МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«КРИМИНОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЕЕ ОБЕСПЕЧЕНИЕ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ»**

Выполнил
Кахриманов Архан Шаванович
обучающийся по специальности
40.05.02 Правоохранительная деятельность
2019 года набора, 925 учебного взвода

Руководитель
доцент кафедры,
кандидат юридических наук
Артамонова Мария Александровна

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
подпись
Дата защиты «___» _____ 2024 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность темы исследования. Текущие процессы цифровизации, охватывающие современное общество, играют ключевую роль в формировании новых социальных структур, основанных на цифровых технологиях, что ведет к улучшению качества жизни и развитию личности, общества, а также повышает международную конкурентоспособность России. Эти изменения требуют особого внимания к обеспечению криминологической безопасности, особенно в контексте цифровых технологий. Существует острая необходимость в адаптации правоохранительных органов к новым вызовам в этой сфере, направленных на защиту ключевых интересов личности, общества и государства в цифровом пространстве.

С ростом проникновения цифровых технологий во все сферы жизни общества появились новые вызовы, включая увеличение преступлений, связанных с этими технологиями. Отмечается, что большая часть этих преступлений совершается в виртуальном пространстве, где используются такие средства, как VPN-шифрование и криптовалюты, что обеспечивает преступникам анонимность и децентрализацию.

Однако правовая база, регулирующая использование цифровых технологий в России, все еще находится в стадии развития. В этой связи требуется модернизация системы криминологической безопасности для адекватного реагирования на угрозы в сфере цифровых технологий. Это включает в себя разработку новых механизмов противодействия криминальным угрозам и методик анализа криминологических рисков в цифровой среде.

В юридической литературе до сих пор недостаточно освещены вопросы криминологической безопасности в контексте цифровых технологий. Несмотря на вклад многих ученых в изучение этой проблематики, существует необходимость в дальнейшем глубоком анализе этих вопросов, учитывая быстрое развитие и проникновение цифровых технологий в различные сферы жизни.

Объектом настоящего исследования является комплекс общественных отношений, формирующихся в рамках обеспечения криминологической безопасности личности, общества и государства от угроз, возникающих в контексте цифровых технологий. Эти отношения включают в себя широкий спектр взаимодействий, охватывающих использование и защиту цифровых технологий, а также меры противодействия преступлениям в этой сфере.

Предмет исследования заключается в анализе российского законодательства, направленного на борьбу с цифровыми преступлениями, изучении закономерностей развития теории криминологической безопасности, её практической реализации в действующей правоприменительной практике. Важной составляющей предмета являются также исследование процессов и явлений, влияющих на уровень криминологической безопасности в контексте цифровизации, анализ международных соглашений и судебной практики по вопросам противодействия цифровым преступлениям, а также изучение официальной статистики и результатов социологических исследований в данной области.

Целью исследования является получение новых знаний о криминологической безопасности в сфере цифровых технологий и разработка стратегических решений для снижения уровня криминологических рисков и угроз в условиях цифровой трансформации.

Для достижения этой цели были поставлены следующие **задачи:**

1) Определить понятие и виды преступности в сфере цифровых технологий.

2) Сформулировать в ходе сопоставительного анализа понятие и сущность обеспечения криминологической безопасности в сфере цифровых технологий и определить ее роль в условиях цифровой трансформации России.

3) Охарактеризовать криминальную обстановку и ее особенности в современной России.

4) Раскрыть особенности влияния цифровой трансформации на криминогенную обстановку в России.

5) Сформулировать обоснованные предложения по подготовке и принятию национальной стратегии обеспечения криминологической безопасности в условиях цифровой трансформации.

6) Определить роль органов внутренних дел в деятельности по обеспечению криминологической безопасности в условиях цифровой трансформации.

Методология данного исследования базируется на диалектическом методе познания, который позволяет всесторонне и объективно анализировать процессы и явления в сфере криминологической безопасности. В рамках этой методологии применяются различные методы и подходы, способствующие глубокому и всестороннему анализу изучаемой тематики.

Структура выпускной квалификационной работы. Структура работы построена с учетом поставленных целей и задач и состоит из: введения, двух глав, включающих в себя четыре параграфа, заключения и списка использованной литературы.

ГЛАВА 1. ПРЕСТУПНОСТЬ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ПОНЯТИЕ И ВИДЫ

§ 1. Понятие и виды преступности в сфере цифровых технологий.

Цифровизация общества влечет за собой радикальные изменения в экономической, политической, социальной и правовой сферах, переформатируя устоявшиеся подходы и уклады. Российское руководство, осознавая важность этого процесса, акцентирует внимание на том, что цифровая экономика представляет собой не просто отдельную отрасль, а новый уклад жизни и основу для развития всех сфер общества, при этом подчеркивая, что это вопрос национальной безопасности и независимости страны.

Цифровая трансформация, как масштабный и комплексный процесс, затрагивает все аспекты общественной жизни, начиная от внедрения сквозных цифровых технологий и заканчивая полной перестройкой системы государственного управления и рынка услуг. Этот процесс включает в себя не только технологические изменения, но и глубокую реорганизацию рабочих процессов, ориентированных на использование цифровых инструментов.

В криминологической сфере цифровая трансформация несет в себе значительные риски, увеличивая потенциал возникновения новых видов преступлений и модификации уже существующих. Правовая основа для противодействия цифровым преступлениям находится в стадии разработки, что затрудняет эффективное борьбу с данным видом преступности.

На международном уровне проблема киберпреступности обсуждается уже длительное время. ООН, начиная с 1990-х годов, активно поднимает вопросы компьютерной преступности и безопасности информационных систем. Разработанные принципы и директивы фокусируются на необходимости осознания и снижения уровня киберугроз, но до сих пор не существует единого

определения для цифровой преступности, что затрудняет формирование общей международной стратегии борьбы с ней[1].

Таким образом, цифровая трансформация общества и экономики представляет собой ключевой вызов современности, требующий адекватного правового регулирования и международного сотрудничества для эффективного противодействия возникающим криминологическим угрозам.

В рамках XI Конгресса ООН в Бангкоке в 2005 году была предложена новая концептуальная модель понятия киберпреступности, охарактеризованной как запрещенное законом поведение, направленное на компьютерную сферу и коммуникационные технологии, включающее использование информационных технологий и компьютера как инструмента при совершении других преступлений. Важным аспектом этого определения является то, что компьютер становится источником электронных процессуальных доказательств.

В 2013 году Управление ООН по наркотикам и преступности представило проект исследований, в котором дается международно-правовое определение киберпреступности и подробно описываются ее виды. Отмечается, что киберпреступность быстро эволюционировала, превратившись в организованную и индустриализированную форму преступности, с участием высококвалифицированных специалистов.

Однако, несмотря на значительные усилия по борьбе с киберпреступностью, процесс их обнаружения остается сложным. Сложность заключается в том, что преступники часто используют широкодоступные средства связи, такие как мессенджеры и интернет, но при этом их самоидентификация и проникновение в их группы затруднена.

В рамках XIV Конгресса ООН в Киото в 2021 году обсуждались вопросы использования современных технологий при совершении преступлений, при этом акцент смещался с традиционных понятий киберпреступности на более широкое понимание информационных и цифровых технологий.

---

[1] Конев Денис Андреевич СОВРЕМЕННЫЕ ПОДХОДЫ К ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ // Философия права. 2020. №4 С. 2.

На постсоветском пространстве понятие преступления в сфере компьютерной информации закреплено в Соглашении о сотрудничестве государств СНГ в борьбе с такими преступлениями. Здесь же упоминается и понятие компьютерной информации, охватывающее данные, находящиеся в памяти компьютера или передающиеся по каналам связи.

Существует определенная доктринальная неопределенность в понимании киберпреступности как в России, так и на международном уровне. В различных источниках используются термины «киберпреступность», «компьютерное преступление», «информационное преступление», что свидетельствует о необходимости дальнейшего уточнения и согласования понятийного аппарата в этой области.

Таким образом, понятие киберпреступности по-прежнему находится в процессе развития и обсуждения как в национальном, так и в международном контексте, что отражает быстрое развитие технологий и необходимость адаптации правовых и следственных рамок к новым вызовам в этой области.

Исследование понятийного аппарата информационных преступлений показывает отсутствие единого подхода к определению этого вида преступлений. В научной литературе можно встретить различные терминологии и определения, отражающие разные аспекты и характеристики информационных преступлений. Например, они определяются как преступления, совершаемые в области информационных правоотношений с использованием информационных ресурсов и технологий, где информация является предметом или средством совершения преступления[1].

Авторы научных работ дополняют это понятие такими элементами, как электронные, технические и социальные системы управления, а также информационно-телекоммуникационные сети и средства вычислительной техники. Это указывает на расширение контекста киберпреступлений за пределы традиционного понимания компьютерных технологий.

