Краснодарский университет МВД России

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ КИБЕРПРЕСТУПНОСТИ

Методические рекомендации

Краснодар
2024

УДК 343.3
ББК 67.515
О-752

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Авторский коллектив: *Х. А. Аккаева, М. М. Хамгоков, А. М. Арипшев, С. А. Тамбиев, Л. Ю. Канокова*

Рецензенты:
Е. Н. Макарова, кандидат юридических наук (Санкт-Петербургский университет МВД России);
Р. Х. Котепахов (Следственное управление УМВД России по г. Нальчику).

Основные направления совершенствования противодействия
О-752 органов внутренних дел Российской Федерации киберпреступности [Электронный ресурс] : методические рекомендации / Х. А. Аккаева, М. М. Хамгоков, А. М. Арипшев и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2024. – 1 электрон. опт. диск.

ISBN 978-5-9266-2113-3

Рассматриваются способы использования возможностей глобального информационного пространства преступными организациями, раскрываются методы и технологии противодействия им. В целях наглядного восприятия теоретического материала рекомендации содержат иллюстративный материал в виде диаграмм и скриншотов.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.3
ББК 67.515

ISBN 978-5-9266-2113-3

Содержание

Введение

В эпоху глобализации, охватывающей все аспекты функционирования современного общества, наметилась крайняя необходимость адаптации и преобразования общественных отношений. Этот процесс оказывает прямое влияние на деятельность государственных структур, в том числе правоохранительных органов, которые сталкиваются с новыми вызовами и задачами. В связи с этим особое значение приобретают анализ и внедрение опыта международного сотрудничества в сфере борьбы с преступностью, ее новыми формами и проявлениями, что требует пересмотра и адаптации существующих концепций функционирования национальных правоохранительных систем.

Современные условия характеризуются усилением транснациональных преступных связей, что делает традиционные границы государственной юрисдикции менее эффективными в борьбе с преступностью. В этом контексте для правоохранительных органов приоритетным направлением становится не столько карательная, сколько предупредительная и профилактическая деятельность, направленная на обеспечение правопорядка и общественной безопасности. Это подразумевает акцент на предотвращение преступлений, разработку и реализацию мер по борьбе с новыми угрозами, выходящими за рамки традиционной криминальной деятельности.

Киберпреступность является одной из наиболее динамичных и сложных форм транснациональной организованной преступности, активно использующей возможности киберпространства для совершения незаконных действий. Расширение сферы применения информационно-коммуникационных технологий (ИКТ) и увеличение числа пользователей сети Интернет способствуют миграции традиционных видов преступлений, таких как детская порнография, мошенничество и нарушение авторских прав, в виртуальное пространство.

Противостояние киберпреступности – комплексная задача для правоохранительных органов всего мира. К уникальным характеристикам киберпространства относятся:

Проблемы идентификации пользователя. Применение преступниками разнообразных методов для сокрытия личных данных в глобальных сетях значительно усложняет процесс их идентификации и отслеживания действий правонарушителей.

Отсутствие понимания индивидуальной безопасности в Интернете. Многие пользователи не осознают потенциальные угрозы, что делает их уязвимыми перед атаками, основанными на методах социальной инженерии.

Горизонтальная структура и децентрализованность Сети. Особенности архитектуры Интернета ограничивают возможности правоохранительных органов в контроле и мониторинге киберпространства, что усложняет расследование преступлений, совершенных онлайн.

Проблема суверенитета. При осуществлении уголовного преследования и расследований в рамках киберпространства возникают проблемы национального суверенитета, поскольку в Интернете данные могут перемещаться через территории множества стран, что затрудняет юрисдикционный контроль и международное сотрудничество.

Актуальность вопроса неравномерной криминализации деяний, совершаемых в киберпространстве, обусловлена масштабами и спецификой киберпреступности на современном этапе. Киберпространство предоставляет преступникам возможности для совершения широкого спектра незаконных действий, целью которых часто является хищение конфиденциальной информации из различных сфер, включая оборонную промышленность, атомную энергетику, банковский сектор и системы государственного управления.

Уникальные вызовы киберпреступности требуют от правоохранительных органов переосмысления традиционных подходов к полицейской деятельности, что предполагает не только разработку и применение новых законодательных и технических инструментов для расследования данных противоправных деяний, но и развитие специализированных навыков работы с электронными доказательствами, а также укрепление взаимодействия с частным сектором.

Для эффективного противодействия киберпреступности на международном уровне необходимо создание правовой базы, обеспечивающей унификацию и согласованность действий в рамках международного сообщества. Это подразумевает:

Разработку и принятие согласованных нормативных правовых актов, регламентирующих использование ИКТ в преступных и других неправомерных целях на региональном и международном уровнях.

Объединение усилий для создания адекватных технических средств, позволяющих оперативно выявлять кибератаки и реагировать на них, что способствует формированию атмосферы доверия и безопасности в киберпространстве.

Разработку минимальных стандартов безопасности и процедур аккредитации для программного обеспечения и систем, что позволит минимизировать риски использования ИКТ в преступных целях.

Кроме того, важным аспектом является повышение компетенций государственных служащих в области кибербезопасности, что не только обеспечивает защиту государственных информационных ресурсов, но и способствует созданию устойчивых систем государственного управления, способных противостоять угрозам киберпространства.

Таким образом, международное сотрудничество и координация усилий в области кибербезопасности являются ключевыми факторами в борьбе с киберпреступностью, требующими комплексного подхода и активного взаимодействия всех заинтересованных сторон.

1. Развитие киберпреступности в современной экономике

Интернет сегодня является неотъемлемой частью повседневной жизни, охватывая все аспекты от профессиональной деятельности до досуга. Параллельно с положительными аспектами его использования, всемирная сеть стала мощным инструментом в руках преступников, предоставив им возможности для разработки и реализации сложных схем совершения преступлений в киберпространстве. Эволюция информационных технологий упростила процессы обмена, поиска и сбора информации, что, в свою очередь, способствовало возникновению и бурному развитию киберпреступности.

Киберпреступность, характеризующаяся использованием цифровых технологий для совершения незаконных действий, приобрела глобальные масштабы, причиняя экономике ущерб на сотни миллиардов долларов ежегодно. В настоящее время киберпреступления становятся все более распространенными, сопровождаясь значительными незаконными финансовыми оборотами, достигающими триллионов долларов. Таким образом, задачи обеспечения информационной и кибербезопасности выступают в ряду приоритетных для большинства государств.

Российская Федерация также сталкивается с растущими вызовами киберпреступности, что подчеркивает актуальность и важность развития и совершенствования нормативно-правовой базы в этой сфере. Киберпреступность для России представляет сравнительно новую угрозу, требующую детального изучения и адаптации существующих законодательных механизмов к новым вызовам. Проблематика киберпреступности для России имеет двойной характер: внутреннее увеличение объемов таких преступлений и участие российских хакеров в крупнейших мировых киберпреступлениях, что ставит перед страной задачу не только борьбы с киберпреступностью внутри государства, но и необходимость участия в международном сотрудничестве для противодействия транснациональным киберугрозам.

Деятельность в сфере киберпреступности часто носит организованный и транснациональный характер, что делает ее

одним из наиболее сложных вызовов для современных систем правопорядка и безопасности. Система противодействия киберпреступности, хотя и развивается активно, все еще находится на этапе становления и требует комплексного укрепления, включая кадровое наполнение и формирование эффективных механизмов международного сотрудничества.

Высокая социальная опасность киберпреступлений обусловлена их способностью оказывать воздействие на широкий круг лиц в различных странах, что подчеркивает их транснациональный характер. Совершение таких преступлений не знает географических границ, а их последствия могут быть масштабными и непредсказуемыми. В связи с этим, расследование киберпреступлений требует от правоохранительных органов не только знаний уголовного и уголовно-процессуального законодательства, но и глубокого понимания специфики информационных технологий, а также способности применять специальные тактики и методы следственных действий.

Период карантина, вызванного пандемией коронавируса, особенно ярко продемонстрировал активизацию киберпреступников, которые использовали увеличенную зависимость общества от цифровых технологий и удаленной работы для совершения преступлений. Это подчеркивает необходимость в адаптации и развитии системы противодействия киберпреступности к постоянно меняющимся условиям и вызовам современного мира.

Проблематика компьютерных преступлений в современном юридическом поле обусловлена нестабильностью законодательной базы и отсутствием адекватных нормативно-правовых актов, способных охватить широкий спектр действий, относимых к данной категории. В Уголовном кодексе Российской Федерации (УК РФ) наблюдается отсутствие конкретных норм, отражающих все аспекты технологического развития, что существенно ограничивает возможности квалификации и, соответственно, борьбы с киберпреступностью. Сложности возникают не только на этапе идентификации преступлений, но и при их фиксации и преследовании, поскольку многие из них

осуществляются анонимно и не оставляют за собой материальных следов.

Основным инструментом для совершения данных преступных действий выступает интернет, что влечет за собой различные виды преступлений: от хищения финансовых средств с банковских счетов до взлома аккаунтов в социальных сетях и мошенничества с переводом средств на счета злоумышленников. Особую сложность представляет длительный характер некоторых преступлений, а также реализация коротких кибератак, которые могут быть осуществлены с использованием как персональных компьютеров, так и мобильных устройств, при условии доступа в интернет. По статистике, для совершения преступлений через интернет в большинстве случаев (около 55%) необходим доступ к сети.

Преступления в сфере информационных технологий часто связаны с кражей личных данных, что указывает на важность разработки комплексных мер по защите персональной информации пользователей. В этом контексте актуализируется вопрос о создании единого информационного центра, который бы способствовал сбору, анализу и обработке данных о киберпреступлениях. Несмотря на наличие некоторых механизмов учета, существующие системы не охватывают все категории преступлений, ограничиваясь лишь теми случаями, которые удалось зафиксировать правоохранительным органам, и преимущественно касаются локальных нарушений [1].

Киберпреступность представляет собой сферу преступной деятельности, реализуемую в цифровой среде, и характеризуется широким спектром преступных действий, выходящих за рамки использования исключительно компьютерных технологий или вредоносного программного обеспечения. Это понятие охватывает действия, направленные на финансовые махинации, включая кражи и мошенничество, где жертвами могут стать как физические, так и юридические лица, в том числе крупные корпорации и финансовые учреждения.

Преступники, действующие в данной сфере, могут использовать разнообразные средства связи, включая телефоны и интернет, для написания сообщений жертвам или ведения с ними разговоров, а также применять различные программы для

общения. Важно отметить, что для совершения киберпреступлений не всегда требуются сложные технические навыки. Многие преступники обучаются необходимым методам на практике, не имея специализированного образования, и начинают свою деятельность с приобретения или незаконного получения доступа к компьютерам или другим устройствам, способным подключаться к интернету.

Существуют как индивидуальные мошенники, так и высокоорганизованные преступные группы, обладающие специализированными навыками, включая хакерские. Такие группировки способны осуществлять не только простые финансовые махинации, но и проводить более сложные операции, например, взломы сайтов, кибератаки против государственных структур, действия террористического характера, нанесение значительного ущерба экономическим системам и компаниям, а также вред государственным архивам.

Независимо от специфики незаконных действий, осуществляемых преступниками, их активность квалифицируется как подлежащая уголовной ответственности в соответствии с положениями внутригосударственного и международного права. В Российской Федерации, несмотря на отсутствие специфического определения "киберпреступности" в законодательных актах, действия, относимые к данной категории, находят свое отражение в различных статьях Уголовного кодекса РФ. Такой подход обусловлен тем, что интернет и другие информационные технологии выступают в качестве инструментов совершения преступлений, что не требует выделения киберпреступности в отдельную категорию статей УК.

Киберпреступники могут быть мотивированы различными целями, включая политические убеждения и стремление к наживе. Преступления, основанные на личных мотивах, такие как шпионаж и шантаж, встречаются реже, но также представляют значительную угрозу.

Спектр киберпреступлений обширен и включает в себя:

- Фишинг – мошеннические действия с целью получения конфиденциальных данных пользователей.

- Взлом сайтов с использованием подбора паролей.
- Кибершантаж, предполагающий требование передачи средств или иных ценностей под угрозой распространения конфиденциальной информации или блокировки доступа к данным.
- Кибершпионаж, направленный на незаконный сбор информации.
- Распространение вирусов и вредоносного программного обеспечения, в том числе для незаконного доступа к данным и их кражи [16].

Отдельное внимание заслуживают программы, способные не только мешать функционированию зараженного компьютера или устройства, красть данные, но и наносить физический вред системе, вызывая, например, скачки напряжения в электросети, что демонстрирует высокий уровень технической оснащенности и изощренности некоторых видов киберпреступлений.

Фишинг является одним из наиболее распространенных методов, используемых киберпреступниками для получения доступа к паролям и личным данным жертв. Этот метод основан на социальной инженерии и манипуляции, целью которой является обмануть жертву и побудить ее перейти по вредоносной ссылке. В результате перехода по такой ссылке пользователь сталкивается с веб-страницей, внешне максимально приближенной к оригинальному ресурсу, на который он планировал зайти. Далее жертве предлагается ввести личную информацию, такую как логин и пароль, номера банковских карт и другие конфиденциальные данные, в зависимости от того, какую цель преследуют злоумышленники и какой сайт имитируется.

Основная защита от фишинга заключается в повышенном внимании к адресу веб-страницы: даже если он выглядит достоверно, необходимо тщательно проверять URL на предмет незначительных, но критически важных отличий от оригинального адреса сайта. Эти отличия могут включать в себя дополнительные символы, опечатки или изменение доменного имени, которые на первый взгляд могут остаться незамеченными.

Взлом пароля является еще одним методом, часто применяемым для несанкционированного доступа к информации жертв. Преступники используют специализированное программное обеспечение, которое автоматически подбирает пароли, опираясь на алгоритмы брутфорса (перебора возможных комбинаций) или социальную инженерию, когда жертве предоставляется фальшивая веб-страница, мимикрирующая под настоящий ресурс, например, страницу в социальной сети. Введя данные на такой странице, пользователь невольно передает их преступникам [13].

Кибершантаж является формой киберпреступления, при котором вредоносное программное обеспечение используется для блокировки доступа к компьютеру или его файлам с последующим требованием выкупа у владельца за восстановление доступа. Часто для этого применяются так называемые программы-вымогатели (ransomware), которые шифруют данные на зараженном устройстве и требуют оплату за их разблокировку. Данная форма киберпреступления, хотя и не является самой распространенной, представляет серьезную угрозу как для индивидуальных пользователей, так и для организаций всех размеров.

Кибершпионаж, в свою очередь, представляет собой нелегальный доступ к конфиденциальной информации, часто с целью ее копирования или перехвата. Целями кибершпионажа часто становятся крупные компании и государственные организации, чьи данные представляют ценность с точки зрения коммерческой тайны, научных разработок или национальной безопасности.

Киберпреступления можно классифицировать по различным критериям, в зависимости от роли компьютерной техники в преступлении:

Когда компьютер является целью атаки: это включает в себя ситуации, когда устройства инфицируются вирусами или другим вредоносным ПО с целью нарушения их функционирования, кражи данных или установления контроля над устройством.

Когда компьютер используется как инструмент для совершения преступления: например, для распространения вредоносного программного обеспечения, осуществления

незаконных финансовых операций, фишинга, спама и других форм мошенничества.

Финансовые угрозы в киберпространстве часто связаны с риском похищения финансовой информации, включая данные банковских карт, доступы к онлайн-банкингу, электронные кошельки и активы в криптовалютах. Для осуществления таких атак преступники могут использовать различные методы, включая фишинг, спам и распространение вредоносного программного обеспечения. Спам, будучи массовой рассылкой нежелательных сообщений, может содержать вредоносные ссылки или рекламу и стать каналом распространения вредоносного ПО [22; 28].

Банковские учреждения часто становятся целями киберпреступников, стремящихся получить несанкционированный доступ к финансовым данным или осуществить нелегальные финансовые операции. Одним из распространенных методов является попытка создания копии банковской карты для последующего изъятия средств со счета владельца. Эффективная защита клиентов требует комплексного подхода, включая как технологические, так и законодательные меры, направленные на укрепление безопасности финансовых транзакций и данных.

На текущий момент в законодательной сфере наблюдается отсутствие достаточно эффективных механизмов защиты, способных противостоять угрозам киберпреступности в экономической сфере. Используемые программные продукты, хотя и являются важным элементом защиты, не всегда способны обеспечить надежную защиту от хакерских атак.

Социальные сети представляют собой одну из наиболее уязвимых площадок для кражи данных, где преступники могут использовать различные методы для получения конфиденциальной информации без необходимости прямого контакта с жертвой. Мотивация киберпреступлений может быть разнообразной, включая финансовые, политические, террористические и другие неявные мотивы, последние из которых могут не нести прямой угрозы, но способны вызвать значительный вред.

Для повышения уровня безопасности в киберпространстве рекомендуется следовать ряду основных принципов:

- Использование антивирусного программного обеспечения: это основа защиты от вирусов, вредоносного ПО и других угроз.
- Применение сложных паролей: комбинации, включающие буквы, цифры и специальные символы, значительно затрудняют подбор пароля.
- Осторожность с электронной почтой и ссылками: важно избегать открытия спам-сообщений и перехода по подозрительным ссылкам.
- Использование безопасных каналов для передачи данных: защищенные соединения (например, HTTPS) предотвращают перехват данных.
- Проверка адресов сайтов: это помогает избежать попадания на фишинговые сайты, маскирующиеся под легитимные ресурсы [20].

С увеличением числа пользователей интернета наблюдается пропорциональное расширение активности киберпреступности, что ставит перед законодательной и исполнительной властями задачу формирования эффективного ответа на эти вызовы. Ключевой аспект борьбы с киберпреступностью заключается в разработке и внедрении законодательных и нормативных актов, способных адекватно регулировать отношения в киберпространстве, обеспечивать фиксацию и расследование преступлений, а также повышать уровень безопасности в цифровом пространстве.

Важность совершенствования законодательства обусловлена необходимостью адаптации правовой базы к быстро меняющимся условиям киберпространства и технологическому прогрессу. Это включает в себя введение норм, регулирующих такие аспекты, как защита персональных данных, борьба с распространением вредоносного программного обеспечения, фишингом, кибершантажом, а также меры по предотвращению незаконного доступа к информационным ресурсам и системам.

Реализация мероприятий по повышению уровня компьютерной грамотности среди населения и государственных

служащих через организацию образовательных программ, конференций и форумов является еще одним важным направлением в борьбе с киберпреступностью. Такие инициативы способствуют формированию осознанного отношения к информационной безопасности и развитию навыков безопасного поведения в интернете.

Для обеспечения защиты информационных активов организаций, включая банковские учреждения, необходимо проведение регулярного обучения сотрудников, использование актуальных антивирусных программ и привлечение квалифицированных специалистов по IT-безопасности для решения специфических задач в области защиты от киберугроз.

Принятие федеральных законов и внесение изменений в Уголовный кодекс Российской Федерации, например, введение главы 28, специально посвященной преступлениям в сфере компьютерной информации, отражает стремление государства к созданию нормативно-правовой базы, способной эффективно противостоять киберпреступности. Эти меры направлены на защиту как индивидуальных пользователей интернета, так и экономической сферы в целом от вредоносных действий киберпреступников.

В рамках развития законодательных и исполнительных механизмов противодействия киберпреступности в структуре Министерства внутренних дел Российской Федерации были созданы специализированные подразделения, такие как управление "К" и отделы по борьбе с экономическими преступлениями (БЭП МВД РФ).

