятельности и организация террористического сообщества и участия в нем. Возросло число публичных призывов к осуществлению террористической деятельности или публичного оправдания терроризма.

Наблюдается тенденция по увеличению количества преступлений экстремистской направленности (+26,9%;1057). В структуре преступлений экстремистской направленности преобладали такие составы, как возбуждение

[1]Азарова И.В. Проблемы противодействия преступлениям террористической направленности, совершаемым на территории России гражданами из стран – участников СНГ // Вестник Воронежского института ФСИН России. 2018. № 1. С. 125.

ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ) и публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ).[1] За 2021 год существенно возросло число выявленных фактов финансирования экстремисткой деятельности, а также организации деятельности экстремисткой организации.

В прогнозируемом периоде не исключены:

– нарастание экстремистских настроений в обществе за счет обострения социально-экономических и внешнеполитических противоречий, розни на национальной, религиозной, политической, идеологической и иной социальной почве;

– создание и поддержка очагов экстремистской и террористической напряженности вблизи Государственной границы России и границ, сотрудничающих с нею стран. Наиболее ярким примером такого рода выступает украинский геополитический кризис, инициированный и поддерживаемый из-за рубежа;

– усиление информационной войны против Российской Федерации со стороны внутренних и внешних подрывных сил с целью искаженного новостного освещения антитеррористических действий государств, вплоть до инсценировок и фальсификаций, направленные на дискредитацию политических лидеров России и руководства силовых структур, включая МВД России.

Все эти негативные действия могут способствовать активизации распространения идеологии терроризма и экстремизма и для «раскачивания» протестной активности населения страны с использованием опыта и приемов так называемых цветных революций[2].

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (принят ГД ФС РФ 24.05.1996 г.) (ред. от 11.06.2021 г.) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

[2]Соловьев В.С. Криминологическое исследование экстремистских проявлений в социальных сетях Интернета (по материалам интернет-опроса пользователей) // Юристъ-правоведъ. 2016. №5. С.65.

Следует ожидать наращивания активности преступной деятельности идеологов радикальных религиозных течений, законспирированных ячеек международных террористических структур, а также националистических организаций, движений и групп. Продолжится перемещение преступной деятельности в виртуальное пространство, способствующее дальнейшему распространению идей радикализма, и приводящего к вовлечению в террористические и экстремистские сообщества новых членов, в том числе несовершеннолетних и молодежи.

С учетом изложенного в текущем году прогнозируется рост преступлений, отнесенных к террористическим и экстремистским.

Киберпреступления. В статистических формах ГИАЦ МВД России сведения о большинстве киберпреступлений выделяются с 2021 года, поэтому проследить их динамику возможно лишь по ограниченному кругу деяний.

В 2021 году таких преступлений было совершено 351,5 тыс. (+17,0 %) от количества всех зарегистрированных преступлений.[1] Отмечаются также:

– сохранение высокой угрозы кибертерроризма и киберэкстремизма против интересов Российской Федерации;

– усложнение и глобализация схем совершения киберпреступлений, посредством которых осуществляются вмешательство со стороны иностранных государств во внутренние дела Российской Федерации;

– попытки влияния через киберпространство на общественное мнение населения России с целью дискредитации государственной власти, финансирование оппозиционных общественных объединений, особенно в связи с эскалацией конфликта на Украине;

– расширение практики использования криптовалют в коррупционных схемах, а также легализация преступных доходов; повышение латентности

[1] Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ. – URL:https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).

преступлений коррупционной направленности вследствие использования криптовалют как средства их совершения;

– рост политических мотивов при совершении киберпреступлений. Так, неформальные группы и общественные движения, используя Интернет и защищенные (зашифрованные) каналы связи (Facebook, Telegram и др.), организуют выступления националистической и антисоциальной направленности за дисбаланс социальной обстановки в Российской Федерации и свержение действующего политического строя;

– широкое распространение таких высоколатентных посягательств, как псевдо-онлайн торговля с предоплатой с использованием электронных платежных систем, телефонное мошенничество с использованием персональных данных пользователей банковских продуктов (фишинг), вымогательство денежных средств за обеспечение сохранности данных, связанное с игровыми и развлекательными порталами, с незаконным контентом;

– постоянное появление новых вирусов, например, новых видов «шифровальщиков», шифрующих сведения из массива информации и впоследствии дающих повод злоумышленникам вымогать денежные средства за их дешифровку;

– усиление организованности хакеров и хакерских групп в связи с расширением сфер криминальных интересов и усложнением применяемых преступных схем;

– транснационализация наркопреступности;

– рост числа специализаций лиц, совершающих киберпреступления (хакеров, фрикеров, крэкеров, вирмейкеров, скиммеров и т.п.).

В краткосрочной перспективе прогнозируется:

– рост числа киберпреступлений в целом;

– рост кибератак на государственные сайты и правительственную инфраструктуру в целях дестабилизации общественно-политической обстановки в РФ;

– появление преступлений, совершаемых с технологиями использования искусственного интеллекта;

– увеличение вирусного программного обеспечения для мобильных приложений, способных перехватить информацию ограниченного доступа, вводимую, в том числе, в банковские программы;

– активное распространение вирусов, которые используют уязвимые компьютерные системы, компоненты компьютеров и серверов, в связи с широким применением устаревшего и не поддерживаемого производителем программного обеспечения;

– распространение программ-паразитов (майнеров), незаметно работающих на любых устройствах и использующих их мощности для майнинга криптовалют;

– увеличение количества преступлений, связанных с незаконным распространением персональных данных лиц, содержащихся в базах данных коммерческих организаций;

– ввиду незаконной деятельности хакерских групп значителен риск утечки биометрических данных граждан, накапливаемых в информационных системах финансовых, правоохранительных, миграционных и иных организаций, чья деятельность связана с использованием подобной информации.

Таким образом, анализ состояния преступности, ее тенденций и прогностических оценок свидетельствует, что сегодня она представляет собой качественно новый феномен как по своим масштабам, так и по степени негативного влияния на всю жизнедеятельность общества, на обеспечение надежной защиты прав и законных интересов граждан. Поэтому все более актуализируется задача усиления противодействия всего общества этому негативному явлению, использования в целях решительного перелома криминальной ситуации сложного комплекса экономических, социально-политических, воспитательных, правоохранительных мер.

Следует отметить, что криминологическое прогнозирование предшествует составлению перспективного плана по противодействию преступности.

Прогнозируется и сам процесс выполнения плана, ожидаемые результаты. Криминологическое планирование представляет собой элемент социального управления, выражающийся в определении субъектов и объектов предупреждения преступности, поиске наиболее эффективных средств и методов противодействия криминальной среде.

Комплексный план по предупреждению и противодействию преступности представляет собой управленческий документ, который должен содержать следующие элементы:

– обоснование проблемы, объяснения необходимости ее разрешения, расчет необходимых затрат;

– количественные и качественные характеристики преступности, отражать общественную опасность и распространенность тех или иных социально-негативных явлений;

– ожидаемые результаты, планируемые изменения в криминогенной обстановке;

– перечень мероприятий, направленный на минимизацию преступности и ее последствий;

– сроки реализации плана и его отдельных мероприятий;

– перечень исполнителей и лиц, осуществляющих контрольные функции;

– материальное и ресурсное обеспечение плана, последствия неисполнения намеченных мероприятий, порядок взаимодействия исполнителей и координации их деятельности.

Приказом МВД России от 1 октября 2020 г. №683 «Об организации планирования в органах внутренних дел Российской Федерации».[1] Данный документ определяет порядок планирования в ОВД РФ, процедуру анализа выполненных мероприятий, виды планов и требования, предъявляемые к ним.

[1] Приказ МВД России от 1 октября 2020 г. №683 «Об организации планирования в органах внутренних дел Российской Федерации». – URL: https://base.garant.ru/74749404 (дата обращения: 21.04.2022).

Такие планы должны соответствовать действующему законодательству, содержать обоснованные и актуальные мероприятия, предусматривать равномерное распределение нагрузки между исполнителями (заинтересованными лицами и подразделениями), обеспечивать ритмичность выполнения запланированных мероприятий, отражать целесообразность выбранных форм и методов достижения поставленных целей.

Исходя из изложенного следует, что криминологическое прогнозирование и планирование играет важную роль в предупреждении преступности, так как они призваны приводить к совершенствованию систему предупреждения преступности, выработке эффективных мер, направленных на предотвращение, пресечение, упреждение преступлений и административных правонарушений.

§3. Деятельность органов внутренних дел по минимизации, выявлению и пресечению преступлений

Ключевым направлением деятельности всех без исключения правоохранительных органов, в частности и органов внутренних дел, состоит в минимизации преступно деятельности.

