УДК 004.056:62-78

*А. А. Стрельникова**

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, ПРЕДСТАВЛЯЮЩИЕ УГРОЗУ ТЕХНОГЕННОЙ БЕЗОПАСНОСТИ

Современные информационно-коммуникационные технологии (ИКТ) занимают центральное положение в развитии цивилизации, становясь основой существования современного общества и экономических отношений. Внедрение цифровых технологий обеспечивает существенный прогресс в производственной сфере, ускоряет передачу информации, повышает комфорт жизни. Однако наряду с преимуществами активное использование ИКТ влечет за собой появление новых угроз, среди которых особо выделяются преступления, непосредственно затрагивающие функционирование технологических систем и инфраструктуру, что ставит под удар техногенную безопасность.

Техногенная безопасность включает широкий спектр аспектов, касающихся поддержания устойчивого функционирования социально-экономических и природных систем. Она охватывает охрану окружающей среды, снижение рисков чрезвычайных происшествий, предупреждение аварий и ликвидацию их последствий [1]. Именно поэтому обеспечение устойчивости технологических систем имеет первостепенное значение для общества и государства. Распространенность и доступность цифровых технологий делают их привлекательной мишенью для различного рода преступных действий, направленных на нарушение нормального функционирования техносферы.

*Работа выполнена под руководством кандидата технических наук, доцента кафедры «Уголовное право и прикладная информатика в юриспруденции» ФГБОУ ВО «ТГТУ» А. В. Селезнева.

Проблема преступлений в сфере информационно-коммуникационных технологий приобретает особую значимость ввиду стремительного роста технологического прогресса современного общества. Статистические данные последнего десятилетия свидетельствуют о резком увеличении числа киберпреступлений, многие из которых связаны с нарушениями работы инфраструктур, поддерживающих эффективное функционирование национальной экономики.

Особое внимание привлекает класс преступлений, воздействующий на стабильность технологических процессов и целостность инфраструктуры. Этот род преступлений создает значительные угрозы возникновения техногенных аварий и масштабных катастроф, последствия которых могут оказаться непредсказуемыми и иметь далеко идущие негативные последствия как для отдельных граждан, так и для государства в целом. А значит, безопасность информационных систем становится ключевым фактором обеспечения устойчивого социально-экономического развития страны и защиты ее от возможных угроз и рисков, возникающих вследствие преступных действий злоумышленников в цифровой среде.

Данные Positive Technologies за период с декабря 2021 года по июнь 2022 года выявили 68% атак, основанных на обмане личности, направленных на выдачу себя за доверенное лицо или бренд. Согласно отчетам Касперского, 105 миллионов атак на устройства Интернета вещей происходят с 276 000 уникальных IP-адресов. Киберпреступники используют сеть для заражения смарт-устройств для проведения DDOS-атак, в качестве прокси-серверов [2].

Еще одним важным направлением являются нарушения безопасности критической инфраструктуры, относящейся к энергосистемам, телекоммуникациям, транспорту и прочим отраслям, чья работа необходима для нормальной жизнедеятельности общества. Атаки на подобные объекты приводят к серьезным последствиям: разрушению инфраструктуры, массовым отключениям электроэнергии, остановке движения поездов и самолетов, прекращению подачи воды и тепла населению. Данные инциденты оказывают негативное влияние на здоровье и безопасность граждан, ухудшают условия проживания и нарушают нормальный ход трудовой деятельности.

Следующая категория преступлений в сфере ИКТ связана с защитой интеллектуальной собственности и коммерческой тайны. Высокий

темп научно-технического прогресса и увеличение объема интеллектуальных активов способствуют увеличению интереса злоумышленников к подобным сведениям. Получение несанкционированного доступа к результатам научной деятельности, проектам инновационных разработок и коммерческим тайнам приносит огромные выгоды преступникам, однако одновременно вызывает серьезные негативные последствия для экономики и общества в целом. В качестве примера можно привести событие 2018 года, когда китайские хакеры незаконно получили доступ к серверам американской компании General Electric Aviation и похитили секретные исходные коды, а также документацию проекта авиационного двигателя LEAP, используемого на самолетах Boeing 737 MAX и Airbus A320neo. Инцидент привел к крупным финансовым потерям и утрате конкурентных позиций компании.