Научно-исследовательская деятельность и разработка технических средств защиты от киберугроз также играют значительную роль в обеспечении кибербезопасности. В этом плане важную роль играют частные компании, специализирующиеся на исследованиях в области информационной безопасности и разработке программного обеспечения для защиты от вредоносных программ. Примером такой компании является "Лаборатория Касперского", которая занимается разработкой антивирусных программ, систем обнаружения вторжений, фильтрации спама и других средств защиты от киберугроз.

Правильное использование и своевременное совершенствование ИКТ играют важную роль. В РФ разработана стратегия развития информационного общества на 2017–2030 годы[1], кроме этого, принята Доктрина информационной безопасности[2]. Однако, несмотря на это, ряд проблем, связанных с киберпреступностью и противодействием ей, остался [26].

Система правоохранительных органов государства играет ключевую роль в защите страны и ее граждан от преступных посягательств. Эффективность этой системы напрямую зависит от ее развития и способности адаптироваться к новым вызовам и угрозам. Однако, несмотря на достижения в области правоохранительной деятельности, полностью исключить все проблемы невозможно. Сложность решения возникающих вопросов часто требует комплексного подхода и многоступенчатых действий.

Одной из серьезных проблем современности является глобальный рост киберпреступности, усугубляемый бурным развитием информационных технологий. Инновационные технологии, с одной стороны, способствуют прогрессу и улучшению качества жизни людей, с другой стороны, они открывают новые возможности для криминальных элементов, стремящихся использовать их в корыстных целях, включая получение незаконной прибыли и реализацию идеологических или политических амбиций.

Технологический прогресс также обострил необходимость в защите персональных данных, информационной безопасности и соблюдении авторских прав в цифровом пространстве. Хотя многие системы и технологии обладают высоким уровнем защиты от внешних угроз, этого не всегда достаточно для обеспечения полной безопасности данных в условиях постоянно развивающихся методов кибератак.

---

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71570570

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646 [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71456224

Рост числа интернет-мошенников, активное распространение фишинга, кражи данных и кибертерроризма напрямую связаны с массовым внедрением интернет-технологий. По данным отчета Digital, в январе 2020 года количество пользователей интернета достигло 4,54 миллиарда, а к 2021 году это число увеличилось до 4,66 миллиарда человек. Такой рост числа пользователей усиливает потенциальную уязвимость перед лицом киберугроз.

Активное использование интернет-технологий создает условия для киберпреступников совершать действия, нарушающие закон, с минимальным риском обнаружения и возможностью находиться в любой точке мира. Согласно статистическим данным Министерства внутренних дел, наблюдается стремительный рост киберпреступности: в 2019 году было зарегистрировано 294 тысячи таких преступлений, в 2020 году – 572 124, а в 2021 году – 715 155. Эта тенденция имеет несколько объяснений.

Первая причина напрямую связана с пандемией COVID-19, которая привела к массовому переходу компаний на удаленную работу. Многие организации оказались не готовы к адекватной защите данных в новых условиях, что увеличило уязвимость перед киберугрозами. Кроме того, введение карантинных ограничений традиционно сопровождается ростом преступности. Однако, в условиях ограничения передвижения, преступные элементы искали новые сферы для своей деятельности, активно переходя в онлайн.

Второй фактор – отсутствие страха перед возможностью быть пойманным. Злоумышленники уверены в своей анонимности и безопасности, поскольку киберпреступления часто не оставляют за собой физических следов, что затрудняет их расследование и снижает вероятность раскрытия. Это усугубляется сложностью международного сотрудничества в сфере кибербезопасности и недостаточной подготовленностью правоохранительных органов к противодействию таким преступлениям [20].

На современном этапе развития информационных технологий перед исследователями в области кибербезопасности стоит задача фильтрации огромного объема данных для

выявления релевантной информации, способствующей пониманию и анализу киберпреступлений. Эффективное противодействие киберпреступности требует комплексного подхода, включающего анализ актуальных данных, разработку и внедрение мер защиты данных и информационных систем.

Перегрузка информационного поля и распространение ложной информации осложняют процесс идентификации угроз и разработки стратегий их нейтрализации. Интернет, будучи источником значительных возможностей, одновременно порождает риски, связанные с использованием вычислительной техники преступниками для дестабилизации работы государственных органов и дезорганизации информационных систем.

По данным Института статистических исследований и экономики знаний НИУ ВШЭ, динамика киберпреступлений демонстрирует смещение интереса преступников в сторону данных государственных служащих и органов государственной власти, период с2014 по 2021 годы число киберпреступлений в отношении физических лиц уменьшилось в 2 раза, вместе с тем, на органы государственной власти и госслужащих повысилось на 51%, что подчеркивает необходимость усиления защиты данных на государственном уровне.

Низкая раскрываемость киберпреступлений, которая, согласно интервью начальника главного организационного аналитического управления Генпрокуратуры РФ Андрея Некрасова информационному агентству ТАСС, составляет менее 25%, свидетельствует о сложностях в противодействии киберпреступности и выявлении виновных лиц. Это обстоятельство требует усиления мер по предотвращению кибератак и защите информации, а также повышения уровня сотрудничества между отделами информационной безопасности и пользователями.

Создание штабов кибербезопасности в каждом регионе России, как отмечается в отчете пресс-службы министерства цифрового развития, иллюстрирует усилия государства по наращиванию потенциала в области кибербезопасности. Отказ России от присоединения к Европейской конвенции о киберпреступности 2001 года подчеркивает стремление к

самостоятельному формированию правовой базы и механизмов защиты в киберпространстве[1].

Несмотря на непринятие Россией Европейской конвенции о киберпреступности, регулирование ключевых аспектов, определенных документом, продолжается на национальном уровне. Российское законодательство предусматривает уголовно-правовую оценку деяний в сфере компьютерной информации, определяя основания для уголовной ответственности и уголовно-процессуальные механизмы борьбы с киберпреступностью. Это включает в себя меры по сбору доказательств и расследованию преступлений в цифровом пространстве, а также нормы, обеспечивающие эффективную работу правоохранительных органов, в частности Министерства внутренних дел.

В контексте международного сотрудничества Россия выступает за взаимодействие в расследовании киберпреступлений и использовании международного информационного пространства для этих целей, подчеркивая готовность к сотрудничеству в области обмена данными и совместных операций против киберпреступности.

Конвенция о киберпреступности определяет следующие основные виды преступлений, имеющих отношение к использованию информационных технологий:

- Незаконный доступ к компьютерным системам или их частям, акцентируя внимание на противоправность такого доступа.
- Незаконный перехват данных, который не ограничивается способом передачи данных и подчеркивает, что перехватываемая информация не была предназначена для свободного доступа.
- Вмешательство в работу компьютерной системы, включая действия, приводящие к сбоям в работе устройств или к их полному выходу из строя, а также распространение вредоносного ПО.

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: https://base.garant.ru/4089723

- Незаконное использование устройств, охватывающее операции купли-продажи, аренды, изготовления и других форм передачи устройств и программного обеспечения, которые могут быть использованы для совершения преступлений.
- Незаконное владение средствами и устройствами, предусмотренными конвенцией, с целью их использования для совершения преступлений [1; 4].

Стоит обратить внимание на ФЗ № 207 от 29.11.2012 года «О внесении изменений в Уголовный Кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[1]. Он был дополнен ст. 159.6 «Мошенничество в сфере компьютерной информации». Судебная практика по статье 159.6 Уголовного кодекса Российской Федерации (УК РФ), посвященной мошенничеству в сфере компьютерной информации, демонстрирует значительное разнообразие в толковании и применении данной нормы. Это разнообразие подчеркивает сложности, с которыми сталкиваются обвинение и судебные органы при попытках корректно истолковать и применить законодательство в контексте киберпреступлений. Различное понимание положений данной статьи может приводить к неоднозначности в судебных решениях и, как следствие, к неопределенности в правоприменительной практике.

В связи с этим возникает необходимость в разъяснении данной нормы со стороны Верховного Суда Российской Федерации, что может способствовать унификации подходов к рассмотрению дел, связанных с киберпреступностью. Кроме того, потребуется анализ существующей нормативной базы и возможное внесение изменений для обеспечения более четкого понимания и эффективного применения законодательства в сфере борьбы с киберпреступлениями.

Рост интернет-преступности, увеличение ее уровня и квалификации преступников, разработка новых методов обхода защитных механизмов и сокрытия следов деятельности требуют от правоохранительных органов постоянного совершенствования

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федер. закон от 29.11.2012 № 207-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_138322

подходов к обеспечению безопасности в киберпространстве. Преступники эксплуатируют уязвимости в защите информационных систем, направляя свои усилия как на личные данные граждан, так и на государственные органы и крупные предприятия, что влечет за собой серьезные финансовые потери и угрозу общественной безопасности.

Предупреждение киберпреступлений является одним из наиболее эффективных методов борьбы с данным видом преступной деятельности. На бытовом уровне это может включать использование безопасных практик в интернете, таких как ограничение доступа к потенциально опасному контенту и активация детских режимов на устройствах для защиты малолетних пользователей. На государственном уровне в Российской Федерации необходимо применение специализированных программ и технологий для мониторинга и предотвращения кибератак, а также развитие международного сотрудничества в сфере кибербезопасности для обмена опытом и информацией о новых угрозах и методах их нейтрализации.

Учитывая значительный рост киберпреступности на глобальном уровне, необходимость в разработке и внедрении эффективных ответных мер становится очевидной как на национальном, так и на международном уровне. Принятие и адаптация национальных законодательств к современным вызовам цифровой эры играют ключевую роль в создании надежной правовой основы для борьбы с киберпреступностью.

Анализ сущности киберпреступности, включая ее причины, виды и особенности, является фундаментальным этапом в разработке стратегий противодействия. Изучение фундаментальных основ киберпреступности позволяет выявить наиболее уязвимые аспекты информационной безопасности и разработать целенаправленные меры для их укрепления [29; 30].

Для эффективной защиты государственной безопасности и личных данных граждан государство должно оперативно реагировать на угрозы в киберпространстве, стремясь предотвратить киберпреступления до их совершения. В этом контексте можно выделить несколько ключевых направлений действий:

- Ужесточение контроля за информационными системами, включая те, которые используют зарубежное программное обеспечение и размещены на территории СНГ. Такой подход требует международного сотрудничества и обмена информацией между странами для эффективного мониторинга и реагирования на киберугрозы.
- Ужесточение уголовного наказания за киберпреступления, в том числе предусмотрение ответственности для провайдеров за ненадлежащее хранение информации, что может привести к утечке или распространению данных, содержащих государственную или коммерческую тайну.
- Повышение уровня квалификации и информационной грамотности сотрудников организаций через проведение специализированных обучающих программ и мероприятий по информационной безопасности.
- Увеличение финансирования для компаний, занимающихся разработкой антивирусного программного обеспечения и других средств защиты от вредоносного ПО и кибератак. Это включает в себя поддержку инновационных проектов и исследований в области кибербезопасности.

Международное сотрудничество, обмен опытом и лучшими практиками в области кибербезопасности, а также разработка общих стандартов и норм являются неотъемлемой частью глобальной стратегии борьбы с киберпреступностью. Только через совместные усилия государств, международных организаций и частного сектора возможно достижение значительного прогресса в обеспечении безопасности киберпространства.

2. Криптопреступность как новый вид киберпреступности: специфика и проблемы

Активное внедрение современных технологий в мировую экономику значительно трансформировало процессы проведения финансовых операций, расчетов и инвестиций. Инновационные решения, такие как блокчейн и криптовалюты, обеспечивают ускорение и упрощение транзакций, а также открывают новые возможности для экономического роста и развития. Электронные платежные системы и бухгалтерская отчетность стали неотъемлемой частью современного финансового мира, привлекая значительные инвестиции и способствуя оптимизации экономических процессов.

Однако, наряду с прогрессом, возрастает и угроза киберпреступности, которая представляет собой значительный вызов для глобальной финансовой безопасности. Преступники, используя передовые технологии, осуществляют атаки на финансовые организации, личные счета граждан, совершают мошеннические действия, что приводит к незаконному изъятию значительных сумм денег. Такие действия не только наносят ущерб отдельным лицам и организациям, но и могут подрывать финансовую стабильность на макроэкономическом уровне.

Рост популярности и ценности криптовалют также влечет за собой определенные риски, включая возможное использование в незаконных целях, таких как отмывание денег и финансирование терроризма, что создает угрозы национальной безопасности государств. В этом контексте, стратегия развития информационного общества в Российской Федерации на 2017–2030 годы акцентирует внимание на повышении цифровой грамотности населения и организаций, а также на обеспечении защиты цифрового пространства[1].

Программа "Цифровая экономика Российской Федерации" представляет собой стратегический документ, задающий направление развития информационно-телекоммуникационных

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71570570

технологий в стране. Она охватывает широкий спектр вопросов, от использования криптографических технологий до вопросов кибербезопасности, и направлена на стимулирование развития новых форм экономической деятельности в цифровой сфере. Однако, в процессе реализации данной программы выявляются определенные проблемы и упущения, затрудняющие полноценное развитие цифровой экономики и интеграцию новейших технологий.

Одним из ключевых вызовов, с которыми сталкивается Российская Федерация в контексте цифровизации экономики, является рост киберпреступности, включая преступления, связанные с использованием криптовалют. Эти преступления несут значительные риски для экономической и национальной безопасности страны, поскольку могут привести к крупным финансовым потерям и подрыву стабильности финансовой системы [7].

В мировой экономике наблюдается активное применение технологии блокчейна и криптовалют, что делает эти инструменты привлекательными не только для финансовых организаций, инвесторов и предприятий, стремящихся к инновациям, но и для киберпреступников. Технологические инновации открывают новые возможности для мошенничества, вымогательства и других видов преступной деятельности в сети.

Развитие киберпреступности тесно связано с динамикой технологического прогресса. Современное программное обеспечение, обеспечивающее анонимность в сети и защиту от отслеживания действий пользователя, создает благоприятные условия для нелегальной деятельности, в том числе с использованием криптовалют. Это значительно усложняет задачу по обеспечению кибербезопасности и требует от правоохранительных органов применения новых методов и подходов к расследованию и противодействию киберугрозам.

Международные законодатели сталкиваются с серьезными вызовами в контексте борьбы с киберпреступностью, особенно в сфере финансовых преступлений, связанных с использованием виртуальной валюты. Виртуальные валюты, не имея физического выражения, создают условия для бесконтрольного вывода средств, полученных незаконным путем, из национальных

финансовых систем в электронный вид, что существенно осложняет контроль за их передвижением [21].

Эта ситуация оказывает значительное давление на правоохранительные органы, поскольку выявление и расследование таких преступлений становится крайне затруднительным, а многие из них остаются незамеченными. В этом контексте наука уголовного права стоит перед необходимостью разработки новых теоретических подходов и законодательных механизмов, способных адаптироваться к особенностям цифровой экономики и обеспечить эффективное противодействие преступлениям, связанным с оборотом криптовалют. Важным аспектом является криминализация определенных действий в экономической сфере и установление четких уголовно-правовых последствий за совершение таких преступлений.

Дополнительную сложность представляет транснациональный характер киберпреступлений, где исполнитель может находиться в любой точке мира, совершая преступления в различных юрисдикциях. Отсутствие строгой иерархии в организации таких преступлений, возможность действовать как индивидуально, так и в группе без четко выраженного лидерства, дополнительно усложняет процесс расследования и привлечения к ответственности.

Bitcoin, являясь первой и наиболее значимой криптовалютой на сегодняшний день, зарекомендовал себя как высокоустойчивое и ценное средство сохранения капитала. Ее стоимость и оборот значительно возросли в период карантинных мероприятий, связанных с пандемией COVID-19, что подчеркивает ее привлекательность для инвесторов и состоятельных лиц как альтернативное средство хранения сбережений. Особенностью денежных операций с использованием криптовалюты является их анонимность, что создает благоприятные условия для их использования в незаконных целях, включая оплату запрещенных товаров и легализацию доходов, полученных преступным путем [21].

Развитие криптовалют способствовало появлению нового направления в преступной деятельности – «криптопреступности», которая имеет ряд отличительных особенностей. В частности,

криптопреступления характеризуются дистанционным форматом совершения, при этом все операции проводятся исключительно через интернет с использованием крипто-токенов. Среди основных направлений криптопреступности выделяются легализация незаконного дохода через виртуальные валюты, незаконный оборот запрещенных предметов, таких как оружие, наркотики и детская порнография, а также преступления против собственности, включая хищение криптовалюты.

С 1 января 2021 г. вступил в силу Федеральный закон Российской Федерации № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 года[1]. Этот документ определяет сферу регулирования цифровых финансов и их предмет, а также регулирует выпуск цифровых активов, их применение, обращение с видами валюты. Кроме этого, финансовые отношения регулируются особенной частью Уголовного кодекса РФ[2]: например, в нем есть раздел, посвященный преступлениям в экономической сфере, преступлениям против собственности, общественной безопасности, а также совершаемым в ИТ-сфере (ст. 272, 273, 274).

В современной юридической науке и уголовном законодательстве отсутствует четкое определение понятия «криптографическая сфера» и специфических преступлений, непосредственно связанных с ней. Это создает сложности при квалификации и расследовании деяний, совершенных с использованием криптовалют и других криптографических технологий. Важно подчеркнуть, что экономическая и киберпреступность представляют существенную угрозу для общественной безопасности, причем преступления в сфере компьютерной информации, связанные с использованием криптовалют, отличаются высокой степенью скрытности

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31.07.2020 № 259-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_358753

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699

(латентности), что затрудняет их эффективное выявление и расследование правоохранительными органами [8; 14].

Криптопреступность характеризуется рядом особенностей, отличающих ее от других видов преступлений:

- Международный характер, преодолевающий временные и территориальные границы. Преступник может осуществлять свою деятельность из любой точки мира, используя преимущества анонимности и доступности интернет-технологий.
- Совершение преступлений исключительно в виртуальном пространстве, что предполагает использование крипто-токенов и других цифровых инструментов для осуществления незаконных операций.
- Широкий спектр объектов посягательства, выходящий за рамки традиционной экономической сферы. Криптопреступность может затрагивать как объекты экономической сферы, так и личные данные, авторские права, а также другие цифровые активы.
- Особенная природа криптовалюты, несравнимая с традиционной компьютерной информацией. Это обусловлено анонимностью транзакций, децентрализованной структурой и отсутствием единого регулирующего органа.

Связь между криптопреступностью и экономической сферой весьма тесная, поскольку криптопреступления по своей сути способны наносить значительный финансовый ущерб экономическим и финансовым системам. Нарушение установленного законом порядка работы экономической и финансовой деятельности, осуществляемое по личным мотивам преступников, требует от правоохранительных органов принятия специализированных мер по идентификации и расследованию таких преступлений. Создание специального реестра для учета криптопреступлений, а также сбор специфических доказательств цифрового формата могут значительно улучшить эффективность расследований в данной сфере.

Развитие цифровых технологий и рост популярности криптовалюты, особенно в условиях глобальных карантинных мер, связанных с пандемией Covid-19, выдвигают на первый план вопросы экономической безопасности. Значительное увеличение

стоимости криптовалют, например, биткойна до уровня около 4,5 млн. руб., подчеркивает изменения в экономической системе и повышает риски криптопреступлений.

Карантинные ограничения оказали существенное влияние на мировую экономику, вызвав упадок валютного рынка, снижение уровня жизни в развитых странах и экономический кризис во многих государствах. При этом некоторые отрасли, включая IT-компании, масс-медиа, службы доставок и криптовалютный рынок, нашли способы адаптации к новым условиям, демонстрируя рост спроса и увеличение объемов деятельности.

