УДК 004.056.5

ПРЕСТУПЛЕНИЯ, СОВЕРШЁННЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ОБЩАЯ ХАРАКТЕРИСТИКА И СОСТОЯНИЕ КИБЕРПРЕСТУПНОСТИ (НА ПРИМЕРЕ ГОРОДА МИЧУРИНСКА ТАМБОВСКОЙ ОБЛАСТИ)

Светлана Валерьевна Белякова
кандидат юридических наук, доцент
belsvet170@mail.ru
Артём Кириллович Мечник
студент
mechnik41@gmail.com
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассмотрены отдельные составы преступлений, совершаемых с использование информационно-телекоммуникационных технологий, определены отдельные трудности, имеющие место при раскрытии таких преступлений, а также осуществлен анализ таких правонарушений, совершенных за период с 2021 по 2023 годы по городу Мичуринску Тамбовской области. Рассмотрены отдельные аспекты, требующие совершенствования систем защиты от киберпреступлений и организации работы правоохранительных органов.

Ключевые слова: информационная безопасность, киберпреступность, защита информации, профилактические меры.

Информация в современном мире играет основополагающее значение в жизни каждого человека, формирует его приоритеты, духовно-нравственные ценности, интересы; владение информацией позволяет не допускать ошибок, которые совершались предыдущими поколениями. Информация сегодня выходит на новый уровень влияния во всех сферах общественной жизни; она становится важнейшим ресурсом постиндустриального общества. При этом любой технический или технологический прогресс, внедрение его результатов в жизнь общества, а также появление и обработка больших информационных баз данных способны решать отдельные социальные проблемы, однако, при этом, неизбежно обострять или порождать новые, ранее не известные, в том числе связанные с обеспечением безопасности личности, организации, корпорации и государства [7].

Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» в статье 2 раскрывает понятие «информации» – это сведения (сообщения, данные) независимо от формы их представления. При этом «защита информации» включает правовые, организационные и технические меры, которые призваны не допустить неправомерный доступ, уничтожение, модификацию, блокировку, копирование информации и другие технические неправомерные действия по отношению к ней; соблюдать конфиденциальность в отношении информации ограниченного пользования [1].

Современное общество большую часть информации получает из сети «Интернет», что влечет массу негативных последствий для ее получателей – от получения недостоверной, а иногда и откровенно вредной информации, до попадания под воздействие мошенников и разного рода действия преступных схем завладения личной информацией, персональными данными и пр. Появляется всё больше мошенников, которые используют неопытность и доверчивость людей в своих личных целях; человечество сталкивается с информационными войнами, зависимостью от виртуального мира,

ухищрениями социальной инженерии. Безопасность и целостность коммерческих данных стали главным приоритетом для компаний во всех секторах российской экономики в 2024 году. Это связано с растущим числом инцидентов в сфере информационной безопасности: только в 2023 году, по данным Роскомнадзора, в сеть незаконно попало более 300 миллионов записей, включая персональные данные. Хакеры нацелены на такие важные сферы, как финансовый сектор, промышленность, розничная торговля, телекоммуникации и другие, независимо от размера компании. В ходе таких инцидентов собирается и обрабатывается конфиденциальная информация, включая данные сотрудников и клиентов [9]. Несмотря на постоянное усовершенствование систем защиты и особенностей хранения данных, пользователи персональных компьютеров, смартофонов, а также клиенты кредитных организацией, пользующиеся банковскими продуктами, по-прежнему являются самым слабым звеном, когда речь заходит о защите информации.

Таким образом сохранность информации, ее защита – это новая проблема, которая стоит сегодня как перед государством и обществом в целом, так и перед каждым конкретным человеком. Каждый человек может стать жертвой кибепреступнтиков, именно поэтому необходимо ориентироваться в разновидностях современных кибератак, понимать, к каким последствиям могут привести необдуманные действия в киберпространстве, а также уметь противостоять правонарушителям.

