8. Латыпова Э. Ю., Мусина Р. Р. Некоторые проблемы мошенничеств с помощью использования банковской карты с голосовым помощником / Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 107–109.

9. Мусина Р. Р. К вопросу о развитии уголовной ответственности за преступления против собственности в законодательстве России // Oeconomia et Jus. 2019. № 1. С. 64–72.

10. Соколова О. А. Использование результатов диагностических экспертиз по следам человека в уголовном судопроизводстве // Вестник Московского университета МВД России. 2019. № 1. С. 94–98.

11. Соловьева С. М. Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51 (289) С. 161–164.

12. Шевко Н. Р. Информационные технологии в деятельности прокуратуры: преимущества и недостатки / В сборнике: Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 102–106.

О. И. Лепешкина,
кандидат юридических наук, доцент,
Северо-Западный институт управления – филиал Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ

Аннотация. Целью исследования является определение основных направлений реализации государственной политики в области противодействия киберпреступности, а также обозначение перспективы развития ее нормативного правового регулирования. В настоящее время нет единого международного правового механизма противодействия киберпреступности, имеющей транснациональный характер, что затрудняет сотрудничество государств в данной области, развитие и унификацию национального законодательства. Автором сделан вывод о необходимости принятия Стратегии кибербезопасности, Закона «О противодействии киберпреступности» и соответствующей государственной программы.

Ключевые слова: цифровые технологии, киберпреступность, киберпреступление, противодействие киберпреступности, высокотехнологичная преступность, компьютерные преступления, кибербезопасность, киберпространство

THE PRINCIPAL DIRECTIONS OF ANTI-CYBERCRIME IN RUSSIA

Abstract. The goal of this article is to define the principal directions of anti-cybercrime in realization of anti-cybercrime state politics, and also to mark perspectives it's law regulation. There is not the international law mechanism of anti-cybercrime in this time. Therefore, there is difficulty of international collaborate with states about anti-

cybercrime and also development and unification national laws. Author makes conclusion about necessity adoption of Strategy on cybersecurity, the Law “About anti-cybercrime” and state program on this sphere.

Keywords: Digital technology, Cybercrime, Anti-cybercrime, High-tech crime, Computer crime, Cybersecurity, Cyberspace

Введение. Киберпреступность в настоящее время уже представляет угрозу национальной безопасности, что признает все мировое сообщество. Основная часть преступлений с использованием информационных технологий корыстные, совершаемые в кредитно-финансовой сфере, и которые наносят государству значительный экономический ущерб, способный спровоцировать финансовый кризис. Кибератаки осуществляются на критическую информационную инфраструктуру, под угрозой и международная информационная безопасность.

Кроме того, преступления в сфере цифровых технологий имеют транснациональный характер и могут затрагивать интересы нескольких государств.

Вместе с тем пока нет единого международного правового механизма противодействия данным преступлениям, что осложняет взаимодействие государств в этой области, как и затрудняет развитие и унификацию национального законодательства государств.

Наличие такого правового механизма необходимо для решения вопросов выдачи лиц, совершивших киберпреступления, оказания взаимной правовой помощи и иного правоохранительного содействия, ареста и конфискации преступных доходов.

С целью противодействия высокотехнологичной преступности Российская Федерация 30 июля 2021 г. внесла в Генеральную Ассамблею ООН проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (резолюция Генеральной Ассамблеи ООН 75/980, принятая на 75-й сессии 10 августа 2021 г.) [8].

На региональном уровне с целью противодействия киберпреступности 23 ноября 2001 г. Советом Европы была принята Конвенция о преступности в сфере компьютерной информации (Конвенция о киберпреступности) [2]. Данную Конвенцию ратифицировали 66 государств, в том числе из не членов Совета Европы Израиль, США и Япония. Российская Федерация сочла положения пункта «b» ст. 32, согласно которому доступ к компьютерным данным другого государства может осуществляться и без его согласия, вмешательством в юрисдикцию и отказалась подписывать Конвенцию.

Кроме того, 17 ноября 2021 г. Комитет министров Совета Европы принял Второй дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств. Данный протокол был открыт для подписания государствами-участниками Конвенции 12 мая 2022 г.

Таким образом, в настоящее время для эффективного противодействия киберпреступности и другим преступлениям, совершаемым с использованием информационных технологий, требуется расширение сотрудничества государств в данной области и сближение их правовых систем.

Основная часть. Стратегия национальной безопасности Российской Федерации в качестве угрозы информационной безопасности указывает на распространенность

преступлений, совершаемых с использованием информационно-коммуникационных технологий, и стратегическим национальным приоритетом является их предупреждение, выявление и пресечение (п. 42) [3].

Центральный банк Российской Федерации ежегодно публикует данные об атаках на информационную инфраструктуру клиентов – физических и юридических лиц. Так, в 2021 г. общее количество и объем операций, совершенных без согласия клиентов, увеличились на 33,8 и 38,8 % соответственно. Объем таких операций составил 13 582,23 млн руб. (в 2020 г. – 9777,3 млн руб.), количество операций 1 035,01 тыс. ед. [5]

Данные статистики ГИАЦ МВД России показывают постоянный рост в последние годы преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации: в 2019 г. было зарегистрировано 294 409 (рост на 68,5 %) преступлений, в 2020 г. – 510 396 (рост на 73,4 %), в 2021 г. – 517 722 (рост на 1,4 %) [7].

Киберпреступность, являющаяся криминологической категорией, может быть определена как совокупность киберпреступлений.