Биткойн и другие криптовалюты испытали значительный рост стоимости и популярности, превратившись в важное инвестиционное направление на Уолл-стрит, особенно в контексте изменения условий жизни, связанных с пандемией COVID-19. К январю 2021 года стоимость биткойна достигла 40 000 долларов, что привлекло внимание крупных инвесторов и компаний, в том числе тех, кто начал покупку крипто-монет через PayPal [5]. Некоторые страны, включая Сальвадор, взяли курс на официальное признание криптовалюты как платежного средства, что отражает глобальные изменения в финансовой системе.

Официальное признание криптовалюты в качестве платежного средства, по заявлению президента Сальвадора, предполагает равное положение электронной валюты с долларом США и другими иностранными денежными средствами, а также создание специальных криптокошельков для обмена биткойна на доллары и наоборот [5]. Это решение может существенно упростить процесс легализации доходов, полученных незаконным путем, и способствовать росту криптопреступности и киберпреступности на международном уровне.

Признание криптовалюты в качестве законного платежного средства представляет собой двоякий феномен: с одной стороны, это способствует интеграции цифровых валют в мировую финансовую систему и предоставляет новые возможности для экономического развития, с другой стороны, создает условия для расширения масштабов криптопреступности.

Учитывая международный характер криптопреступлений и их высокую латентность, важно разработать международные нормативные акты и механизмы сотрудничества для эффективного регулирования оборота криптовалют и борьбы с преступлениями, связанными с их использованием. Также необходимо усилить меры по информационной безопасности, включая мониторинг и контроль за финансовыми потоками в цифровом пространстве, для предотвращения легализации незаконных доходов и других видов криптопреступлений.

Таким образом, глобальное признание и интеграция криптовалют требуют не только адаптации финансовой системы, но и разработки комплексных мер по обеспечению кибербезопасности и правопорядка в новых условиях цифровой экономики.

3. Кибертерроризм как новый вид киберпреступности: проблемы выявления и расследования

В начале XXI века мир стал свидетелем беспрецедентного развития технологий, включая значительное увеличение мощности вычислительных систем и всемирную доступность интернета. Эти технологические достижения привели к масштабной цифровизации информации, что, в свою очередь, упростило и ускорило многие процессы, связанные с обменом данными. Однако, параллельно с этим, наблюдается и значительный рост преступности в сфере информационных технологий. В частности, это относится к таким явлениям, как кибертерроризм, кибервойны и киберпреступность, которые напрямую связаны с использованием и злоупотреблением технологическими инновациями.

Кибертерроризм характеризуется как деятельность, основанная на идеологии насилия, целью которой является дестабилизация социального порядка и влияние на принятие решений государственными органами через механизмы устрашения. Данное направление преступности осуществляется посредством применения информационных технологий для

осуществления террористических акций в киберпространстве, включая атаки на информационные ресурсы и инфраструктуру.

Отличительной чертой кибертерроризма является его целевая направленность на киберпространство, то есть на сети и системы, которые поддерживают функционирование современного общества. Кибертеррористы, используя методы хакерства и взлома, стремятся внедрить вредоносное ПО, которое способно парализовать работу веб-сайтов, критически важных для функционирования государственного аппарата и экономики, а также запускать автоматизированные атаки, целью которых является блокировка доступа к важнейшим информационным ресурсам.

Кибертеррористические атаки могут принимать различные формы, от распространения вредоносных программ, предназначенных для кражи или уничтожения данных, до организации DDoS-атак (распределенных отказов в обслуживании), направленных на выведение из строя веб-серверов правительственных учреждений. Такие действия не только наносят непосредственный ущерб целевым системам, но и подрывают доверие общества к информационной безопасности в целом [2; 24; 25].

Хакерские атаки и действия кибертеррористов представляют собой серьезную угрозу для общественной безопасности, иногда даже ставя под угрозу жизни людей в зависимости от масштабов и целей совершаемых атак. Методы кибертерроризма включают в себя перехват, модификацию или отключение коммуникационных сигналов, неправомерный доступ к защищенной информации, а также контроль над военной техникой и инфраструктурой. Эти действия обладают потенциалом нанесения значительного ущерба и могут привести к катастрофическим последствиям.

Основные характеристики кибертерроризма включают следующие аспекты:

- Применение информационно-телекоммуникационных технологий: Это основной инструмент кибертеррористов, позволяющий осуществлять атаки на информационные системы, сети и базы данных с целью их дестабилизации или уничтожения.

- Тяжелые последствия действий: Кибертеррористические акты предусматривают достижение определенных негативных последствий, таких как значительный имущественный ущерб, гибель людей или создание угрозы общественно опасных действий. Эти последствия служат демонстрацией мощи и влияния террористических группировок.
- Цели кибертерроризма: Нарушение общественного порядка, нанесение вреда государственным структурам или гражданскому населению, создание атмосферы страха и неопределенности, давление на органы власти с целью вынуждения их к принятию определенных решений, выгодных для террористов.

Современные технологии предоставляют преступникам новые возможности для совершения террористических актов. В частности, развитие информационных технологий позволило преступным группировкам отказаться от традиционных иерархических структур в пользу децентрализованных, что значительно усложняет их идентификацию и преследование со стороны правоохранительных органов. Децентрализация также увеличивает гибкость и адаптивность преступных сетей, позволяя им более эффективно избегать обнаружения и преследования.

Кибертеррористические группировки стремятся к дестабилизации государственного управления и общественной жизни, нацеливаясь на критически важные информационные структуры, компьютерные системы и базы данных. Основная цель этих организаций – нанесение ущерба государственной инфраструктуре, что может привести к серьезным последствиям для национальной безопасности и общественного порядка. Важность таких атак усугубляется потенциальными последствиями для широких слоев населения, включая как отдельные группы граждан, так и общество в целом.

Киберпространство предоставляет террористам уникальные возможности для реализации своих злонамеренных планов. Среди причин, делающих киберпространство привлекательным для террористических группировок, можно выделить анонимность, возможность дистанционного управления атаками, низкий уровень риска для самих преступников, а также

способность наносить значительный ущерб, используя относительно ограниченные ресурсы. Эти факторы делают кибертерроризм одной из наиболее сложных проблем современной международной безопасности.

Методы кибертерроризма могут включать в себя взлом систем управления критической инфраструктурой, распространение вредоносного программного обеспечения, фишинг, атаки на информационные базы данных с целью кражи или изменения данных. Эти действия могут привести не только к непосредственным материальным потерям, но и к долгосрочным негативным последствиям для социальной стабильности и экономического развития.

Особое внимание следует уделить синергетическому эффекту, возникающему при взаимодействии кибертерроризма и физического терроризма. Интеграция усилий в этих двух сферах позволяет преступникам усиливать воздействие своих атак, делая их более разрушительными и труднопредсказуемыми для правоохранительных органов.

Развитие технологий искусственного интеллекта открывает новые горизонты для обработки и анализа больших объемов данных, что, безусловно, является значительным прогрессом во многих областях, включая кибербезопасность. Однако, одновременно с этим, появляются и новые вызовы, связанные с потенциальным использованием ИИ в целях кибертерроризма. Это включает в себя разработку автоматизированных систем для проведения масштабных и высокоэффективных кибератак, способных самостоятельно обходить системы защиты, анализировать уязвимости и адаптироваться к противодействиям со стороны кибербезопасности [3; 6].

Международные террористические организации активно используют интернет и цифровые технологии для реализации своих целей, что включает в себя обмен информацией между филиалами, планирование террористических актов, вербовку новых членов, распространение идеологии, а также использование средств массовой информации для достижения своих стратегических задач. Интернет предоставляет террористам уникальные возможности для осуществления этих

действий на глобальном уровне с высокой степенью анонимности и эффективности.

Мотивация играет ключевую роль в определении уровня риска, который кибертеррористы могут представлять для общества и государственных структур. Мотивация кибертеррористов может варьироваться от стремления распространить определенную идеологию до желания достичь морального удовлетворения от потенциального успеха своих действий. Это разнообразие мотивов делает кибертерроризм особенно опасным и непредсказуемым, поскольку действия, основанные на иррациональных или субъективных убеждениях, могут быть особенно трудными для предотвращения и противодействия.

Выделяют два основных типа целей, преследуемых кибертеррористами:

- Четко определенные цели, такие как пропаганда идеологии или давление на государственные структуры. Эти цели обычно направлены на достижение конкретных, заранее определенных результатов и могут включать в себя акты кибервандализма, кибершпионажа или деструктивные кибератаки на критически важную инфраструктуру.
- Поиск морального удовлетворения от потенциального успеха действий. Такой тип мотивации может быть связан с психологическими аспектами личности преступника, включая стремление к самоутверждению через совершение заметных и шокирующих действий. Эта форма мотивации делает кибертеррористов особенно непредсказуемыми, так как их действия не всегда рациональны и могут быть направлены на достижение внутренних психологических целей, а не внешних политических изменений.

Сам термин «кибертерроризм» является предметом активных дискуссий в научном сообществе и средствах массовой информации. Несмотря на широкое использование, не существует универсально признанного определения кибертерроризма, что отражает сложность классификации и оценки киберугроз. Дискуссии вокруг этого термина часто касаются его приложимости, точности и влияния на

общественное восприятие угрозы. Использование термина в СМИ часто направлено на создание эффектного и запоминающегося заголовка.

В анализе коммуникационных стратегий террористических группировок особое внимание уделяется различиям в доступе и использовании платформ для распространения информации. Традиционные средства массовой информации (СМИ), действующие в рамках строгих редакционных и этических стандартов, устанавливают определенные критерии для отбора и публикации материалов. Эти критерии включают проверку достоверности информации и ее соответствие нормам общественной морали и законодательства. В контрасте с этим, цифровые платформы и интернет предоставляют террористическим группировкам возможность обхода традиционных ограничений и создания собственных каналов коммуникации с целевой аудиторией.

Использование интернета террористами открывает широкие возможности для распространения идеологических посланий, вербовки новых членов, планирования и координации террористических актов, а также сбора финансовых средств. Цифровое пространство служит платформой для:

- Распространения идеологии: Создание и публикация контента, направленного на пропаганду радикальных взглядов, привлечение сторонников и формирование общественного мнения.
- Доступ к засекреченной информации: Хакерские атаки и другие формы кибердействий позволяют террористам получать сведения, недоступные широкой публике, включая данные государственных органов и частных компаний.
- Распространение дезинформации: Создание и публикация ложной информации с целью дестабилизации общественной ситуации, подрыва доверия к государственным институтам и международным организациям.
- Вербовка новых членов: Использование интерактивных и мультимедийных ресурсов для привлечения и обучения потенциальных террористов, в том числе через социальные сети, форумы и специализированные веб-сайты.

- Планирование и координация действий: Обмен информацией и координация террористических актов, включая физические атаки и кибертерроризм.
- Сбор средств: Организация кампаний по финансированию террористической деятельности через криптовалюты, онлайн-платежные системы и другие цифровые каналы.
- Управление группами: Эффективное распределение ролей и задач между членами террористических группировок, использование зашифрованных сообщений для защиты от слежки правоохранительных органов [3; 23].

Все чаще в научных кругах можно встретить термин «информационный терроризм». Термин "информационный терроризм" отражает специфическую форму террористической деятельности, основанную на использовании информационных технологий для достижения своих целей. Эта форма терроризма стала возможной благодаря глобализации информационных коммуникаций и широкому распространению цифровых технологий. Информационный терроризм включает в себя различные виды деятельности, направленные на дестабилизацию общества, нарушение функционирования государственных и частных информационных систем, а также манипуляцию общественным сознанием.

Виды информационного терроризма:

- Атаки на информационно-коммуникационные сети: Этот вид включает в себя действия, направленные на разрушение или нарушение работы информационных систем, сетей передачи данных и критически важной инфраструктуры. Целью таких атак является создание хаоса, нарушение жизненно важных функций общества и экономики, что может привести к значительным материальным и моральным потерям.
- Использование интернета для поддержки террористической деятельности: Включает в себя различные формы использования цифровых технологий террористами для финансирования своей деятельности, вербовки новых членов, обучения, планирования и координации террористических актов. Интернет предоставляет террористам удобный инструмент для

общения на глобальном уровне, облегчая распространение идеологии и координацию действий.

- Психологическое давление и манипуляция информацией: Осуществляется через распространение пропагандистских материалов, дезинформации и провокационных сообщений с целью воздействия на общественное мнение, создания атмосферы страха и неопределенности. Жертвами такого воздействия могут стать как отдельные лица, так и целые социальные группы.

Особенности информационного терроризма включают в себя его анонимный и трансграничный характер, что значительно усложняет процесс идентификации и привлечения к ответственности его исполнителей. Также стоит отметить высокую степень его эффективности и относительно низкие затраты по сравнению с традиционными формами терроризма.

Активное использование интернета экстремистскими и террористическими группировками выступает как один из ключевых факторов их оперативной деятельности в современном мире. Интернет предоставляет этим группировкам возможности для расширения своего влияния за пределы традиционных географических и физических барьеров, позволяя им осуществлять действия, направленные на дестабилизацию политических систем отдельных государств, в том числе Российской Федерации.

Методы действий экстремистов в интернете включают:

- Атаки на информационно-коммуникационные системы: Проникновение в системы управления критически важной инфраструктуры, включая транспортные и государственные учреждения, что создает угрозы как для функционирования этих систем, так и для безопасности граждан.
- Пропаганда через интернет-сайты и социальные сети: Распространение идей насилия, подрыва авторитета государства, продвижение экстремистских установок. Несмотря на включение таких сайтов в реестры запрещенных материалов и блокировку доступа к ним, преступники находят способы обхода блокировок, создавая новые страницы и используя анонимайзеры и сеть Tor для скрытого доступа.

- Использование социальных сетей для вербовки и распространения материалов: Личные страницы и группы в социальных сетях становятся инструментом для вербовки новых членов, распространения пропагандистских материалов и призывов к экстремистской деятельности. Это позволяет террористам формировать сообщества единомышленников, координировать свои действия и обмениваться информацией.
- Использование видеохостингов: Публикация видеоматериалов с целью пропаганды, демонстрации силы и привлечения внимания к своим действиям. Несмотря на усилия администрации видеохостингов по удалению экстремистского контента, террористы продолжают загружать новые видео, используя сложности контроля и модерации в цифровом пространстве [2; 24].

Таким образом, интернет представляет собой мощный инструмент в руках террористических группировок и экстремистских организаций, обеспечивающий им возможности для широкомасштабного воздействия на общественное мнение с относительно низкими затратами ресурсов. Эта технология позволяет осуществлять информационное противоборство, влияя на большое количество людей и проводя комплексные информационные кампании с минимальной вероятностью обнаружения организаторов и исполнителей действий.

Преимущества интернета для террористических и экстремистских организаций:

- Многофункциональность и интерактивность: Интернет позволяет использовать разнообразные форматы контента, включая текст, изображения, видео и аудио, что делает коммуникацию более эффективной и позволяет взаимодействовать с аудиторией напрямую. Это способствует активному участию пользователей в процессе восприятия информации, что повышает эффективность пропагандистских и агитационных сообщений.
- Целевая аудитория и персонализация: В отличие от традиционных СМИ, интернет предоставляет пользователям возможность самостоятельного выбора контента, что позволяет экстремистским группировкам таргетировать свои сообщения на

конкретные социальные группы или индивидуумов, предрасположенных к их идеологии.

- Сложность контроля и анонимность: Интернет облегчает анонимное распространение идеологических материалов и координацию действий, усложняя процесс идентификации и преследования организаторов экстремистской деятельности со стороны правоохранительных органов.
- Воздействие на общественное сознание: Пропаганда и информационное воздействие через интернет могут исказить восприятие реальности у массовой аудитории, создавая предвзятые мнения и стимулируя социальные напряжения. Это влияет на объективность восприятия информации и может способствовать дестабилизации политической обстановки в государстве.
- Использование пропаганды политическими силами: Не только террористические группировки, но и некоторые политические движения могут прибегать к экстремистским методам информационного воздействия с целью подрыва доверия к действующей власти и манипулирования общественным мнением в пользу своих интересов. Эти действия могут включать целенаправленные атаки на государственные институты и использование интернета для распространения дезинформации и подрывных идей.

Информационно-психологическое воздействие, основанное на распространении слухов и создании инфоповодов, представляет собой значимый инструмент в современной информационной войне. Такое воздействие способно индуцировать состояние общественной тревоги, страх, панику и даже истерию среди населения. Используемая в этом контексте информация часто касается чрезвычайных событий, таких как эпидемии, дефицит товаров, военные действия или технологические катастрофы.

Механизмы информационно-психологического воздействия включают создание и распространение так называемых информационных вирусов, которые представляют собой недостоверные или искаженные сведения, целью которых является негативное влияние на социальное сознание и

поведение. Примером такого воздействия может служить реакция населения на пандемию COVID-19, когда распространение непроверенной информации приводило к массовым покупкам и созданию необоснованного дефицита товаров.

Риски, связанные с распространением фальшивых новостей, усугубляются тем, что многие веб-платформы и социальные сети не осуществляют должной проверки информации и не придерживаются научной терминологии, что облегчает восприятие и распространение недостоверных данных среди широкой аудитории. Простота подачи и отсутствие аналитической обработки способствуют тому, что такая информация легко принимается за достоверную.

Динамика распространения дезинформации обусловлена также некоординированной работой СМИ, стремлением к сенсациям и отсутствием ссылок на проверенные источники. Использование вымышленных экспертных мнений и ссылок на несуществующие авторитеты создает иллюзию достоверности и подкрепляет эффект от информационного воздействия.

Здесь террористические и экстремистские организации находят благодатную почву для манипуляции общественным сознанием, используя информационное поле для распространения своих идеологий, дестабилизации общественного порядка и подрыва доверия к институтам власти. Фейковые новости и информационные провокации могут служить инструментом для усиления социального напряжения и создания условий, благоприятных для достижения целей этих организаций [25].

В современной информационной среде наблюдается явление, известное как "инфодемия", характеризующееся распространением большого объема недостоверной информации, что способствует созданию альтернативного восприятия реальности. Это явление обостряется при дефиците проверенной информации, когда средства массовой информации (СМИ) начинают опираться на непроверенные источники, домыслы и субъективные мнения отдельных лиц и журналистов, которые затем сами превращаются в источники так называемой "информации". Такой контент часто противоречит официально предоставленным данным и может нести в себе деструктивный

потенциал, воздействуя на общественно-политический строй и формируя отрицательное восприятие решений государственной власти. Таким образом, инфодемия нередко приобретает черты информационного терроризма.

Информационный терроризм проявляется через создание альтернативных реальностей, искажение и неполное представление информации, когда определенные факты демонстрируются, в то время как другие умышленно скрываются. Это приводит к значительному расхождению между реальной ситуацией и ее восприятием обществом, способствуя формированию основанных на заблуждениях мнений и убеждений.

Сложность борьбы с информационным терроризмом заключается в невозможности полного контроля за распространением недостоверных данных и деятельностью СМИ в глобальной сети. Эта проблема становится особенно актуальной для Российской Федерации и других государств, стремящихся обеспечить национальную безопасность, поскольку информационный терроризм способен подорвать стабильность и целостность общественного строя.

Расширение влияния террористических группировок через использование интернета увеличивает их способность к осуществлению как информационных, так и физических актов террора. Для террористов глобальная сеть является инструментом достижения широкой огласки и привлечения внимания к своим действиям, что делает информационный терроризм эффективным средством воздействия на общественное мнение и политические процессы.

Разработка эффективных стратегий противодействия информационному терроризму требует комплексного подхода, включающего усиление мер по верификации информации, повышение медиаграмотности населения, развитие правовых и технологических механизмов контроля за распространением контента в интернете, а также международное сотрудничество в области обмена данными и координации действий по борьбе с трансграничными информационными угрозами.

