DOI 10.22394/2686-7834-2022-2-65-69

Киберпреступность как угроза национальной безопасности России

Лепешкина Оксана Ивановна

Северо-Западный институт управления Российской академия народного хозяйства и государственной службы при Президенте Российской Федерации (Санкт-Петербург, Российская Федерация)

доцент, кандидат юридических наук, e-mail: lepeshkina-oi@ranepa.ru.

АННОТАЦИЯ

Целью статьи является определение основных направлений по повышению эффективности противодействия киберпреступности в России. В статье рассмотрены правовая основа России и международные правовые акты о противодействии киберпреступности, а также положения проекта Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях, направленного в ООН 30 июля 2021 г.

В статье определены понятия «киберпреступление», «киберпространство», «кибербезопасность» в соответствии с международными стандартами Международной организации по стандартизации и Международного союза электросвязи. В статье рассмотрена предложенная в уголовно-правовой науке классификация киберпреступлений.

Автор вносит предложения по основным направлениям государственной политики в области противодействия киберпреступности.

Ключевые слова: киберпреступность, компьютерная преступность, высокотехнологичная преступность, киберпространство, кибербезопасность, киберзащищенность.

Cybercrime as Threat of National Security of Russia

Oksana I. Lepeshkina

North-West Management Institute of the Russian Presidential Academy of National Economy and Public Administration (Saint Petersburg, Russian Federation)

PhD in Jurisprudence, Associate Professor; e-mail: lepeshkina-oi@ranepa.ru.

ABSTRACT

The aim of this article is determination of main lines on rise efficacy of anti- cybercrime in Russia. This article describes the Russian law base and international law acts about anti-cybercrime, and also norms of project of Convention United Nations Countering the use of information and communications technologies for criminal purposes, which Russia sent to United Nations in 30 July of 2021.

There are the terms “cybercrime”, “cyberspace”, “cybersecurity” in according with international standards of International Organization for Standardization and International Telecommunication Union in this article. There is classification of cybercrimes in this article, which is in criminal law theory.

The author makes proposals of main lines of national politics in sphere of anti-cybercrime.

Keywords: cybercrime, computer crime, high-tech crime, cyberspace, cybersecurity, cybersafety.

Информационная безопасность является одной из составляющих национальной безопасности.

Стратегией национальной безопасности Российской Федерации рост числа преступлений, совершаемых с использованием информационно-коммуникационных технологий, рассматривается как одна из угроз национальной безопасности, а их предупреждение, выявление, пресечение является стратегическим национальным приоритетом (п. 42)[1].

Как показывает статистика, количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в последние годы значительно увеличилось. По данным ГИАЦ МВД России, таких преступлений было зарегистрировано: в 2019 г. — 294 409 (рост на 68,5%), в 2020 г. — 510 396 (рост на 73,4%), в 2021 г. — 517 722 (рост на 1,4%)[2].

Преступления с использованием IT-технологий в основной массе совершаются в кредитно-финансовой сфере и влекут для государства большой экономический ущерб, который, по оценке

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 2 июля 2021 г. № 400 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 05.03.2022).

[2] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://мвд.рф/ (дата обращения: 04.03.2022).

Банка России, способен спровоцировать финансовый кризис. Так, к основным рискам в данной сфере Банк России относит финансовые потери клиентов, отдельных финансовых организаций, нарушение операционной надежности и непрерывности предоставления финансовых услуг, развитие системного кризиса в результате кибератак в значимых для финансового рынка организациях[3]. Предпочтительными становятся финансовые услуги государств с более высоким уровнем киберустойчивости финансовых организаций, например таких, как США, Великобритания, Канада, Сингапур, Япония, Австралия, Австрия, Новая Зеландия, Малайзия.

По данным Банка России, в 2020 г. количество операций без согласия клиента увеличилось на 34,0% (773 008 операций против 576 897 операций за 2019 г.). Объем таких операций вырос на 52,2%, составив 9777,3 млн руб. (в 2019 г. — 6425,8 млн руб.)[4]. В основном такие операции осуществлялись с использованием методов социальной инженерии.

Под угрозой кибератак находятся объекты критической информационной инфраструктуры и международная информационная безопасность.