Минимизация преступности представляет собой комплекс взаимосвязанных мероприятий, направленных на выявление, ослабление и нейтрализацию причин и условий преступности, ее отдельных видов, а также на удержание от перехода или возврата на преступный путь лиц с асоциальным (противоправным) прошлым или настоящим.

Нейтрализация преступлений установлена как в нормативно-правовых актах федерального уровня, так и в локальных актах отдельных специализированных субъектов. К таким органам относятся: Совет Безопасности РФ, Правительственная комиссия по профилактике правонарушений, суды, прокуратура, органы внутренних дел, Федеральная служба безопасности, таможенная, налоговая службы и иные правоохранительные органы.

Объектами рассматриваемой деятельности выступают физические лица, в отношении которых существует необходимость по установлению контроля и надзора стороны правоохранительных органов, к такой категории относятся: несовершеннолетние из неблагополучных семей, лица, освободившиеся из мест лишения свободы, потенциально склонных к совершению преступления и множество других категорий.

Центральным субъектом борьбы с преступностью остаются органы внутренних дел. К их компетенции относится широкий круг задач и обязанностей в рамках предупреждения, пресечения и предотвращения преступлений.

Для эффективной минимизации преступных проявления органы внутренних дел должны быть ориентированы единовременно на различные направления, среди которых: профилактика правонарушений, выявление и своевременное предотвращение и пресечение преступлений.

Предотвращение преступлений - деятельность правоохранительных органов, направленная на недопущение совершения преступлений на этапе их замысла и подготовки.

Пресечение преступлений - направлено на недопущение окончания преступного деяния, то есть предупреждение общественно опасных последствий совершаемого преступления. Другими словами, пресечение осуществляется преимущественно на стадии покушения или подготовки к тяжкому и особо тяжкому преступлению.

Задачи органов внутренних дел, направленные на минимизацию правонарушения состоят в:

1. Устранении причин и условий, способствующих совершению преступлений и других форм противоправной деятельности;

2. Создание механизма эффективного и быстрого реагирования на угрозы нарушения правовых норм;

3. Возмещение причиненного ущерба неправомерными действиями физических и юридических лиц.

Основные функции по снижению числа преступлений, совершаемых на территории Российской Федерации, возлагаются непосредственно на территориальные органы внутренних дел. Для устранения причин и условий развития преступности производится большая аналитическая работа, включающая детальное изучение особенностей совершения преступлений на конкретной территории, это позволяет профилактировать большое количество лиц, обладающих преступным умыслом, выявлять готовящиеся преступления и успешно предотвращать начатые деяния.

Среди аналитических мер можно выделить:

1. Подготовку ежемесячных обзоров криминологической обстановки;

2. Осуществление оценки по результатам предыдущей профилактической деятельности, а также предотвращенным преступлениям;

3. Осуществление оценки эффективности взаимодействие с соответствующими государственными, муниципальными органами, ведомствами, учреждениями, организациями, общественными объединениями.

Каждому подразделению органов внутренних дел отведен собственный перечень функций, исполнение которых должно приводить к снижению уровня преступности.

Так, участковые уполномоченные полиции выявляют и устраняют причины и условия преступлений на закрепленном за ними административном участке, проводят повседневную воспитательно-профилактическую работу с лицами, поведение которых указывает на возможность совершения преступлений. Осуществляют административный надзор за лицами, освобожденными из мест лишения свободы.

Так же к наиболее важным направлениям относится и профилактическая работа среди несовершеннолетних и их семей, которую проводят сотрудники подразделений по делам несовершеннолетних.

Важнейшая роль отводиться и подразделениям уголовного розыска. Сотрудники этой службы проводят оперативно-розыскные мероприятия, позволяющие не только установить преступный замысел на первоначальном

этапе его формирования, но и беспрерывно получать информацию из преступной среды.

Основу нейтрализации, прежде всего, составляет профилактическая деятельность, подразделяющаяся на два вида:

1) общая профилактика - направлена на выявление ликвидацию причин и условий, способствующих совершение преступлений;

2) специальная профилактика - это система мер, воздействующая на отдельные группы преступлений (например, на женскую преступность, преступность несовершеннолетних, против собственности, против общественного порядка.

Для систематической борьбы с преступностью органы внутренних дел проводят различные мероприятия, среди которых «Арсенал», «Мак», «Притон», «Алкоголь», «Подросток» и др.

Отметим, что в современных условиях противодействие преступности должно сочетаться с наиболее современными методами и способами. На сегодняшний день, в связи с трансформацией преступности, которая детерминирована развитием информационно-телекоммуникационных технологий, возникают определённые трудности в выявлении, пресечении, раскрытии и расследовании отдельных видов преступлений, в том числе совершенных в ИТКС Интернет. Основной трудностью, в частности, выступает возможность анонимизации личности злоумышленников в ИТКС Интернет путём прикладного применения специального программного обеспечения.

Согласно словарю С.И. Ожегова: «анонимным называется что-либо без указания имени того, кто пишет, сообщает о чём-нибудь без подписи».[1] Определение, данное С.И. Ожеговым можно также спроецировать и на современные реалии, однако с учётом некоторых особенностей.

Под анонимностью в ИТКС Интернет подразумевается использование специальных технических и программных способов, маскирующих интернет-

[1] Толкование и значение слова "анонимный". - URL: https://ozhegov.textologia.ru/definit/anonimniy/ (дата обращения: 15.04.2022).

трафик и адрес технических средств в ИТКС Интернет. Как правило, сокрытие соединений производится путём подключения через 2, 3, 5 и более IP-адресов по всему миру. Этот факт значительно затрудняет, а иногда делает невозможным установление реального IP-адреса злоумышленников.

Следует отметить, что одним из наиболее распространенных и эффективных программных средств, маскирующих сетевые пакеты обращения злоумышленников к доменам ИТКС Интернет является сеть TOR.

Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов на уровне onion-маршрутизаторов, что обеспечивает маскировку исходящих соединений, а также защиту анализа трафика, обеспечивая практически полную конфиденциальность действий в ИТКС Интернет. Помимо этого, сеть TOR позволяет маскировать IP-адреса путём пропуска трафика пользователя через прокси-сервер на своей машине, обращаемого к серверам TOR, периодически образуя сетевую цепь с многоуровневым шифрованием исходящих пакетов. Каждый такой пакет данных проходит через три различных прокси-сервера – сетевые узлы, которые определяются случайным образом.

Перед отправлением пакет последовательно шифруется тремя ключами: сначала - для третьего сетевого узла, потом - для второго и в конце - для первого. Когда первый узел получает пакет, он расшифровывает первый уровень шифруемой информации и направляет сетевые пакеты на следующие прокси-сервера. Второй и третий сервер поступают аналогичным образом. Указанные прокси-серверы работают на SOCKS-интерфейсе, что позволяет использовать для подключения к сети TOR программные продукты, основанные на том же принципе работы. К данному виду программного обеспечения можно отнести, например, браузер DuckDuckGO.

Следует отметить, что повышенный криминогенный интерес к сети TOR обусловлен тем, что в ней реализуются оружие, наркотические средства, детская порнография, поддельные денежные средства, краденое имущество и иные виды вещей, оборот которых ограничен либо запрещен на территории Российской

Федерации. Расчеты по сделкам в ней производится при помощи цифровых финансовых активов в виде криптовалюты, которая позволяет сторонам сделок оставаться анонимными.

Под криптовалютой следует понимать цифровую валюту, учёт внутренних расчётов которой производит автономная децентрализованная платёжная система, основанная на системе криптографического шифрования. Сама по себе криптовалюта не имеет какой-либо материально выраженной формы. По факту, она представляет собой число, обозначающих количество данных расчётных единиц, который записывается в соответствующие позиции протокола передачи данных. При этом на криптографических методах шифрования основана проверка полномочий на операции с адресом, сам механизм образования адреса, а также формирование пакета транзакции и его взаимосвязь с другими пакетами.

Для большей надежности злоумышленники работают с сетью TOR через соединения VPN, шифрующие интернет-трафик с использованием модемов, анонимных sim-карт и других средств анонимизации личности. Помимо этого, для сокрытия деятельности в сети, наиболее продвинутые злоумышленники, посредством сканирования и использования уязвимостей посредством загрузки на технические средства жертвы эксплойтов при помощи специализированного ПО в ИТКС Интернет, также используют удалённое рабочее место через виртуальную машину (Рис.3.1).

Клиент – Double VPN – Удаленное рабочее место + Виртуальная машина – VPN – Жертва

Рис.3.1 Схема анонимизации действий злоумышленников в сети

При использовании указанной схемы установить личность злоумышленников путем направления запросов интернет-провайдерам и интернет-сервисам практически не представляется возможным, поскольку ответы, получаемые по международным каналам, направляются достаточно продолжительное время. В связи с этим получение компьютерной информации

путем последовательной отправки запросов владельцам серверов, через которые проходил трафик злоумышленника, не дает результатов.

