СТАТЬЯ

УДК 343.3/.7

КИБЕРПРЕСТУПНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ОСНОВНЫЕ МЕТОДЫ БОРЬБЫ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Шикула И.Р., Куркин Е.Н.

ФГБОУ ВО «Российский государственный университет правосудия», Москва, e-mail: ila.vnii@mail.ru, zhenja-kurk0@mail.ru

В настоящее время процессы цифровизации распространились на все сферы общественной жизни, что породило новый вид преступности – киберпреступность. У нее существует особенность, заключающаяся в наличии киберпространства, которое не имеет каких-либо границ и пределов. В связи с этим, чтобы обеспечить информационную безопасность государства, были приняты пять федеральных законов и введена 28 глава в Уголовный кодекс Российской Федерации, содержание которых раскрыто в данной работе. Для реализации указанных законодателем положений в структуре Министерства внутренних дел РФ были созданы Управление «К» и отделы БЭП МВД РФ. Также частными компаниями проводятся исследования в области защиты конфиденциальной информации и мероприятия по обеспечению кибербезопасности – ярким примером является Лаборатория Касперского. При этом важно правильно использовать и совершенствовать ИКТ, что предусматривают Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы и Доктрина информационной безопасности Российской Федерации, основные положения которых отражены авторами в данной работе. Несмотря на проделанный путь в области профилактики и противодействия киберпреступности, существует ряд проблемных аспектов в методах борьбы с ней, которые освещены в настоящей статье.

Ключевые слова: цифровизация, киберпреступность, противодействие, Управление «К», Лаборатория Касперского

CYBERCRIME IN THE RUSSIAN FEDERATION: MAIN METHODS OF FIGHTING AND PROBLEMS OF COUNTERING

Shikula I.R., Kurkin E.N.

Russian State University of Justice, Moscow, e-mail: ila.vnii@mail.ru, zhenja-kurk0@mail.ru

Currently, digitalization processes have spread to all spheres of public life, which has given rise to a new type of crime – cybercrime. It has the peculiarity of having a cyberspace that does not have any boundaries and limits. In this regard, five federal laws were adopted and Chapter 28 was introduced into the Criminal Code of the Russian Federation to ensure the information security of the state, the content of which is disclosed in this work. In order to implement the provisions specified by the legislator in the structure of the Ministry of Internal Affairs of the Russian Federation, the Directorate «K» and the Departments of the BEP of the Ministry of Internal Affairs of the Russian Federation were created. Private companies also conduct research in the field of protecting confidential information and cybersecurity activities – a prime example is Kaspersky Lab. At the same time, it is important to correctly use and improve ICT, which is envisaged by the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 and the Doctrine of Information Security of the Russian Federation, the main provisions of which are reflected author in this work. Despite the progress made in the field of preventing and combating cybercrime, there are a number of problematic aspects in the methods of combating it, which are highlighted in this article.

Keywords: digitalization, cybercrime, counteraction, K Management, Kaspersky Lab

В данный момент цифровизация охватила все мировое сообщество. Многие повседневные вопросы и задачи стали практически моментально решаться отдельными лицами и организациями даже на расстоянии десятков тысяч километров. Такая тенденция вызвана массовым увеличением пользователей интернет-технологий. Согласно отчету Digital в январе 2020 г. было зафиксировано 4,54 млрд пользователей интернета, а в начале 2021 г. количество интернет-пользователей составило 4,66 млрд чел. Такое активное использование интернет-технологий породило угрозу появления злоумышленников. Об этом свидетельствуют статистические отчеты Министерства внутренних дел Российской Федерации, а именно в 2019 г. количество киберпреступлений составило 294 000, в 2020 г. – 572 124, в 2021 г. – 715 155. Это обусловлено объективным и субъективным факторами. Первый связан с пандемией COVID-19, потому что было введено множество ограничений в короткий промежуток времени, касающихся масочного режима; запрета массовых мероприятий; перехода на дистанционный режим обучения и работы. К таким условиям не были готовы ни обычные пользователи, ни поставщики интернет-сети. Второй фактор относится к психологии преступника, так как правонарушитель совершает противоправные действия, на которые не осмелился бы в реальном мире [1, с. 139].

Поэтому противодействие киберпреступности становится одним из приоритетных направлений уголовной политики в Российской Федерации и целью исследования является выявление проблемных аспектов в методах борьбы с ней.

Материалы и методы исследования

Основу работы составил анализ нормативно-правовой базы, теоретических и практических исследований в области противодействия и борьбы с киберпреступностью.