Стратегическим, основополагающим документом в области обеспечения информационной безопасности является Доктрина информационной безопасности Российской Федерации, согласно которой «обеспечение информационной безопасности — осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления» (п. 2)[5].

В соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[6] создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Обеспечение функционирования Государственной системы возложено на Федеральную службу безопасности РФ, и создан Национальный координационный центр по компьютерным инцидентам.

Следует отметить, что в ряде государств приняты стратегии по кибербезопасности, что было рекомендовано Международным союзом электросвязи в Руководстве по разработке национальной стратегии кибербезопасности 2018 г. Стратегии кибербезопасности приняты в таких государствах, как США, Великобритания, Финляндия, Германия, Канада, Новая Зеландия, Индия. В государствах СНГ, например в Казахстане, принята Концепция кибербезопасности («Киберщит Казахстана») (утв. Постановлением Правительства Республики Казахстан от 30 июня 2017 г. № 407). В Кыргызстане принята Стратегия кибербезопасности Кыргызской Республики на 2019–2023 гг. (утв. Пост. Правительства Кыргызской Республики от 24 июля 2019 г. № 369).

Вопросы обеспечения информационной безопасности, в том числе международной информационной безопасности, в настоящее время в числе приоритетных в международном сотрудничестве государств.

Однако международная правовая основа регулирования противодействия совершению преступлений в сфере кибертехнологий только создается. Более интенсивно сотрудничество государств в этой области осуществляется на региональном уровне.

В рамках Совета Европы непосредственно на противодействие киберпреступности направлена Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г.[7] Данную Конвенцию ратифицировали 66 государств, в том числе из не членов Совета Европы — Израиль, США и Япония. В числе государств СНГ данную Конвенцию ратифицировали Азербайджанская Республика, Республика Армения и Республика Молдова.

---

[3] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 гг. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_363745/ (дата обращения: 05.03.2022).

[4] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 г. [Электронный ресурс]. URL: https://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (дата обращения: 29.07.2021).

[5] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 г. № 646 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 05.03.2022).

[6] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 05.03.2022).

[7] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. [Электронный ресурс]. Доступ из СПС «Гарант». URL: https://base.garant.ru/4089723/ (дата обращения: 05.03.2022).

Россия не подписала эту Конвенцию, усмотрев в положениях п. «b» ст. 32 о возможности трансграничного доступа к хранящимся компьютерным данным без согласия другого государства, по сути, вмешательство в юрисдикцию и нарушение прав и законных интересов граждан и юридических лиц.

В ООН резолюцией Генеральной Ассамблеи 74/247 от 27 декабря 2019 г. был учрежден Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

По инициативе России 26 мая 2021 г. на 75-й сессии Генеральная Ассамблея ООН приняла резолюцию 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Согласно данной резолюции Специальный комитет должен представить Генеральной Ассамблее ООН проект конвенции на ее 78-й сессии[8].

Письмом от 30 июля 2021 г. Россия направила в Генеральную Ассамблею ООН проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. Проект этой Конвенции включен в резолюцию Генеральной Ассамблеи ООН 75/980, принятой на 75-й сессии 10 августа 2021 г.[9]

Терминология в области обеспечения кибербезопасности определена в двух межгосударственных стандартах — Международной организации по стандартизации (International Organization for Standardization, ISO) и Международного союза электросвязи (International Telecommunication Union, ITU).

В Международном стандарте «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity) содержатся термины: «кибербезопасность», «киберпреступление», «киберпространство», «киберзащищенность»[10].

Кибербезопасность — «сохранение конфиденциальности, целостности и доступности информации в киберпространстве».

Киберпреступление — «преступная деятельность, при которой сервисы или приложения киберпространства являются орудием или целью преступления или при которой само киберпространство является источником, инструментом, целью или местом преступления».

Киберпространство — «сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в сети Интернет посредством связанных с ней технологических устройств и сетей, не существующая в физической форме».

Киберзащищенность — «состояние защищенности от физических, социальных, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или иных негативных последствий, наступивших в результате отказов, повреждений, ошибок, инцидентов, несчастных случаев и прочих событий в киберпространстве, рассматриваемых как нежелательные».