При этом особую тревогу вызывают хищения денежных средств с банковских карт, совершённые с использованием автоматизированных агрегаторов фишинговых сайтов. В настоящее время в сети ИТКС Интернет, в частности на форумах преступной направленности, а также в мессенджере «Telegram», функционируют организованные преступные группы, нацеленные на кражу денежных средств с банковских карт граждан. Участники преступных групп делятся на 4 категории: организаторы; операторы, отвечающие за списание денежных средств с карт потерпевших; технические работники (программисты) и лица, непосредственно контактирующие с жертвой, в преступной среде именуемые как «воркеры».

Сложность раскрытия и расследования данной категории преступлений заключается в том, что вышеуказанные лица работают по чётко налаженной и автоматизированной системе взаимодействия. Организаторы осуществляют набор участников преступной группы посредством анонимных Telegram-чатов и взаимодействуют с «воркерами» через Telegram-ботов. Telegram-боты представляют собой административную панель, посредством которой «воркер» создаёт ссылки на фишинговые сайты с идентичными данными реального объявления, заранее размещенного злоумышленником на досках объявлений. Данные фишинговые сайты интегрируются с Telegram-ботом и, как правило, защищены системами «DDOS Protection», предназначенными в первую очередь для сокрытия реального IP-адреса сервера. После предоставления ссылки на фишинговый ресурс, «воркер» предлагает потерпевшему либо оплатить, либо получить денежные средства за товар перед отправкой. При переходе на форму оплаты потерпевший вводить данные банковской карты, которые моментально попадают «оператору». Тем временем «оператор» вводит полученные данной банковской карты в платежную форму и ожидает 3D-Secure кода подтверждения списания денежных средств. Поскольку форма оплаты внешне выглядит как форма получения денежных средств, потерпевший вводит код для

подтверждения операции в окно мошеннического веб-сайта. «Оператор» ретранслирует данный код и производит списание денежных средств. После успешного осуществления мошеннических действий, на аккаунте в Telegram-боте «воркера» увеличивается баланс денежных средств в размере заранее обозначенного процента от суммы, полученной организатором. Вывести денежные средства возможно исключительно в криптовалюте через Telegram-ботов P2P-обменников, что затрудняет получение дальнейшее информации и установление причинно-следственной связи между лицом, контактировавшим с потерпевшим и движением похищенных денежных средств с банковской карты.

Таким образом, хищение денежных средств с банковских карт, совершенное с использованием автоматизированных агрегаторов фишинговых сайтов, на данном этапе представляется наиболее общественно опасным. В связи с этим актуализируется проблема расследования подобного рода деяний, что обусловлено, с одной стороны отсутствием современной методической базы исследования этого вида деяний, недостаточными знаниями IT-технологий, изменением способов совершения преступлений и т.д.

Вышеуказанные обстоятельства требуют международного взаимодействия не только на уровне правоохранительных органов и интернет-провайдеров, но и операторов сотовой связи. Наиболее перспективным решением указанной проблемы, по мнению авторов, является создание общей автоматизированной информационной системы с информационными базами данных, в которых будет храниться контактная информация пользователей телефонных номеров, IP-адресов и иной информации сетевого взаимодействия, а также искусственного интеллекта, при обращении к которому по специализированному запросу предоставлялась информация, содержащаяся в базах данных на закрытом сервере с современными мерами защиты информации. Указанная система, позволила бы в считанные минуты деанонимизировать злоумышленников в ИТКС Интернет, однако на сегодняшний день, в связи с происходящими в мире событиями и высокой стоимостью, это не представляется возможным. В связи

этим возникает потребность в иных способах идентификации лиц, совершивших общественно опасные деяния посредством ИТКС Интернет.

По мнению автора, одним из таких способов выступает использование специализированного программного обеспечения удалённого доступа к техническим средствам злоумышленников в рамках оперативно-технических мероприятий для решения проблемы идентификации лиц, подготавливающих, совершающих или совершивших общественно опасное деяние посредством использования ИТКС Интернет. Одним из таких способов выступает применение вредоносного программного обеспечения (далее – вредоносное ПО), позволяющих предоставлять доступ к информации, хранящейся на персональных компьютерах и иных технических средствах, используемых киберпреступниками в противоправных целях.

Под вредоносным ПО следует понимать программный код, внедряемый на технические устройства жертвы для кражи паролей, получения доступа к файловой система, причинения вреда либо изменения системных файлов. Данный способ проникновения значим тем, что при комплексном использовании в совокупности с иными программными средствами он позволяет полностью исключить возможность обнаружения действий на технических средствах жертвы, что, в результате, позволит тайно и негласно получить всю представляющую интерес информацию, в частности, о личности жертвы, его контактных данных, текущем местоположении и т.д. Наиболее распространенными вирусами удалённого доступа к системе жертвы являются трояны и бэкдоры. Рассмотрим подробнее их функциональные характеристики.

Одним из наиболее распространенных видов вредоносного программного обеспечения является бэкдор-вирус Glupteba-AFJK, являющийся подвидом трояна Glupteba. Данный вирус по своей сути до недавнего времени являлся вирусом-вымогателем, пока не был переделан и модернизирован в бэкдор, позволяющий получить доступ к компьютерной системе в целях проникновения либо внедрения иного вредоносного ПО. Помимо этого, в пример также следует привести разработанный иранской киберпреступной группировкой Charming

Kitten бэкдор PowerLess, разработанный на основе PowerShell-бэкдора, предназначенный для кибершпионажа путём загрузки в систему через расширяемое средство автоматизации.[1] Новый бэкдор PowerLess способен загружать и выполнять дополнительные модули, такие как инфостилеры и кейлоггеры, позволяющие завладеть учетными данными, данными браузера и финансовой информацией пользователя клиентской машины.

Особенность применения бэкдоров заключается в том, что их зачастую невозможно обнаружить в системе. Это обусловлено тем, что бэкдоры, при их внедрении в систему, автоматически перемещаются в автозагрузку. Из этого следует, что суть работы бэкдоров заключается в том, что они, проникая в систему, маскируются под исполняемые системные файлы, как, например, файл CL.exe, который является средством управления Microsoft C++. Из этого следует, что практически все бэкдоры являются резидентными, то есть активными во время работоспособности системы либо в момент работы какого-либо программного обеспечения. Указанное свойство даёт возможность самовоспроизводится вредоносному ПО с каждой перезагрузкой системы, что обусловлено внесением изменений в значениях регистров. При этом основной целью бэкдоров является создание уязвимостей путём встраивания дефектов в алгоритмы работы системы, чтобы внедрить на клиентскую машину другие типы вредоносного ПО. К подобным вредоносным программам относятся руткиты, key-логгеры и другие типы вирусов, позволяющие получить доступ к данным, хранящимся на технических средствах, а также к их операционной системе и подключенным средствам ввода и вывода.

Таким образом, использование вредоносного ПО для обеспечения расследования по уголовным делам позволит получить данные по идентификации лиц, представляющих оперативный интерес, путём установки MAC-адреса клиентской машины, получения биометрических данных

[1] Иранские хакеры Charming Kitten используют новый PowerShell-бэкдор в целях кибершпионажа. - URL: https://www.securitylab.ru/news/529389.php (дата обращения: 15.04.2022).

посредством удаленного подключения к web-камерам, микрофону, а также фиксации иной представляющей интерес информации через систему ввода и вывода на технических средствах.

Следует отметить, что применение бэкдор-атак предполагает ограничения прав и свобод граждан. Использование вредоносного программного обеспечения влечет за собой ответственность в соответствии с действующим российским законодательством, что противоречит принципам и целям ОРД. Однако, если разобраться в дефиниции статьи 138.1 УК РФ, а также в иных нормативно-правовых актах, регулирующих применение оперативными подразделениями средств, изъятых из гражданского оборота, мы увидим, что использование предлагаемого программного решения возможно в качестве специального техничемкого средства, предназначенного для негласного съема информации.

Так, ст. 138.1 УК РФ предусматривается ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.[1] В соответствии с п.7 Постановлением Пленума Верховного Суда Российской Федерации от 25 августа 2018 года №46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина» (далее – ППВС РФ), уголовная ответственность возникает в случае, если специальные технические средства были использованы с нарушением норм действующего законодательства, к которым, в частности, относятся нормы Федерального Закона от 12 августа 1994 года №144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ №144). [2]

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (принят ГД ФС РФ 24.05.1996 г.) (ред. от 11.06.2021 г.) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

[2] Постановление Пленума Верховного Суда Российской Федерации от 25.08.2018 №46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)». - URL: http://www.consultant.ru/document/cons_doc_LAW_314616/ (дата обращения: 15.04.2022).