По данным Министерства внутренних дел Российской Федерации, неуклонного растут показатели зарегистрированных в органах МВД преступлений, совершенных с использованием информационно-телекоммуникационных технологий (ИТКТ). С 2022 года каждое четвертое преступление в России совершается с использованием ИТКТ, а с 2023 года – уже каждое третье. Кроме того, увеличилось количество заведомо ложных сообщений об актах терроризма, из которых более 92% совершены дистанционно. Таким образом фиксируется значительное увеличение

количества преступлений с использованием высоких технологий. В этой сфере в 2023 году было зарегистрировано на 29,7% больше уголовно наказуемых деяний, чем в январе-декабре 2022 года. Подобных преступлений раскрыто на 21% больше, чем в 2022 году. Однако их профилактика, как считают в ведомстве, по-прежнему остается одной из важнейших задач органов внутренних дел [8].

Таким образом, анализируя официальную статистику МВД РФ, прослеживается тенденция к дальнейшему росту количества преступлений, совершенных с использованием ИТКТ, киберпреступлений.

Киберпреступление выступает как родовое понятие, охватывающее как компьютерную преступность, в собственном значении этого слова, где компьютер является предметом, а информационная безопасность – объектом преступления, так и рассматривается в настоящее время более широко: сюда относят и иные посягательства, где компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности, безопасности личности (например, компьютерное мошенничество и т.п.). Такие составы иногда именуются как «связанные с компьютерными преступлениями». К киберпреступлениям причисляют и иные действия, направленные на поддержание условий для существования киберпреступности и ее развития (создание специальных социальных сетей, онлайн-торговых площадок, электронной почты, атаки компьютерных сетей, создание сайтов, направленных на распространение деструктивной идеологии, а также обмен противозаконной информацией и т.п.). Преступления в сфере ИТКТ включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации – клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.д. через сеть «Интернет», а также вредоносное вмешательство через компьютерные сети в работу различных систем.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства. Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации (УК РФ) [2].

В соответствии с УК РФ преступлениями в сфере компьютерной информации являются:

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ),

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ),

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ) [10)].

По информации компании «Ростелеком-Солар», в 2022 году только в России было выявлено 911 тысяч событий информационной безопасности (information security event) – то есть наличия определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [6], грозят утечками данных, выходом серверов из строя и другими проблемами в сфере информационной безопасности. При этом количество information security event растёт из года в год, и существенную их долю составляют кибератаки [11].

Общественная опасность противоправных деяний в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ

и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия.

В современном мире увеличивается тенденция и усложняются методы, средства и способы завладения информацией граждан и предприятий, которое влечёт причинение имущественного и интеллектуального ущерба [12].

С 2012 года в УК РФ введена уголовная ответственность по статье – 159.6 «Мошенничество в сфере компьютерной информации». Согласно данной норме мошенничество в сфере компьютерной информации – это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В целях обеспечения единообразного правоприменения нормы указанной статьи УК РФ, Верховным Судом Российской Федерации даны соответствующие разъяснения в Постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [4].

В частности, высшей судебной инстанцией разъяснено, что по смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или

приобрести право на него.

Если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, Интернет-магазинов, использование электронной почты), то такое мошенничество квалифицируется как общеуголовное по статье 159 УК РФ (Мошенничество), а не по статье 159.6 УК РФ. Статья 187 УК РФ устанавливает ответственность за изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами.

Предметом данного преступления могут являться пластиковые карты, позволяющие лицу пользоваться денежной суммой, находящейся на кредитном или дебетовом счете, а также иные платежные документы, не являющиеся ценными бумагами, например, платежные требования, платежные поручения и пр. Общественная опасность такого преступления состоит в прямом финансовом ущербе, причиненном как держателям, так и эмитентам платежных документов, а также в подрыве оборотоспособности платежных инструментов, снижении доверия к ним. Таким образом, в связи с развитием и совершенствованием информационных технологий, киберпреступность расширяется и совершенствуется, представляя все новые серьезные угрозы.

В период с 2021 по 2023 годы преступления, совершённые с использованием ИТКТ продолжали оставаться одними из самых актуальных вопросов и в городе Мичуринске Тамбовской области – зарегистрировано 223 указанных факта (2020г.– 220); из них 145 мошенничеств, 78– краж с банковских карт).