Международным союзом электросвязи утверждена рекомендация МСЭ-Т X.1205 (04/2008) «Серия X: Сети передачи данных, взаимосвязь открытых систем и безопасность. Безопасность электросвязи». В данной рекомендации определены термины «киберсреда», «кибербезопасность»[11].

Киберсреда «включает пользователей, сети, устройства, всё программное обеспечение, процессы, сохраненную или транзитную информацию, приложения, услуги и системы, которые могут быть прямо или косвенно соединены с сетями».

Кибербезопасность — «это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств

---

[8] Резолюция, принятая Генеральной Ассамблеей 26 мая 2021 г. [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/75/282 (дата обращения: 05.03.2022).

[9] Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 г. на имя Генерального секретаря [Электронный ресурс]. URL: https://undocs.org/ru/A/75/98 (дата обращения: 05.03.2022).

[10] ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity [Electronic resources]. URL: https://www.iso.org/standard/44375.html (дата обращения: 30.03.2022).

[11] Рекомендация МСЭ-Т X.1205 (04/2008) [Электронный ресурс]. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru (дата обращения: 30.03.2022).

безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее:

- доступность;
- целостность, которая может включать аутентичность и неотказуемость;
- конфиденциальность».

В Конвенции о преступности в сфере компьютерной информации от 23 ноября 2001 г. к киберпреступлениям отнесены: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств); 2) преступления, связанные с использованием компьютерных средств (подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий); 3) преступления, связанные с содержанием данных (преступления, связанные с детской порнографией); 4) преступления, связанные с нарушением авторского права и смежных прав (ст. 2–10).

В проекте Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях, внесенном Россией в Генеральную Ассамблею ООН 30 июля 2021 г., указаны следующие преступления: неправомерный доступ к цифровой информации; неправомерный перехват; неправомерное воздействие на цифровую информацию; нарушение функционирования информационно-коммуникационных сетей; создание, использование и распространение вредоносных программ; неправомерное воздействие на критическую информационную инфраструктуру; несанкционированный доступ к персональным данным; незаконный оборот устройств; хищение с использованием ИКТ; преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ; склонение к самоубийству или доведению до его совершения; преступления, связанные с вовлечением несовершеннолетних в совершение противоправных действий, опасных для их жизни и здоровья; создание и использование цифровой информации для введения пользователя в заблуждение; подстрекательство к подрывной или вооруженной деятельности; преступления, связанные с террористической деятельностью; преступления, связанные с экстремистской деятельностью; преступления, связанные с распространением наркотических средств и психотропных веществ; преступления, связанные с незаконным оборотом оружия; реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности; незаконное распространение фальсифицированных лекарственных средств и медицинских изделий; использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом; нарушение авторских и смежных прав с использованием ИКТ (ст. 6–27).

По вопросу понятия киберпреступности в уголовно-правовой науке имеются разные точки зрения, определение ее как «компьютерная преступность», «интернет-преступность», «цифровая преступность», «высокотехнологичная преступность», «технотронная преступность»[12].

В целом киберпреступность представляет собой совокупность киберпреступлений.

В соответствии с Международным стандартом «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012) киберпреступление — это преступление, полностью совершенное в киберпространстве.

По мнению В. Ф. Джафарли, «киберпреступление — это совокупность объективных и субъективных факторов, характеризующихся посягательствами на специфичный основной (сфера инновационных информационно-коммуникационных технологий) и дополнительные объекты, предметом посягательства (чужие электронные ресурсы), а также реализуемых путем использования кибертехнологий (средств) и дистанционным способом основных общественно опасных действий и желаемых последствий, происходящих и наступающих исключительно в киберпространстве (обстановка и место преступления), во время сеанса связи злоумышленника с ИКТ-устройством»[13].

В. Ф. Джафарли классифицировал все преступления, совершаемые с использованием информационно-коммуникационных технологий, на три группы: 1) «киберпреступления, основные действия и последствия которых происходят исключительно в киберпространстве, причем ИКТ-компонент формально установлен в конкретной норме»; 2) «киберпреступления, основные действия и последствия которых могут происходить исключительно в киберпространстве, причем ИКТ-компонент формально не отражен в конкретной норме»; 3) «преступления, действия в которых в той или иной

[12] См.: *Евдокимов К. Н.* К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации. Российский следователь, 2021. № 10.