ФЗ №144 регламентирует вопросы применения специальных технических средств, предназначенных для негласного получения информации (оперативной техники).[1] Согласно ст. 6 ФЗ №144 оперативным подразделениям разрешается «использовать в ходе проведения оперативно-розыскных мероприятий информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде».

В соответствии со ст.8 ФЗ №144, применение оперативно-розыскных мероприятий, ограничивающих конституционные права и свободы человека и гражданина, допускаются на основании судебного решения при наличии информации о признаках состава преступления, по которому производство предварительного следствия обязательно, либо о лицах, подготоваливающих, совершающих или совершивших подобного рода деяния, а равно о событиях и деяниях, создающих угрозу военной, экономической, государственной, информационной либо экологической безопасности России.

Таким образом, при соблюдении всех правил, предусмотренных законодателем в ФЗ №144, а также при наличии соответствующего судебного решения, оперативным подразделениям разрешается применение специальных технических средств для негласного получения компьютерной информации. Исходя из этого следует, что применение вредоносного ПО в рамках оперативно-розыскной деятельности возможно.

Помимо этого, для оказания комплексного воздействия на киберпреступность, также необходимо:

1. Разработать, апробировать и распространить по всем структурным подразделениям методические рекомендации по выявлению, пресечению, расследованию и раскрытию хищений денежных средств с электронных платежных карт, совершённых с использованием автоматизированных

[1] Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 №144-ФЗ (последняя редакция). - URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 15.04.2022).

агрегаторов фишинговых сайтов, с подробным описанием взаимодействия органов предварительного расследования с оперативными подразделениями и иными участниками производства по делу;

2. Повысить уровень взаимодействия правоохранительных органов и банковских организаций (служб безопасности) в целях создания общих комплексных мер профилактики хищений денежных средств с банковских карт;

3. Разработать перечень организаций, оказывающих услуги по перенаправлению интернет-трафика с целью пользователем смены IP-адреса и направить их подразделения органов внутренних дел;

4. Аналогично требованиям, изложенным в ч. 4 ст. 13 ФЗ «О полиции» установить срок исполнения запроса государственных органов для организаций, осуществляющих деятельность в сфере предоставления услуг связи, услуг по размещению информации и прочую деятельность, входящую в класс ОКВЭД № 64, а также уменьшить срок для организаций, осуществляющих деятельность по приему платежей физических лиц платежными агентами (код ОКВЭД 66.19.62) до 5 дней;

5. Увеличить размер штрафа, предусмотренного ст. 19.7 КоАП РФ, до пяти тысяч рублей – на должностных лиц, до пятидесяти тысяч рублей – на юридических лиц.

Подводя итог, следует отметить, что в специальной литературе слабо отражены вопросы об использовании специальных технических средств и возможностей при раскрытии преступлений, совершенных с использованием ИТКС Интернет. Изменение злоумышленниками IP-адресов, MAC-адресов клиентских машин, а также использование иных способов анонимизации в сети сводит поиск указанных лиц практически к минимуму, что в итоге может привести к негативным социально-экономическим последствиям. Реализация вышеуказанных мер, а также разработка и внесение соответствующих изменений в законодательство Российской Федерации окажет положительное влияние на эффективность деятельности правоохранительных органов по расследованию преступлений, совершённых с использованием ИТКС Интернет.

Исходя из вышеизложенного следует, что органы внутренних дел занимают ведущее место в системе субъектов, на которые возложены функции по минимизации, выявлению, предупреждению и пресечению преступлений. Такая деятельность предполагает последовательную реализацию мер политического, экономического, нравственного, воспитательного, правового характера и будет способствовать ликвидации криминогенных факторов, стабилизации оперативной обстановки, своевременному реагированию на противоправные (асоциальные) поступки и нарушения общественного порядка.

Именно поэтому для эффективной деятельности в данном направлении, необходимо не только сочетать методы воздействия на преступные элементы, но и осуществлять тесное взаимодействие правоохранительных, государственных, муниципальных органов, а также отдельных лиц.

ЗАКЛЮЧЕНИЕ

Подводя итог, необходимо отметить, что поставленные нами задачи были разрешены в ходе исследования, а главная цель работы – успешно достигнута. Так, мы пришли к следующим выводам.

Одной из задач теоретической части исследования являлось изучение сущности преступности как социально-негативного явления. В рамках указанной задачи были выявлены основные признаки данного явления, его формы, количественные и качественные характеристики, дано определение. В ходе исследования установлено, что преступность представляет собой негативную девиацию, деструктивную, исторически изменчивую социальную систему, которая обладает определённой совокупностью присущих ей существенных признаков, позволяющих отграничивать ее от иных социальных явлений, детерминируемую определённой совокупностью причин и условий и, в некоторых случаях, носящую латентный характер.

Согласно поставленной задаче, было рассмотрено современное состояние преступности, спрогнозированы тенденции по развитию отдельных видов её проявлений к 2023-2024 годам. Отмечается увеличение преступлений, совершённых с использованием информационно-телекоммуникационных технологий, а также качественное изменение организованной, коррупционной и других форм преступности. В частности, на основании результатов анкетирования сотрудников Центра по противодействию экстремизму МВД по Республике Татарстан, а также анализа состояния преступности, за последние 5 лет прослеживается качественное изменение преступлений экстремистской и террористической направленности, которое выражается в их интеграции в ИТКС Интернет и смешивании деструктивных идеологий.

В ходе анализа отечественных технологий по противодействию и профилактике установлено, что деятельность субъектов профилактики по предупреждению преступлений и административных правонарушений является одним из ведущих криминологически значимых направлений, состоящем в

воздействии на детерминанты преступности, провоцирующие и способствующие совершению и распространению антисоциальных явлений.

В ходе анализа существующих концепций по борьбе с киберпреступлениями выявлены эффективные практики противодействия, реализуемые как на государственном уровне и уровне профессиональных объединений, так и на уровне отдельных субъектов противодействия. Исследование специфики способов совершения киберпреступлений позволяет сформулировать следующие предложения для совершенствования практик противодействия IT-преступлениям.

Направления совершенствования системы противодействия киберпреступлениям в России:

1) совершенствование нормативно-правовой базы:

– установление срока исполнения запроса государственных органов для организаций, осуществляющих деятельность в сфере предоставления услуг связи, услуг по размещению информации и прочую деятельность, входящую в класс ОКВЭД № 64, аналогично требованиям, изложенным в ч. 4 ст. 13 ФЗ «О полиции».

– уменьшение срока исполнения запроса государственных органов для организаций, осуществляющих деятельность по приему платежей физических лиц платежными агентами (код ОКВЭД 66.19.62) до 5 дней, аналогично требованиям, изложенным в ч. 4 ст. 13 ФЗ «О полиции».

– увеличение размера штрафа, предусмотренного ст. 19.7 КоАП РФ, до пяти тысяч рублей – на должностных лиц, до пятидесяти тысяч рублей – на юридических лиц.

2) повышение уровня взаимодействия правоохранительных органов с иными субъектами профилактики:

– сокращение дистанции между правоохранительными органами и молодёжными общественными организациями в Республике Татарстан с последующим их включением в профилактическую деятельность.

– повышение уровня взаимодействия правоохранительных органов и банковских организаций (служб безопасности) в целях создания общих комплексных мер профилактики мошенничества, хищений денежных средств с банковских карт и иных форм киберпреступлений в рамках межведомственных рабочих групп.

3) интеграция вредоносного ПО в деятельность оперативных подразделений в рамках производства оперативно-технических мероприятий, необходимого для установления личности злоумышленников.

4) подготовка организационных мероприятий:

– разработка новой системы профессионального образовательного процесса, направленного на обучение будущих специалистов правоохранительных органов и повышение квалификации действующего сотрудников способам, методам, приемам и формам выявления, раскрытия и расследования преступлений, совершаемых в сфере цифровых технологий путём внесения изменений в федеральные государственные образовательные стандарты.

– внесение изменений в учебные программы подготовки и повышения квалификации сотрудников правоохранительных органов путём внедрения учебных дисциплин по разведке данных в открытых источниках, анализу и практическому применению вредоносного ПО, разработке программного обеспечения.

– разработка методических рекомендаций по противодействию киберпреступности.

– повышение уровня технической оснащенности правоохранительных органов новейшими технологиями цифрового мира.

– пропаганда и обучение граждан основам цифрового права, противодействия мошенничеству.

Основой реализации указанных направлений совершенствования системы противодействия киберпреступлениям и новым формам преступности является

внесение законодательных изменений, а также обеспечение комплексного подхода в предупредительной деятельности путём:

– взаимодействие и активизация государственных органов и общественных организаций в сфере предупреждения цифровой преступности.

– использование форм и методов предупреждения цифровой преступности, основанных на результатах научных исследований и внедренных в практическую деятельность правоохранительных органов.

– разработка и реализация федеральных и региональных программ предупреждения цифровой преступности.