С целью стабилизации оперативной обстановки на данном направлении сотрудниками правоохранительных органов раскрыто 38 краж с банковских счетов (п. «г» ч.3 ст. 158 УК РФ) (2020г.– 27), количество раскрытых

преступлений увеличилось на 40,7%.

В сложившейся ситуации в 2021 году проводились масштабные профилактические мероприятия, в ходе которых сотрудниками ОМВД России по городу Мичуринску было проведено более 30 тысяч бесед с гражданами, а также осуществлён обзвон более 4 тысяч пользователей сайта «Авито», разместивших на нем свои контактные данные; в городских СМИ размещено более 30 тематических материалов (в общей сложности более 8 тысяч просмотров в сети Интернет).

При этом, в рассматриваемый период, отмечено повышение результативности работы по раскрытию мошенничеств общеуголовной направленности. При общем снижении количества преступлений на 4,9 % (с 203 до 193), число нераскрытых снизилось на 23,7% (со 173 до 132), тогда как число оконченных производством уголовных дел возросло на 53,1% (с 32 до 49); раскрываемость составила 27,1% (по области – 23,2%).

В этой связи следует указать, что из 132 приостановленных производством уголовных дел, 116 составили преступления, совершённые с применением ИТКТ, которые по истечении сроков расследования не имели дальнейших перспектив раскрытия.

Тем не менее, работа по раскрытию преступлений рассматриваемой категории осуществляется сотрудниками ОМВД на постоянной основе – в 2022 году удалось окончить производством и направить в суд 49 уголовных дел (из них 10 – по преступлениям, совершённых в IT сфере, в основном, по фактам внесения заведомо ложных сведений при оформлении онлайн-кредитов).

Правоохранительными органами города инициативно выявлены и раскрыты 24 кражи с банковский счетов (п. «г» ч. 3 ст. 158 УК РФ). В 2022 году также проведено большое количество профилактических бесед, обзвонов преимущественно пользователей сайта «Авито», разместивших свои персональные данные на онлайн-платформе, публикации информационных материалов в СМИ и оповещения граждан посредством громкой связи в

общественных местах.

Следует указать, что на протяжении всего 2023 года продолжала оставаться актуальной проблема эффективности профилактики мошенничеств.

Количество таких преступлений возросло со 164 до 227, нераскрыто 171 преступление, из 308 преступлений, находящихся в расследовании, окончено – 67. Всего окончено производством и направлено в суд 67 уголовных дел рассматриваемой категории, тогда как 171 преступление остались нераскрытыми (из них 76 тяжких), что является негативным показателем. Уровень неотвратимости наказания обеспечен на 28,2% (2022 г. – 6,2%, по области –16,6%).

В сложившейся ситуации на постоянной основе продолжали проводиться различные мероприятия по информированию граждан о новых угрозах и действиях злоумышленников. Проведённый анализ показал, что в 2023 году в дежурную часть поступило более 600 сообщений от граждан о звонивших мошенниках, однако, в результате проведённой профилактической работой с гражданами, факты мошенничества по ним допущены не были.

Однако, следует указать, что статистические данные о киберпреступности по городу Мичуринску Тамбовской области, и по стране в целом, не дают полной и объективной картины состояния преступности в этой сфере из-за высокой ее латентности. Для уяснения и понимания феномена киберпреступности необходимо изучение мнений экспертов, которые позволяют определить ее современные тенденции в России. Повышение роли высоких технологий, по мнению специалистов, обусловливает нарастание киберпреступности, ее усложнение, усиление организованности, влечет появление все новых преступных схем и еще большую латентизацию. Наиболее распространенными преступлениями сегодня становятся преступления, связанные с обслуживанием кредитных карт, пользованием интернет-банкингом, в том числе с применением мобильных устройств, незаконные снятия денежных средств, преступления в сфере интернет-торговли,

вымогательство, имеет место кибернаемничество как новый вид преступного бизнеса [5].