Основные методы, используемые в работе:

1. Диалектический метод стал методологической основой данного исследования, так как явление киберпреступности рассматривается всесторонне (предпосылки, изменения, перспективы развития).

2. Сравнительно-правовой метод позволил проанализировать действующие нормативно-правовые акты, регулирующие аспекты охраны виртуального пространства в РФ.

3. Системный метод использовался, чтобы изучить структуру и полномочия органов государственной власти, занимающихся вопросами кибербезопасности.

4. Статистический метод применялся, чтобы выявить основные причины и тенденции развития киберпреступности.

Результаты исследования и их обсуждение

Следует заметить, что принято пять федеральных законов о защите информации и информационной безопасности. Первый из них вводит ключевые понятия, принципы правового регулирования информации и устанавливает наличие цифровых правоотношений. Он запрещает сбор и оборот информации о жизни человека без его согласия и пропаганду информации, касающейся насилия и дискриминации; устанавливает равенство цифровых технологий, то есть запрет на применение каких-либо определенных технологий, и наличие государственного реестра запрещенных сайтов; закрепляет общедоступную информацию, к которой не может быть ограничен доступ; возлагает обязанности по защите информации от третьих лица на субъекта, который ее хранит [2].

Второй акт регулирует работу с персональными данными отдельных людей. Он обязывает осуществлять сбор и обработку персональных данных с конкретной целью и получать согласие владельца; запрещает транснациональную пересылку персональных данных, то есть их хранение возможно только на территории Российской Федерации [3].

Третий нормативно-правовой акт вводит коммерческую тайну; определяет, каким образом ее охранять и какие возникнут последствия в случае разглашения. Он предоставляет субъективное право на самостоятельное определение сведений, составляющих коммерческую тайну путем составления специального документа, а также определяет, какая информация не может быть отнесена к коммерческой тайне; обязывает организацию предоставить сведения, составляющие коммерческую тайну, по запросу государственных органов и вести учет лиц, кому она доступна [4].

Четвертый закон касается электронной подписи, которая выступает аналогом традиционной. Для ее создания можно применять любое программное обеспечение, которое обеспечит надежную защиту. Электронная подпись может быть простой, усиленной и квалифицированной. При этом лица, которые используют третий вариант, обязаны хранить ее ключ, и только специальный орган может выдавать сертификат, подтверждающий подлинность электронной подписи [5].

Пятый акт регулирует деятельность организаций, работающих в критически важных сферах, таких как энергетика, связь, транспорт и др. Для защиты этих объектов создана государственная система обнаружения, предупреждения и ликвидации кибератак, поэтому каждая организация обязана к ней подключиться. В свою очередь, субъекты критической информационной инфраструктуры должны докладывать о случившихся инцидентах. Также государственные органы уполномочены проводить внеплановые проверки на предмет использования сертифицированного программного обеспечения, потери информации после взлома и на соблюдение остальных особых требований, установленных законодательством [6].

На современном этапе фундаментальным документом является «Стратегия информационного общества РФ» [7]. Принятие данного нормативно-правового акта обусловлено тем, что цифровые инструменты, среди которых социальные сети, СМИ, стали неотъемлемой составляющей образа жизни граждан РФ. Она отразила развитие до 2030 г., которое предусматривает цели, задачи и способы проведения внутренней и внешней политики РФ в области использования и совершенствования ИКТ. Приоритетом является достоверная и качественная информация, которая выступает предпосылкой к становлению цифрового общества РФ и востребованности российских IT-технологий на международном уровне. Это достигается за счет исключения анонимности и привлечения правонарушителей к ответственности путем создания системы защиты конфиденциальной информации при использовании цифровых устройств.

Следует заметить, что «Доктрина информационной безопасности РФ» предусматри-

вает цели, задачи, принципы и направления такого вида безопасности в России [8]. Она представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Под цифровой безопасностью понимается всесторонняя защита интересов личности, общества и государства в IT-среде. Стабильное и безопасное получение информации, а также ее охрана от неправомерного доступа органами предварительного расследования позволяют удовлетворить интересы отдельной личности. Такой подход в сочетании с формированием механизмов правового государства в информационной среде соответствует интересам общества. Интересы государства достигаются посредством создания современной цифровой инфраструктуры, эффективного международного взаимодействия для защиты национальной безопасности.