---

[1] Варыгин, А. Н. Основы криминологии и профилактики преступлений : учебное пособие для вузов / А. Н. Варыгин, В. Г. Громов, О. В. Шляпникова ; под редакцией А. Н. Варыгина. — 2-е изд. — Москва : Издательство Юрайт, 2023. С.80.

Современные технологии, такие как искусственный интеллект, блокчейн, BigData, облачные технологии и цифровые близнецы, способствуют возникновению новых форм противоправных деяний. Однако отсутствие четких уголовно-правовых норм и неопределенность в определении цифровых преступлений затрудняет учет и классификацию уголовной статистики в этой области.

Классификация цифровых преступлений может включать деяния, совершаемые с использованием компьютерных устройств и программ, а также преступления, совершаемые в отношении развивающихся цифровых технологий. Кроме того, преступления могут быть классифицированы по сферам применения цифровых технологий, включая электронную коммерцию, цифровую медицину, интернет вещей и другие.

В целом, несмотря на предпринимаемые усилия, единое понимание и классификация цифровой преступности еще не сформировались на доктринальном уровне. С учетом постоянного развития цифровых технологий, проблематика требует дальнейшего исследования и разработки уголовно-правовых норм, адекватно отражающих новые вызовы в сфере цифровой преступности.

Согласно Хайрусову Д. С. и другим авторам, преступность в сфере цифровых технологий заслуживает отдельного внимания и анализа в контексте современного развития информационных технологий. Данное направление выделяется как отдельный вид преступности, учитывая:

1) Интенсивное развитие и внедрение цифровых технологий.

2) Рост числа преступлений, зарегистрированных в сфере цифровых технологий.

3) Расширение спектра преступной деятельности с использованием цифровых технологий, охватывающее различные области жизни и

деятельности, включая экономику, здоровье граждан, национальную безопасность и т.д[1].

На текущий момент в России не существует законодательного определения преступности в сфере цифровых технологий, что свидетельствует о необходимости развития и оптимизации нормативно-правовой базы для регулирования этой области.

Преступность в сфере цифровых технологий характеризуется рядом особенностей:

1) Высокая латентность и общественная опасность.

2) Трансграничный характер, не связанный с географическими границами.

3) Использование цифровых технологий для совершения преступлений в виртуальной среде.

4) Классификация преступлений в этой сфере может включать:

5) Преступления, совершаемые в отношении цифровых технологий и сквозных цифровых технологий.

6) Преступления, совершаемые с использованием цифровых технологий в различных отраслях, включая цифровую медицину, IT, страхование, логистику, электронную коммерцию, интеллектуальную собственность и другие[2].

Учитывая быстрое развитие цифровых технологий, исследование преступности в этой сфере является актуальным и непрерывным процессом. Оно требует постоянного анализа и адаптации уголовного законодательства, чтобы эффективно реагировать на новые угрозы и вызовы в сфере криминологической безопасности. Развитие доктринальных подходов и определение конкретных направлений деятельности по противодействию

---

[1] Хайрусов, Д. С. Криминология : учебное пособие для вузов / Д. С. Хайрусов. — Москва : Издательство Юрайт, 2023. — 95 с. — (Высшее образование). — ISBN 978-5-534-17544-8. — URL : https://urait.ru/bcode/533298

[2] Лунеев, В. В. Курс мировой и российской криминологии в 2 т. Том 1. Общая часть в 3 кн. Книга 3 : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. С. 21.

цифровым преступлениям становятся ключевыми задачами в контексте усиления роли информационно-цифровых технологий в современном мире.

§ 2. Влияние цифровой трансформации на криминогенную обстановку в России.

Особенности криминогенной обстановки в условиях цифровой трансформации требуют всестороннего анализа, учитывая развитие и внедрение цифровых технологий, которые оказывают значительное влияние на общественные отношения. Программа «Цифровая экономика Российской Федерации» и стратегии развития отдельных цифровых технологий, таких как искусственный интеллект, способствуют экономическому росту и повышению конкурентоспособности страны. Однако вместе с положительными аспектами эти изменения влекут за собой увеличение криминологических рисков.

С ростом цифровой экономики наблюдается беспрецедентный рост преступности в сфере цифровых технологий. Отсутствие стратегических направлений противодействия цифровой преступности и неопределенность в понятийном аппарате, а также отсутствие механизмов криминологической безопасности усугубляют ситуацию. Необходимость в методологических рекомендациях по оценке угроз криминологической безопасности в цифровой среде становится все более актуальной.

Цифровая трансформация, кроме усиления криминогенной обстановки, также влияет на криминологические риски, связанные с внедрением и использованием цифровых технологий. Эти риски могут быть классифицированы как:

1) Риски, непосредственно связанные с внедрением и использованием цифровых технологий.

2) Высокие технологические риски.

3) Системные причины и условия, способствующие совершению преступлений в данной сфере (социально-политические, экономические, психологические, правовые, организационно-технические и т.д.)[1].

Технология блокчейна и возникновение криптовалюты привели к новым вызовам в области криминологической безопасности. Блокчейн обладает потенциалом для борьбы с преступлениями, такими как коррупция и экономические преступления, но также создает новые риски, особенно связанные с криптовалютами.

В этом контексте критически важно определение и классификация криминологических рисков, их уровня и характера с учетом существующих угроз для разработки эффективных мер обеспечения криминологической безопасности. Такой подход позволит выявить критически важные объекты инфраструктуры, требующие защиты, и сформировать стратегию устранения или минимизации рисков, способствующих преступности. Рекомендация 15 ФАТФ подчеркивает необходимость риск-ориентированного подхода в отношении новых технологий, включая оценку рисков и принятие мер для их снижения до запуска новых продуктов или технологий.

В целом, комплексный анализ и оценка криминологических рисков и угроз, связанных с цифровой трансформацией, являются ключевыми для формирования эффективной стратегии противодействия цифровой преступности и обеспечения криминологической безопасности в современных условиях.

Проблемы, связанные с преступлениями в сфере виртуальных активов, таких как криптовалюты, в условиях цифровой трансформации, представляют собой сложное и многогранное явление. Эти преступления включают в себя легализацию денежных средств, мошенничество, вымогательство, финансирование терроризма и другие, и, как предполагается, будут только увеличиваться в связи с расширением использования цифровых технологий.

---

[1] Варыгин, А. Н. Основы криминологии и профилактики преступлений : учебное пособие для вузов / А. Н. Варыгин, В. Г. Громов, О. В. Шляпникова ; под редакцией А. Н. Варыгина. — 2-е изд. — Москва : Издательство Юрайт, 2023. С. 90.

Одной из основных проблем является криминологический риск, связанный с использованием криптовалют и искусственного интеллекта. Искусственный интеллект может использоваться для гражданских и военных целей, а также в преступных действиях, включая фишинговые атаки и распространение дезинформации. Сочетание искусственного интеллекта с интернетом создает новые угрозы, такие как доступ к интеллектуальной собственности и технологическим разработкам.

Создание систем, включающих искусственный интеллект и роботизированные устройства, также увеличивает риски их использования преступниками. Например, боевые дроны, управляемые искусственным интеллектом, уже активно используются в преступных целях.

Развитие технологий также способствует увеличению рисков, связанных с интернетом вещей (IT). Умные домашние устройства могут быть использованы для сбора данных о жителях дома, что создает новые возможности для преступлений, включая шпионаж и вымогательство.

Технологии обработки больших данных (BigData) представляют собой еще одну область, где существует риск преступного использования данных для целей, включая идентификацию и отслеживание лиц для совершения преступлений.

Квантовые технологии, включая квантовые компьютеры, могут использоваться как для борьбы с преступлениями, так и для их совершения. Существует опасность, что квантовые технологии могут быть использованы для взлома кодов и расшифровки криптографических алгоритмов, что представляет угрозу для сохранности государственных и коммерческих данных.

Таким образом, в условиях цифровой трансформации возникают новые криминологические вызовы, требующие комплексного подхода к обеспечению безопасности и противодействию преступности, связанной с использованием цифровых технологий.

В контексте цифровой трансформации и внедрения новых технологий, таких как квантовые вычисления, возникают новые технологические риски. Эти

риски могут принимать различные формы, от хакерских атак до использования в создании биооружия и оружия массового поражения[1].

1) Хакерские атаки и кибербезопасность увеличение вычислительных мощностей открывает новые возможности для кибератак, включая нарушение работы критически важной инфраструктуры и доступ к конфиденциальной информации. Это особенно актуально для промышленности и IoT-устройств.

2) Экономическое влияние вычислительные технологии могут использоваться для создания экономических преимуществ на мировом рынке, включая разработку новых продуктов и услуг, которые могут радикально изменить рыночную динамику.