Помимо этого для оценки общественно-политической обстановки в Республике Татарстан автором было разработано и внедрено в деятельность Совета Безопасности Республики Татарстан специализированное программное средство мониторинга социальных сетей «Anancy» (далее-СПО «Anancy»), предназначенное для анализа участников деструктивных групп экстремистской и террористической направленности в социальной сети «Вконтакте» с фильтрацией результата поиска по заданному региону (Республика Татарстан). Выборка групп осуществляется путём проведения специализированных экспертиз Автономной некоммерческой организацией «Казанский межрегиональный центр экспертиз», в их число входят праворадикальные, леворадикальные, псевдоисламистские, суицидальные и иные сообщества деструктивной направленности. Результаты исследованы, апробированы, акт внедрения прилагается.

Подводя итог необходимо отметить, что для минимизации киберпреступлений в России важен комплексный подход, основанный на взаимодействии всех субъектов профилактической деятельности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята на всенародном голосовании 12 декабря 1993 г., с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // Собрание Законодательства РФ. – 2014. – № 31. – Ст. 4398.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (принят ГД ФС РФ 20.12.2001 г.) (ред. от 25.03.2022 г.) // Собрание законодательства РФ. – 07.01.2002. - № 1. – Ст. 1.
3. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (принят ГД ФС РФ 24.05.1996 г.) (ред. от 11.06.2021 г.) // Собрание законодательства РФ. – 17.06.1996. - № 25. – Ст. 2954.
4. Федеральный закон от 08.01.1998 г. № 3-ФЗ (ред. от 08.12.2020 г.) «О наркотических средствах и психотропных веществах» // Собрание законодательства РФ. – 11.01.1998. – № 2. – Ст. 219.
5. Федеральный закон от 12.08.1995 (ред. от 01.04.2022 г.) №144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. – 14.08.1995. – № 33. – Ст. 3349.
6. Федеральный закон от 23.06.2016 №182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ. – 27.06.2016. – № 26 (ч.1). – Ст. 3851.
7. Указ Президента РФ от 29.05.2020 №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. – 01.06.2020. – № 22. – Ст. 3475.
8. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. Режим доступа: https://base.garant.ru/71556224/ (дата обращения: 20.03.2022).

9. Указ Президента РФ от 23.11.2020 №733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_368501/ (дата обращения: 20.03.2022).
10. Указ президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 20.03.2022).
11. Уголовный кодекс РСФСР от 27 октября 1960 г. [Электронный ресурс]. Режим доступа: https://base.garant.ru/3983897/055d1b82a84145ca60b96f2b0fee8ae8 (дата обращения: 20.03.2022).

II. Монографии, учебники, учебные пособия

1. Аванесов Г.А., Иншаков С.М., Аминов Д.И., Эриашвили Н.Д. Криминология: учебник / Под ред. Г.А. Аванесова. – М.: ЮНИТИ-ДАНА, 2017. – 576 с.
2. Антонян Ю.М. Криминология: учебник для академического бакалавриата. – М.: Юрайт, 2019. – 388 с.
3. Демидов В.Н., Сафиуллин Н.Х. Криминологическое прогнозирование: современное состояние и перспективы: учеб. пособие. - Казань: КЮИ МВД России, 2000. - 90 с.
4. Жданов Ю.Н., Кузнецов С.К., Овчинский В.С. COVID-19: преступность, кибербезопасность, общество, полиция. М.: Международные отношения. – 2020. – 447 с.
5. Иншаков С.М. Криминология: практикум: учебное пособие. – М.: ЮнитиДана, 2017. – 432 с.
6. Криминология: учебное пособие для бакалавров и специалистов / под ред. В.Н. Бурлакова, Н.М. Кропачева. – СПб.: Питер, 2020. – 304 с.

7. Криминология. Особенная часть: учебник / Ф.К. Зиннуров [и др.].. – Казань: Казанский юридический институт МВД России, 2016. – 525 с.
8. Криминопенология: учебное пособие / Старков О.В. - М.: Экзамен, 2004. - 480 с.
9. Предупреждение преступлений и административных правонарушений органами внутренних дел: учебное пособие / под общей редакцией Ф.К. Зиннурова. - Казань: КЮИ МВД России, 2022. – 187 с.
10. Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т.В. Пинкевич. Москва: Юрлитформ, 2020. – 392 с.

III. Статьи, научные публикации

1. Азарова И.В. Проблемы противодействия преступлениям террористической направленности, совершаемым на территории России гражданами из стран – участников СНГ // Вестник Воронежского института ФСИН России. – 2018. – № 1. – С. 123 - 130.
2. Актуальные проблемы уголовного права, криминологии и уголовно-исполнительного права. Выпуск 6: научные труды кафедры уголовного права / А.А. Арямов [и др.].. — Москва : Российский государственный университет правосудия, 2017. — 192 с.
3. Акутаев Р.М. Латентная преступность: актуальные проблемы и понятие // Государство и право. – 1997. – № 12. – С.78 - 87.
4. Арапов В.В., Заруцкая Н.А. Почему киберпреступления – угроза национальной безопасности [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti (дата обращения: 15.04.2022).
5. Галуева В.О. Латентная преступность как неотъемлемая составляющая преступности // Общество и право. – 2019. – № 11. – С. 75 – 81.

6. Дегтярева, М.О. Классификация и виды латентной преступности на примере Уральского федерального округа // Молодой ученый. – 2021. – № 5 (347). – С. 177-179.
7. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. – 2018. – №10. – С. 109 - 115.
8. Дремлюга, Р.И. Преступный мир Darknet // Юридическая наука и практика. Владивосток – 2018 – № 1. – С. 52–60.
9. Иранские хакеры Charming Kitten используют новый PowerShell-бэкдор в целях кибершпионажа [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/529389.php (дата обращения: 15.04.2022).
10. Исаев, А.А. История формирования права и тенденция его развития // Молодой ученый. – 2020. – № 49 (339). – С. 240-241 .
11. Итоги исследования: Киберпреступность в России и мире [Электронный ресурс]. Режим доступа: https://rb.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/ (дата обращения: 11.04.2022)
12. Казиев А.З. Проблемы квалификации латентных преступлений // Вестник магистратуры. – 2019. – № 5-5(92). – С. 70-71.
13. Киберпреступность в 2021 году выросла на 25% [Электронный ресурс]. Режим доступа: https://pravo.ru/news/232676/ (дата обращения: 15.04.2022).
14. Конев Д.А. Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: постановка проблемы: автореф. дис. ... канд. юрид. наук. – М., 2020. – 38 с.
15. Криминальный Татарстан: меньше грабежей, больше тяжких преступлений и «кровавый» 2020-й // Сетевое издание «Снег» [Электронный ресурс]. Режим доступа: https://sntat.ru/news/kriminalnyi-tatarstan-mense-grabezei-bolse-tyazkix-prestuplenii-i-krovavyi-2020-i-5832553 (дата обращения: 15.04.2022).
16. Кудрявцев В.Н. Проблемы причинности в криминологии // Вопросы философии. – 1971. – № 10. – С. 50-51.

17. «Лаборатория Касперского» фиксирует рост сложных кибератак на российские компании [Электронный ресурс]. Режим доступа: https://habr.com/ru/news/t/657473/ (дата обращения: 15.04.2022).
18. Мазур А.А. Актуальные проблемы предупреждения преступности в сети Даркнет // Вестник Российского института кооперации. – 2018. – № 3. – С. 125-129.
19. Миронов, Р.В. Darknet как источник получения доказательственной и иной информации при расследовании преступлений // Актуальные вопросы юридических наук: материалы V Междунар. науч. конф. (г. Краснодар, июнь 2019 г.). – Краснодар : Новация, 2019. – С. 38-40.
20. Мухин С.М. Преступления в сети Darknet: краткая характеристика, проблемы противодействия // Альманах молодого исследователя. – 2018. – № 5. – С. 110–114.
21. Обзор: Эксперты выявили скачок числа кибератак на стратегические предприятия РФ [Электронный ресурс]. Режим доступа: https://www.interfax.ru/russia/739380 (дата обращения: 15.04.2022).
22. Овчинский В.С. Как изучать организованную преступность в XXI веке [Электронный ресурс]. Режим доступа: https://izborsk-club.ru/15222 (дата обращения: 15.04.2022).
23. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов// Официальный сайт Центрального Банка России [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения: 15.04.2022).
24. Подросток в Кукморе напал на отдел полиции – его застрелили // Деловая информационная газета «Бизнес Онлайн» [Электронный ресурс]. Режим доступа: https://yandex.ru/turbo/business-gazeta.ru/s/news/486484 (дата обращения: 05.04.2022).
25. Расширенное заседание коллегии МВД России // Официальный сайт Президента России [Электронный ресурс]. Режим доступа:

http://www.kremlin.ru/catalog/persons/310/events/65090 (дата обращения: 12.04.2022).