Помимо этого, действующий Уголовный кодекс Российской Федерации включает в себя 28 главу, которая предусматривает отдельные виды киберпреступлений. Она устанавливает ответственность за несанкционированное вмешательство в компьютерную информацию; деятельность с вредоносным программным обеспечением; нарушение правил применения средств по работе с информационно-коммуникационных сетями, при этом не выделяя общие киберпреступления [9].

В настоящее время главным органом по противодействию киберпреступности стало Министерство внутренних дел РФ. В его структуре существует Управление «К», центральной задачей которого является борьба с киберпреступностью. История данного подразделения начинается с 1986 г., когда в составе МВД СССР было учреждено Управление «Р» для противодействия незаконному доступу в информационные сети ведомства через устранение радиопомех. На тот момент подразделение решало только оперативные задачи. Затем в 1997 г. ему были переданы оперативно-розыскные полномочия в связи с принятием 28 главы УК РФ.

Кроме того, в 1997 г. в субъектах федерации были учреждены Отделы по борьбе с преступлениями в сфере компьютерной информации и экономики. ОБЭП наделялись полномочиями органа дознания и плотно сотрудничали с Управлением «К». Наряду с этим в 1998 г. в Волгоградской академии МВД РФ были выпущены первые специалисты по расследованию преступлений в сфере компьютерной информации.

Помимо этого, существуют частные компании, которые занимаются исследованиями по защите конфиденциальной информации и обеспечению кибербезопасности. Среди них Лаборатория Касперского, которая вышла на международный уровень. В настоящее время более 400 млн физических лиц и более 270 тыс. юридических лиц стали пользователями программного обеспечения, разработанного высококвалифицированными специалистами и проверенного многолетним опытом.

Таким образом, основные методы борьбы с киберпреступностью сводятся к нормативно-правовому регулированию и созданию специальных органов. Законодателем был разработан и принят ряд документов, который предусматривает цели, задачи, приоритеты и угрозы кибербезопасности РФ, а также криминализацию отдельных составов в УК РФ. Наряду с этим происходило учреждение государственных органов и частных компаний по противодействию киберпреступности. Среди первых Управление «К» и отделы БЭП МВД РФ, ко вторым относится Лаборатория Касперского.

В настоящее время, несмотря на всю проделанную работу, законодательство о виртуальном пространстве находится на начальной стадии, потому что бурное развитие цифровых технологий и рост киберпреступности произошли относительно недавно. В связи с этим существуют определенные пробелы, которые порождают безнаказанность действий злоумышленников.

В данный момент ст. 171.2 УК РФ установлена ответственность за неправомерную организацию и проведение азартных игр. На современном этапе информационные технологии усовершенствовали такие посягательства, в частности появились онлайн-казино. Оно обладает большей степенью общественной опасности, так как предоставляет удаленный доступ игрокам; участники могут скрывать свои подлинные имена, используя никнейм; требования к стартовому капиталу для учредителей таких заведений гораздо меньше, чем для традиционных [10, с. 15]. В основном совершаются мошеннические действия с персональными данными, реквизитами банковских карт. Это обусловлено тем, что такая информация предоставляется организаторам при входе в онлайн-казино. При этом факт мошенничества трудно доказать из-за возможности анонимного входа.

На современном этапе затрудняется сотрудничество между банковскими, финансово-кредитными организациями, операторами сотовой связи и правоохранительными органами, потому что отсутствует общая система оперативного обмена информацией. В связи с этим киберпреступникам удается скрыть следы общественно опасного

посягательства, так как получение сведений происходит через долгие бюрократические процедуры. Были предприняты меры для преодоления такой проблемы, а именно обязали операторов связи хранить всю необходимую информацию с телефонов в базах данных на территории Российской Федерации. При этом отсутствует практическое применение данной нормы, и возникла новая проблема, связанная с хранением такого большого объема данных.

В настоящее время не предусмотрена уголовная ответственность за фишинг. Он представляет собой противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией. Как и обычные люди, использующие множество способов ловли рыбы, злоумышленники также применяют разнообразные методы, позволяющие «поймать на крючок» свою жертву. Например, потерпевший получает электронное письмо или текстовое сообщение, отправитель которого выдает себя за определенное лицо или организацию, которым он доверяет. Когда получатель открывает данное сообщение, то он обнаруживает пугающий текст, который требует от жертвы перейти на веб-сайт и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий. Если пользователь «клюет на наживку» и переходит по ссылке, то он попадает на веб-сайт, имитирующий тот или иной законный интернет-ресурс. На этом веб-сайте пользователя просят «войти в систему», используя логин и пароль. Введенные данные попадают напрямую к злоумышленникам, которые затем используют их для кражи конфиденциальной информации или денежных средств с банковских счетов.