Как мы уже отмечали, развитие информационных технологий оказывает значительное влияние на современное

общество, преобразуя многие аспекты жизни, включая способы коммуникации, доступ к информации и выполнение финансовых операций. Интернет стал фундаментальным элементом в повседневной жизни, предоставляя пользователю широкие возможности для обмена данными, взаимодействия и управления собственными ресурсами. Однако эти же возможности создают условия для развития и адаптации террористических и экстремистских группировок к новым технологическим условиям.

Террористы используют прогресс в сфере информационных технологий для обеспечения конспирации своих действий, координации атак и анализа результатов совершенных операций. Последовательный анализ и устранение ошибок, выявленных в ходе предыдущих акций, позволяют преступным группировкам повышать эффективность своих действий и избегать обнаружения со стороны правоохранительных органов.

В этом плане ключевой задачей для системы обеспечения национальной безопасности и правоохранительных органов является разработка и внедрение адаптивных механизмов противодействия кибертерроризму. Это предполагает создание гибкой и динамичной системы реагирования, способной оперативно адаптироваться к изменениям в методах и тактиках действий террористических группировок.

Акты кибертерроризма представляют собой сложный многокомпонентный процесс, который охватывает широкий спектр действий, начиная от пропаганды и заканчивая непосредственным выполнением террористических актов с использованием цифровых технологий. Эти действия осуществляются с использованием переносной незарегистрированной техники и частных серверов, что обеспечивает высокую степень анонимности и затрудняет идентификацию и преследование преступников.

Этапы осуществления кибертеррористической деятельности включают:

- Пропаганда: Использование онлайн-платформ для распространения идей и привлечения новых членов. Эффективность этого этапа обусловлена доступностью и

широким охватом аудитории в интернете, где террористы могут использовать видео, аудио, текстовые сообщения и социальные сети для поддержания связей и налаживания коммуникаций.

- Финансирование: Поиск финансовых ресурсов также происходит через киберпространство с использованием онлайн-платежных систем и коммерции. Террористы могут использовать легальные и подложные сайты для совершения финансовых операций, маскируя их под обычные коммерческие транзакции.
- Подготовка: Интернет предоставляет возможности для обучения новобранцев, включая доступ к материалам по созданию взрывчатых веществ, оружия и методикам проведения атак. Существуют специализированные онлайн-платформы и форумы, где обмениваются знаниями и опытом в области террористической деятельности.
- Планирование: Цифровые технологии упрощают координацию и планирование атак, позволяя террористам находиться в постоянном контакте друг с другом, независимо от географического расположения. Используются зашифрованные сообщения, специальные программы и социальные сети для обмена информацией и разработки планов действий.
- Выполнение: Все перечисленные выше этапы способствуют реализации намеченных террористических актов. Кибертеррористы используют преимущества анонимности и сложности выявления для осуществления атак на информационные системы, в том числе на правительственные ресурсы и критически важную инфраструктуру.
- Кибератаки: эта деятельность нашла отражение в УНП ООН, хотя и не стала предметом прямого обсуждения, а лишь стала темой для будущего изучения [2; 23].

Сегодня, в современной юридической и криминалистической науке акцентируется внимание на растущей сложности борьбы с киберпреступностью, которая обусловлена не только необходимостью применения высокотехнологичных методов и инструментов, но и постоянным совершенствованием преступниками своих технических и программных средств. Это ведет к увеличению их способности действовать анонимно и разрабатывать инновационные способы совершения

правонарушений. Такая динамика развития киберпреступности создает серьезные препятствия для правоохранительных органов, которые сталкиваются с трудностями в обеспечении оперативного и эффективного расследования преступлений в киберпространстве. Особенно это касается необходимости иметь высококвалифицированный персонал и современное техническое обеспечение, наличие которых не всегда гарантировано.

Расследование преступлений, осуществляемых международными группами хакеров, требует особо высокого уровня профессиональной подготовки следователей и наличия специализированного, часто дорогостоящего оборудования, доступ к которому имеется не во всех подразделениях. Длительность таких расследований может значительно превышать два месяца, что добавляет дополнительные сложности в привлечение виновных к ответственности.

Важным аспектом в правовом регулировании киберпреступности является отсутствие в законодательстве унифицированного определения киберпреступления, что затрудняет классификацию и квалификацию таких деяний. Вместо этого, законодательные акты оперируют рядом терминов, которые фактически выступают синонимами правонарушений в области информационных технологий, что требует дополнительной юридической интерпретации и уточнения.

Помимо этого, существует проблема формирования альтернативных информационных реальностей через социальные медиа, которые используют интерактивные подходы и могут способствовать распространению недостоверной информации и манипуляции общественным сознанием. Это создает дополнительные вызовы для правоохранительных органов, так как киберпреступники могут использовать такие платформы для координации своих действий, вербовки новых членов и распространения манипулятивных техник влияния на общество.

Таким образом, анализ действий террористических организаций в современной информационной эпохе показывает их активное использование компьютерных технологий не только для проведения кибератак, но и для координации своих действий, вербовки новых членов, распространения идеологических постулатов и управления деятельностью групп. Инструментарий

цифровых технологий позволяет этим организациям осуществлять атаки на государственные и частные телекоммуникационные системы, облегчает обмен конфиденциальной информацией и способствует расширению их влияния за пределы физических границ.

В этой связи, вопросы кибербезопасности выходят на передний план в политических и стратегических дискуссиях на международном уровне. Создание и реализация национальных стратегий кибербезопасности становятся ключевым элементом обеспечения национальной безопасности и защиты критически важной инфраструктуры. Наличие таких стратегий позволяет странам систематизировать подходы к защите от киберугроз и координировать усилия в рамках международного сотрудничества.

Трансграничный характер киберпреступности делает уязвимыми все секторы, подключенные к глобальной сети. Это обуславливает необходимость комплексного подхода к обеспечению кибербезопасности, включающего в себя не только национальные усилия, но и активное международное сотрудничество. Преступники, действующие из-за рубежа, могут использовать передовые технологии для реализации своих замыслов, что делает задачу их противодействия особенно сложной.

Зависимость критически важных инфраструктур от международных информационных систем и сервисов подчеркивает риски, связанные с возможностью их дестабилизации. В этом контексте особое внимание уделяется защите IT-платформ, обеспечивающих работу критически важных секторов экономики, в том числе:

- Международные платформы и программное обеспечение, формирующие основу глобальных информационных инфраструктур;
- Сервисы, гарантирующие функционирование и безопасность сетевых взаимодействий;
- Системы обмена финансовыми сообщениями, такие как SWIFT;
- Инфраструктура сотовой связи;

- Системы сертификации и шифрования, обеспечивающие защиту передаваемой информации;
- Глобальные логистические цепочки поставок ПО и технологического оборудования;
- Методы обработки и хранения данных, соответствующие международным стандартам безопасности.

Таким образом, в условиях глобализации и все возрастающей зависимости от цифровых технологий, международное сотрудничество и согласование действий в области кибербезопасности приобретают решающее значение. Это требует не только разработки и внедрения национальных стратегий, но и активного обмена информацией, технологиями и лучшими практиками между государствами для создания устойчивой и безопасной глобальной информационной среды.

4. Способы защиты финансов от киберпреступности

Вступление России в систему глобальных цифровых сетей, включая механизмы передачи данных и инфраструктурные решения, обеспечивает стране возможность интеграции в мировое информационное пространство. Это способствует проведению разнообразных операций в сети интернет с высокой скоростью обработки информации. Тем не менее, данный процесс сопровождается повышенными рисками в области кибербезопасности, поскольку международная интеграция усложняет задачу обеспечения данных надежной защитой от внешних угроз, используя исключительно национальные ресурсы.

Данная ситуация акцентирует важность разработки и внедрения унифицированных международных стандартов в области криминалистики, которые бы регулировали процессы сбора, передачи, хранения и аутентификации данных. Эти стандарты должны учитывать требования к обеспечению высокого уровня защиты информации, которая может быть использована в качестве доказательств в уголовном процессе или в других юридически значимых ситуациях.

Проникновение информационных технологий во все сферы жизнедеятельности общества, включая бытовую технику и устройства, подключенные к интернету, а также массовое использование социальных сетей, увеличивает уровень киберугроз. Взаимодействие людей в цифровом пространстве, несмотря на его удобство и способность преодолевать географические барьеры, создает благоприятные условия для деятельности киберпреступников. Социальные сети становятся ареной для мошенников, террористов и других злоумышленников, нацеленных на незаконное получение доступа к личной информации пользователей с целью совершения преступлений, включая доступ к финансовым ресурсам жертв [1; 4; 12].

Пандемия COVID-19 стимулировала массовый переход многих аспектов общественной жизни в виртуальное пространство, что привело к значительному увеличению численности пользователей интернета. Всемирная сеть стала неотъемлемой частью повседневной деятельности большинства людей, обеспечивая не только возможности для коммуникации и доступа к информации, но и поддерживая функционирование профессиональной деятельности, образовательного процесса и торговли. В связи с этим, даже те группы населения, которые ранее ограничивали использование цифровых технологий, были вынуждены адаптироваться к новым условиям, что неизбежно сопряжено с повышением рисков стать жертвами киберпреступлений из-за отсутствия достаточного уровня компьютерной грамотности.

Экспансия интернет-пользователей и их ограниченные знания в области кибербезопасности создают благоприятные условия для киберпреступников, которые ищут возможности для незаконного доступа к персональным и финансовым данным, а также осуществления атак, целью которых является извлечение прибыли. Следственно, расширение диапазона и сложности киберпреступлений требует от правоохранительных органов адаптации существующих подходов к борьбе с такими угрозами и развития новых механизмов реагирования.

Однако, несмотря на усилия правоохранительных органов, существует ряд препятствий, затрудняющих эффективное

противодействие киберпреступности. В частности, высокая техническая оснащенность преступников и их способность быстро адаптироваться к изменениям в сфере кибербезопасности приводят к тому, что многие преступления остаются нераскрытыми. Преступники используют продвинутые методы для сокрытия следов своей деятельности или успевают их уничтожить до того, как информация о преступлении достигнет компетентных органов, что в свою очередь увеличивает сложность расследований и приводит к необходимости сокращения времени бюрократических процессов.

В области кибербезопасности выделяются различные методики и стратегии, применяемые преступниками для незаконного доступа к личной информации пользователей или для непосредственного мошенничества. Ниже приведены наиболее распространенные виды кибератак и мошеннических действий:

- Фишинг представляет собой технику обмана, направленную на незаконное получение конфиденциальных данных пользователя, таких как идентификационные номера, пароли, пин-коды, паспортные данные и другую чувствительную информацию. Злоумышленники создают поддельные интернет-ресурсы, визуально схожие с легитимными сайтами, но имеющие незначительные отличия в доменном имени. Пользователи, вводя свои данные на таких сайтах, невольно передают их преступникам.
- Мошенничество при онлайн-покупках заключается в создании фиктивных интернет-магазинов или товарных предложений, где потребителям предлагается оплатить товары или услуги, которые затем не доставляются или оказываются существенно отличными от ожидаемых.
- Взлом аккаунтов в социальных сетях используется для незаконного доступа к чужим аккаунтам с целью дальнейшего мошенничества, например, запросов денежных средств у друзей жертвы под видом срочной помощи.
- Мошенничество с фальшивыми уведомлениями о поступлении денег вводит в заблуждение жертв, уведомляя их о якобы поступивших средствах на счет, с требованием оплаты

комиссии для их получения, что ведет к перечислению денег мошенникам без реального поступления средств.

- Создание поддельных государственных сервисов является методом, при котором злоумышленники имитируют официальные государственные ресурсы для обмана пользователей с целью получения доступа к их личной и финансовой информации, включая данные банковских карт.
- Мошенничество с лотереями и выигрышами заключается в обещании жертвам крупных выигрышей в несуществующих лотереях, конкурсах или викторинах, с требованием оплаты за доставку приза или предоставления данных банковской карты для перевода выигрыша [9; 31].

В рамках современных экономических и социальных процессов, а также в свете ускоренной цифровизации общественной жизни, мошенничество в интернете приобретает все более разнообразные и изощренные формы. Особое внимание заслуживают схемы, появившиеся с 2022 года, когда физические лица привлекаются к участию в мнимых проектах. В таких случаях мошенники могут перечислить небольшую сумму денег на счет жертвы, создавая видимость доверительных отношений и вовлекая ее в роль инвестора, после чего проект внезапно "исчезает", оставляя жертву без вложенных средств.

Другим распространенным методом является использование социальной инженерии, когда злоумышленники, выдавая себя за сотрудников правоохранительных органов или финансовых институтов, убеждают жертв совершить перевод средств под предлогом их "защиты" от предполагаемых киберугроз. Такие действия неизменно приводят к потере финансовых средств потерпевшими.

Анализируя ситуацию в Российской Федерации, можно отметить, что уровень финансовой безопасности вызывает определенные опасения среди специалистов, стремящихся усилить защитные меры в сфере кибербезопасности. Проблема киберпреступности остается актуальной для многих государств, включая Россию, где она демонстрирует высокие темпы роста и сложность в идентификации и преследовании преступников. Эффективность противодействия киберпреступности осложнена

глобальным характером интернета, позволяющим злоумышленникам оперировать из любой точки мира, а также постоянным совершенствованием их методов и инструментов, включая специализированное программное обеспечение и технические средства. Это не только облегчает совершение преступлений, но и создает значительные препятствия для их раскрытия и расследования.

Преступления в информационной сфере представляют серьезную угрозу как для индивидуальных граждан, так и для национальной безопасности государства. В соответствии с пунктом 1 статьи 159 УК РФ, мошенничество определяется как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Несмотря на отсутствие в УК РФ специфического определения киберпреступности, подразумевается, что к ней относятся преступления, осуществляемые с использованием информационно-телекоммуникационных технологий.

Киберпреступления обладают рядом характеристик, затрудняющих их расследование традиционными методами. Во-первых, они часто не оставляют физических следов, что усложняет сбор доказательств. Во-вторых, преступник может находиться в значительном удалении от места совершения преступления, включая возможность его пребывания в другой юрисдикции. Это создает дополнительные препятствия для правоохранительных органов, связанные с необходимостью международного сотрудничества и экстрадиции.

Отмечается, что интервал времени между совершением киберпреступления и моментом его обнаружения может быть значительным, в течение которого следы преступления могут быть утрачены или уничтожены. Специалисты прогнозируют усиление тенденции к росту киберпреступности, что делает эту проблему еще более актуальной для будущего.

Распространение удаленной работы и использование домашних компьютерных сетей, как правило, характеризующихся более низким уровнем защиты по сравнению с корпоративными сетями, увеличивает уязвимость потенциальных жертв кибератак. Отсутствие на домашних компьютерах качественных антивирусных программ и широкое

использование социальных сетей для личного общения открывают дополнительные возможности для злоумышленников реализовывать мошеннические схемы, включающие непосредственное взаимодействие с жертвами.

В корпоративной среде ограничения на использование социальных сетей и личных коммуникаций в рабочее время могут способствовать снижению риска киберугроз, однако это не исключает необходимость внедрения комплексных мер по обеспечению кибербезопасности, включая обучение сотрудников основам безопасного ведения дел в интернете, использование современных средств защиты информации, а также разработку и реализацию стратегий реагирования на инциденты в области кибербезопасности [12].

Исследование, проведенное среди интернет-пользователей, направленное на выявление их опыта взаимодействия с мошенничеством в сети, демонстрирует значимость проблемы киберпреступности. В ходе социального опроса, в котором участвовало 132 человека, было установлено, что большинство респондентов (59,8%) сталкивались с действиями мошенников в интернете. При этом 20,5% участников опроса подверглись обману, а 15,9% не сталкивались лично с мошенниками, но знают о подобных инцидентах, произошедших с их знакомыми. Относительно небольшой процент участников (3,8%) не сталкивались с киберпреступностью.

Анализ видов мошенничества, с которыми сталкивались респонденты, показывает, что наибольшую долю составляет интернет-мошенничество (34,8%), за ним следует мошенничество с банковскими картами (25,8%), использование мошеннической рекламы (14,4%) и схемы, реализуемые с применением смартфонов (16,7%).

Из всех опрошенных лишь 6,1% обратились за помощью в правоохранительные органы, тогда как подавляющее большинство (84,8%) не стали обращаться с заявлением. Такое поведение может быть обусловлено скептицизмом в эффективности расследований или недостаточной осведомленностью о процедуре обращения за помощью.

Опрос также выявил обеспокоенность участников по поводу защищенности банковских карт. 43,2% считают, что необходимо

разработать дополнительные меры защиты, в то время как 28% высказались за необходимость проведения просветительской работы среди населения. Меньшая доля респондентов (18,9%) убеждена, что существующих мер защиты достаточно, при условии более внимательного отношения пользователей к предложениям в интернете.

Относительно защиты личных данных и посещения ненадежных сайтов, большинство респондентов (40,9%) указали, что посещают только проверенные и надежные интернет-ресурсы. Тем не менее, значительная доля участников опроса выразила уверенность в своей способности самостоятельно справиться с мошенниками (45,5%), в то время как 33,3% планируют обращаться за помощью в полицию в случае необходимости.

Отношение пользователей к безопасности интернет-покупок с использованием банковских карт выявляет значимые аспекты восприятия кибербезопасности в современном обществе. Согласно проведенному опросу, большинство респондентов (81,8%) выразили готовность совершать покупки в интернете через официальные сайты, что свидетельствует о доверии к установленным механизмам защиты на таких платформах. Однако 12,1% участников опроса не считают интернет-пространство достаточно надежным для проведения финансовых операций, а 5,3% полагаются на систему безопасности своего банка для защиты средств.

Статистические данные, относящиеся к 11 месяцам 2021 года, демонстрируют масштабы проблемы телефонного мошенничества, в результате которого граждане потеряли более 45 миллиардов рублей. Учитывая, что мошенники атаковали каждого седьмого жителя страны и что большая часть жертв добровольно перечислила деньги и информацию злоумышленникам, обозначается критическая необходимость повышения финансовой и компьютерной грамотности среди населения.

Потери, которые мошенники могут нанести одному потерпевшему, варьируются, в среднем составляя около 15 000 рублей, однако зафиксированы случаи, когда сумма ущерба достигала нескольких миллионов рублей, с максимальной

зафиксированной суммой в 25 миллионов рублей. Эти данные подчеркивают серьезность финансовых последствий мошенничества для жертв.

Для эффективного противодействия киберпреступности важно принимать комплексные меры, направленные не только на ужесточение ответственности для преступников, но и на повышение уровня информированности и грамотности населения в области финансовой безопасности и безопасного поведения в интернете. Это включает в себя разработку и реализацию образовательных программ, направленных на улучшение понимания рисков и методов защиты личных и финансовых данных в цифровом пространстве, а также на формирование критического отношения к различным предложениям и запросам, поступающим через интернет и мобильные коммуникации [10; 11].

5. Уголовная ответственность за несанкционированное изменение критической информационной инфраструктуры Российской Федерации

Постепенный переход общества к цифровой экономике сопровождается возрастающей ролью информационных технологий, которые находят отражение в развитии самых разных сфер деятельности. Внедрение ИТ открывает широкий спектр возможностей, от минимизации промышленных затрат до наращивания объемов производства. При этом подавляющее большинство внедряемых технологий базируется на заграничных инновациях, что обуславливает некоторую степень их уязвимости. Наибольший интерес с этой точки зрения вызывает их применение на объектах, которые относятся к критической информационной инфраструктуре (в дальнейшем по тексту – КИИ).