3) Разработка оружия и биотехнологии вычислительные мощности могут способствовать разработке новых форм оружия и биотехнологий, включая патогены и вирусы, что представляет собой серьезную угрозу для мировой безопасности.

Социально-экономические изменения, вызванные цифровой трансформацией, также несут в себе риски. Развитие цифровых технологий ведет к изменению рынка труда, сокращению традиционных профессий и возникновению новых специализаций. Эти процессы могут привести к увеличению безработицы и социальной нестабильности, что, в свою очередь, способствует росту преступности.

Таким образом, важным аспектом в области противодействия киберпреступности и минимизации технологических рисков является разработка стратегий, направленных на укрепление кибербезопасности, защиту критически важной инфраструктуры, а также адаптацию социально-экономических систем к новым условиям цифровой экономики. Это включает в себя как разработку новых законодательных и нормативных мер, так и внедрение технологических решений для улучшения безопасности и устойчивости цифровой инфраструктуры.

---

[1] Антонян, Ю. М. Криминология : учебник для вузов / Ю. М. Антонян. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. С. 89.

Увеличение теневой занятости и рост внутренней миграции в России в значительной степени связаны с цифровой трансформацией и изменениями на рынке труда. Эти социальные процессы способствуют развитию криминогенности в обществе и создают условия для расширения влияния организованной преступности:

1) Теневая занятость: Увеличение числа лиц, занятых в теневом секторе экономики, увеличивает риски их вовлечения в криминальные структуры. Теневая экономика часто тесно связана с организованной преступностью, что усиливает преступное влияние и создает условия для "пополнения кадров" в преступных группах.

2) Миграция: Рост внутренней миграции, вызванный поиском работы, способствует увеличению криминогенности. Трудовые мигранты из других государств также несут риски увеличения преступности, этнических и религиозных конфликтов.

3) Социальное неравенство и цифровое неравенство: Социальное неравенство усугубляется в эпоху цифровизации, создавая "новых бедных", которые либо не имеют доступа к интернету и цифровым устройствам, либо используют их неэффективно. Региональное различие в доступе к цифровым технологиям способствует углублению этого неравенства.

4) Уязвимость общества и государства к криминальным проявлениям: Ускоренная цифровая трансформация увеличивает круг криминологических угроз и повышает их уровень. Развитие и использование цифровых технологий изменяют рынки труда и типы экономического развития, что увеличивает криминогенные риски.

5) Социально-правовые риски: Развитие цифровой экономики в России требует соответствующей правовой базы, которая пока не полностью сформирована, включая регламенты для специалистов в области цифровых технологий и стандарты их использования.

6) Влияние деструктивной информации: Распространение дезинформации и провокационных сообщений, особенно во время кризисов как пандемии

COVID-19, усугубляет социальную и экономическую нестабильность, способствуя росту преступности[1].

Эти факторы указывают на сложность и многоуровневость проблем, связанных с цифровой трансформацией, требующих комплексного подхода к их решению, включая социальные, экономические и правовые аспекты.

В период пандемии COVID-19 наблюдается значительное увеличение преступлений, связанных с использованием цифровых технологий. Это включает мошенничество, фишинг, распространение фальшивых продуктов и лекарств, а также хакерские атаки на медицинские учреждения. Преступники адаптируют свои методы к текущей ситуации, эффективно используя цифровые технологии для своих целей.

Однако, кроме непосредственного преступного использования цифровых технологий, важно обратить внимание на организационно-технические и правовые аспекты, которые влияют на уровень криминологических рисков:

1) Неподготовленность правоохранительных органов: Отсутствие современного оборудования и специализированных знаний в сфере цифровых технологий затрудняет борьбу с киберпреступностью.

2) Недостаток правовой базы: В России пока не сформирована полноценная правовая база, регулирующая использование цифровых технологий, что создает пробелы в обеспечении криминологической безопасности.

3) Отсутствие эффективных механизмов противодействия: Не разработаны механизмы для эффективного пресечения криминологических угроз и определения рисков, связанных с цифровыми технологиями.

4) Необходимость прогнозирования и планирования мер: Прогнозирование криминальной ситуации и криминогенных факторов должно стать основой деятельности по обеспечению криминологической безопасности.

---

[1] Шишкин Радий Владимирович ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ // Вестник Уральского юридического института МВД России. 2022. С. 4-6.

5) Криминогенные риски: Важно выделить и анализировать основные группы криминогенных рисков, включая риски, связанные с внедрением инновационных технологий, высокие технологические риски и риски, обусловленные системой причин и условий преступлений[1].

Для эффективного противодействия киберпреступности необходим комплексный подход, включающий улучшение правового регулирования, повышение квалификации правоохранительных органов, разработку эффективных методик прогнозирования и планирования мер по обеспечению криминологической безопасности.

[1] Пинкевич Татьяна Валентиновна ОБЕСПЕЧЕНИЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ // Вестник Казанского юридического института МВД России. 2022. С. 8.

ГЛАВА 2. ОБЕСПЕЧЕНИЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Обеспечение криминологической безопасности: понятие, сущность и ее роль в условиях цифровой трансформации России.

В условиях цифровой трансформации российского общества, обеспечение криминологической безопасности становится особенно актуальным и требует инновационного подхода. Рост числа зарегистрированных преступлений в сфере цифровых технологий, высокий уровень их латентности и динамичность киберпреступлений подчеркивают необходимость адаптации правоохранительной системы к новым угрозам.

Основываясь на определении криминологической безопасности, представленном в Стратегии национальной безопасности Российской Федерации, а также на подходах, предложенных И. Я. Козаченко и К. В. Корсаковым, можно выделить следующие ключевые направления деятельности по обеспечению криминологической безопасности в цифровой сфере.

Во-первых, повышение осведомленности общества о рисках и угрозах киберпространства является фундаментальной задачей. Обучение граждан и повышение их осознанности в вопросах кибергигиены включают не только информирование о методах защиты от киберпреступлений, но и формирование устойчивых навыков безопасного поведения в сети. Распространение знаний о потенциальных угрозах, таких как фишинг, вредоносные программы и социальная инженерия, способствует снижению уровня уязвимости населения перед киберугрозами. Важно организовывать регулярные образовательные кампании, вебинары и тренинги, которые помогут гражданам понять важность соблюдения основных правил кибербезопасности и научат их, как защитить свои личные данные и финансовые ресурсы.

Во-вторых, усиление законодательной базы является критически важным аспектом в условиях стремительного развития цифровых технологий.

Совершенствование нормативно-правовых актов должно учитывать динамичную природу киберпространства и появление новых видов преступлений. Это требует регулярного пересмотра и обновления законодательных положений, направленных на защиту информации и обеспечение правопорядка в цифровой сфере. Разработка специальных законов и регламентов, регулирующих вопросы кибербезопасности, а также усиление ответственности за киберпреступления, позволят создать более надежную правовую основу для борьбы с угрозами в интернете.

Третье направление включает развитие технических и аналитических способностей правоохранительных органов. Для эффективного реагирования на киберугрозы необходимо не только обновление технического оборудования и программного обеспечения, но и постоянное повышение квалификации сотрудников. Это включает в себя проведение специализированных курсов и тренингов, направленных на обучение методам выявления, анализа и расследования киберпреступлений. Внедрение современных аналитических инструментов, таких как системы искусственного интеллекта и машинного обучения, позволит правоохранительным органам более оперативно и точно выявлять подозрительную активность и предотвращать преступления.

Четвертое направление касается содействия международному сотрудничеству. Учитывая трансграничный характер киберпреступлений, взаимодействие с международными партнерами и организациями является ключевым элементом в борьбе с глобальными угрозами. Международное сотрудничество позволяет обмениваться информацией, лучшими практиками и совместно разрабатывать стратегии и меры по противодействию киберпреступлениям. Участие в международных форумах, конференциях и рабочих группах способствует укреплению глобальной системы кибербезопасности и повышению уровня защиты на национальном уровне.

Пятое направление связано с исследованием и анализом криминологических угроз. Регулярное изучение данных о киберпреступности, анализ тенденций и паттернов позволяет формировать эффективные стратегии

противодействия. Важно создавать специализированные аналитические центры и исследовательские группы, которые будут заниматься мониторингом и прогнозированием киберугроз, а также разработкой рекомендаций по их нейтрализации. Использование больших данных (Big Data) и других современных технологий для анализа криминогенной ситуации способствует более глубокому пониманию природы и динамики киберпреступлений.