26. Смольянинов Е.С. Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий // Вестник РГГУ. Серия «Экономика. Управление. Право». – 2021. – № 3 (13). – С. 134–141.
27. Соловьев В.С. Криминологическое исследование экстремистских проявлений в социальных сетях Интернета (по материалам интернет-опроса пользователей) // Юристъ-правоведъ. – 2019. – № 5. – С.63-69.
28. Состояние преступности в России за январь-декабрь 2021 г.// Основные статистические данные ГИАЦ МВД РФ [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/28021552/ (дата обращения: 12.04.2022).
29. Статистические данные Генеральной прокуратуры РФ за 2021 г./ Официальный сайт Генеральной прокуратуры РФ [Электронный ресурс]. Режим доступа: http://genproc.gov.ru/ (дата обращения: 12.04.2022).
30. Толкование и значение слова "анонимный" [Электронный ресурс]. Режим доступа: https://ozhegov.textologia.ru/definit/anonimniy/ (дата обращения: 15.04.2022).
31. Черноусов М.М. Исследование латентной преступности: теоретические и практические аспекты [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/issledovanie-latentnoy-prestupnosti-teoreticheskie-i-prakticheskie-aspekty (дата обращения: 15.04.2022).
32. Шалагин А.Е. Предупреждение социально-негативных явлений, представляющих угрозу здоровью населения и общественной нравственности [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/preduprezhdenie-sotsialno-negativnyh-yavleniy-predstavlyayuschih-ugrozu-zdorovyu-naseleniya-i-obschestvennoy-nravstvennosti (дата обращения: 15.04.2022).

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

IV.Эмпирические материалы

1. Постановление Пленума Верховного Суда Российской Федерации от 25.08.2018 №46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_314616/ (дата обращения: 15.03.2022).
2. Кассационное определение от 7 августа 2012 г. Верховный суд Республики Татарстан [Электронный ресурс]. Режим доступа: https://sudact.ru (Дата обращения:05.04.2022).
3. Дело № 1-311/2016: приговор Ленинского районного суда г. Челябинска № 1-311/2016 от 6 июня 2016 г. [Электронный ресурс]. Режим доступа: https://sudact.ru/regular/doc/Lj3BFNVNdudt/ (дата обращения 18.04.2022).
4. Дело № 1-337/2017: приговор Ялтинского суда Республики Крым и железнодорожного районного суда г. Хабаровска № 1-337/2017 от 17 августа 2017 г. [Электронный ресурс]. Режим доступа: https://sudact.ru/regular/doc/fgchbvws7ExX (дата обращения 18.04.2022).

Приложение 1

Апробация и внедрение в практику результатов исследования

1. Основные положения выпускной квалификационной работы были разработаны при подготовке следующих научно-исследовательских работ:

1. «Методика расследования пропаганды экстремизма» - Всероссийский конкурс научно-исследовательских работ «Закон и правопорядок», 2020 г.

2. «Детерминанты и тенденции преступности в России на современном этапе» - Всероссийский конкурс научно-исследовательских работ «Закон и правопорядок», 2019 г.

3. «Технико-криминалистическое обеспечение расследования преступлений в телекоммуникационной сфере» - конкурс по присуждению Премии Министра внутренних дел Российской Федерации, 2019 г.

2. Основные положения выпускной квалификационной работы были доложены на следующих научно-практических конференциях, круглых столах, лекториях, форумных кампаниях:

1. Технико-криминалистическое обеспечение расследования преступлений с использованием сети Darknet // Всероссийская научно-практическая конференция КЮИ МВД России «Технико-криминалистическое обеспечение расследования и предупреждения преступлений», (КЮИ МВД России, 2019 г.).

2. Проблемные аспекты реализации уголовной политики в области операций с криптовалютой // V Международная научно-практическая конференция «Новеллы права, экономики и управления, 2019» (Гатчина, 22 ноября 2020 г.).

3. Особенности использования технико-криминалистических средств при расследовании преступлений, совершенных с использованием теневой сети Darknet // Международная научно-практическая конференция студентов, магистрантов, аспирантов и молодых учёных «Тенденции развития правовой системы глазами молодёжи» (Саратовская государственная юридическая академия, 23 апреля 2020 г.).

4. К вопросу о применении технологии распределенного реестра (технологии блокчейн) // Всероссийский круглый стол с участием сотрудников отдела «К» и ГСУ МВД по РТ на тему «Дистанционные хищения и кибербезопасность» (КЮИ МВД России, 22 октября 2021 г.).

5. Применение бэкдор-атак в деятельности оперативных подразделений по

противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Всероссийский круглый стол с участием сотрудников отдела «К» и ГСУ МВД по РТ на тему «Дистанционные хищения и кибербезопасность» (КЮИ МВД России, 26 марта 2022 г.).

6. Расследование хищений денежных средств, совершенных с использованием информационно телекоммуникационной сети Интернет // Межведомственный круглый стол «Вопросы взаимодействия правоохранительных органов и подразделений при раскрытии и расследовании преступлений» (Тверской филиал Московского института МВД России им. Кикотя, 6 апреля 2022 г.).

3. Положения выпускной квалификационной работы были опубликованы в следующих научных сборниках:

1. Сборник научных статей по результатам Международной научно-практической конференции «преступность в СНГ: проблемы предупреждения и раскрытия преступлений» – Хамидуллин С.А. «Вопросы реализации уголовной политики при совершении преступлений с использованием цифровых финансовых активов» – с.44-45 (РИНЦ).

2. Сборник научных трудов по результатам V Международного фестиваля Саратовской юридической науки – Хамидуллин С.А. «Особенности использования технико-криминалистических средств при расследовании преступлений, совершенных с использованием теневой сети Darknet» – с.42-43.

3. Сборник трудов Межведомственного круглого стола «Вопросы взаимодействия правоохранительных органов и подразделений при раскрытии и расследовании преступлений» – Лебедева А.В., Кибатов М.А., Хамидуллин С.А. «Расследование хищений денежных средств, совершенных с использованием информационно телекоммуникационной сети Интернет» – с.142-149 (РИНЦ).

4. Положения выпускной квалификационной работы были доложены на следующих круглых столах, лекториях, форумных кампаниях:

1. Основы манипуляций, как не стать жертвой опытных вербовщиков? // Лекция, посвящённая дню солидарности в борьбе с терроризмом (Казанская кадетская школа им. Героя Советского Союза Б.К. Кузнецова, 4 сентября 2020 г., охват 40 человек).

2. Лекторий «Безопасность» // КФУ (КФУ, Институт психологии и образования, 19 октября 2020 г., охват 120 человек).

3. Лекторий «Безопасность», КГЭУ (КГЭУ, 22 октября 2020 г., охват 60 человек).

4. Лекторий «Интернет безопасность» // КФУ (КФУ, Высшая школа информационных

технологий и интеллектуальных систем, 25 ноября 2020 г., охват 60 человек).

5. Внедрение контента. алгоритм и способы // экспертное сопровождение республиканского онлайн-форума «Концепция безопасного интернета» (27 – 29 ноября 2020 г., охват 1500 человек).

6. Свобода мысли и слова // республиканский медиаинтенсив по гражданской журналистике «СпецКор», 4 сентября 2021 г. (охват 20 человек).

7. Особенности проявлений экстремизма в сети Интернет // экспертное сопровождение республиканского онлайн-форума «Концепция безопасного интернета», 25 – 27 ноября 2021 г. (охват 2500 человек).

5. Внедрение в практику результатов исследования:

Автором было разработано и внедрено в деятельность Совета Безопасности Республики Татарстан специализированное программное средство мониторинга социальных сетей «Anancy», предназначенное для анализа участников деструктивных групп экстремистской и террористической направленности в социальной сети «Вконтакте» с фильтрацией результата поиска по заданному региону (Республика Татарстан). Выборка групп осуществляется путём проведения специализированных экспертиз Автономной некоммерческой организацией «Казанский межрегиональный центр экспертиз», в их число входят праворадикальные, леворадикальные, псевдоисламистские, суицидальные и иные сообщества деструктивной направленности. Результаты исследованы, апробированы, акт внедрения прилагается.

Приложение 2

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на проведение социологического исследования для изучения состояния идеологий экстремизма (терроризма) в информационной среде в Республике Татарстан

Цель исследования:
1) Установить наиболее распространенные на сегодняшний день деструктивные идеологии.
2) Выявить качественные изменения деструктивных идеологий на территории Республики Татарстан.
3) Проанализировать актуальные способы вовлечения в деструктивные идеологии.