Следует уделить фишингу должное внимание, так как доходы, полученные в результате посягательства, являются достаточно прибыльными. Также потерпевшими наряду с обычными гражданами становятся дети и пенсионеры, которые составляют особую группу риска. В дополнение к этому злоумышленники совершенствуют инструменты фишинга, потому что «фейковый» сайт становится трудно отличить от подлинного [11, с. 167].

Помимо этого распространение получила молодежная киберпреступность. Это обусловлено тем, что несовершеннолетние имеют разнообразные гаджеты и доступ к неограниченному потоку информации в интернет-пространстве. В такой ситуации их нестабильная психика легко подвергается отрицательному воздействию.

Кроме того, возникает проблема с видеоиграми, которые распространились до введения федерального закона [12], а также имеют международные стандарты. В дополнение к этому родители перед приобретением не уделяют должного внимания изучению презентационного материала и легкомысленно относятся к возрастным ограничениям. Также онлайн-игры, которые были официально запрещены в российском виртуальном пространстве, встречаются на различных «торрент»-ресурсах и пиратских сайтах.

Помимо этого, преследования и домогательства приобрели виртуальный формат. Подобные деяния именуются кибersталкингом. Под ним понимается система действий в отношении отдельного пользователя с целью запугать жертву с применением цифровых технологий. Законодатель привлекает к уголовной ответственности за определенные действия, такие как клевета и доведение до самоубийства.

Кроме того, доведение до самоубийства происходит посредством киберунижения. Оно осуществляется путем подрыва авторитета личности в сети через оскорбления и шантаж, например необоснованная критика жертвы нецензурными словами или демонстрация смонтированных фото, отражающих интимную сторону жизни потерпевшего. При этом возникают проблемы с привлечением к уголовной ответственности, связанные с возрастом злоумышленников или отсутствием тяжких последствий при совершении кибersталкинга, что служит отказом в возбуждении уголовного дела.

Стоит отметить, что киберпреступления имеют свои особенности, в отличие от традиционных, к которым относятся транснациональный характер и сложность в объединении национальных законодательств для проведения расследования и сбора доказательной базы. Российская Федерация приняла нормативно-правовые акты, регулирующие развитие цифрового общества и борьбу с возникающими угрозами. Они содержат основные цели, задачи, приоритеты, методы и способы противодействия киберпреступности. При этом принципы, применяемые в деятельности органов предварительного расследования в традиционных преступлениях, малоэффективны, также окончательно не поставлена система государственных экспертных учреждений; существует наличие затяжных правовых процедур во взаимодействии между органами предварительного расследования, обществом и частными учреждениями.

Заключение

Таким образом, киберпреступность стремительно расширяет свой масштаб, она проникла во все сферы общественной жизни, включая бизнес-структуры, общественную и личную жизнь граждан. Законодательство РФ не содержит определения данного понятия, но существуют смежные понятия, среди которых информационно-коммуникационные технологии; преступления в сфере компьютерной информации и др. Проведенный анализ затрагивает не все проблемы, связанные с киберпреступностью, так как цифровые технологии стремительно развиваются, что порождает появление новых способов совершения киберпреступлений и методов борьбы с ними.

Список литературы

1. Брылева Т.О. Основополагающие принципы противодействия киберпреступности в Российской Федерации // Киберпреступность: риски и угрозы: материалы всероссийского студенческого круглого научно-практического стола с международным участием (Санкт-Петербург, 11 февраля 2021 г.). СПб.: Астерион, 2021. 139 с.

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 08.01.2023).

3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 08.01.2023).

4. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 08.01.2023).

5. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 08.01.2023).

6. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 08.01.2023).

7. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 08.01.2023).

8. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: https://base.garant.ru/71556224/ (дата обращения: 08.01.2023).

9. Уголовный кодекс Российской Федерации от 13.06.1996 г. (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 08.01.2023).

10. Лихолетов А.А. Преступления в сфере игорного бизнеса: уголовно-правовые и криминологические аспекты. Волгоград, 2015. 15 с.

11. Журмухамбетова С. Тенденции развития кибербезопасности в борьбе с киберпреступностью // Киберпреступность: риски и угрозы: материалы всероссийского студенческого круглого научно-практического стола с международным участием (Санкт-Петербург, 11 февраля 2021 г.). СПб.: Астерион, 2021. 167 с.

12. Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями и дополнениями) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 08.01.2023).