Шестое направление касается формирования культуры кибербезопасности среди населения и в бизнес-сообществе. Развитие культуры кибербезопасности включает в себя не только обучение основным принципам защиты данных, но и внедрение стандартов и лучших практик в повседневную деятельность организаций. Важно, чтобы руководители предприятий и сотрудники понимали значимость защиты информации и принимали активное участие в обеспечении безопасности своих цифровых ресурсов. Создание корпоративных политик по кибербезопасности, проведение регулярных аудитов и тренингов, а также поощрение ответственного поведения в сети помогут повысить уровень защиты как на индивидуальном, так и на организационном уровне[1].

Эти направления помогут формировать эффективную систему криминологической безопасности, которая будет адаптирована к вызовам цифровой эры и способна снизить риски, связанные с киберпреступностью.

Криминологическая безопасность в контексте цифровой трансформации общества занимает ключевое место в системе национальной безопасности Российской Федерации. Это обусловлено тесной связью криминологической безопасности со всеми аспектами национальной безопасности, как подчеркнуто в Стратегии национальной безопасности РФ, где противодействию преступности уделено особое внимание.

Развитие и внедрение цифровых технологий повышают авторитет государства на мировом рынке и способствуют укреплению его суверенитета и экономической конкурентоспособности. Однако, как указывает А. А. Лапин,

[1] Козаченко, И. Я. Криминология : учебник и практикум для вузов / И. Я. Козаченко, К. В. Корсаков. — Москва : Издательство Юрайт, 2023. С. 130.

криминологическая безопасность приобретает особое значение в контексте цифровизации, поскольку криминология обладает необходимыми средствами для оценки и предотвращения преступлений в цифровой сфере.

Основной задачей криминологической безопасности в сфере цифровых технологий является обеспечение защиты личности, общества и государства от цифровых и информационных угроз. Для достижения этой цели необходимо реализация комплекса мер, направленных на противодействие преступным посягательствам и создание надежной системы безопасности. Эти меры включают следующие ключевые направления.

Во-первых, обеспечение защиты от источников угроз, включая снижение уязвимости к преступным посягательствам, требует системного подхода к анализу и устранению рисков. Это включает в себя разработку и внедрение современных технических средств защиты информации, регулярное обновление программного обеспечения и проведение аудитов безопасности для выявления и устранения потенциальных уязвимостей. Важно также формирование культуры информационной безопасности среди населения и сотрудников организаций, что предполагает проведение обучающих мероприятий и повышение осведомленности о методах защиты от киберугроз. Эффективная защита требует не только технических, но и организационных мер, таких как регулярное обновление политик безопасности и проведение тренингов по реагированию на инциденты.

Во-вторых, создание эффективно функционирующей государственной системы обеспечения безопасности в сфере цифровых технологий предполагает разработку и реализацию стратегических программ и инициатив, направленных на укрепление кибербезопасности. Это включает в себя координацию деятельности различных государственных и частных структур, развитие национальной инфраструктуры кибербезопасности и формирование специализированных подразделений, занимающихся борьбой с киберпреступностью. Важную роль играет также международное сотрудничество, позволяющее обмениваться опытом и лучшими практиками с

другими странами, а также совместно разрабатывать и внедрять меры по противодействию глобальным киберугрозам.

Третьим направлением является повышение эффективности профилактической деятельности в области цифровых технологий. Профилактика преступлений предполагает не только реактивные, но и проактивные меры, направленные на предотвращение возможных угроз. Это включает в себя разработку и внедрение программ по повышению осведомленности населения о киберугрозах, обучение безопасному поведению в цифровой среде и проведение регулярных кампаний по информированию о новых методах защиты. Важно также проведение научных исследований в области кибербезопасности, которые помогут выявить новые угрозы и разработать инновационные методы их предотвращения.

Кроме того, важным аспектом является разработка и внедрение современных технологий для мониторинга и анализа данных, что позволяет своевременно выявлять подозрительную активность и предотвращать преступления. Это может включать использование искусственного интеллекта и машинного обучения для анализа больших объемов данных и выявления аномалий, а также разработку автоматизированных систем для реагирования на инциденты.

В рамках государственной политики в области криминологической безопасности в сфере цифровых технологий особое внимание должно быть уделено созданию условий для сотрудничества между различными субъектами системы безопасности, включая правоохранительные органы, частные компании, образовательные учреждения и общественные организации. Такое сотрудничество позволяет эффективно распределять ресурсы и объединять усилия для достижения общей цели – защиты от цифровых угроз.

Таким образом, комплексный подход к обеспечению криминологической безопасности в цифровой сфере включает в себя множество взаимосвязанных мер, направленных на защиту личности, общества и государства. Это требует постоянного совершенствования технологий, нормативно-правовой базы, а

также повышения уровня осведомленности и квалификации всех участников процесса. Только таким образом можно создать надежную и устойчивую систему защиты от киберугроз, способную эффективно реагировать на современные вызовы и обеспечивать безопасность в цифровую эпоху.

Нормативно-правовое регулирование играет ключевую роль в обеспечении криминологической безопасности, требуя постоянного адаптирования к изменениям в сфере цифровых технологий. Информационное обеспечение включает сбор и анализ данных о преступности и ее предупреждение с использованием цифровых технологий.

Таким образом, в условиях цифровой трансформации, обеспечение криминологической безопасности требует комплексного подхода, включающего законодательные, организационные, технические и информационные меры.

Мониторинг, как основное направление получения информации в рамках обеспечения криминологической безопасности, играет критически важную роль. Этот процесс позволяет не только фиксировать зарегистрированные преступления, но и выявлять латентную, то есть скрытую, часть преступности в условиях цифровой трансформации общества. Важным дополнением к мониторингу является проведение социологических опросов среди населения, что способствует формированию более полной картины восприятия безопасности гражданами и уровня их осведомленности о криминальных угрозах. Такие опросы помогают понять, насколько население осознает существующие риски и какие меры по их предотвращению считает наиболее эффективными. Таким образом, мониторинг и социологические исследования выступают как взаимодополняющие методы, которые вместе обеспечивают комплексный подход к оценке и улучшению криминологической безопасности.

Организационное обеспечение криминологической безопасности включает в себя стратегическое планирование, контрольные и надзорные функции в сфере цифровых технологий, а также усиление взаимодействия между различными структурами, ответственными за обеспечение безопасности. Ключевое значение в этом контексте имеет подготовка и переподготовка

сотрудников правоохранительных органов, которые непосредственно занимаются решением задач в данной сфере. Регулярное обновление знаний и навыков этих специалистов позволяет им эффективно противостоять новым вызовам и угрозам, возникающим в результате цифровой трансформации. Также следует отметить важность разработки и внедрения специализированных программ обучения, направленных на повышение квалификации сотрудников в области информационных технологий и кибербезопасности.

Система криминологической безопасности представляет собой комплексно взаимосвязанных элементов, включающих в себя силы и средства обеспечения безопасности. "Силы" в данном контексте понимаются как совокупность субъектов безопасности, к которым относятся федеральные органы исполнительной власти, органы прокуратуры и следствия, органы государственной власти субъектов Российской Федерации и местного самоуправления, а также граждане, общественные объединения и другие организации, действующие в соответствии с Федеральным законом "Об основах системы профилактики правонарушений в Российской Федерации". "Средства" же включают в себя меры различного характера, направленные на поддержание приемлемого уровня безопасности, такие как технические и программные средства, нормативно-правовые акты, а также методы и стратегии, используемые для предотвращения и расследования преступлений.

Особо важную роль в обеспечении криминологической безопасности играют организации, занимающиеся проектированием, производством, внедрением и эксплуатацией информационных продуктов и услуг, включая объекты национальной критической информационной инфраструктуры. Эти организации отвечают за разработку и поддержание технологий, которые используются для защиты информации и предотвращения киберпреступлений. Важность их работы трудно переоценить, так как они обеспечивают техническую основу для всех мероприятий по защите от киберугроз. В их обязанности входит создание безопасных информационных систем, проведение

регулярных аудитов безопасности, а также разработка и внедрение инновационных решений для защиты данных.

Таким образом, комплексный подход к обеспечению криминологической безопасности, включающий мониторинг, социологические исследования, организационные меры и технологическое обеспечение, позволяет эффективно противостоять современным угрозам и обеспечивать высокий уровень защиты для всех участников цифрового пространства. Эти меры, применяемые в совокупности, формируют надежную систему, способную адаптироваться к быстро меняющимся условиям и новым вызовам, что особенно важно в условиях постоянного развития и усложнения цифровых технологий[1].

Важно отметить, что каждый субъект системы криминологической безопасности выполняет свои задачи в соответствии с установленной компетенцией и полномочиями, определенными российским законодательством. Такая структурная организация позволяет эффективно распределять функции и ответственность между различными участниками процесса, что, в свою очередь, способствует созданию надежной и скоординированной системы противодействия преступлениям в цифровой сфере.