Использование компьютерных данных в преступных целях правонарушителями часто влечет совершение других преступлений, совершаемых по совокупности, к примеру, похищение персональных данных лица может повлечь совершение другого общественно опасного деяния – вымогательства и т.п. [13].

Следует также обратить внимание, что современные трансформации киберпреступности отражаются на характеристиках лиц, совершающих киберпреступления. Если ранее это были люди, обладавшие специальными познаниями в IT-сфере, преследующие не столько противозаконные цели, сколько ищущие новые «горизонты», или подростки, использующие чужие реквизиты доступа либо распространяющие вредоносное программное обеспечение, или «проповедники» свободы доступа к информации, то в настоящее время за киберпреступлениями стоят организованные преступные сообщества [14].

Доктрина информационной безопасности России, утверждённая Указом Президента РФ 5 декабря 2016 г. № 646, под информационной безопасностью Российской Федерации определяет состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [3].

Деятельность по обеспечению информационной безопасности в государстве является непрерывным и целенаправленным процессом, поскольку киберпреступность активно усовершенствуется и уже представляет серьезную угрозу не только нашему обществу, но и непосредственно государству.

В этой связи на первый план выступает задача определения упреждающих

мер борьбы с огромным спектром преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, создание эффективных средств и механизмов, которые при их грамотном дальнейшем развитии и использовании могли бы помочь правоохранительным структурам более эффективно бороться с киберпреступностью.

Список литературы:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3448.

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 14.02.2024) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

3. Доктрина информационной безопасности России, утв. Указом Президента РФ 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

4. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. № 2. Февраль, 2018.

5. Криминология и предупреждение преступлений / О.Р. Афанасьева, М.В. Гончарова, В.И. Шиян // 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 356с. (Профессиональное образование).

6. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (Переиздание) // Официальное издание. М.: Стандартинформ, 2020.

7. Козачок В.И, Власова С.А. Информация и ее значение в процессе развития современного общества // Гуманитарные, социально-экономические и общественные науки. 2014. №2.

8. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2023 года // МВД Российской Федерации. – URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 12.03.2024).

9. Маклаков А. От почты до смартфона: как обеспечить устойчивую защиту корпоративной сети // Коммерсантъ. – URL: https://www.kommersant.ru/doc/6495748?erid=4CQwVszH9pWvp5fYL7u (дата обращения: 12.03.2024).

10. О преступлениях в сфере информационных технологий// URL: https://epp.genproc.gov.ru/web/proc_50/activity/legaleducation/explain?item=57103504(дата обращения 20.03.2024).

11. Отчет о кибератаках на российские компании в 2022 году // URL: https://rt-solar.ru/analytics/reports/3332 / (дата обращения: 01.03.2024).

12. Что такое киберпреступность? Защита от киберпреступности // URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 04.03.2024).

13. Федоров А.В. Информационная безопасность в мировом политическом процессе: учебное пособие // Московский гос. ин-т международных отношений (ун-т) МИД России. Москва: МГИМО-Ун-т, 2006. – 218с.

14. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор / Ю. М. Антонян, Д. А. Бражников, М. В. Гончарова и др. // М.: ФГКУ «ВНИИ МВД России», 2018. 86 с.

УДК 004.056.5

CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES: GENERAL

CHARACTERISTICS AND STATE OF CYBERCRIME (ON THE EXAMPLE OF THE CITY OF MICHURINSK, TAMBOV REGION)

Svetlana V. Belyakova
candidate of law sciences, associate professor
belsvet170@mail.ru
Artyom K. Mechnik
student
mechnik41@gmail.com
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. The article considers certain corpus delicti committed using information and telecommunication technologies, identifies certain difficulties that occur in solving such crimes, and also analyzes such offenses committed in the period from 2021 to 2023 in the city of Michurinsk, Tambov Region. Some aspects that require improving cybercrime protection systems and organizing the work of law enforcement agencies are considered.

Key words: information security, cybercrime, information protection, preventive measures.

Статья поступила в редакцию 03.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 27.06.2024.

The article was submitted 03.05.2024; approved after reviewing 13.06.2024; accepted for publication 27.06.2024.