Для создания стабильно действующей системы КИИ законодательные органы предприняли комплекс соответствующих мер. Так, чтобы обеспечить для нее безопасное

и полноценное функционирование с защитой от компьютерных атак, был разработан Федеральный закон №187 «О безопасности КИИ РФ» от 26 июля 2017 года. Данный нормативно-правовой акт содержит определение данного понятия, формулируя его как перечень объектов КИИ и сетей электросвязи, необходимых для организации внутренних связей между ними. Иначе говоря, законодательная суть этих объектов выражается через инфосистемы, информационно-телекоммуникационные и автоматизированные сети для управления. Сфера эксплуатации таких объектов весьма обширна, они встречаются в следующих направлениях:

- Медицина и здравоохранение.
- Наука и техника.
- Транспорт.
- Связь.
- Финансы и экономика.
- Атомная энергетика.
- Оборонная промышленность.
- Ракетостроение.
- Горнодобывающая отрасль.
- Металлургия.
- Химическое производство.

Повышенное значение объектов КИИ обусловлено тем фактом, что нарушение их стабильного функционирования способно стать причиной серьезных последствий. Пояснительная записка к законопроекту делает акцент на том, что компьютерная атака при ее правильном планировании и реализации может на 100% остановить работу государственных КИИ, что приведет к катастрофе в общественной, экономической или финансовой сфере. Борьба с противоправными действиями подобного рода предусмотрена дополнением ФЗ № 194 «О внесении изменений в УК РФ» и ст. 151 УПК РФ за счет ст. 2741, которая затрагивает вопросы неправомерного воздействия на КИИ в государстве. Последняя вошла в состав гл. 28 4 раздела «Преступления, направленные против общественной безопасности и социального правопорядка». Хотя после включения новой статьи уже прошло определенное количество времени, а судебная практика

понемногу накапливается, правоприменение сопровождается рядом трудностей, а разъяснений ВС РФ еще не поступало.

Структура статьи 2741 характеризуется довольно высоким уровнем сложности, поскольку в ней объединено сразу несколько составов преступлений, рассматриваемых уголовным законодательством. Подобный прием обычно свойственен характеру описания признаков, свойственных конкретному деянию, но не отдельной норме. Статья обозначает наступление уголовной ответственности в случае трех форм противоправного посягательства на КИИ:

- Несанкционированный доступ.
- Разработка и распространение вредоносного ПО.
- Несоблюдение требований по применению, обработке и распространению данных.

В качестве непосредственного объекта преступной деятельности, рассматриваемой в ст. 272–274 УК РФ, выступают социальные правоотношения, связанные с обеспечением целостного состава и сохранности компьютерных данных; в случае с рассматриваемым преступлением объект будет другим. С учетом того, что функционирование объектов КИИ возможно в разнообразных отраслях, исследователи предлагают несколько подходов к определению того, что может выступать в роли объекта противоправного посягательства.

Предполагается, что в качестве последнего могут выступать правоотношения, нацеленные на соблюдение безопасности КИИ как комплекса объектов повышенной государственной значимости. Подобное определение проистекает из тезисов ФЗ № 187 «О безопасности КИИ в РФ» от 27 июля 2017 года. В этом акте предусмотрена классификация данных объектов по категориям с учетом степени их важности и последовательности учета. Хотя конкретная значимость объектов в ст. 2741 не обозначается с точки зрения квалифицирующего критерия, она может учитываться при подсчете количества последствий и оценивании их масштаба.

В качестве предмета анализируемой преступной деятельности может рассматриваться компьютерная информация, входящая в состав КИИ, а также средства, предназначенные для

ее хранения, обработки и распространения. К этому же списку относятся инфосистемы, телекоммуникационное оборудование, средства автоматизации сети и компоненты электросвязи, которые можно классифицировать как часть КИИ государства. Ч. 1 ст. 2741 УК РФ обозначает наступление уголовной ответственности за разработку, передачу, применение компьютерного ПО и других компьютерных данных, созданных специально для несанкционированного влияния на объекты КИИ.

Обозначение в законодательной отрасли заведомо противоправного назначения подобных программ и информации приводит к появлению вопроса о том, как может быть квалифицировано уже имеющееся ПО, которое предназначено для противоправного уничтожения, блокировки, изменения или копирования информации, а также принудительной остановки инструментов по защите компьютерных данных при влиянии на объекты КИИ. Законодатель не сообщает о принципиальной разнице таких программ, но анализ накопленной судебной практики позволяет прийти к выводу, что преступники применяют вредоносное ПО, созданное не только с прямой целью нанести ущерб структуре КИИ, но и различные инструменты, разработанные для иных задач. Состав по конструкции носит формальный характер, из чего следует, что преступное деяние считается совершенным с момента разработки, передачи или применения подобных программ вне зависимости от результата.

Ч. 2 ст. 2741 УК РФ обозначает факт наступления уголовной ответственности за несанкционированный доступ к компьютерным данным, находящимся под защитой и входящим в состав КИИ, если подобное действие спровоцировало нанесение ущерба. Это позволяет прийти к выводу, что состав преступления носит материальный характер. По отзыву ВС РФ на законопроект «О внесении изменений в законодательные акты РФ…» от 15 мая 2015 года, существует риск применения для квалификации социально опасных последствий в большей степени субъектно-оценочных критериев, что приведет к недостаточно объективному пониманию их значения.

Анализ судебной практики позволяет прийти к выводу, что данные опасения не лишены смысла. В некоторых случаях

судебные органы не уделяют внимания характеру нанесенного ущерба, и в приговоре используются обобщенные формулировки. Размытая трактовка полученного вреда позволяет отнести к противоправным действиям любое деяние, сопровождающееся или выраженное в получении неправомерного доступа к защищенным данным. Предполагается, что относительно изучаемой нормы требуется рассматривать именно причинение материального ущерба, поскольку причинение физического вреда в отношении КИИ требует квалифицировать его по тезисам гл. 21 УК РФ, где рассматриваются преступные деяния, направленные против собственности. Что касается субъективной стороны, то деяние, предусмотренное в ч. 1 ст. 2741, может быть охарактеризовано лишь наличием прямого злого умысла, а преступления в ч. 2 ст. 2741 могут совершаться и косвенно-умышленно. В качестве субъекта рассматривается дееспособное физлицо, возраст которого равен или превышает 16 лет.

Ч. 3. ст. 2741 УК РФ устанавливает уголовную ответственность за нарушение правил обращения со средствами хранения, обработки и распространения компьютерных данных, находящихся под защитой, а также инфосистем, телекоммуникационных сетей, автоматизированных систем для управления и компонентов электросвязи, входящих в состав КИИ, если правонарушение нанесло ущерб объектам последней. Эти правила не отражены в составе ФЗ № 187; вместо этого в законодательстве государства применяется понятие требований по созданию безопасных условий для значимых объектов КИИ. Полномочиями по определению последних обладает государственная служба ФСТЭК.

В тексте приказа ФСТЭК РФ № 275 от 21 декабря 2017 года перечислены конкретные требования, предъявляемые, в частности, к организационной и распорядительной документации, необходимой для обеспечения безопасности важных объектов КИИ. В ее состав должны входить следующие моменты:

- Ключевые цели и задачи обеспечения безопасности для данных объектов.

- Список организационно-технических процедур и действий.
- Актуальные данные о системе безопасности.
- Требования к рабочим обязанностям сотрудников субъектов КИИ.
- Перечень действий сотрудников в случае наступления инцидентов, связанных с компьютерными данными или сетями.

Организационно-распорядительная документация, затрагивающая вопросы безопасности ключевых объектов КИИ, проходит обязательное утверждение руководящим лицом, а затем с ним ознакомляют всех сотрудников субъекта. Итак, в федеральном законодательстве сообщается о необходимости соблюдения требований, а наступление уголовной ответственности совершается при их нарушении, а сами требования определяются руководством субъекта с учетом специфики конкретного рода деятельности. Из этого следует, что каждый субъект обязан заняться разработкой этой документации, состав которой может сильно меняться в зависимости от вида деятельности и с учетом нескольких оснований. К примеру, субъектом деятельности одного объекта может являться государственная структура, а другого — ИП. Правоприменитель всякий раз обязан руководствоваться положениями конкретного документа, чтобы определить основания для соблюдения перечисленных в нем требований.

В список квалифицирующих критериев несанкционированного влияния на КИИ законодательство относит совершение преступного деяния с участием группы лиц в рамках предварительного сговора или в составе организованной группы, а также одним лицом с применением возможностей своего служебного положения (ч. 4 ст. 2741 УК РФ) с проявлением тяжелых последствий (ч. 5 ст. 2741 УК РФ). Как было обозначено выше, подобные результаты могут проявиться в любой отрасли, поскольку классификация объектов КИИ построена на категориях, обладающих конкретной важностью для определенной сферы деятельности. Пояснительная записка к законопроекту «О безопасности КИИ РФ» уточняется, что наступившие последствия могут носить катастрофический

характер. Поскольку КИИ выступает в роли связующего элемента между целой группой секторов национальной инфраструктуры, нанесение ущерба этому звену негативно сказывается и на функциональности этих направлений. Из этого следует, что тяжелые последствия могут найти выражение в критическом повреждении объектов жизнеобеспечения, оборонной отрасли, а это повлечет серьезный ущерб имущественного характера, может спровоцировать массовые смерти граждан. До вхождения ст. 2741 в текст УК РФ в узкоспециализированных источниках литературы указывалось на то, что деятельность преступника в случае совершения противоправного деяния в сфере компьютерных данных, направленного на нарушение безопасности КИИ, квалификация состава должна определяться по совокупности с терактом.

Из вышесказанного можно сделать вывод, что ст. 2741 УК РФ рассматривается как специальная по отношению к ст. 272-274 этого же нормативно-правового акта. Дифференциация уголовной ответственности за несанкционированные действия относительно объектов КИИ возможна в том числе в рамках вышеуказанных статей, однако законодатель выбрал другую стратегию.

Выполненный анализ дает возможность вычленить перечень недостатков действующего законодательства в части ст. 2741 УК РФ, которые способны стать причиной ошибочных действий в современной правоприменительной отрасли. Из этого следует, что законодателю необходимо пересмотреть проблемные места для минимизации подобных рисков.

6. Пути совершенствования мер противодействия киберпреступности органами внутренних дел

Эволюция общественных отношений и технологий оказывает значительное влияние на развитие экономической среды и формы взаимодействия между людьми. В исторической перспективе обмен товаров и услуг проходил эволюцию от натурального хозяйства к использованию денег как универсального средства платежа, что значительно упростило и ускорило процесс торговли. С развитием цифровых технологий финансовая сфера также претерпела значительные изменения, переместившись в виртуальное пространство, что принесло как удобство и доступность для пользователей, так и новые риски, связанные с угрозой кибермошенничества.

Кибермошенничество, как форма преступной деятельности, использует информационно-коммуникационные технологии для незаконного доступа к финансовым средствам или конфиденциальной информации пользователей. Отличительной особенностью такого рода преступлений является их анонимный и трансграничный характер, что затрудняет процесс идентификации и привлечения к ответственности злоумышленников. Киберпреступления могут не оставлять физических следов, а использование различных цифровых платформ и технологий обеспечивает преступникам возможность действовать на значительном удалении от жертв.

В свете постоянного развития и адаптации киберпреступников к новым технологиям, общество и правоохранительные органы сталкиваются с необходимостью постоянного совершенствования методов предотвращения и борьбы с кибермошенничеством. Это предполагает не только разработку и внедрение новых технологических решений для защиты данных и финансов, но и повышение уровня осведомленности граждан о потенциальных угрозах и способах их предотвращения [27].

Возможности для мошенников появляются не только в связи с развитием технологий, но и все большей цифровизации общества, перехода практически всех сфер жизни в цифровой

формат. Способы совершения киберпреступлений постоянно меняются, киберпреступники развиваются, учатся новому, осваивают новые технологии и придумывают новые схемы обмана населения. Президент Российской Федерации издал приказ от 12 апреля 2021 года № 213, утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности[1].

В этом документе перечислены все возможные угрозы МИБ, новый документ существенно расширяет аналогичный старый — Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Указом Президента Российской Федерации от 24 июля 2013 года № Пр-1753)[2]. Например, в нем не только более широкий список возможных угроз, но и совершенно новый подход к пониманию того, что именно можно называть угрозами использования ИКТ в преступных целях.

Чтобы сформировать более четкое представление о том, с какими угрозами приходится сталкиваться органам внутренних дел, занимающихся вопросами ИКТ, следует сперва дать определение самим понятиям «киберпространство» и «киберпреступность». Киберпространство представляет собой виртуальное пространство, возникшее в результате развития и взаимосвязи глобальных информационно-коммуникационных технологий, включая интернет и другие компьютерные сети, которые обеспечивают обмен данными между пользователями по всему миру. Киберпреступность, соответственно, описывает действия, совершенные в киберпространстве с намерением нанесения вреда физическим или юридическим лицам, ущемления их прав и свобод или получения незаконной выгоды за счет использования информационных технологий.

---

[1] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: указ Президента РФ от 12 апреля 2021 г. № 213 [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/400473497

[2] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_178634

Особенностью киберпреступлений является их высокая анонимность и трансграничный характер, что значительно усложняет процесс их выявления, расследования и привлечения виновных к ответственности. Киберпреступности присущи специфические черты, такие как использование сложных технологий для взлома систем безопасности, распространение вредоносного программного обеспечения, фишинг, кража и незаконное использование личных и финансовых данных пользователей, а также атаки на критически важную инфраструктуру.

Проблема законодательного регулирования киберпреступлений заключается в динамичности и постоянном развитии информационных технологий, что требует от законодателя гибкости и способности оперативно адаптировать нормативную базу к меняющимся условиям киберпространства. Существующие законы часто не успевают за темпами развития технологий, что создает пробелы в правовом регулировании и ограничивает возможности правоохранительных органов в борьбе с киберпреступностью.

В современном мире, где информационные технологии играют ключевую роль в жизни общества, киберпространство становится ареной для новых видов преступлений, требующих от правоохранительных органов особого внимания и адаптации существующих методов борьбы с преступностью к условиям цифровой эпохи. В этом контексте особенно важным становится понимание специфики киберпреступности и угроз, характерных для киберсреды:

1. Сложность атрибуции киберпреступлений является одной из главных проблем, с которой сталкиваются правоохранительные органы. Атрибуция, то есть определение источника кибератаки и установление личности злоумышленника, осложняется использованием технологий, обеспечивающих высокий уровень анонимности. Сетевые атаки могут исходить из различных точек мира, при этом маскировка цифровых следов и использование сложных сетевых конфигураций делают процесс установления личности преступника крайне сложным.

2. Непредсказуемость кибератак также является значимой характеристикой киберпреступлений. Злоумышленники способны мгновенно менять тактику и цели своих атак, реагируя на меры кибербезопасности и используя новейшие уязвимости в программном обеспечении и системах безопасности. Эта черта требует от правоохранительных органов гибкости и способности к быстрой адаптации к меняющимся условиям киберсреды.

3. Фрагментация руководства в области кибербезопасности и розыскной деятельности представляет собой вызов в координации между различными уровнями власти и специалистами в сфере информационных технологий. Эффективное решение задач в сфере кибербезопасности требует тесного взаимодействия между правоохранительными органами и IT-специалистами, однако различия в подходах и приоритетах могут затруднять совместную работу и принятие оптимальных решений.

4. Разнородность участников киберпространства делает киберсреду сложной для мониторинга и контроля. Кроме традиционных участников, таких как государственные структуры и частные компании, в киберпространстве активно действуют различные неформальные группы и индивидуальные пользователи, включая хакеров и активистов, которые могут иметь собственные цели и мотивации, не всегда соответствующие закону.

Таким образом, переосмысление традиционных подходов к борьбе с преступностью в условиях информационной эпохи представляет собой важный аспект в деятельности органов внутренних дел. Развитие информационно-коммуникационных технологий (ИКТ) и их интеграция во все сферы жизни общества привели к появлению новых угроз и вызовов, требующих адаптации правоохранительной системы к новым условиям. В этом контексте создание специализированных подразделений, таких как Управление по организации борьбы с противоправным использованием ИКТ в структуре Министерства внутренних дел Российской Федерации, является ответом на углубление проблемы киберпреступности. [7; 24].

Согласно официальной статистике, рост числа преступлений, совершаемых с использованием информационных

технологий, отражает не только интенсификацию преступной деятельности в цифровой среде, но и указывает на проблематику текущего законодательства, не в полной мере отражающего специфику и масштабы киберпреступлений. Отсутствие в законодательстве РФ четко определенного понятия киберпреступности и квалифицирующих признаков осложняет процесс идентификации, расследования и квалификации таких преступлений [33].

Проблематика кибербезопасности охватывает широкий спектр вопросов, от технических аспектов защиты информационных систем до правовых механизмов противодействия киберпреступности. В этом контексте ключевую роль играют правоохранительные органы, задача которых не только в расследовании конкретных преступлений, но и в разработке эффективных стратегий предотвращения кибератак и повышения общественной осведомленности о потенциальных угрозах.

Современная правоохранительная система сталкивается с необходимостью освоения новых методологий и технологий для эффективного противодействия киберпреступности. Это включает в себя не только улучшение технической оснащенности и повышение квалификации персонала, но и разработку международных соглашений и сотрудничество с частным сектором в области обмена информацией о киберугрозах и методах их нейтрализации.

Активное сотрудничество МВД РФ с различными государственными и общественными организациями, включая Роскомнадзор, интернет-провайдеров, Генеральную прокуратуру РФ, а также средства массовой информации, является ключевым фактором в формировании эффективной стратегии борьбы с киберпреступностью. Особую роль в этом процессе играют СМИ, выполняющие функцию информатора и образователя для широкой аудитории, повышая компьютерную грамотность граждан и информируя их о методах и способах защиты от мошеннических действий в интернете.

Одним из ключевых аспектов в повышении эффективности борьбы с киберпреступлениями является решение проблемы кадрового дефицита в органах МВД. Это предполагает не только

набор необходимого числа квалифицированных сотрудников, но и их комплексное обучение современным методам расследования преступлений, совершенных с использованием информационных технологий. При этом стоит учесть, что традиционные методы расследования могут оказаться неэффективными при работе с преступлениями, совершенными в киберпространстве, что делает необходимым внедрение специализированных образовательных программ для подготовки и повышения квалификации как будущих, так и действующих сотрудников органов внутренних дел.

В борьбе с киберпреступностью привлекается широкий круг специалистов не только из МВД, но и из других государственных структур, общественных организаций, а также компаний, предоставляющих услуги в области информационных технологий и связи. Деятельность этих специалистов направлена не только на расследование уже совершенных преступлений, но и на разработку и реализацию мер, направленных на предотвращение и профилактику киберпреступлений. К числу таких мер относятся, например, разработка и внедрение технологий блокировки устройств, используемых преступниками, а также применение средств для подавления радиосигналов и обеспечения безопасности сетевого трафика.

Следует отметить, что применение комплексных мер против киберпреступности в Российской Федерации влечет значительное снижение уровня таких преступлений, что отражается в официальной статистике Министерства внутренних дел. Согласно данным МВД, за первый квартал 2021 года рост киберпреступности составил 33,7%, однако спустя 9 месяцев этот показатель снизился до 11,1%. Это свидетельствует о положительном эффекте от реализации технологических решений и новых алгоритмов, направленных на противодействие цифровым правонарушениям.

Технологические инновации и разработка специализированного программного обеспечения играют ключевую роль в совершенствовании мер по борьбе с киберпреступностью. Внедрение новых алгоритмов и методов обработки данных позволяет не только эффективно выявлять и предотвращать попытки мошенничества, но и обеспечивает

возможность для оперативного реагирования на угрозы безопасности в цифровом пространстве.

Законодательная база Российской Федерации также претерпела изменения в ответ на вызовы, связанные с развитием цифровой экономики. Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» регулирует правовые отношения, возникающие в контексте использования криптовалюты и обращения цифровых финансовых активов, что является значимым шагом в формировании правового поля для цифровой экономики.