Система обеспечения криминологической безопасности в сфере цифровых технологий играет ключевую роль в противодействии современным криминологическим угрозам. Она включает в себя не только меры правового регулирования и контроля, но и широкий спектр средств, направленных на достижение эффективной защиты. Среди основных направлений деятельности в этой области можно выделить несколько ключевых аспектов.

Во-первых, реализация государственной политики в области криминологической безопасности предусматривает разработку и применение законодательных и нормативных актов, которые регулируют все аспекты борьбы с преступностью в цифровом пространстве. Эти документы

[1] Криминология : учебник для вузов / В. И. Авдийский [и др.] ; под редакцией В. И. Авдийского, Л. А. Букалеровой. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. С. 132.

устанавливают правовые рамки для деятельности всех субъектов системы и обеспечивают согласованность их действий.

Во-вторых, активное взаимодействие всех субъектов обеспечения криминологической безопасности является необходимым условием для эффективного снижения уровня угроз. Это включает в себя координацию действий между различными государственными и частными структурами, обмен информацией и опытом, а также проведение совместных мероприятий по предотвращению и расследованию преступлений.

Третьим важным направлением является использование цифровых технологий для выявления, раскрытия и расследования преступлений. Современные информационные системы и программное обеспечение позволяют значительно повысить эффективность работы правоохранительных органов, обеспечивая им доступ к необходимым данным и инструментам для анализа и расследования инцидентов.

В-четвертых, внедрение современных технологий для проведения мероприятий по снижению уровня криминологических угроз также является приоритетной задачей. Это включает в себя разработку и применение новых методик и технических средств, которые позволяют оперативно реагировать на возникающие угрозы и предотвращать их развитие.

Мониторинг и анализ законодательства, регулирующего область цифровой безопасности, являются еще одним важным аспектом работы в этой сфере. Регулярное обновление нормативно-правовой базы и адаптация её к новым вызовам и угрозам позволяет поддерживать актуальность и эффективность принимаемых мер.

Кроме того, разработка и реализация федеральных и региональных программ, направленных на предупреждение цифровой преступности, играет важную роль в системе обеспечения криминологической безопасности. Эти программы включают в себя комплекс мероприятий, направленных на повышение осведомленности населения о рисках, обучение сотрудников

правоохранительных органов, а также разработку и внедрение новых технологий и методик борьбы с преступностью.

Таким образом, система обеспечения криминологической безопасности в сфере цифровых технологий представляет собой комплексный и многоуровневый механизм, включающий в себя различные аспекты правового, организационного и технического характера. Эффективное функционирование этой системы возможно только при условии скоординированной работы всех её элементов и постоянного совершенствования применяемых методов и средств.

Однако, несмотря на значительные усилия, существуют серьезные проблемы в реализации мер по обеспечению криминологической безопасности. Эти проблемы требуют тщательного анализа и принятия комплексных мер для их преодоления. Основные из них включают следующие аспекты.

Во-первых, отсутствие современной нормативной базы, соответствующей требованиям цифрового общества, представляет собой существенное препятствие. Текущие законодательные акты зачастую не успевают за стремительным развитием цифровых технологий, что приводит к возникновению правовых пробелов и недостаточной эффективности правоприменительной практики. Для успешного противодействия цифровым угрозам необходимо регулярно обновлять законодательство, учитывая новые виды преступлений и методы их совершения. Это требует не только разработки новых нормативно-правовых актов, но и пересмотра существующих положений, чтобы они соответствовали современным реалиям.

Во-вторых, недостаточное кадровое обеспечение современными специалистами в цифровой сфере также является серьезной проблемой. В условиях цифровой трансформации важность наличия квалифицированных кадров, обладающих глубокими знаниями в области информационных технологий и кибербезопасности, возрастает многократно. Недостаток таких специалистов ограничивает возможности правоохранительных органов в расследовании и предотвращении преступлений в цифровом пространстве. Для решения этой проблемы необходимо уделять больше внимания подготовке и

переподготовке кадров, создавая условия для обучения и повышения квалификации сотрудников, а также привлекать молодых специалистов и обеспечивать им достойные условия труда.

Третьим серьезным вызовом является зависимость от иностранных цифровых технологий. Использование зарубежного программного обеспечения и оборудования создает риск утечки данных и нарушений безопасности, что может быть использовано злоумышленниками для совершения преступлений. В этом контексте важно развивать и внедрять отечественные технологические решения, которые позволят снизить зависимость от внешних поставщиков и повысить уровень защиты информации.

Социальное и цифровое неравенство, рост безработицы и миграции также играют значительную роль в усложнении обеспечения криминологической безопасности. Социальные проблемы и экономические трудности могут способствовать росту преступности, в том числе в цифровой сфере. В условиях увеличивающегося разрыва между разными слоями населения доступ к современным технологиям и средствам защиты становится привилегией, что создает благоприятную почву для преступной деятельности. Решение этих проблем требует комплексного подхода, включающего меры по снижению социального неравенства, созданию новых рабочих мест и улучшению условий жизни населения.

Таким образом, для успешного обеспечения криминологической безопасности в цифровом обществе необходимо учитывать множество факторов и реализовывать комплексные меры, направленные на преодоление существующих проблем. Это включает в себя разработку современной нормативной базы, повышение квалификации кадров, развитие отечественных цифровых технологий и устранение социальных и экономических дисбалансов. Только при условии системного подхода и координации усилий всех заинтересованных сторон можно достичь значительного прогресса в этой важной сфере.

Эти проблемы требуют комплексного подхода и скоординированных действий на всех уровнях государственной и общественной деятельности. Важно также формирование в обществе атмосферы защищенности от криминальных угроз, что будет способствовать снижению страхов и опасений граждан, связанных с цифровыми технологиями и преступностью в этой сфере.

§ 2. Стратегические направления обеспечения криминологической безопасности в сфере цифровых технологий

С развитием цифровой экономики и цифровой трансформации общества, обеспечение криминологической безопасности становится ключевым аспектом национальной безопасности государства. Это обусловлено не только увеличением числа преступлений, связанных с использованием цифровых технологий, но и сложностью и масштабностью этих угроз. Современная борьба с киберпреступностью требует инновационного подхода, учитывающего быстро меняющиеся тенденции и появление новых способов совершения преступлений.

Основные направления обеспечения криминологической безопасности включают:

1) Совершенствование Законодательства: Правовые основы обеспечения криминологической безопасности необходимо постоянно адаптировать к меняющимся условиям цифровой сферы.

2) Международное Сотрудничество: Важность разработки международных стандартов и кодексов поведения в киберпространстве, особенно в контексте глобальной сети Интернет.

3) Инновационные Решения: Необходимость принятия передовых технологических решений для эффективного противодействия киберпреступности.

4) Анализ Рисков и Угроз: Систематический анализ текущих и потенциальных угроз в цифровой среде для разработки стратегических планов противодействия.

5) Защита Критической Инфраструктуры: Специальное внимание защите объектов критической инфраструктуры от кибератак.

6) Развитие Правоохранительной Системы: Необходимость обновления подходов и методов работы правоохранительных органов, включая обучение и переподготовку специалистов.

7) Общественное Восприятие и Профилактика: Важно не только бороться с киберпреступностью, но и формировать в обществе атмосферу защищенности и осведомленности о киберугрозах[1].

Проблемы в этой сфере многообразны и требуют комплексного подхода, включающего как усиление законодательной базы, так и развитие технологических и организационных мер. Важным аспектом является и сотрудничество на международном уровне для разработки общих стандартов и принципов поведения в киберпространстве.

Реализация национальной стратегии обеспечения криминологической безопасности в условиях цифровой трансформации требует комплексного подхода, включающего следующие ключевые аспекты:

1) Теоретическая Подготовка Проекта: Стратегия должна базироваться на глубоком анализе криминологической обстановки, включая криминальные угрозы, криминогенные риски, а также мониторинг социально-экономического и социально-правового развития общества.

2) Прогнозирование Преступности: Важным элементом стратегии является прогнозирование тенденций цифровой преступности, позволяющее планировать меры по её предотвращению.

3) Комплексные Решения: Президент России Владимир Путин выделил необходимость комплексных решений для противодействия правонарушениям в цифровой среде, включая систему обмена информацией об угрозах и приоритетное внедрение отечественного программного обеспечения.

4) Обучение и Переподготовка Специалистов: Следует обратить особое внимание на подготовку и переподготовку специалистов, способных работать с цифровыми технологиями и противодействовать киберпреступности.

5) Определение Ключевых Мер Защиты: Национальная стратегия должна определить основные меры защиты личности, общества и государства от преступных посягательств в цифровой среде.

---

[1] Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общей редакцией О. С. Капинус. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. С. 900.

6) Развитие Нормативно-Правовой Базы: Необходимо реформировать уголовное законодательство и нормативную базу для адекватного реагирования на вызовы цифровой эпохи, включая регулирование отношений в сфере робототехники, больших данных, искусственного интеллекта.