Особую тревогу вызывает тот факт, что киберпреступность, совершаемая преступниками, находящимися вне пределов территории конкретного государства, нередко носит международный характер. Сложность расследования подобных преступлений обусловлена отсутствием согласованной правовой базы и достаточного уровня международного сотрудничества в рамках борьбы с киберпреступностью. Проблемы привлечения к уголовной ответственности лиц, находящихся за пределами конкретной страны, зачастую оказываются трудноразрешимыми, что ограничивает способность государств защищать свою территорию и население от разрушительных последствий киберпреступлений.

Обеспечение стабильности и защищенности технологической среды требует комплексного подхода, объединяющего совершенствование правовых норм, проведение управленческих мероприятий и внедрение инженерных решений [3]. Основой является создание соответствующей правовой базы, регламентирующей применение цифровых технологий и устанавливающей четкую ответственность за преступления. Законодательство должно своевременно адаптироваться к современным вызовам и предусматривать соответствующие санкции для нарушителей.

Среди организационных мер можно выделить разработку единых стандартов информационной безопасности, усиленный контроль за их соблюдением и повышение уровня квалификации сотрудников,

обрабатывающих большие объемы персональных данных и обеспечивающих функционирование объектов техносферы. Одну из важных ролей также играет тесное сотрудничество государства с представителями бизнеса и науки, направленное на выявление потенциальных угроз и минимизацию рисков.

Безусловно, техническое оснащение критически значимых предприятий представляет собой практически ключевую составляющую современных систем безопасности. Актуальными инженерными решениями целесообразно назвать специальные ПО для защиты данных, способы биометрической аутентификации, использование криптосистем. Подобные идеи способствуют снижению вероятности какой-либо кибератаки и уменьшению последствий возможных инцидентов.

Кроме того, при внедрении Интернета вещей необходимо учитывать риски кибератак и сразу принимать соответствующие меры. Следует подчеркнуть, что анализ рисков должен учитывать особенности отрасли и специфику конкретного производства. Это позволит обнаружить слабые места и укрепить защиту гораздо раньше, чем произойдет происшествие, которое может нести серьезные негативные последствия.

Научные исследования в области информационной безопасности и криминалистического анализа киберпреступлений приобретают огромное значение в настоящее время. Ученые работают над методологией оценки угроз и профилактики преступлений в сфере техногенной безопасности [4]. Реализация федеральных целевых программ, поддержка инициатив научных коллективов и подготовка профессиональных кадров обеспечивают долговременную стабильность и высокую степень защиты технологической инфраструктуры.

В заключение стоит отметить, что борьба с преступлениями в сфере информационно-коммуникационных технологий является одной из приоритетных задач современного общества. Устойчивость технологической инфраструктуры определяет безопасность общества и экономику страны, поэтому требуются скоординированные усилия государства, сектора бизнеса и научного сообщества для минимизации рисков и устранения угроз, вызванных этими преступлениями. Решение этой сложной задачи возможно лишь при условии комплексного подхода, учитывающего опыт предыдущих поколений исследователей, и используя передовые научные методики и технологии.

Список литературы

1. Рассолов, И. М. Право и Интернет. Теория кибернетического права : монография / И. М. Рассолов. – 3-е изд. – М. : Норма, 2021. – 303 с.

2. Платенкин, А. В. Обзор киберпреступлений и видов кибератак при использовании технологии интернета вещей / А. В. Платенкин // Уголовно-процессуальное и технико-криминалистическое обеспечение для борьбы с киберпреступлениями в современном обществе : сб. науч. тр. I Всерос. науч.-практ. конф. – Тамбов, 2022. – С. 157 – 162.

3. Яшин, А. В. Современные проблемы противодействия киберпреступлениям в Российской Федерации / А. В. Яшин // Вестник Пензенского государственного университета. – 2023. – № 2. – С. 58 – 62.

4. Корабельников, С. М. Преступления в сфере информационной безопасности : учеб. пособие для вузов / С. М. Корабельников. – М. : Юрайт, 2024. – 111 с.

Кафедра «Уголовное право и прикладная информатика в юриспруденции» ФГБОУ ВО «ТГТУ»