Кроме того, Федеральный закон от 1 июля 2021 года № 250-ФЗ вводит запрет на распространение в интернете и других информационно-телекоммуникационных сетях информации финансового характера, содержащей признаки мошеннических действий. Это положение направлено на защиту граждан от распространения недостоверной финансовой информации и снижение риска потерь средств в результате мошеннических схем[1].

В этом проекте учтены современные возможные угрозы в сфере МИБ, уже отражены новые составы преступлений, при которых для достижения преступной цели используются ИКТ. Этот документ позволяет расширить степень взаимодействия между разными странами. Поднимается не только вопрос о правовой помощи, но и выдаче злоумышленников, их арест, розыск и возврат похищенных активов [32].

Эффективное расследование кибермошенничества сталкивается с целым рядом сложностей, присущих специфике цифровых преступлений. Отсутствие материальных следов преступления, сложность криминалистической характеристики действий злоумышленников и разнообразие способов совершения преступлений на расстоянии создают значительные препятствия для правоохранительных органов:

[1] О внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 01.07.2021 № 250-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_358753

1. Отсутствие материального следа является одной из ключевых проблем, так как традиционные методы расследования часто опираются на физические улики, которые могут быть обнаружены на месте преступления или у лица, совершившего преступление. В киберпространстве действия преступников не оставляют таких следов, что требует от следователей высокой квалификации в области информационных технологий и использования специализированного программного обеспечения для анализа цифровых данных.

2. Невозможность криминалистической характеристики действий обусловлена анонимностью и трансграничным характером киберпреступлений. Преступники могут использовать защищенные каналы связи, анонимизаторы и другие технологии, затрудняющие установление их личности и деталей совершенных ими действий.

3. Разнообразие способов совершения преступлений включает в себя такие методы, как вишинг, фишинг, DDoS-атаки и смс-рассылки, каждый из которых имеет свои особенности и требует индивидуального подхода к расследованию. Кроме того, кибермошенники постоянно совершенствуют свои методы, что требует от правоохранительных органов постоянного обновления знаний и технологий для борьбы с ними.

Установление времени и места совершения преступления представляет собой одну из наиболее сложных задач, учитывая, что злоумышленник может находиться в любой точке мира, а его действия могут затрагивать жертв в разных странах. Это требует международного сотрудничества и обмена информацией между различными правоохранительными агентствами.

Эффективное расследование кибермошенничества требует комплексного подхода, включая оперативное взаимодействие между различными службами внутри страны и за рубежом, использование передовых технологий для сбора и анализа данных, а также повышение квалификации сотрудников правоохранительных органов в области информационных технологий и кибербезопасности. Ключевую роль в этом процессе играет качество собранной информации и полнота доказательной базы, что определяет успешность расследования и возможность привлечения преступников к ответственности [19].

Эффективное расследование киберпреступлений требует от правоохранительных органов комплексного подхода и тесного взаимодействия между различными подразделениями МВД и другими службами. Синергия усилий позволяет формировать наиболее полное представление о совершенном преступлении, фиксировать следы деяний в цифровой среде, собирать доказательную базу и определять местонахождение злоумышленников. Временной фактор играет критическую роль: чем раньше будут получены и проанализированы данные о преступлении, тем выше вероятность успешного раскрытия дела.

Методика расследования киберпреступлений включает в себя специализированные подходы к фиксации цифровых следов, которые по своей природе являются нематериальными и могут быть легко уничтожены или искажены. Важно понимать, что цифровая информация сама по себе не может рассматриваться как носитель следов преступления в традиционном понимании, однако она содержит данные, которые могут быть использованы в качестве доказательств.

Тактические приемы и стратегии следственных действий приобретают особое значение в контексте кибермошенничества. Специфика таких преступлений требует от следователей не только юридической подготовки, но и глубоких знаний в области информационных технологий. Отсутствие таких знаний может стать препятствием для эффективного допроса и может дать возможность злоумышленникам использовать свои специализированные знания для введения следствия в заблуждение.

В рамках судебной экспертизы недостаточная компетенция следователей в вопросах кибермошенничества может привести к неправильной постановке вопросов перед экспертом, что, в свою очередь, снижает эффективность экспертизы и может привести к получению недостоверных или не точных выводов.

Решение проблемы эффективного расследования киберпреступлений требует комплексного подхода, включающего в себя как обучение следователей специфическим методикам раскрытия таких преступлений, так и модернизацию технического обеспечения правоохранительных органов. Основополагающим аспектом является повышение

квалификации сотрудников в области кибербезопасности и информационных технологий, что предполагает глубокое понимание устройства киберпространства, особенностей его функционирования, а также специфики кибермошенничества.

Следователям необходимо обладать знаниями, позволяющими эффективно анализировать действия преступников в киберпространстве, правильно формулировать вопросы в ходе допросов и взаимодействия с экспертами, а также грамотно использовать специфическую терминологию. Это потребует не только теоретической подготовки, но и практических навыков работы с цифровыми данными и технологиями.

Улучшение технического обеспечения и создание новых криминалистических лабораторий, способных проводить квалифицированные экспертизы в области кибербезопасности, являются еще одним важным направлением совершенствования системы борьбы с киберпреступностью. Наличие современного оборудования и программного обеспечения позволит проводить более глубокий анализ доказательств и ускорит процесс расследования.

Перегрузка государственных экспертных учреждений и, как следствие, затягивание сроков проведения экспертиз являются серьезной проблемой, осложняющей раскрытие киберпреступлений. Это делает актуальным вопрос разработки и внедрения новых методов и инструментов экспертизы, способных сократить время на анализ и обработку данных.

В свете этих задач крайне важно стимулировать развитие междисциплинарного взаимодействия между правоохранительными органами, научными учреждениями и частным сектором, чтобы обеспечить обмен знаниями и опытом в области кибербезопасности. Кроме того, необходимо акцентировать внимание на разработке и реализации образовательных программ, направленных на подготовку специалистов в данной сфере, что позволит формировать кадровый резерв для эффективной борьбы с киберпреступностью на современном этапе [17; 18].

Итак, опасность киберпреступности в современном мире заключается не только в ее широком спектре действий, но и в

способности злоумышленников воздействовать на критически важные инфраструктуры, переходя из виртуального в физическое пространство. Электронные технологии, обеспечивая анонимность и трансграничный доступ, упрощают достижение целей преступников, в том числе путем взлома банковских счетов и несанкционированного доступа к финансовым ресурсам.

Сложность борьбы с киберпреступностью усугубляется неоднородностью законодательства в различных странах и наличием пробелов в правовом регулировании, что создает условия для безнаказанности злоумышленников. Несмотря на наличие международных соглашений и усилий по созданию единой системы противодействия киберугрозам, не во всех государствах преступления в сфере информационных технологий преследуются с должной строгостью.

Особую проблему представляет высокая степень анонимности киберпреступников, что затрудняет их идентификацию и привлечение к ответственности. Даже в случаях успешного раскрытия преступлений вопрос экстрадиции злоумышленников остается сложным, особенно если речь идет об атаках, совершаемых по заказу или с поддержкой других государств. Это делает международное сотрудничество и диалог в сфере кибербезопасности особенно актуальными, хотя и чрезвычайно сложными для реализации.

Для усиления эффективности борьбы с киберпреступностью необходимо совершенствовать международное правовое поле, обеспечивать постоянное обновление законодательства в соответствии с развитием технологий и углублять сотрудничество между странами в обмене информацией и опытом противодействия киберугрозам. Также крайне важно развивать технологическую базу и повышать компетенции специалистов в области кибербезопасности на национальном и международном уровнях для создания устойчивой и эффективной системы противодействия киберпреступности.

Формирование эффективной правовой основы для борьбы с киберпреступностью требует комплексного подхода, включающего в себя как разработку и совершенствование национального законодательства, так и международное сотрудничество в данной области. Основные направления

правового регулирования в этой сфере должны включать следующие аспекты:

Упорядочение действий в киберпространстве и их подчинение национальному законодательству. Необходимо обеспечить, чтобы все операции, проводимые в цифровой среде, соответствовали установленным правилам и нормам, предусмотренным национальным законодательством, что позволит эффективно пресекать незаконную деятельность в интернете.

Формирование единого мирового понятия киберпреступности. Разработка общепринятого определения киберпреступности является ключевым моментом для международного правового сотрудничества и координации усилий в борьбе с такими преступлениями. Единое понимание позволит синхронизировать законодательные и правоприменительные механизмы разных стран.

Введение специального состава уголовного преступления "киберпреступление" в законодательство. Нормативное закрепление киберпреступлений как отдельной категории в уголовном законодательстве необходимо для четкой квалификации таких деяний и разработки соответствующих мер наказания.

Исследования в области кибербезопасности показывают значительные различия в национальных подходах к обеспечению безопасности информационных инфраструктур и управлению в сфере киберпространства. Тем не менее, существует ряд общих проблем и вызовов, которые требуют скоординированного решения:

- Построение государственной системы управления в сфере кибербезопасности, что предполагает создание эффективной организационной структуры для координации действий различных ведомств и служб.
- Определение и реализация национальной политики кибербезопасности, включая разработку стратегий защиты критически важных информационных инфраструктур и обозначение ролей различных участников в этом процессе.

Различия в понимании кибербезопасности и отсутствие единых международных стандартов затрудняют эффективное обсуждение и реализацию мер по обеспечению безопасности в киберпространстве [5]. В отношении Российской Федерации актуализируется необходимость разработки федерального закона "О кибербезопасности", который бы обеспечил системное регулирование взаимоотношений в сфере киберпространства. Такой закон должен включать положения, направленные на защиту критически важной информационной инфраструктуры, предотвращение кибератак и мошенничества, а также укрепление международного сотрудничества в области кибербезопасности.

Реализация указанных мер требует совместных усилий государства, общественных организаций, бизнеса и международного сообщества, а также постоянного совершенствования законодательства и технологий в ответ на постоянно меняющиеся угрозы в киберпространстве.

Заключение

Анализ современного состояния киберпреступности и мер противодействия, реализуемых органами внутренних дел, выявляет необходимость комплексного подхода к обеспечению информационной безопасности в условиях все более интенсивного проникновения цифровых технологий в различные сферы общественной жизни. На основании изложенного можно сделать следующие основные выводы.

Проникновение цифрового пространства во все сферы общественной жизни приводит к появлению новых форм преступлений, не имеющих географических и физических границ. Это обстоятельство требует от органов внутренних дел разработки и внедрения новых механизмов защиты, способных адаптироваться к постоянно меняющимся условиям киберпространства.

Отличительные черты киберпреступлений, такие как анонимность, сложность атрибуции и высокая технологичность, делают их особенно опасными. Статистика, предоставленная Институтом статистических исследований и экономики знаний (НИУ ВШЭ) и Росстатом, подтверждает смещение фокуса интересов киберпреступников с физических лиц на органы государственной власти, госслужащих и крупные базы данных. Это указывает на необходимость усиления защиты информационных ресурсов государственного сектора и корпоративного сегмента.

Развитие киберпреступности требует от государства не только реактивных мер по расследованию и пресечению уже совершенных преступлений, но и превентивной работы, направленной на предотвращение кибератак, в том числе улучшение технической защиты информационных систем, а также повышение осведомленности граждан и организаций о потенциальных угрозах.

Транснациональность киберпреступности. Одной из ключевых характеристик киберпреступлений является их неограниченность географическими рамками одного государства, что делает их по своей сути международными. Исполнители

могут находиться в одной юрисдикции, а совершать преступления в другой, что затрудняет процесс их идентификации и привлечения к ответственности. Отсутствие четкой иерархии в структуре преступных группировок дополнительно усложняет расследование, так как во многих случаях не существует лидера, ответственного за совершение преступления.

Развитие криптопреступности. Махинации с использованием криптовалюты порождают новую категорию киберпреступлений – криптопреступность. Указанные противоправные деяния характеризуются дистанционным форматом совершения и использованием крипто-токенов. Данная категория преступлений объединяет в себе элементы как цифрового, так и экономического пространства, что требует специализированных знаний и подходов к их расследованию.

Специфика криптопреступлений. Криптопреступности присущи признаки, свойственные нескольким категориям преступлений одновременно, что расширяет традиционные рамки экономических и информационных преступлений. Международный характер, совершение действий исключительно в виртуальном пространстве, а также уникальная природа криптовалют как объекта посягательства обособляют криптопреступность в отдельный класс, требующий особого внимания со стороны законодателей и правоохранительных органов.

В современном обществе на фоне стремительного развития информационных технологий, в том числе мощных вычислительных машин и мировой сети Интернет, произошел значительный сдвиг в парадигме обмена информацией. Этот процесс, несомненно, облегчил и ускорил многие аспекты повседневной жизни, в то же время спровоцировав увеличение преступной активности, особенно в области кибертерроризма. Основополагающей чертой кибертерроризма является идеология насилия, которая используется для устрашения населения, воздействия на государственные структуры и применения различных форм насилия в киберпространстве. Террористы используют киберпространство для разнообразных целей, включая распространение радикальных идей, добычу

конфиденциальной информации, вербовку сторонников, планирование атак и даже управление своими группировками. Это создает значительные вызовы для правоохранительных органов, требующие разработки адаптивных стратегий борьбы с кибертерроризмом, способных быстро реагировать на изменчивость тактик и действий террористических групп.

Одним из наиболее распространенных и опасных видов преступлений в киберпространстве является кибермошенничество, в случаях совершения которого жертва не всегда имеет прямое взаимодействие с преступником, а мошеннические схемы часто автоматизированы. Преступления происходят в виртуальной среде, лишенной определенного места совершения. В силу быстрого темпа развития технологий и их широкого распространения преступники активно адаптируются, осваивают новые методы совершения мошенничества, что приводит к увеличению статистики по таким преступлениям из года в год.

Для противодействия киберпреступности в настоящее время активно мобилизуются специалисты из различных секторов, включая не только сотрудников МВД России, но также представителей других государственных органов, общественных организаций и компаний, занимающихся предоставлением услуг связи. Их деятельность нацелены не только на борьбу с уже совершенными преступлениями, но и на разработку и внедрение мер, направленных на превентивное противодействие подобным деяниям. В рамках этих усилий разрабатываются технические средства блокировки устройств, используемых преступниками, и применяются методы подавления радиоволн в сотовой связи. Благодаря комплексному подходу к борьбе с киберпреступностью с 2021 г. отмечается значительное снижение уровня преступности. Например, по данным МВД России, если на первый квартал 2021 г. отмечался рост преступности на 33,7%, то спустя 9 месяцев этот показатель снизился до 11,1%. В Российской Федерации разрабатываются и активно применяются технологические решения, способные эффективно противодействовать данному виду преступности, они постоянно совершенствуются и дополняются новыми алгоритмами для достижения поставленных целей по снижению уровня преступности.

Множество случаев кибермошенничества остаются нераскрытыми или даже не обнаруживаются. Частично это связано с тем, что обманутые граждане не обращаются в правоохранительные органы. Сложность в борьбе с такими преступлениями обусловлена несколькими факторами, в том числе отсутствием материальных следов, трудностью в криминалистической характеристике действий кибермошенников и многообразием способов и схем совершения преступлений удаленно.

Пункт 3 ст. 2741 Уголовного кодекса Российской Федерации предусматривает уголовную ответственность за нарушение правил обращения со средствами хранения, обработки и распространения компьютерных данных, находящихся под защитой, а также инфосистем, телекоммуникационных сетей, автоматизированных систем для управления и компонентов электросвязи, входящих в состав критической информационной инфраструктуры (КИИ), если правонарушение причинило ущерб этим объектам. Правила, установленные данным законом, не включены в положения Федерального закона № 187. Вместо этого в российском законодательстве используется терминология, касающаяся требований к обеспечению безопасности значимых объектов КИИ. Определение этих объектов и назначение требований по их защите осуществляются Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Особое значение объектов КИИ обусловлено тем, что нарушение их стабильного функционирования способно стать причиной серьезных последствий.

Эффективность раскрытия кибермошенничества в значительной мере зависит от использования тактических приемов при проведении следственных действий. Необходимо отметить, что этот вид преступной деятельности обладает спецификой, требующей особых знаний для его эффективного расследования. Отсутствие таких знаний у сотрудников правоохранительных органов может затруднить выстраивание правильной стратегии допроса, что предоставляет мошеннику возможность ввести следствие в заблуждение.

Литература

1. Антипин Л.А., Криворучко И.С. Кибербезопасность и киберпреступность // Национальная безопасность России: актуальные аспекты: сб. избр. ст. Всерос. науч.-практ. конф. СПб., 2022. С. 10–14.

2. Абазов И.С. О путях противодействия кибертеррористическим угрозам // Журнал прикладных исследований. 2022. Т. 2. № 6. С. 178–181.

3. Арипшев А.М. Кибертерроризм: проблемы в понимании и способах противодействия // Журнал прикладных исследований. 2023. № 4. С. 109–112.

4. Асеев К.Э. Киберпреступность: состояние и проблемы // Экономика и общество: перспективы развития: сб. докладов VI Всерос. науч.-практ. конф. Киров, 2022. С. 28–34.

5. Батуев Т.Б. Криптовалюта как цель и средство совершения преступления // Студенческий. 2019. № 20-5(64). С. 17–20.

6. Брадул Е.В. Кибертерроризм: проблемные вопросы толкования и квалификации // Киберпреступность: риски и угрозы: материалы Всерос. студенческого круглого науч.-практ. стола с междунар. участием. СПб., 2021. С. 134–138.

7. Бушкевич Н.С., Якимов А.А. Характеристика основных проблем расследования криптопреступлений // Законность и правопорядок. 2020. № 4(56). С. 39–43.

8. Ганичева Е.А. Противодействие использованию криптовалюты в незаконных целях // Современная наука: актуальные проблемы теории и практики. Сер.: Экономика и право. 2022. № 3. С. 124–128.

9. Голубева С.А. Киберпреступность: классификация, виды, профилактика // Власть и общество: история, современное состояние и тенденции развития: сб. материалов Всерос. науч.-практ. конф. / науч. ред. В.В. Наумкина; отв. ред. В.Н. Козлова. Абакан, 2023. С. 110–111.

10. Горовой В.В. Противодействие киберпреступности // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сб. ст. LIX Междунар. науч.-практ. конф. Пенза, 2022. С. 117–119.

11. Дауров А.И. Факторы, оказывающие влияние на состояние борьбы с кибепреступностью в современном мире // Пробелы в российском законодательстве. 2021. Т. 14. № 4. С. 155–158.

12. Герцен А.А. Киберпреступность в современной экономике: состояние и тенденции развития // Проблемы и перспективы развития российской экономики: сб. ст. по материалам XI науч.-практ. конф. / под общ. ред. И.А. Сергеевой, А.Ю. Сергеева. М., 2022. С. 18–21.

13. Дементьева А.А. Киберпреступность в современной экономике // Обеспечение экономической безопасности россии в современных условиях: сб. науч. тр. Всерос. науч. конф. М., 2022. С. 203–208.

14. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109–115.

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

16. Завгородняя Е.В. Киберпреступность в современной экономике // Державинские чтения: сб. ст. XIV Междунар. науч.-практ. конф. / отв. ред. О.И. Александрова. 2019. С. 275–277.

17. Иванятова Ю.С. Преступления в киберпространстве // Студенческий вестник. 2022. № 13-7(205). С. 24–26.

18. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1(53). С. 58–74.

19. Левашова О.В., Сотников И.Л. Киберпреступность: основные направления международного сотрудничества в противодействии ей // Modern Science. 2022. № 1-2. С. 145–149.