7) Формирование Системы Криминологической Безопасности: Создание системы, обеспечивающей бесперебойность, надежность и защищенность важных инфраструктур, является ключевым для поддержания уровня криминологической безопасности.

8) Мониторинг и Профилактика: Важно не только реагировать на преступления, но и активно применять меры по их предупреждению, включая мониторинг финансовых операций и использование современных технологий для блокировки подозрительных действий.

Реализация этих мер требует скоординированных усилий различных государственных органов, правоохранительных структур и образовательных учреждений, а также активного вовлечения общества в процесс обеспечения кибербезопасности.

Эффективное противодействие цифровой преступности и обеспечение криминологической безопасности в эпоху цифровой трансформации общества требуют комплексного подхода, включающего следующие ключевые аспекты:

1) Образовательные Программы: В Академии управления МВД России и других вузах МВД внедряются новые дисциплины, такие как "Цифровая криминология" и "Противодействие преступлениям, совершаемым с использованием криптовалюты". Эти курсы направлены на повышение квалификации сотрудников в области борьбы с цифровой преступностью.

2) Технологическое Оснащение: Сотрудникам правоохранительных органов необходимо предоставить доступ к передовым технологиям, таким как блокчейн, BigData и искусственный интеллект, для повышения эффективности раскрытия и предотвращения преступлений.

3) Экспертное Сопровождение: Важную роль играет экспертная поддержка на всех этапах расследования, особенно в случаях транснациональной организованной преступности.

4) Модернизация Автоматизированных Систем: Необходимо обновить и расширить функционал существующих автоматизированных систем для более эффективного предотвращения и выявления преступлений.

5) Взаимодействие с Частным Сектором: Сотрудничество с операторами связи, интернет-провайдерами, социальными сетями и мессенджерами, а также банковскими учреждениями критически важно для оперативного получения необходимой информации.

6) Международное Сотрудничество: Важность международного взаимодействия усиливается в условиях глобализации цифровых преступлений, требуя координации усилий на международном уровне.

Эти меры направлены на создание комплексной системы борьбы с цифровой преступностью, адаптированной к современным условиям и вызовам, обеспечивающей защиту интересов государства, общества и личности в цифровом пространстве.

Для эффективного обеспечения криминологической безопасности в сфере цифровых технологий, особенно в контексте снижения криминологических рисков и угроз, необходимо принять следующие меры:

1) Создание Устойчивой Системы Цифровой Безопасности: Эта система должна быть независимой и целостной, способной обеспечивать эффективную работу по предотвращению и реагированию на киберугрозы.

2) Совершенствование Нормативно-Правовой Базы: Необходимо обновить законодательство для более эффективного предупреждения преступлений, использующих цифровые технологии, а также регулирования самих технологий.

3) Системный и Комплексный Подход: Подход к криминологической безопасности должен быть всесторонним и включать различные уровни

деятельности, от мониторинга и анализа до активного противодействия и реагирования на угрозы.

4) Противодействие Различным Видам Преступлений: Это включает в себя борьбу с терроризмом, экстремизмом, коррупцией, незаконным оборотом наркотиков и оружия, а также другими преступлениями, совершаемыми с использованием цифровых технологий.

5) Международное Сотрудничество: Эффективное взаимодействие с международными организациями, такими как Интерпол и Европол, критически важно для комплексного реагирования на криминологические угрозы.

6) Взаимодействие на Межведомственном и Внутриведомственном Уровне: Сотрудничество с организациями, обеспечивающими информационную безопасность, финансовыми учреждениями, операторами связи и интернет-провайдерами, является ключевым для оперативного обмена информацией и принятия решений.

7) Непрерывное Профилактическое Воздействие и Виктимологическая Профилактика: Постоянное предотвращение преступлений и осведомленность населения о рисках в сфере цифровых технологий через инновационные каналы криминологической пропаганды[1].

Эти меры помогут формировать устойчивую и эффективную систему обеспечения криминологической безопасности, способную адаптироваться к быстро меняющемуся цифровому ландшафту и предотвращать широкий спектр киберугроз.

Для повышения информированности населения о преступлениях, совершаемых с использованием цифровых и телекоммуникационных технологий, и для снижения рисков, особенно среди уязвимых групп, таких как старшее поколение и подростки, необходимо принять следующие меры:

[1] Криминология. Особенная часть : учебник для вузов / Ю. С. Жариков, В. П. Ревин, В. Д. Малков, В. В. Ревина. — 2-е изд. — Москва : Издательство Юрайт, 2023. С. 172.

1) Разработка Программы Виктимологической Профилактики: Использование СМИ, мессенджеров и других платформ для распространения информации о киберугрозах и методах защиты.

2) Создание Правовых Групп в Мессенджерах: Проведение просветительской работы, разъяснение уголовно-правовых аспектов цифровых преступлений и повышение осведомленности общества.

3) Организация Вебинаров и Информационных Сессий: Обучение населения основам информационной безопасности и предоставление практических советов по защите от киберпреступлений.

4) Формирование Цифровой Гигиены Среди Несовершеннолетних: Обучение подростков основным правилам безопасности в интернете и социальных сетях.

5) Распространение Информационных Памяток: Публикация и распространение памяток с рекомендациями по безопасному использованию интернета и социальных сетей в общественных местах.

6) Организация Встреч Сотрудников ОВД с Населением: Проведение встреч для обсуждения вопросов кибербезопасности и предоставление конкретных рекомендаций по предотвращению преступлений в цифровой среде.

7) Подготовка Правил Безопасности для Использования Интернета и Социальных Сетей: Предоставление четких инструкций о том, как избежать рисков при использовании интернета и социальных сетей.

8) Проведение Мероприятий по Предупреждению Преступлений: Организация образовательных и профилактических мероприятий для повышения осведомленности о киберугрозах.

9) Принцип Приоритета Защиты Личности: Сосредоточение усилий на защите основных прав и свобод граждан, уделяя особое внимание индивидуальной криминологической защите.

10) Исследование Уровня Защищенности Населения: Анализ текущего состояния информированности населения о киберугрозах и определение наиболее эффективных методов повышения их безопасности[1].

Эти меры помогут снизить риски и повысить уровень безопасности населения в условиях цифровой трансформации, а также предотвратить распространение киберпреступлений.

В контексте криминологической безопасности, защищенность является ключевой правовой категорией, подразумевающей состояние защиты от различных угроз. Определение защищенности тесно связано с восприятием гражданами уровня безопасности своих жизненно важных интересов от негативных факторов криминогенной и криминальной природы. Важно отметить, что обеспечение защищенности личности от криминальных угроз и рисков — это приоритетная задача государства.

Мониторинг криминологической обстановки играет критическую роль в обеспечении криминологической безопасности в сфере цифровых технологий. Этот мониторинг должен проводиться с применением передовых цифровых технологий, включая искусственный интеллект и Big Data, что позволит анализировать большие объемы информационных данных. Результаты мониторинга дают возможность прогнозировать развитие преступности и определять эффективность мер по обеспечению криминологической безопасности.

Однако, существующие практики мониторинга и прогнозирования в системе МВД России могут быть недостаточно эффективными, часто носят фрагментарный и формальный характер, и не всегда учитывают полную картину криминогенной ситуации. Важно обратить внимание на уровень латентности и организованности преступлений, а также на социально-экономические и политические процессы, влияющие на преступность.

---

[1] Лунеев, В. В. Криминология : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. С. 741.

Применение результатов прогнозирования в условиях цифровой трансформации поможет более эффективно устранять криминологические риски и угрозы, формируя основу для разработки стратегий и мер по обеспечению криминологической безопасности. Это подразумевает комплексный анализ состояния преступности, обеспечения общественной безопасности, миграционных процессов и других аспектов, важных для разработки эффективных мер противодействия преступности.

В свете текущих вызовов, особенно в период пандемии COVID-19, анализ и прогнозирование криминологической ситуации становятся еще более важными. Результаты таких исследований должны активно использоваться для разработки эффективных стратегий и программ, направленных на укрепление криминологической безопасности на национальном и международном уровне.

Усиление деятельности правоохранительных органов в сфере совершенствования средств противодействия преступности, связанной с цифровыми технологиями, сопровождается активным вовлечением частного сектора в процесс обеспечения цифровой безопасности. Ключевым трендом здесь является использование интегрированных систем безопасности, способных автоматически собирать, сопоставлять и анализировать данные из множества источников для эффективного обнаружения и реагирования на угрозы, включая хакерские атаки.

Особое внимание следует уделить вопросам конфиденциальности, которая должна стать фундаментальным элементом корпоративной стратегии каждого юридического субъекта. Согласно консалтинговой компании Gartner, необходимо разработать централизованную модель управления информационной безопасностью, охватывающую все аспекты хранения и обработки данных.