Задачи исследования:
1) Установить возрастной профиль лиц, подверженных деструктивному влиянию.
2) Выявить наиболее распространенные деструктивные идеологии в ИТКС Интернет.
3) Выявить тенденции по качественному изменению деструктивных идей в ИТКС Интернет.
4) Установить наиболее распространенные информационные ресурсы по вовлечению в деструктивные идеологии.

Целевая аудитория:
- Сотрудники отделения по борьбе с IT-преступлениями Центра по противодействию экстремизму МВД по Республике Татарстан.

Метод исследования:
- Количественное исследование, онлайн опрос.

Выборка:
Генеральная совокупность – сотрудники подразделений МВД России по борьбе с преступлениями экстремистской и террористической направленности РФ.
Выборка – сотрудники отделения по борьбе с IT-преступлениями Центра по противодействию экстремизму МВД по Республике Татарстан.
Метод выборки – выборка типичных случаев (признак – практический опыт).

География:
- Республика Татарстан.

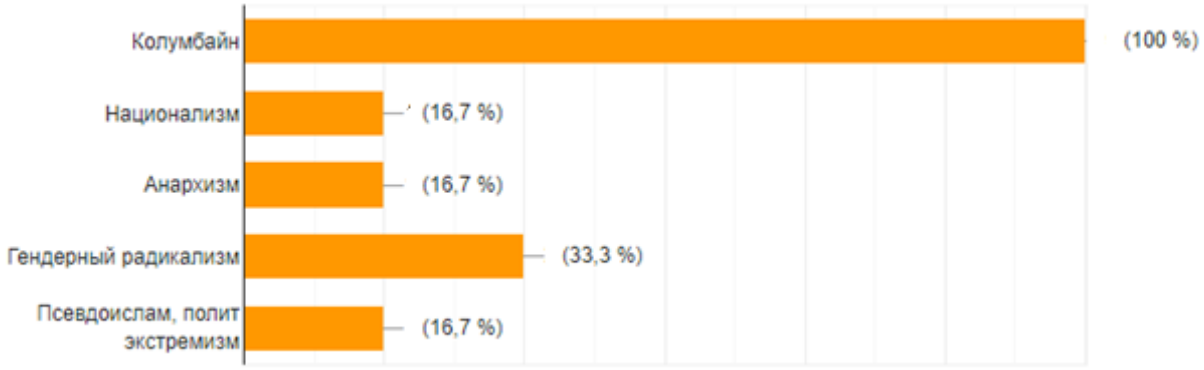
Предоставляемые материалы по результатам исследования:
- Диаграммы в форме приложений к выпускной квалификационной работе.

Сроки исследования:
- Предоставление результатов к 15.03.2022 г.

Приложение 3

Результаты анкетирования сотрудников отделения по борьбе с IT-преступлениями Центра по противодействию экстремизму МВД по Республике Татарстан

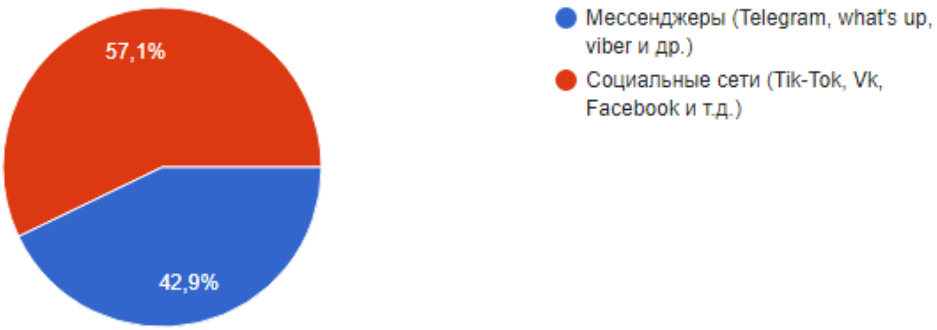
1. Какие деструктивные идеи на сегодняшний день наиболее распространены в сети Интернет?



2. Прослеживаются тенденции по качественному изменению деструктивных идей в сети Интернет? Если да, то какие?

- Да, прослеживаются – 77,5 % респондентов.
- Нет, не прослеживаются – 22,5 репондентов.

3. Посредством каких информационных ресурсов производится вовлечение в деструктивные идеологии?



4. Какие возрастные категории больше всего подвержены деструктивному влиянию?
- От 14 до 18 лет – 65,4 %.
- Лица, старше 18 лет – 34, 6%.

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Казанский юридический институт МВД России

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

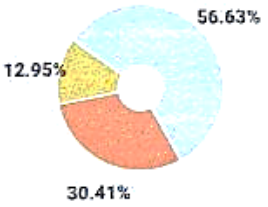
ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Хамидуллин Салават Айратович
Самоцитирование рассчитано для: Хамидуллин Салават Айратович
Название работы: Трансформация преступности на современном этапе и способы её минимизации
Тип работы: Выпускная квалификационная работа
Подразделение: слушатель 5 курса 173 уч. гр. очной формы обучения КЮИ МВД России

РЕЗУЛЬТАТЫ

ЗАИМСТВОВАНИЯ	30.41%
ОРИГИНАЛЬНОСТЬ	56.63%
ЦИТИРОВАНИЯ	12.95%
САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 17.04.2022



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: Шалагин Антон Евгеньевич
ФИО проверяющего

Дата подписи: 17.04.22

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.

ОТЗЫВ

о работе обучающегося 173 учебной группы,
очной формы обучения, 2017 года набора,
по специальности 40.05.01 – Правовое обеспечение национальной безопасности
Хамидуллина Салавата Айратовича
в период подготовки выпускной квалификационной работы
на тему «Трансформация преступности на современном этапе и способы её минимизации»

При выборе темы выпускной квалификационной работы автор проявил заинтересованность и желание разобраться в поставленной проблеме. Актуальность выбранной темы обусловлена тем, что киберпреступность представляет реальную угрозу для экономической, общественной, политической безопасности общества. В соответствии с выбранной темой автор сформулировал цель, задачи, объект и предмет, теоретическую и практическую значимость, методологическую и эмпирическую основы проведенного исследования.

В процессе работы слушателем были рассмотрены понятие, признаки и общественная опасность преступности, проанализированы количественно-качественные характеристики преступности, а также способы оценки латентной преступности. Изучены состояние и основные тенденции преступности в Российской Федерации, спрогнозировано возможное развитие отдельных форм киберпреступности. Предложены меры предупреждения и минимизации преступности на современном этапе. Таким образом, в представленной выпускной квалификационной работе демонстрируется умение формулировать цель и задачи научного исследования, анализировать, обобщать, выявлять, систематизировать научные проблемы и предлагать пути их решения.

Выпускная квалификационная работа состоит из введения, трех глав, объединяющих девять параграфов, заключения, списка использованной литературы, приложений. В первой главе проанализировано понятие преступности, её основные признаки, дано определение латентной

преступности, отражены её виды. Во второй главе исследовано современное состояние преступности в России, а также особенности совершаемых киберпреступлений. В третьей главе проанализированы и обобщены проблемные аспекты противодействия преступлениям в сфере информационно-телекоммуникационных технологий.

В работе использованы современные нормативные, научные, учебные, справочные источники. Изложенный материал подкреплен примерами из следственной и судебной практики. Выводы и предложения, содержащиеся в выпускной квалификационной работе, могут быть использованы в деятельности органов внутренних дел, а также в учебном процессе при освоении дисциплин «Криминология», «Предупреждение преступлений и административных правонарушений органами внутренних дел», «Виктимология».

Следует указать, что основные результаты исследования С.А. Хамидуллина прошли апробацию на: Всероссийском конкурсе научно-исследовательских работ «Закон и правопорядок», конкурсе по присуждению Премии Министра внутренних дел Российской Федерации, научно-практических конференциях «Технико-криминалистическое обеспечение расследования и предупреждения преступлений», «Технико-криминалистическое обеспечение расследования преступлений с использованием сети Darknet», иных научно-представительских мероприятиях «Дистанционные хищения и кибербезопасность», «Деятельность оперативных подразделений по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий». Слушателем были подготовлены научные публикации в журнале Вестник Казанского юридического института МВД России и в иных печатных изданиях РИНЦ.

Оформление выпускной квалификационной работы соответствует предъявляемым требованиям. Оригинальность текста составляет 56%,

цитирование 12,9%. На основании вышеизложенного считаю, что выпускная квалификационная работа Хамидуллина Салавата Айратовича является самостоятельным и логически завершенным исследованием. Заслуживает высокой оценки и может быть рекомендована к публичной защите.

Научный руководитель:

Начальник кафедры криминологии и
уголовно-исполнительного права
Казанского юридического института МВД России
кандидат юридических наук, доцент
полковник полиции _____ А.Е. Шалагин

«17» 05 2022 г.

С отзывом ознакомлен _____ С.А. Хамидуллин

«17» 05 2022 г.