20. Серебрякова О.М., Соколовский А.В. Борьба с киберпреступнотью и кибербезопасность // Актуальные проблемы международного сотрудничества в борьбе с преступностью: материалы Междунар. науч.-практ. конф., приуроченной к 20-летию образования Московского университета МВД России имени В.Я. Кикотя: сб. науч. тр. М., 2022. С. 536–541.

21. Солдатова Ю.А. Использование криптовалюты в преступной деятельности // Перспективы развития институтов права и государства: сб. науч. тр. IV Междунар. науч. конф. Курск, 2021. С. 47–49.

22. Таков А.З. Социальные и политические мотивированные формы проявления киберпреступности // Пробелы в российском законодательстве. 2022. Т. 15. № 5. С. 190–194.

23. Тамбиев С.А., Теунаев А.С.У. Основные направления деятельности оперативных подразделений органов внутренних дел по выявлению и предупреждению киберпреступлений, связанных с экстремистской деятельностью // Пробелы в российском законодательстве. 2022. Т. 15. № 5. С. 139–143.

24. Тамбиев С.А., Кочесокова З.Х. Международный опыт противодействия кибертерроризму // Право и управление. 2023. № 2. С. 160–164.

25. Тарчоков Б.А. К вопросу о понятии кибертерроризма и некоторых способах противодействия // Право и управление. 2023. № 2. С. 170–174.

26. Теуважуков А.Х. Некоторые проблемы выявления и предупреждения преступлений, совершаемых в киберпространстве // Журнал прикладных исследований. 2023. № 4. С. 152–155.

27. Усачев С.И., Алиев Т.Ф. Киберпреступность: современное состояние и актуальные способы противодействия // Искусство правоведения. 2023. № 1(5). С. 75–79.

28. Хамурзов А.Т. Преступность в сфере информационно-коммуникационных технологий как проблема информационного общества // Пробелы в российском законодательстве. 2022. Т. 15. № 4. С. 265–269.

29. Цримов А.А. Отражение киберпреступлений в российском и международном правовом поле // Право и управление. 2023. № 2. С. 146–150.

30. Черкесов А.Ю. Актуальные проблемы противодействия киберпреступности на современном этапе // Журнал прикладных исследований. 2022. Т. 2. № 9. С. 129–132.

31. Шондиров Р.Х. Киберпространство: новая платформа для терроризма // Право и управление. 2023. № 2. С. 141–145.

32. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. Электронный вестник. 2021. № 89. С. 184–196.

33. Юдинцев К.О. Киберпреступность в современной цифровой экономике // Актуальные проблемы менеджмента, экономики и экономической безопасности: сб. матер. Междунар. науч. конф. Чебоксары: Среда, 2019. С. 311–314.

Приложение 1

Анкетирование

Изучив информацию об информационной безопасности, угрозах и методах защиты, нами проведено анонимное анкетирование, которое позволило сделать вывод о том, насколько осведомлены люди разной возрастной категории в вопросах по данной теме (Приложение 1).

На вопросы анкеты ответило 90 слушателей.

Вопросы:

1. Выполняете ли Вы правила безопасной работы на компьютере?
2. Как Вы считаете, что является информационной безопасностью в современном мире?
3. Какой антивирусной программой Вы пользуетесь?
4. Сталкивались ли Вы когда-нибудь с компьютерными вирусами?
5. Какие аккаунты у Вас взламывали злоумышленники?
6. Установлена ли на вашем компьютере программа-фильтр, не допускающая Вас на вредоносные сайты?
7. Что Вы делаете, когда приходит предложение о добавлении в «друзья» от незнакомых людей?

Сравнительный анализ антивирусных программ

Антивирус лаборатории Касперского – Internet Security. Самая известная антивирусная программа на территории Российской Федерации. Данный антивирус работает с операционными системами Windows, Mac, а также планшетными и мобильными устройствами на базе Android. Лаборатория Касперского предоставляет антивирусные программы для малого, среднего и крупного бизнеса, которые защищают Интернет-соединения, банковые операции, веб-камеру и имеют функцию родительского контроля. Антивирус предоставляет возможность поиска и установки обновлений программ и удаление

неиспользуемых программ, имеется бесплатный тестовый период – 30 дней.

Avast Free Antivirus – интуитивно понятная и не требующая значительных ресурсов программа для защиты компьютера. Данное антивирусное программное обеспечение распространяется бесплатно, но можно приобрести расширенную или максимальную версии, которые содержат в себе дополнительные функции. Avast совместим с большинством современных операционных систем, а также смартфонов на базе Android и iPhone. Как и Антивирус лаборатории Касперского предоставляет антивирусные программы для бизнеса, защищает Интернет-соединения, банковые и финансовые операции и проверяет безопасность сети Wi-Fi.

360 Total Security. Данный антивирус быстр и прост в использовании, практически с каждым обновлением программы ее арсенал функций возрастает. Данная антивирусная программа совместима с теми же операционными системами, что и ее конкуренты. Этот продукт защищает веб-браузер, сжимает данные в памяти компьютера, проверяет и очищает системный реестр, защищает сеть Wi-Fi от внешних угроз. Для опытных пользователей имеются гибкие настройки приложения, возможность оптимизировать работу системы через антивирус и выбора темы оформления интерфейса на интересующую тематику. Данный антивирус также является бесплатным, но можно купить премиум версию, которая отличается расширенным функционалом.

В таблице 1 представлены результаты сравнительного анализа функционала рассмотренных антивирусных программ.

Из представленной таблицы видно, что безусловным лидером по функционалу являетсяантивирус Касперского – Internet Security, два других претендента немного отстают. Таким образом, самым оптимальным вариантом является антивирус Касперского – Internet Security. Ели же нет желания платить за лицензию Avast Free Antivirus и 360 Total Security являются неплохим выбором, потому что базовые версии отлично подходят для повседневной работы за компьютером. Особенно они будут удобны для новичков, благодаря автоматизации множества функций и удобному, простому интерфейсу.

Таблица 1

Результаты сравнительного анализа антивирусных программ

Функционал антивирусной программы	**Антивирус Касперского – Internet Security**	**Avast Free Antivirus**	**360 Total Security**
Антивирусный сканер и антивирусный монитор	+	+	+
Защита персональных данных	+	+	+
Система обновлений	+	+	+
Веб-защита	+	+	+
Поведенческий блокиратор	+	+	+
Эвристический анализ	+	+	+
Анти-фишинг	+	-	-
Анти-спам	+	-	-
Возможность работы в облаке	+	+	+
Цена базовой версии	1490 руб.	бесплатно	бесплатно
Цена премиум версии	2022 руб.	1800 руб.	999 руб.

Результатом нашей работы над данным исследованием станет буклет «*Информационная безопасность*», в котором будут представлены основные рекомендации по безопасной работе в сети Интернет.

Результаты анкетирования

Результаты ответов на 1 первый вопрос анкеты показывают, что слушатели хорошо осведомлены о правилах безопасной работы на компьютере.

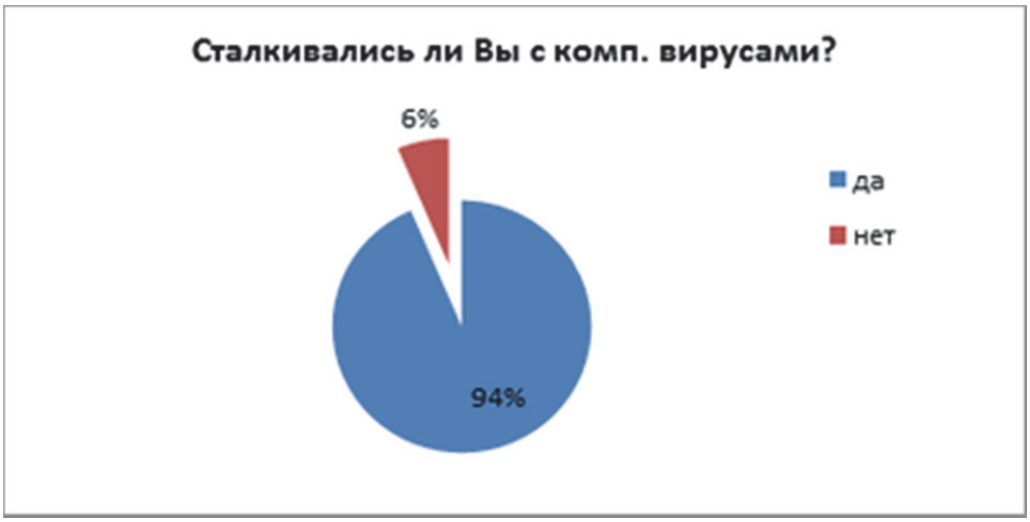
Однако, стоит отметить, что 20% респондентов искренне ответили, что правила безопасности они соблюдают очень редко, так как забывают о них, 11% не знают и не соблюдают правила.

Анализируя данные диаграммы по второму вопросу, можно сказать, что большинство опрошенных считают пароли основой информационной безопасности.

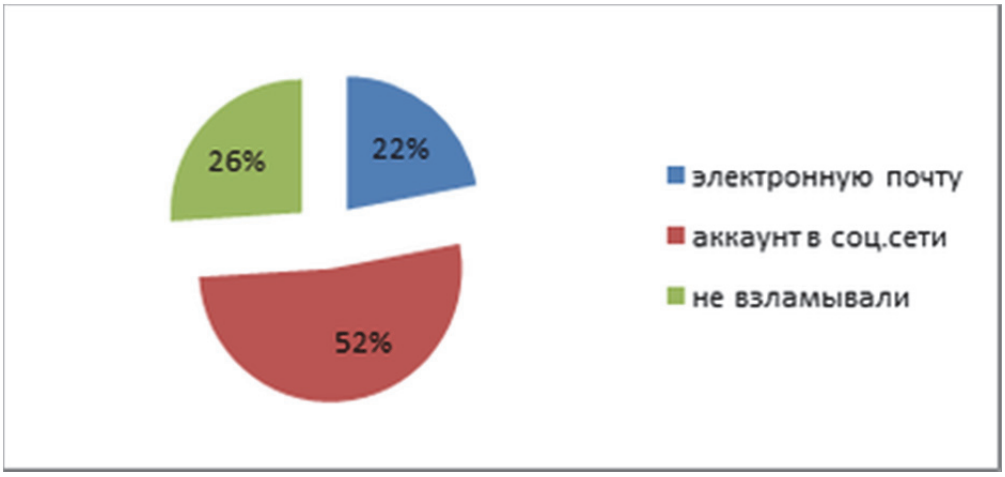
Следующий вопрос анкетирования выявил, что 16% респондентов не пользуются антивирусными программами. Считаю, что данная цифра является высокой, так как в современном мире без защиты данных от вирусов не обойтись. Самыми популярными программами оказались Антивирус Касперского (26%) и Dr.Web (22%).

Из диаграммы видно, что большинство респондентов (94%) сталкивались с вирусами на своих устройствах. На наш взгляд, это еще раз подтверждает необходимость использования антивирусных программ.

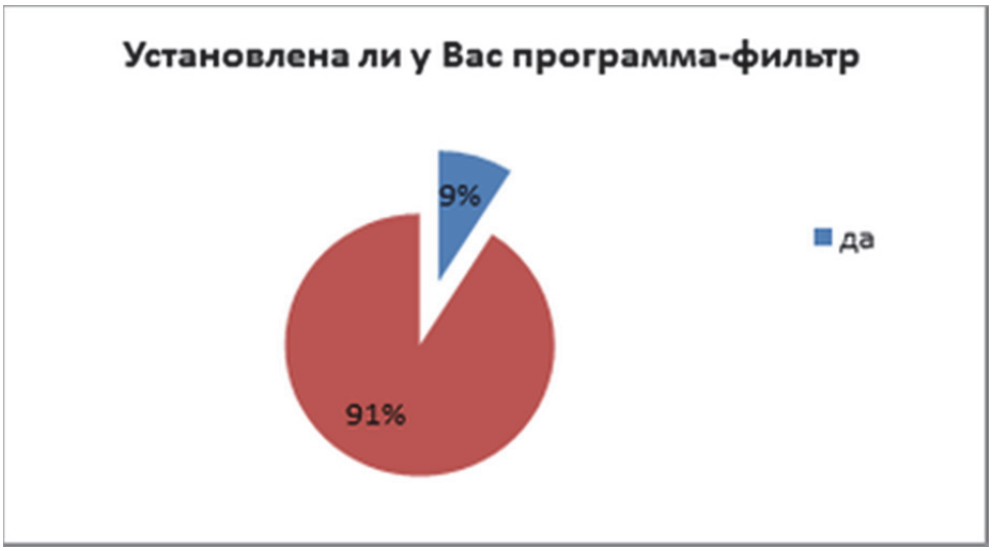
На вопрос: «*Какие аккаунты у Вас взламывали злоумышленники?*» были получены следующие ответы:



Из следующей диаграммы видно, что у большинства опрошенных аккаунты взламывались, но тем не менее 26% не подвергались «*взламыванию*», это говорит о том, что они серьезно относятся к работе в сети Интернет и надежно защищают свои данные.



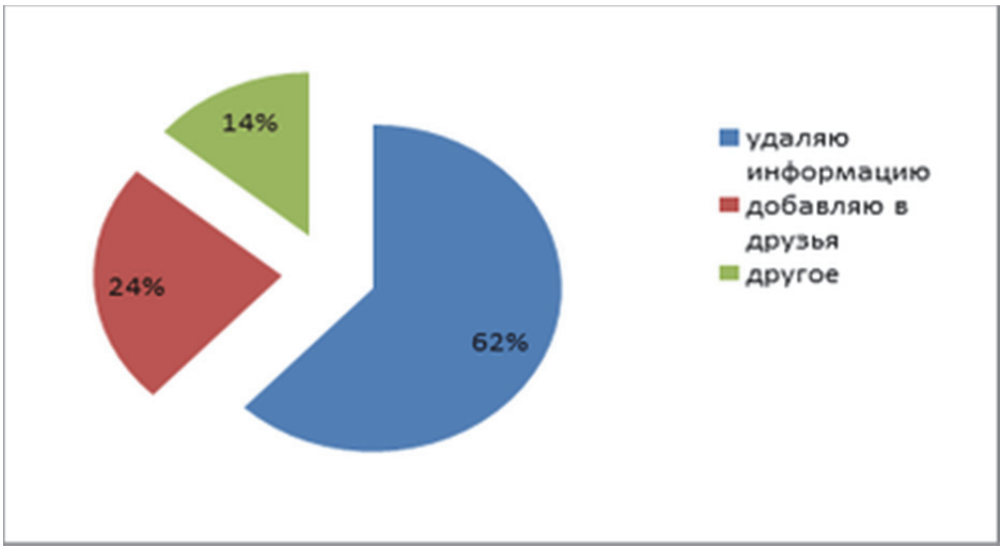
Следующий вопрос анкеты, об установленной на компьютере программе – фильтре для детей поставил в тупик многих участников опроса.



Исследование показало, что у 91% респондентов не установлено таких программ на ПК, а это значит, что любой подросток может зайти в интернете на любой сайт с любым содержательным контентом и вредоносностью.

Также все порошенные подтвердили, что в социальных сетях выставляют информацию о своей семье (указывают родственников), в открытом доступе представлена информация о школе, месте жительства, иногда номер телефона. И все 90 респондентов ответили положительно на вопрос о выставлении в социальных сетях своих настоящих фамилии и имени, а также о выставлении личных фотографий.

На следующий вопрос: «*Что ты делаешь, когда приходит предложение о добавлении в «друзья»* от незнакомых людей?» большинство респондентов ответили, что удаляют запрос, не принимая дружбу (62%), смотрят их аккаунт, выясняя личность и потом добавляют (24%).



Проанализировав информацию, полученную при анкетировании, мы можем сказать следующее: опрос показал средний уровень компетентности слушателей в вопросах, связанных с информационной безопасностью в сети интернет, что лишний раз является подтверждением незащищенности пользователей от действий киберпреступников.

Приложение 2

Глоссарий терминов

1. Аутентификация – процесс установления личности пользователя при попытке получения доступа к компьютеру или к файлам.

2. APT-угроза, APT-атака – сложная, технологически продвинутая атака, направленная на получение конфиденциальных данных в течение длительного периода.

3. Резервные копии – копии ваших файлов, которые сохраняются на сервере, жестком диске, компьютере или съемном диске на тот случай, если оригиналы окажутся утеряны.

4. Облачные вычисления, вычисления в облаке – вычислительные сервисы, предоставляемые с удаленных серверов.

5. Кибербезопасность – действия стратегического характера, направленные на защиту информации и коммуникаций при помощи ряда передовых инструментов, политик и процессов.

6. Утечка данных – несанкционированный доступ к данным.

7. Шифрование – трансформация данных с целью их сокрытия.

8. Безопасность оконечных – обеспечение безопасности устройств, находящихся в оконечных точках сети; к числу таких устройств относятся используемые сотрудниками мобильные устройства (планшеты, ноутбуки).

9. Управление рисками предприятия – комплексный подход к защите активов компании путем выявления рисков, принятия контрмер и реагирования на угрозы в режиме реального времени.

10. Межсетевой экран (файрволл, брандмауэр) – апаратное или программное решение, направленное на блокирование доступа в сеть для нежелательных пользователей.

11. Хакер, злоумышленник – человек, который со злоумышленными намерениями нарушает правила безопасности для получения доступа к данным.

12. Провайдер интернет-услуг (ISP, internet service – компания, которая предоставляет доступ к интернету.

13. Система предотвращения вторжений (IPS, intrusion prevention system) – программа, которая распознает и блокирует действия хакеров, направленные на получение доступа к вашему компьютеру или данным.

14. Клавиатурный шпион (кейлоггер) – ПО или аппаратное устройство, регистрирующее нажатия клавиш для перехвата вводимой информации, например паролей.

15. Вредоносное ПО (вредоносные программы) – ПО, направленное на выполнение несанкционированных вредоносных действий на компьютере.

16. Фишинг – мошеннические электронные сообщения, рассылаемые злоумышленниками с целью получить доступ к конфиденциальной информации, такой так банковская информация или пароли.

17. Оценка рисков – процесс выявления потенциальных рисков, актуальных для вашей компании или сети.

18. Шпионское ПО (шпионские программы) – вредоносное ПО, которое без вашего ведома отслеживает действия или информацию на вашем компьютере и пересылает ее другому человеку.

19. VPN (виртуальная частная сеть, virtual private network) – более безопасный способ получения доступ к Сети путем маршрутизации вашего соединения через специальный сервер, который скрывает ваше местоположение.

20. Вирус – самовоспроизводящаяся вредоносная программа.

21. Червь – вредоносная программа, которая устанавливает себя при проникновении на компьютер и распространяет собственные копии на другие компьютеры.

22. VPN (англ. Virtual Private Network «виртуальная частная сеть») – обеспечивает конфиденциальность и безопасность при доступе пользователей к потенциально небезопасным сетям. Обычно, когда пользователь подключается к

Интернету, его действия могут быть просмотрены поставщиком Интернет-услуг (ISP). Однако при использовании VPN соединение шифруются, а это означает, что провайдер не участвует в процессе. При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. Скрывая свой настоящий IP-адрес, пользователи могут пользоваться услугами, которые ранее были для них запрещены.

23. Backdoor (бэкдор, тайный вход) – один из способов вторгнуться в сеть – проложить секретный путь в систему, позволяющий проникнуть посторонним. Это называется «бэкдор» – способ проникнуть в систему, продукт или устройство путем установки программного обеспечения или настройки программного обеспечения для обхода существующие механизмы безопасности.

24. Кейлоггер – это шпионское ПО или программное обеспечение для мониторинга, которое отслеживает каждое нажатие по клавише. Это означает, что имена пользователей, пароли и любая другая личная информация может быть перехвачена через это ПО.