Эффективность обеспечения криминологической безопасности возможна только при комплексном подходе, который включает в себя как модернизацию корпоративных информационно-цифровых систем, так и активное взаимодействие с правоохранительными органами. К примеру, сотрудничество

со службами безопасности крупных банков, таких как Сбербанк, может играть значительную роль в противодействии цифровой преступности.

Одним из важнейших аспектов национальной безопасности государства в современных условиях становится обеспечение криминологической безопасности в сфере цифровых технологий. В этом контексте требуется разработка и реализация стратегических направлений, направленных на поддержание социально значимого уровня криминологической безопасности. Эти направления должны включать ревизию законодательства, мониторинг уголовного законодательства, мониторинг финансовых операций, использование криминологической экспертизы, эффективное противодействие угрозам и их последствиям, виктимологическую профилактику и снижение криминологических рисков и угроз[1].

Важным элементом является также мониторинг криминологической обстановки, который поможет определить реальное состояние криминологической безопасности и создать новые направления деятельности для ее обеспечения. Эта деятельность должна строиться на основе тесного взаимодействия всех правоохранительных органов и коммерческих структур с опытом в области противодействия цифровой преступности.

[1] Лунеев, В. В. Курс мировой и российской криминологии в 2 т. Том 1. Общая часть в 3 кн. Книга 3 : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. С. 251.

§ 3. Деятельность органов внутренних дел по обеспечению криминологической безопасности в сфере цифровых технологий

Исследование проблем обеспечения криминологической безопасности в сфере цифровых технологий в контексте цифровой трансформации в России подчеркивает необходимость повышения уровня этой безопасности. Для достижения этой цели требуется комплексный подход, включающий упреждающее воздействие, профилактику преступлений и адаптацию к новым технологическим вызовам.

Органы внутренних дел, как одни из ключевых субъектов в обеспечении криминологической безопасности, имеют широкий спектр задач, включая противодействие преступности и охрану общественного порядка. Однако, в свете быстрого развития цифровых технологий, возникает необходимость расширения их полномочий и компетенций, особенно в контексте преступлений, связанных с использованием цифровых технологий.

В этом контексте следует акцентировать внимание на:

1) Профилактике преступлений, совершаемых с использованием цифровых технологий, с упором на виктимологическую профилактику. Это особенно важно учитывая рост преступлений против собственности, совершаемых через мобильные устройства и интернет.

2) Организации оперативно-розыскных мероприятий для выявления и пресечения преступлений в сфере цифровых технологий.

3) Профилактике в сфере защиты объектов критической инфраструктуры от хакерских атак и других угроз.

4) Обеспечении оперативного реагирования на инциденты в сфере государственной безопасности[1].

Для эффективного противодействия преступности в сфере цифровых технологий необходима организационно-техническая реорганизация органов

[1] Конев Денис Андреевич СОВРЕМЕННЫЕ ПОДХОДЫ К ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ // Философия права. 2020. С. 10.

внутренних дел. Примером такой работы является создание Управления по борьбе с преступлениями в сфере высоких технологий в МВД России. Это подразделение специализируется на борьбе с преступлениями в сфере телекоммуникаций, компьютерной информации и незаконного оборота радиоэлектронных устройств, что отражает важность адаптации к меняющимся условиям в области цифровых преступлений.

Начало XXI века действительно ознаменовалось значительными изменениями в сфере информационных технологий и интернета, что привело к изменениям в характере и масштабах криминальной деятельности. Распространение интернета, социальных сетей и мессенджеров привело к росту преступлений, связанных с распространением вредоносных программ, хакерскими атаками, хищениями интеллектуальной собственности, а также к появлению преступлений с транснациональным характером.

Реорганизация Управления по борьбе с преступлениями в сфере высоких технологий МВД РФ в Бюро специальных технических мероприятий (БСТМ) является ответом на эти новые вызовы. Это подразделение занимается противодействием преступлениям, связанным с цифровой информацией, а также незаконным оборотом технических средств для негласного получения информации. Важным аспектом деятельности БСТМ является борьба с преступлениями против здоровья несовершеннолетних, включая распространение вредоносного контента в социальных сетях и преступления, связанные с криптовалютами.

Примером международного сотрудничества в области борьбы с киберпреступностью является совместная операция итальянской и российской полиции, направленная на раскрытие сети, занимавшейся распространением детской порнографии и сексуальным насилием над детьми. Этот случай подчеркивает транснациональный характер таких преступлений и необходимость международного сотрудничества для их пресечения.

Таким образом, развитие цифровых технологий и интернета требует от правоохранительных органов новых подходов и методов работы, включая

укрепление международного сотрудничества, для эффективного противодействия преступлениям в сфере цифровых технологий.

Формирование специализированных подразделений в Следственном департаменте МВД России и в Главном управлении по контролю за незаконным оборотом наркотиков (ГУНК МВД России) отражает реакцию на увеличение числа преступлений в сфере цифровых технологий. Отсутствие квалифицированных специалистов в этой области усиливает необходимость в создании подразделений, способных эффективно выявлять и расследовать преступления, совершенные с использованием инновационных технологий, включая незаконный оборот наркотиков и пропаганду в социальных сетях и на темных рынках в интернете (DarkNet).

Противодействие экстремистским и террористическим проявлениям в интернете также является приоритетной задачей для органов внутренних дел. Это требует не только значительных человеческих ресурсов, но и использования передовых технологий, включая искусственный интеллект и обработку больших данных (Big Data), для выявления, раскрытия и расследования преступлений.

Развитие и применение искусственного интеллекта в деятельности органов внутренних дел, как предусмотрено в Концепции научно-технической политики МВД России до 2030 года, включает разработку современных технических средств и специального вооружения, а также совершенствование подготовки и повышение квалификации специалистов[1].

Искусственный интеллект и Big Data будут использоваться для распознавания, классификации объектов и субъектов, выявления аномалий и скрытых связей, а также для цифрового профилирования и выявления оперативно значимой информации. Эти технологии играют ключевую роль в программах обеспечения криминологической безопасности, позволяя

[1] Козаченко, И. Я. Криминология : учебник и практикум для вузов / И. Я. Козаченко, К. В. Корсаков. — Москва : Издательство Юрайт, 2023. С. 173.

эффективно анализировать большие объемы данных и выявлять угрозы в цифровом пространстве.

Использование искусственного интеллекта в деятельности органов внутренних дел, в соответствии с Европейской Этической Хартией, требует учета принципов уважения фундаментальных прав личности, недискриминации, качества и безопасности, прозрачности и пользовательского контроля. Эти принципы крайне важны для эффективного и этичного применения технологий в правоохранительной сфере.

С учетом увеличения количества преступлений, совершаемых с использованием цифровых технологий, МВД России предлагает внедрить модуль "Антимошенник" в своем мобильном приложении. Это позволит блокировать номера, связанные с дистанционным мошенничеством, и предотвратить соответствующие преступления.

Аппаратно-программный комплекс "Безопасный город" является одним из ключевых инструментов обеспечения криминологической безопасности, способствующим решению широкого спектра задач, включая профилактику и раскрытие преступлений.

Биометрическая платформа, создаваемая в рамках системы ИСОД МВД России, улучшит идентификацию физических лиц и неопознанных трупов по различным биометрическим данным, что повысит эффективность правоохранительных органов.

Важным аспектом является и взаимодействие с негосударственными структурами в сфере информационной безопасности, а также с финансовыми учреждениями и провайдерами связи и интернета, что позволит сформировать комплексный подход к противодействию цифровой преступности.

Проблематика контроля за использованием криптовалют в преступных целях также выступает важным аспектом обеспечения криминологической безопасности. Необходима разработка механизмов, позволяющих эффективно отслеживать и пресекать преступные действия, связанные с цифровыми валютами.

В целом, комплексность и постоянное изучение ситуации в обществе, в том числе анализ рисков и угроз безопасности, становятся ключевыми условиями успешного обеспечения криминологической безопасности в сфере цифровых технологий.

Сложности, возникающие при выявлении, пресечении и расследовании преступлений в сфере цифровых технологий, связаны с рядом факторов:

1) Сложности установления IP-адресов и идентификации владельцев криптокошельков: использование зарубежных хостингов, шифровальных программ и серверов-посредников, а также анонимность при регистрации криптокошельков значительно усложняет выявление преступников.

2) Отсутствие механизма взаимодействия с финансовыми организациями и интернет-провайдерами: необходимо улучшить координацию с этими структурами, особенно в контексте транснациональных преступных групп.

3) Быстрота удаления и изменения цифровой информации: в отличие от физических следов, цифровые следы легко удаляются или изменяются, что требует быстрого реагирования и фиксации данных.