Киберпреступление – это преступление, полностью совершенное в киберпространстве.

Такое определение понятия киберпреступления соответствует указанному в Международном стандарте Международной организации по стандартизации «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information Technology – Security Techniques – Guidelines for Cybersecurity) [9]. В соответствии с положениями этого Международного стандарта ИСО киберпреступление – это «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».

Поэтому следует согласиться с В. Ф. Джафарли в том, что киберпреступления в отличие от иных преступлений с использованием информационно-коммуникационных технологий – только те, «основные действия и последствия которых происходят исключительно в киберпространстве» [1. С. 61–62].

В Содружестве Независимых Государств в настоящее время разрабатывается проект модельного закона «О противодействии киберпреступности». Полагаем, что принятие такого закона в России настоятельно необходимо и позволит создать правовой механизм противодействия киберпреступности, скоординировать деятельность государственных органов, органов местного самоуправления, институтов гражданского общества, граждан и организаций по реализации государственной политики в данной области.

С учетом мирового опыта представляется целесообразным принять Стратегию кибербезопасности государства, в которой определить стратегические цели, задачи и основные направления государственной политики в области обеспечения кибербезопасности государства. Следует отметить, что Концепция Стратегии кибербезопасности Российской Федерации была размещена для обсуждения на официальном сайте Совета Федерации Федерального Собрания РФ еще в 2014 г.

Для последовательности реализации государственной политики в области противодействия киберпреступности может быть принята государственная программа по противодействию киберпреступности.

По мнению автора, к основным направлениям противодействия киберпреступности можно отнести следующие: 1) совершенствование организации деятельности правоохранительных и судебных органов, а также органов прокуратуры; 2) совершенствование системы подготовки, профессиональной переподготовки и повышения квалификации кадров правоохранительных и судебных органов, а также органов прокуратуры; 3) осуществление контроля доступа и обработки персональных данных; 4) обеспечение безопасности предоставления финансовых услуг в электронной форме; 5) повышение уровня киберграмотности клиентов финансовых организаций; 6) взаимодействие государственных органов с провайдерами хостинга, операторами связи, оказывающими услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», операторами поисковых систем, владельцами социальных сетей, регистраторами доменных имен и операторами подвижной радиотелефонной связи; 7) повышение степени информированности общества в области противодействия киберпреступности; 8) повышение эффективности профилактики киберпреступлений; 9) развитие государственно-частного взаимодействия; 10) мониторинг правоприменения; 11) развитие деятельности по лицензированию, сертификации и стандартизации в области технической защиты информации и обеспечения информационной безопасности; 12) развитие криптографической деятельности.

В числе мер по предупреждению киберпреступности важным является взаимодействие с институтами гражданского общества. В настоящее время активное сотрудничество правоохранительных и других контрольно-надзорных органов осуществляется с кибердружинами. Так, «Кибердружина» организации «Лига безопасного Интернета» представляет собой межрегиональное молодежное общественное движение, объединяющее волонтеров в России, государствах СНГ, Западной и Восточной Европе [6]. Целью кибердружин является выявление в сети Интернет противоправной информации.

Результаты деятельности кибердружин показывают их значительную роль в выявлении и расследовании киберпреступлений, что указывает на перспективность этого направления в профилактике киберпреступлений. Например, в субъекте Российской Федерации Белгородской области кибердружины были созданы еще в 2017 г. [4]

В 2019 г. депутатами «Единой России» был подготовлен законопроект «О кибердружинах».

Заключение. В заключение следует отметить, что для эффективного противодействия киберпреступности в России требуется соответствующая нормативная правовая база. Поэтому в ближайшей перспективе необходимо принять Закон «О противодействии киберпреступности» и Стратегию кибербезопасности.

Список литературы

1. Джафарли В. Ф. Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. Москва: Проспект, 2021. 280 с.

2. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. // СПС «Гарант». URL: https://base.garant.ru/4089723/ (дата обращения: 05.03.2022).

3. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 05.03.2022).

4. Об организации деятельности кибердружин Белгородской области: Постановление Правительства Белгородской области от 22 мая 2017 г. № 181-пп // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/3100201705240004?rangeSize=20 (дата обращения: 22.07.2022).

5. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://cbr.ru/analytics/ib/operations_survey_2021/#:~: text=B 2021 году доля объема,— 0%2C00120%25)1. (дата обращения: 22.07.2022).

6. Официальный сайт Лиги безопасного Интернета. URL: http://www.ligainternet.ru/ (дата обращения: 22.07.2022).

7. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/ (дата обращения: 04.03.2022).

8. Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря. URL: https://undocs.org/ru/A/75/98 (дата обращения: 20.03.2022).

9. ISO/IEC 27032:2012 Information Technology – Security Techniques-Guidelines for Cybersecurity. URL: https://www.iso.org/standard/44375.html (дата обращения: 30.03.2022).

Н. Д. Лопатина,
заведующий лабораторией, преподаватель,
Курский государственный политехнический колледж
С. С. Лопатин,
преподаватель,
Курский монтажный техникум

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ BIG DATA В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. Исследование посвящено изучению роли Единой информационной системы в сфере закупок для обеспечения эффективности государственного заказа с точки зрения обеспечения конкуренции и экономии бюджетных денежных средств. Рассматриваются электронные торговые площадки, и обосновывается необходимость сокращения их количества в целях преодоления административных барьеров для субъектов предпринимательской деятельности. Оцениваются важность и значимость электронных сервисов с точки зрения определения путей их дальнейшего совершенствования.