25. SSL – криптографический протокол, который подразумевает более безопасную связь. Является обязательным для веб-сайтов, особенно если они обрабатывают конфиденциальную информацию, такую как кредитные карты или имена и адреса клиентов. SSL обеспечивает безопасное зашифрованное соединение между браузером и сервером.

26. FIDO (от англ. Fast Identity Online — быстрая онлайн-идентификация) – лучший пароль простой, безопасный и уникальный. FIDO – это набор спецификаций безопасности, поддерживающих многофакторную аутентификацию и криптографию с открытым ключом. Аутентификация, соответствующая требованиям FIDO, означает, что пользователям не нужно использовать традиционную комбинацию имени пользователя и пароля, а вместо этого для входа в какую-либо систему используется биометрическая аутентификация, которая может включать в себя отпечатки пальцев или вход по радужке глаза.

27. Dark Web – это часть всемирной паутины, доступ к которой возможен только при установке специального программного обеспечения. После установки которой, позволяет пользователям получить доступ к зашифрованной сети, где пользователи и операторы остаются анонимными и не отслеживаемыми.

28. WAF или брандмауэр веб-приложений – это устройство, которое фильтрует, отслеживает и блокирует трафик к веб-приложению и от него. Многим известен термин «брандмауэр», но WAF отличается тем, что фильтрует содержимое определенных веб-приложений, потому что большинство кибератак нацелено на уровень приложений. WAF работают по-разному.

Приложение 3

Проведение деловой игры № 1

Методические рекомендации к организации и проведению игры.

Для закрепления изучаемого материала проводиться деловая игра «Нормативно-правовое обеспечение кибербезопасности».

Слушателям предлагается выполнить задания.

Деловая игра позволит лучше усвоить слушателям изучаемый материал, расширить знания о системе противодействия коррупции, повысить активность на занятии.

Цели проведения игры:

- углубление знаний по основам правового регулирования алкогольной и спиртосодержащей продукции;
- развитие у слушателей интереса к изучаемой теме;
- воспитание правовой культуры слушателей;
- развитие творческой активности слушателей;
- формирование навыков коллективной деятельности слушателей.

Задачи игры:

- закрепление умений и навыков по решению проблемных вопросов;
- развитие правового мышления и умение выделить главное.

Форма игры: игра проходит в форме конкурса. Каждая команда сидит за отдельным рядом столов. Побеждает та команда, которая наберет в конце игры большее количество балов. Игра оценивается по рейтинговой системе. За каждый правильно выполненный ответ команда получает 1 балл.

Подготовительный этап. Команда формируется по желанию студентов. Игроки заранее знакомятся с правилами игры.

Ход игры. Игра рассчитана на 30 минут. В игре принимают участие 2 команды. Каждой команде выдаются таблички со словами «Ответ готов», которую они используют для оповещения готовности ответить на вопрос. Преподаватель зачитывает задание и дает время для обсуждения. После фразы преподавателя «Время вышло. Ваш ответ» слушатели должны поднять табличку «Ответ готов», после чего дать

аргументированный ответ. Ведет игру и осуществляет судейство преподаватель.

Задание № 1. Каждой команде предлагается раскрыть следующие вопросы:

- нормативно-правовая основа кибербезопасности?
- назовите составы административных правонарушений и преступлений посягающих на компьютерную безопасность?
- что такое критическая инфраструктура информации?
- какие методы защиты могут быть применены в целях нивелирования воздействия киберпреступности?

Задание № 2. «Ты мне – я тебе».

Командам предлагается обменяться двумя вопросами по теме семинарского занятия. Команда, правильно ответившая на вопрос, получает 2 балла.

Заключительный этап игры.

Подсчитываются баллы. Подведение итогов игры.

Проведение деловой игры № 2

Методические рекомендации к организации и проведению игры.

Для закрепления изучаемого материала проводиться деловая игра «Принципы обеспечения кибербезопасности». Слушателям предлагается выполнить задания.

Деловая игра позволит лучше усвоить слушателям изучаемый материал, расширить знания об основных принципах обеспечения кибербезопасности, повысить активность на занятии.

Цели проведения игры:

- углубление знаний по основам правового регулирования алкогольной и спиртосодержащей продукции;
- развитие у слушателей интереса к изучаемой теме;
- воспитание правовой культуры слушателей;
- развитие творческой активности слушателей;
- формирование навыков коллективной деятельности слушателей.

Задачи игры:

- закрепление умений и навыков по решению проблемных вопросов;

- развитие правового мышления и умение выделить главное.

Форма игры: игра проходит в форме конкурса. Каждая команда сидит за отдельным рядом столов. Побеждает та команда, которая наберет в конце игры большее количество балов. Игра оценивается по рейтинговой системе. За каждый правильно выполненный ответ команда получает 1 балл.

Подготовительный этап. Команда формируется по желанию студентов. Игроки заранее знакомятся с правилами игры.

Ход игры. Игра рассчитана на 30 минут. В игре принимают участие 2 команды. Каждой команде выдаются таблички со словами «Ответ готов», которую они используют для оповещения готовности ответить на вопрос. Преподаватель зачитывает задание и дает время для обсуждения. После фразы преподавателя «Время вышло. Ваш ответ» слушатели должны поднять табличку «Ответ готов», после чего дать аргументированный ответ. Ведет игру и осуществляет судейство преподаватель.

Задание № 1. Каждой команде предлагается раскрыть следующие вопросы:

- Огласите основные принципы обеспечения кибербезопасности?
- Что такое кибератака?
- Типы киберпреступлений?
- Распространенные типы кибератак?
- Способы защиты от кибератак?
- Что такое протокол TCP-IP?
- Что такое домен?
- Что такое хостинг?
- Чем отличие эммитируемых денежных средств от криптовалют?
- Что такое MAC-адрес?
- Что такое VPN технология?
- Что такое Darknet?

Задание № 2. «Ты мне – я тебе».

Командам предлагается обменяться двумя вопросами по теме семинарского занятия. Команда, правильно ответившая на вопрос, получает 2 балла.

Заключительный этап игры.

Подсчитываются баллы. Подведение итогов игры.

Проведение деловой игры № 3

Методические рекомендации к организации и проведению игры.

Для закрепления изучаемого материала проводиться деловая игра на тему: «Защита информации от утечек, основные виды утечек данных». Слушателям предлагается выполнить задания.

Деловая игра позволит лучше усвоить слушателям изучаемый материал, расширить знания о системе противодействия утечек информации, повысить активность на занятии.

Цели проведения игры:

- углубление знаний по основам правового регулирования алкогольной и спиртосодержащей продукции;
- развитие у слушателей интереса к изучаемой теме;
- воспитание правовой культуры слушателей;
- развитие творческой активности слушателей;
- формирование навыков коллективной деятельности слушателей.

Задачи игры:

- закрепление умений и навыков по решению проблемных вопросов;
- развитие правового мышления и умение выделить главное.

Форма игры: игра проходит в форме конкурса. Каждая команда сидит за отдельным рядом столов. Побеждает та команда, которая наберет в конце игры большее количество балов. Игра оценивается по рейтинговой системе. За каждый правильно выполненный ответ команда получает 1 балл.

Подготовительный этап. Команда формируется по желанию студентов. Игроки заранее знакомятся с правилами игры.

Ход игры. Игра рассчитана на 30 минут. В игре принимают участие 2 команды. Каждой команде выдаются таблички со словами «Ответ готов», которую они используют для оповещения готовности ответить на вопрос. Преподаватель зачитывает задание и дает время для обсуждения. После фразы преподавателя «Время вышло. Ваш ответ» слушатели должны поднять табличку «Ответ готов», после чего дать аргументированный ответ. Ведет игру и осуществляет судейство преподаватель.

Задание № 1. Каждой команде предлагается раскрыть следующие вопросы:

- Огласите основные принципы обеспечения кибербезопасности?
- Что такое кибератака?
- Типы киберпреступлений?
- Распространенные типы кибератак?
- Способы защиты от кибератак?
- Что такое протокол TCP-IP?
- Что такое домен?
- Что такое хостинг?
- Чем отличие эммитируемых денежных средств от криптовалют?
- Что такое MAC-адрес?
- Что такое VPN технология?
- Что такое Darknet?

Задание № 2. «Ты мне – я тебе».

Командам предлагается обменяться двумя вопросами по теме семинарского занятия. Команда, правильно ответившая на вопрос, получает 2 балла.

Заключительный этап игры.

Подсчитываются баллы. Подведение итогов игры.

Проведение деловой игры № 4

Методические рекомендации к организации и проведению игры.

Для закрепления изучаемого материала проводиться деловая игра на тему: «Особенности следообразования и фиксации следов при расследовании преступлений, совершаемых с применением современных информационно-коммуникационных технологий».

Слушателям предлагается выполнить задания.

Деловая игра позволит лучше усвоить слушателям изучаемый материал, расширить знания о системе противодействия утечек информации, повысить активность на занятии.

Цели проведения игры:

- углубление знаний по основам правового регулирования алкогольной и спиртосодержащей продукции;
- развитие у слушателей интереса к изучаемой теме;
- воспитание правовой культуры слушателей;
- развитие творческой активности слушателей;
- формирование навыков коллективной деятельности слушателей.

Задачи игры:

- закрепление умений и навыков по решению проблемных вопросов;
- развитие правового мышления и умение выделить главное.

Форма игры: игра проходит в форме конкурса. Каждая команда сидит за отдельным рядом столов. Побеждает та команда, которая наберет в конце игры большее количество балов. Игра оценивается по рейтинговой системе. За каждый правильно выполненный ответ команда получает 1 балл.

Подготовительный этап. Команда формируется по желанию студентов. Игроки заранее знакомятся с правилами игры.

Ход игры. Игра рассчитана на 30 минут. В игре принимают участие 2 команды. Каждой команде выдаются таблички со словами «Ответ готов», которую они используют для оповещения готовности ответить на вопрос. Преподаватель зачитывает задание и дает время для обсуждения. После фразы преподавателя «Время вышло. Ваш ответ» слушатели должны

поднять табличку «Ответ готов», после чего дать аргументированный ответ. Ведет игру и осуществляет судейство преподаватель.

Задание № 1. Каждой команде предлагается раскрыть следующие вопросы:

- Что такое троянский конь?
- Какие вы можете назвать электронные следы преступлений?
- Распространенные типы кибератак?
- Способы защиты от кибератак?
- Что такое протокол TCP-IP?
- Что такое домен?
- Что такое хостинг?
- Чем отличие эммитируемых денежных средств от криптовалют?
- Что такое MAC-адрес?
- Что такое VPN технология?
- Что такое Darknet?

Задание № 2. «Ты мне – я тебе».

Командам предлагается обменяться двумя вопросами по теме семинарского занятия. Команда, правильно ответившая на вопрос, получает 2 балла.

Заключительный этап игры.

Подсчитываются баллы. Подведение итогов игры.

Приложение 4

Тестовые задания

1. Кибербезопасность – это?

а) совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных;

б) процесс шифрования данных согласно которому возникает необходимость установления требований в установке специального графического программного обеспечения;

в) сложная, технологически продвинутая атака, направленная на получение конфиденциальных данных в течение длительного периода.

2. Заражение компьютерными вирусами может произойти в процессе:

а) Работы с файлами

б) Форматирования дискеты

в) Выключения компьютера

г) Печати на принтере

3. Защита информации:

а) Это комплекс мероприятий, направленных на обеспечение компьютерной защиты

б) Это комплекс мероприятий, направленных на обеспечение безопасности сети

в) Это комплекс мероприятий, направленных на обеспечение информационной безопасности

г) Все ответы верны

4. Попытка реализации компьютерной угрозы называется:

а) Нападение

б) Атака

в) Завладение

г) Уничтожение

5. Компьютерные угрозы направлены на изменение целостности информационной безопасности, а именно:

а) Прогрессивной целостности

б) Активной целостности

в) Динамической целостности

г) Все ответы верны

6. Федеральный закон от 27 июля 2006 г "Об информации, информационных технологиях и о защите информации"

а) N 129-ФЗ

б) N 139-ФЗ

в) N 149-ФЗ

г) N 159-ФЗ

7. Назовите один из классов программного обеспечения:

а) Пользовательское программное обеспечение

б) Административное программное обеспечение

в) Прикладное программное обеспечение

г) Сетевое программное обеспечение

8. Чтобы основной процессор компьютера мог управлять всеми устройствами, была создана:

а) Загрузочная система

б) Поисковая система

в) Операционная система

г) Административная система

д) Пользовательская система

9. Компьютерный вирус:

а) Специально загруженная компьютерная программа, которая самостоятельно внедряется в другие существующие компьютерные программы, изменяет или разрушает данные, самопроизвольно размножается и инфицирует другие компьютеры

б) Специально написанная компьютерная программа, которая самостоятельно внедряется в другие существующие компьютерные программы, изменяет или разрушает данные,

самопроизвольно размножается и инфицирует другие компьютеры

в) Специально придуманная компьютерная программа, которая самостоятельно внедряется в другие существующие компьютерные программы, изменяет или разрушает данные, самопроизвольно размножается и инфицирует другие компьютеры

г) Все ответы верны

10. Для защиты и борьбы с вирусами применяются специальные антивирусные программы:

а) Программы-детективы

б) Программы-детекторы

в) Программы-защитники

г) Программы-искатели

11. Для защиты и борьбы с вирусами применяются специальные антивирусные программы:

а) Программы-врачи

б) Программы-лечилки

в) Программы-скорой помощи

г) Программы-доктора

12. Файлы или папки, удаляемые с флеш-носителя или сетевого диска:

а) Уничтожаются окончательно, без помещения в корзину

б) Перемещаются в корзину

в) Перемещаются в системную папку TEMP

г) Уничтожаются, но копия файлов и папок находится в папке TEMP

13. Значок рабочего стола, который в своих свойствах имеет ссылку на объект, а не сам объект, расположенный каком-либо носителе информации, называется:

а) Ярлык

б) Иконка

в) Ссылка

г) Объект

14. Специальная папка, содержащая список всех удаленных файлов и папок называется:

а) Контейнер

б) Мусорка

в) Корзина

г) Хранилище

15. Специальная папка, которая позволяет просматривать содержимое дисков компьютера и выполнять различные операции с файлами и папками называется:

а) Мой компьютер

б) Пуск

в) Локальный диск

г) Program Files

16. Когда получен спам по e-mail с приложенным файлом, следует:

а) Прочитать приложение, если оно не содержит ничего ценного – удалить

б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

в) Удалить письмо с приложением, не раскрывая (не читая) его

г) Все ответы верны

17. Виды защиты информации?

а) Криптографическая защита;

б) Технологическая защита;

в) Амбиетная защита;

18. Стандартная модель информационной безопасности включает в себя:

а) либеральность;

б) преемственность

в) целостность;

19. Процесс установления личности пользователя при попытке получения доступа к системе:

а) аутентификация

б) абсорбция

в) логинирование и паролирование

20. Компания которая представляет доступ к интернету:

а) проводник

б) провайдер

в) продюсер интернет-сети;

21. Программное обеспечение или аппаратное устройство, регистрирующее нажатие определенных клавиш на клавиатуре:

а) фишер

б) кейлогер

в) файрвол

г) антивирус

22. Мошеннические электронные сообщения, рассылаемые злоумышленниками с целью получить доступ к конфиденциальной информации, такой так банковская информация или пароли:

а) трайл-пассинг

б) фишинг

в) хантинг

г) пауэр-лифтинг

23. Более безопасный способ получения доступ к Сети путем маршрутизации вашего соединения через специальный сервер, который скрывает ваше местоположение:

а) DDOS

б) Скрытый DarkNet

в) VPN

24. Вредоносная программа, которая устанавливает себя при проникновении на компьютер и распространяет собственные копии на другие компьютеры

а) Файрвол

б) Kaspersky Spy-Ware

в) Червь

г) Вредоносный ползун

25. Общие понятия и положения о критической инфраструктуры кибербезопасности содержатся в Федеральном законе:

а) №187-ФЗ

б) №149-ФЗ

в) №3-ФЗ

г) №342-ФЗ

26. Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры:

а) компьютерные инциденты

б) аналоговые сети

в) объекты критической информационной инфраструктуры

г) аппаратные криптографические средства, предназначенные для шифрования передаваемой информации и передачи их конечным пользователям в режиме открытости

27. Принципами обеспечения безопасности критической информационной инфраструктуры не являются:

а) законность

б) непрерывность

в) гуманизм

28. Вредоносная, осуществляемая сознательно попытка человека или организации проникнуть в информационную систему другого человека или организации.

а) кибератака

б) кибервирус

в) компьютерная угроза обхода антивирусной системы

29. Передача вредоносного кода на сервер, обрабатывающий запросы, в результате чего сервер раскрывает данные, которые не предполагалось раскрывать.

а) внедрение SQL-кода

б) внедрение DDOS-кода

в) внедрение VPN кода

30. Что не относится к способам защиты от кибератак?

а) обновление антивирусного программного обеспечения

б) вскрытие спам-писем

в) проверка надежных интернет-адресов

31. Неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной

а) утечка информации

б) тунелированние DNS

в) обход надежных интернет-узлов с помощью VPN

г) инсайдерство в программном комплексе информационной системы

32. К основным видам угроз утечки данных не относятся:

а) Угроза нарушения конфиденциальности

б) Угроза нарушения целостности

в) Угроза нарушения приоритетности использования интернет технологий

33. Основной целью и задачей технической защиты является

а) предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения

б) получение доступа к ключам шифрографированию защищенных данных

в) механизированный ввод паролей и логинов в целях аутентификации

34. Доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы

а) телефонное мошенничество

б) инсайдерная атака

в) мошенничество в сфере кредитования и компьютеризации банковских данных и платежных карт с использованием стационарных и мобильных телефонов

35. Средство переноса компьютерной информации в пространстве и во времени с помощью электромагнитных колебаний (волн)

а) электромагнитный сигнал

б) спутниковый сигнал

в) радио-визионный сигнал

36. Поименованная область записей на электронном носителе информации, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать.

а) файл

б) папка

в) документ

г) .exe образ

37. Вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций

а) транснациональная валюта

б) криптовалюта

в) электронно-виртуальная валюта

г) бонусные баллы

38. Тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях

а) логический троян

б) логическая бомба

в) логическая система

г) логическая задача

39. Тайное введение в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность

а) спартанский конь

б) троянский конь

в) кабардинский конь

г) арабский скакун

40. Скрытая сеть, соединения которой устанавливаются только доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов

а) випнет

б) руснет

в) даркнет

г) апарнет

Ключ к тестовому заданию

1 а	2 а	3 в	4 б	5 в	6 в	7 в	8 в	9 б	10 б
11 г	12 а	13 а	14 в	15 а	16 в	17 а	18 в	19 а	20 б
21 б	22 б	23 в	24 в	25 а	26 в	27 в	28 а	29 а	30 б
31 а	32 в	33 а	34 а	35 а	36 а	37 б	38 б	39 б	40 в

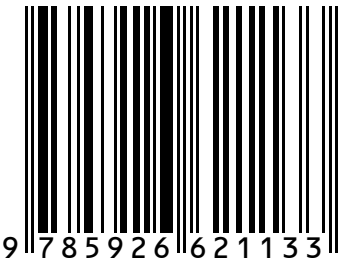
Учебное издание

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ КИБЕРПРЕСТУПНОСТИ

Методические рекомендации

В авторской редакции
Компьютерная верстка *С. В. Коноваловой*

ISBN 978-5-9266-2113-3



Подписано в печать 02.05.2024.
Авт. л. 4,4. Заказ 245.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.