4) Проблемы с кадровым обеспечением и технической оснащенностью: недостаток специалистов в информационно-цифровых технологиях и необходимое оборудование являются значительными препятствиями.

5) Отсутствие правового регулирования глобального пространства Интернет: необходимо разработать международные стандарты и нормы для борьбы с цифровой преступностью[1].

Для улучшения ситуации предлагается создать единый реестр регистрации уникальных идентификаторов (MAC-адресов) электронной техники и налаживание взаимодействия между правоохранительными органами и коммерческими структурами, включая финансовые учреждения и интернет-провайдеров. Это позволит повысить эффективность выявления и расследования преступлений, совершаемых в цифровой среде.

---

[1] Пинкевич Татьяна Валентиновна ОБЕСПЕЧЕНИЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ // Вестник Казанского юридического института МВД России. 2022. С. 6-7.

В целом, обеспечение криминологической безопасности в сфере цифровых технологий требует комплексного подхода, включая усиление взаимодействия на ведомственном, межведомственном и региональном уровнях, а также активное привлечение негосударственных структур и общественности к противодействию цифровой преступности.

ЗАКЛЮЧЕНИЕ

В результате проведенного дипломного исследования выявлены следующие ключевые выводы, которые имеют важное значение для понимания современных вызовов в области цифровых технологий и преступности. Прежде всего, цифровая трансформация радикально изменила общественную жизнь, открыв новые горизонты через внедрение цифровых технологий. Эти изменения привели к трансформации природы преступной деятельности, что отражается в возникновении новых форм преступлений и изменении методологии совершения уже известных деяний, включая используемые инструменты и средства. Преступления в сфере цифровых технологий стали представлять собой значительную угрозу национальной безопасности, вызывая обеспокоенность как государственных, так и частных структур. Однако противодействие этим преступлениям осложняется недостатком четкого понятийного аппарата, правовой базы и методических рекомендаций для их расследования, которые все еще находятся в стадии разработки и требуют значительных усилий по их совершенствованию.

Во-вторых, преступления, регулируемые российским уголовным законодательством в данной области, можно условно подразделить на две категории: компьютерные преступления и преступления, совершенные с использованием информационно-телекоммуникационных технологий, включая Интернет. Тем не менее, текущее законодательство не охватывает общественные отношения, складывающиеся в цифровом пространстве, что приводит к необходимости разработки новых нормативно-правовых актов. Виртуальная система взаимодействий требует обновленного правового регулирования, способного адекватно реагировать на современные вызовы. В связи с этим предложено следующее определение преступности в сфере цифровых технологий: объективно существующее общественно опасное социальное явление, представляющее собой систему преступлений, не ограниченных географическими и юрисдикционными границами, обладающих

количественными и качественными характеристиками, совершаемых в виртуальной среде за определенный промежуток времени. К ключевым признакам такой преступности относятся: общественная опасность, противоправность, высокий уровень латентности, значительные социальные последствия, транснациональный и трансграничный характер, использование цифровых технологий при совершении преступлений и их осуществление в виртуальной среде. Эти характеристики требуют особого внимания и комплексного подхода для их изучения и противодействия. Также были раскрыты особенности различных видов данных преступлений, что позволяет более глубоко понять их природу и способы борьбы с ними.

В-третьих, обеспечение криминологической безопасности в сфере цифровых технологий рассматривается как реализация комплекса мер социально-политического, социально-экономического и социально-психологического характера, направленных на поддержание оптимального уровня криминологических угроз для личности, общества и государства. Эти меры включают в себя разработку и внедрение новых технологий для предотвращения и расследования преступлений, повышение уровня образования и информированности населения о рисках и методах защиты, а также совершенствование сотрудничества между различными государственными и частными структурами. Важную роль играет и международное сотрудничество, так как преступления в сфере цифровых технологий зачастую носят транснациональный характер, требующий координации усилий на глобальном уровне. Современная практика показывает, что эффективное противодействие преступности в цифровой сфере возможно только при условии комплексного подхода и активного взаимодействия всех заинтересованных сторон. Таким образом, результаты данного исследования подчеркивают необходимость дальнейшего развития и совершенствования мер по обеспечению безопасности в цифровом пространстве, что будет способствовать защите прав и интересов граждан, а также укреплению национальной безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Официальный интернет–портал правовой информации: [сайт] – URL: http://pravo.gov.ru. – Текст: электронный.

2. Кодекс Российской Федерации об административных правонарушениях: федер. закон Рос. Федерации от 30 декабря 2001 г. № 195–ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 20 дек. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Собр. зак. – 2002 г. – № 1 (часть I), ст. 1.

3. О полиции: федер. закон Рос. Федерации от 7 февраля 2011 г. № 3–ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 28 января 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 2 февраля 2011 г. // Рос. газ. – 2011. – 8 – февраля.

II. Учебная, научная литература и иные материалы

1. Антонян, Ю. М. Криминология : учебник для вузов / Ю. М. Антонян. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 388 с. — (Высшее образование). — ISBN 978-5-9916-4891-2. — URL : https://urait.ru/bcode/534424

2. Афанасьева, О. Р. Криминология : учебник и практикум для вузов / О. Р. Афанасьева, М. В. Гончарова, В. И. Шиян. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 356 с. — (Высшее образование). — ISBN 978-5-534-16560-9. — URL : https://urait.ru/bcode/531286

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

2023. — 165 с. — (Высшее образование). — ISBN 978-5-534-10050-1. — URL : https://urait.ru/bcode/516954

4. Козаченко, И. Я. Криминология : учебник и практикум для вузов / И. Я. Козаченко, К. В. Корсаков. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-06729-3. — URL : https://urait.ru/bcode/511457

5. Криминология : учебник для вузов / В. И. Авдийский [и др.] ; под редакцией В. И. Авдийского, Л. А. Букалеровой. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 301 с. — (Высшее образование). — ISBN 978-5-534-03566-7. — URL : https://urait.ru/bcode/510960

6. Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общей редакцией О. С. Капинус. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 1132 с. — (Высшее образование). — ISBN 978-5-534-09795-5. — URL : https://urait.ru/bcode/517394

7. Криминология. Особенная часть : учебник для вузов / Ю. С. Жариков, В. П. Ревин, В. Д. Малков, В. В. Ревина. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 206 с. — (Высшее образование). — ISBN 978-5-534-00178-5. — URL : https://urait.ru/bcode/532159

8. Лунеев, В. В. Криминология : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. — 686 с. — (Высшее образование). — ISBN 978-5-534-16806-8. — URL : https://urait.ru/bcode/531728

9. Лунеев, В. В. Курс мировой и российской криминологии в 2 т. Том 1. Общая часть в 3 кн. Книга 1 : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. — 291 с. — (Высшее образование). — ISBN 978-5-534-03992-4. — URL : https://urait.ru/bcode/512639

10. Лунеев, В. В. Курс мировой и российской криминологии в 2 т. Том 1. Общая часть в 3 кн. Книга 3 : учебник для вузов / В. В. Лунеев. — Москва : Издательство Юрайт, 2023. — 413 с. — (Высшее образование). — ISBN 978-5-534-03998-6. — URL : https://urait.ru/bcode/512647

11. Решетников, А. Ю. Криминология : учебное пособие для вузов / А. Ю. Решетников, О. Р. Афанасьева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 166 с. — (Высшее образование). — ISBN 978-5-534-01633-8. — URL : https://urait.ru/bcode/510581

12. Хайрусов, Д. С. Криминология : учебное пособие для вузов / Д. С. Хайрусов. — Москва : Издательство Юрайт, 2023. — 95 с. — (Высшее образование). — ISBN 978-5-534-17544-8. — URL : https://urait.ru/bcode/533298

13. Конев Денис Андреевич СОВРЕМЕННЫЕ ПОДХОДЫ К ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ // Философия права. 2020. №4 (95). URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-deyatelnosti-po-obespecheniyu-kriminologicheskoy-bezopasnosti-v-sfere-tsifrovyh-tehnologiy (дата обращения: 26.02.2024).

14. Пинкевич Татьяна Валентиновна ОБЕСПЕЧЕНИЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ // Вестник Казанского юридического института МВД России. 2022. №2 (48). URL: https://cyberleninka.ru/article/n/obespechenie-kriminologicheskoy-bezopasnosti-v-usloviyah-tsifrovoy-transformatsii (дата обращения: 26.02.2024).

15. Шишкин Радий Владимирович ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ // Вестник Уральского юридического института МВД России. 2022. №4 (36). URL: https://cyberleninka.ru/article/n/prestupleniya-sovershaemye-s-ispolzovaniem-tsifrovyh-tehnologiy-problemy-protivodeystviya (дата обращения: 26.02.2024).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

А.Ш. Кахриманов