[13] *Джафарли В. Ф.* Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. М.: Проспект, 2021. С. 24.

мере связаны с использованием ИКТ-средств»[14]. По этой классификации к киберпреступлениям относятся только две первые группы.

Таким образом, в действующем Уголовном кодексе РФ 1996 г.[15] к киберпреступлениям можно отнести преступления, предусмотренные гл. 28 «Преступления в сфере компьютерной информации» (ст. 272–274.1), а также предусмотренные, например, п. «г» ч. 3 ст. 158 (кража с банковского счета, а равно в отношении электронных денежных средств), ст. 159.3 (мошенничество с использованием электронных средств платежа), ст. 159.6 (мошенничество в сфере компьютерной информации) и ст. 163 (вымогательство), ст. 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием), ст. 135 (развратные действия), ст. 242.1 (изготовление и оборот материалов с порнографическими изображениями несовершеннолетних), если они совершены с использованием ИКТ.

В заключение определим дальнейшие направления по совершенствованию государственной политики в области противодействия киберпреступности.

Для более эффективного противодействия киберпреступности в России, с учетом международного опыта, представляется целесообразным принять Стратегию кибербезопасности.

Кроме того, настоятельно необходимым видится принятие Федерального закона «О противодействии киберпреступности». В настоящее время в рамках Содружества Независимых Государств осуществляется разработка проекта модельного закона «О борьбе с киберпреступностью». Принятие данного модельного закона позволит создать единый правовой механизм противодействия киберпреступности в национальном законодательстве государств — участников СНГ, в том числе в России.

К основным направлениям государственной политики в области противодействия киберпреступности, с учетом положительного зарубежного опыта, по мнению автора, следует отнести следующие: 1) обеспечение безопасности критической информационной инфраструктуры; 2) совершенствование организации деятельности правоохранительных органов; 3) совершенствование системы подготовки и переподготовки сотрудников правоохранительных органов, судей; 4) обеспечение безопасности персональных данных; 5) повышение уровня защищенности информационной инфраструктуры организаций финансово-банковской системы; 6) развитие культуры информационной безопасности и кибергигиены клиентов — потребителей банковских услуг; 7) взаимодействие государственных органов с интернет-провайдерами и операторами сотовой связи; 8) правовая охрана авторских прав на программы для ЭВМ и базы данных и смежных прав; 9) взаимодействие государственных органов с институтами гражданского общества, физическими и юридическими лицами; 10) мониторинг применения законодательства в области противодействия киберпреступности; 11) повышение уровня правовой грамотности и правосознания граждан, создание атмосферы нетерпимости к совершению киберпреступлений; 12) укрепление международного сотрудничества с иностранными государствами, их правоохранительными органами, специальными службами, судебными органами, а также с международными организациями в области противодействия киберпреступности.

Литература

1. *Джафарли В. Ф.* Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. М.: Проспект, 2021. 280 с.
2. *Евдокимов К. Н.* К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации. Российский следователь, 2021. № 10. С. 69–72.

References

1. Dzhafarli, V. F. Criminology of Cybersecurity: in 5 vol. Vol. 2: Criminal Law Preservation of Criminology Cybersecurity [Kriminologiya kiberbezopasnosti: v 5 t. T. 2: Ugolovno-pravovoe obespechenie kriminologicheskoi kiberbezopasnosti]. Editor-in Chief S. Ya. Lebedev. Moscow: Prospekt, 2021. 280 p. (In Rus.)
2. Evdokimov, K. N. On the Improvement of the Technotronic Crime Combating System in the Russian Federation [K voprosu o sovershenstvovanii sistemy protivodeistviya tekhnotronnoi prestupnosti v Rossiiskoi Federatsii]. Russian Examiner [Rossiiskii sledovatel'], 2021. No. 10. P. 69–72. (In Rus.)

[14] Там же. С. 61–62.

[15] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Редакция от 25.03.2022 (с изм. и доп., вступ. в силу с 25.03.2022) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 26.03.2022).