РЕЦЕНЗИЯ

на выпускную квалификационную работу
слушателя 173 учебной группы, очной формы обучения, 2017 года набора, по специальности 40.05.01 – Правовое обеспечение национальной безопасности
Хамидуллина Салавата Айратовича на тему
«Трансформация преступности на современном этапе и способы её минимизации»

Актуальность темы выпускной квалификационной работы не вызывает сомнений, так как в настоящее время информационные технологии повышают уровень латентности преступлений. Преступные деяния, совершенные с использованием информационно-телекоммуникационных технологий, представляют серьёзную общественную опасность, что обусловлено распространением подобного рода общественно опасных проявлений, а также негативными тенденциями трансформации преступности. Тема исследования соответствует её содержанию.

Представленная выпускная квалификационная работа состоит из введения, трех глав, девяти параграфов, заключения, списка использованной литературы. Во введении автор обосновал актуальность проблемы, указал использованные методы, а также теоретическую и практическую значимость. Цель выпускной квалификационной работы определена верно и способствует комплексному рассмотрению поставленной проблемы. Решение поставленных задач прослеживается на протяжении всей выпускной квалификационной работы. Автором использованы различные источники, в том числе специальная, научная литература, судебная практика, а также нормативно-правовые акты, регламентирующие деятельность по противодействию киберпреступлениям.

Заявленная тема раскрыта достаточно полно, цель и задачи соответствуют содержанию работы. Автору удалось выработать свою позицию и аргументировано отстоять её. Сказанное позволяет сделать вывод о том, что теоретический и практический уровень выпускной квалификационной работы соответствует предъявляемым требованиям.

В первой главе «Преступность как социально-негативное явление и ее основные характеристики» проанализировано понятие преступности, её существенные признаки, дано определение латентной преступности, отражены её виды. При изучении данного вопроса автор опирался на точки зрения известных специалистов в области юриспруденции.

Во второй главе «Трансформация преступности на современном этапе» Хамидуллин С.А. приводит статистические данные, указывающие на увеличение количества совершаемых преступлений с использованием современных технологий на территории Российской Федерации. Помимо этого, автор приводит результаты исследования, проведенного 25.01.2022 г. в форме интервьюирования действующих сотрудников отделения по борьбе с IT-преступлениями Центра по противодействию экстремизму МВД по РТ, по результатам которого приходит к выводу о качественной трансформации

деструктивных идеологий, а также их смешении между собой. На основании указанных данных Хамидуллин С.А. приходит к выводу о том, что современные формы преступности находятся в процессе активного видоизменения, что обусловлено интеграцией информационных технологий в преступную деятельность. Также автором выделяются тенденции по качественному изменению отдельных видов преступлений.

В третьей главе «Предупреждение и прогнозирование преступности органами внутренних дел» автор приводит современную систему мер по противодействию киберпреступности, которая подразделяется на три уровня. Им предложены меры по повышению эффективности пресечения и предупреждения преступлений, совершенных с использованием информационно-телекоммуникационных технологий. В заключении изложены основные результаты и выводы выпускной квалификационной работы.

При подготовке работы Хамидуллин С.А. проявил способность к самостоятельному и комплексному изучению научной, специальной литературы, нормативно-правовых актов, а также проведению криминологического исследования. В работе законодательные источники использованы с учетом их последних изменений, приведены выдержки из диссертационных исследований, научной литературы.

Список литературы соответствует библиографическим требованиям. К достоинствам исследования следует отнести грамотный и понятный стиль изложения, глубокое и тщательное изучение исследуемой проблемы.

Представленная выпускная квалификационная работа на тему «Трансформация преступности на современном этапе и способы её минимизации» по форме и содержанию соответствует предъявляемым требованиям и может быть рекомендована к публичной защите.

Рецензент:
Начальник отдела «К» МВД по Республике Татарстан
майор полиции Афанасьев А.И.

«16» 05 2022 г.

С рецензией ознакомлен _____ Хамидуллин С.А.
подпись

«16» 05 2022 г.

Кафедра криминологии и уголовно-исполнительного права

УТВЕРЖДАЮ
Начальник кафедры
криминологии и уголовно-
исполнительного права,
кандидат юридических наук,
доцент
полковник полиции
_____ Шалагин А. Е.
«15» 06 2021 г.

ПЛАН-ГРАФИК

выполнения выпускной квалификационной работы

Тема: Трансформация преступности на современном этапе и способы её минимизации

Курсант: Хамидуллин Салават Айратович Учебная группа № 173

Специальность: 40.05.01 - Правовое обеспечение национальной безопасности

Форма обучения: очная Год набора: 2017 г.

№ п/п	Характер работы (главы, параграфы и их содержание)	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1.	Составление плана содержания выпускной квалификационной работы	5%	до 20 июля 2021 г.	исполнено
2.	Написание §1 главы 1 «Понятие, признаки и общественная опасность преступности»	5%	до 20 сентября 2021 г.	исполнено
3.	Написание § 2 главы 1 «Количественные и качественные характеристики преступности»	10%	до 20 октября 2021 г.	исполнено
4.	Написание § 3 главы 1 «Латентная преступность: понятие, виды, способы оценки»	5%	до 20 ноября 2021 г.	исполнено

5.	Исправление недочетов, выявленных руководителем в ходе проверки главы 1	10%	до 10 декабря 2021 г.	исполнено
6.	Написание § 1 главы 2 «Анализ состояния и тенденций преступности в Российской Федерации»	5%	до 20 декабря 2021 г.	исполнено
7.	Написание § 2 главы 2 «Трансформация преступности в XXI веке»	10%	до 20 января 2022 г.	исполнено
8.	Написание § 3 главы 2 «Киберпреступность как угроза национальной безопасности»	10%	до 20 февраля 2022 г.	исполнено
9.	Исправление недочетов, выявленных руководителем в ходе проверки главы 2	5%	до 10 марта 2022 г.	исполнено
10.	Написание § 1 главы 3 «Современные технологии профилактики и предотвращения преступлений»	10%	до 20 марта 2022 г.	исполнено
11.	Написание § 2 главы 3 «Прогнозирование и планирование в сфере предупреждения преступлений»	10%	до 15 апреля 2022 г.	исполнено
12.	Написание § 3 главы 3 «Деятельность органов внутренних дел по минимизации, выявлению и пресечению преступлений»	10%	до 18 апреля 2022 г.	исполнено
13.	Исправление недочетов, выявленных руководителем в ходе проверки главы 3	5%	до 29 апреля 2022 г.	исполнено

Подпись выпускника _____

«15» 06 2021г.

СОГЛАСОВАНО
Руководитель _____

АКТ ВНЕДРЕНИЯ

научной, научно-технической продукции

1. Наименование ННТП: специализированное программное обеспечение по мониторингу социальных сетей «Anancy».
2. Вид выходного результата: программное обеспечение.
3. Заказчик ННТП: Совет Безопасности Республики Татарстан.
4. Исполнитель работ: слушатель 5 курса 173 учебной группы факультета подготовки специалистов по программам высшего образования ФГКОУ ВО «Казанский юридический институт МВД России» младший лейтенант полиции Хамидуллин Салават Айратович.
5. Основание выполнения научного исследования (НИОКР): на основе заявки аппарата антитеррористической комиссии в Республике Татарстан.
6. Дата и сведения о приеме результатов научного исследования (НИОКР): 11.05.2022, принято главным советником аппарата антитеррористической комиссии Зайнуллиным Р.Р.
7. Характеристика работы (НИОКР): специализированное ПО «Anancy» предназначено для анализа подписчиков деструктивных групп экстремистской и террористической направленности в социальной сети «Вконтакте» с фильтрацией результата поиска по заданному региону. Выборка деструктивных групп производиться на основании экспертиз, проводимых Автономной некоммерческой организацией «Казанский межрегиональный центр экспертиз»
8. Рекомендуется в деятельности советников аппарата антитеррористической комиссии в Республике Татарстан, секретарей антитеррористической комиссии в Республике Татарстан и иных субъектов профилактической деятельности, а также в работе сотрудников и работников отделения по борьбе с IT-преступлениями

Центра по противодействию экстремизму МВД по Республике Татарстан, отдела «К» МВД по Республике Татарстан

9. Сведения о внедрении ННТП: специализированное ПО внедрено в деятельность аппарата антитеррористической комиссии в Республике Татарстан и используется для осуществления оценки текущей общественно-политической обстановки в регионе в совокупности с иными программными средствами.
10. Сведения об эффективности внедрения ННТП: данное программное обеспечение позволяет получать выкладку подписчиков деструктивных групп в социальной сети «Вконтакте» в формате таблицы Excel, что, в совокупности с иными методами, повышает результативность оценки текущей обстановки в регионе в максимально короткие сроки

Р.В. Гильманов

«17» мая 2022 г.

М.П.