ГОСУДАРСТВО И ПРАВО, 2023, № 9, с. 189–196
STATE AND LAW, 2023, No. 9, pp. 189–196

ЗА РУБЕЖОМ

ПРАВОВАЯ ПОЛИТИКА ЗАРУБЕЖНЫХ СТРАН В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

© 2023 г. А. Ю. Соколов*, О. Л. Солдаткина**

Саратовский филиал Института государства и права Российской академии наук

**E-mail: aysockolov@mail.ru*
***E-mail: buzum@mail.ru*

Поступила в редакцию 25.01.2023 г.

Аннотация. В статье проводится сравнительный анализ подходов разных стран к вопросам противодействия преступлениям, совершаемым с использованием информационных технологий. Актуальность подобных исследований обусловлена рядом факторов, среди которых нарастание количества компьютрных преступлений, сложность правового регулирования информационного пространства, возможность заимствования апробированных юридических конструкций и др. Методологическую основу исследования составляет сравнительно-правовой метод. В статье определены перспективные направления совершенствования правовой системы (дальнейшая разработка терминологического аппарата, уточнены составы компьютерных преступлений в Уголовном кодексе РФ, предложено формирование новой Доктрины информационной безопасности (с учетом опыта Сингапура), создание специальных групп реагирования на киберинциденты, введение законодательно закрепленных обязанностей для организаций уведомлять о компьютерных инцидентах соответствующие органы и др.).

Ключевые слова: компьютерные преступления, киберпреступления, информационная безопасность, правовая политика, приоритеты правовой политики, группы реагирования на киберинциденты, уголовные санкции, Доктрина информационной безопасности, профилактика киберпреступлений.

Цитирование: *Соколов А. Ю., Солдаткина О. Л.* Правовая политика зарубежных стран в сфере противодействия преступлениям, совершаемым с использованием информационных технологий // Государство и право. 2023. № 9. С. 189–196.

DOI: 10.31857/S102694520027662-9

THE LEGAL POLICY OF FOREIGN COUNTRIES IN THE FIELD OF COUNTERACTION TO CRIME COMMITTED WITH THE USE OF INFORMATION TECHNOLOGIES

© 2023 A. Yu. Sokolov*, O. L. Soldatkina**

Saratov Branch of Institute of State and Law of the Russian Academy of Sciences

**E-mail: aysockolov@mail.ru*
***E-mail: buzum@mail.ru*

Received 25.01.2023

Abstract. The article provides a comparative analysis of the approaches of different countries to the issues of combating crimes committed using information technology. The relevance of such studies is due to a number of factors, including the increase in the number of computer crimes, the complexity of the legal regulation of the information space, the possibility of borrowing proven legal structures, etc. The methodological basis of the study is the comparative legal method. The article identifies promising areas for improving the legal system (further development of the terminological apparatus, clarified the composition of computer crimes in the Criminal Code of the Russian Federation, the formation is proposed of a new Doctrine of information security (taking into account the experience of Singapore), the creation of special response teams to cyber incidents, the introduction of legislative assigned obligations for organizations to notify relevant authorities about computer incidents, etc.).

Key words: computer crimes, cybercrimes, information security, legal policy, legal policy priorities, cyber incidents response teams, criminal sanctions, Information Security Doctrine, cybercrime prevention.

For citation: *Sokolov, A. Yu., Soldatkina, O.L. (2023).* The legal policy of foreign countries in the field of counteraction to crime committed with the use of information technologies // Gosudarstvo i pravo=State and Law, No. 9, pp. 189–196.

Преступления, совершаемые с использованием информационных технологий (в дальнейшем будем использовать термины «преступления, совершаемые с использованием информационных технологий», «компьютерные преступления», «киберпреступления» в качестве синонимов) и благодаря трансграничности сети Интернет и цифровизации большинства коммуникаций (в том числе экономических, банковских), являются одними из самых массовых, а учитывая анонимность в Глобальной сети – сложно раскрываемых. Относительная новизна используемых технологий и сложность сбора доказательств приводит к неэффективности традиционных методов противодействия преступлениям.

Статистика подтверждает эти выводы. В частности, согласно данным портала tadviser.ru[1], эксперты «Лаборатории Касперского» сообщили о росте количества целевых кибератак на промышленные предприятия в России (количество атак на системы автоматизации с помощью вредоносных документов в первом полугодии 2022 г. выросло на 80%). Согласно статистике, в Италии также совершается 800 киберпреступлений в день[2], а средняя стоимость, например, атаки программы-вымогателя составила около 680 тыс. долл.[3] В 2021 г. потери от различных видов преступлений в США составили 4 млрд долл.[4]

Не может справиться с исследуемым видом правонарушений и одно из самых технически развитых государств – Республика Сингапур. Доля преступлений в сфере информационных технологий (обозначаются термином “cybercrime”, киберпреступления) в общем количестве

[1] URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F: APT_-_%D0%A2%D0%B0%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B8%D0%BB%D0%B8_%D1%86%D0%B5%D0%BB%D0%B5%D0%B2%D1%8B%D0%B5_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8#.2A_.D0.A7.D0.B8.D1.81.D0.BB.D0.BE_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_.D0.B0.D0.B2.D1.82.D0.BE.D0.BC.D0.B0.D1.82.D0.B8.D0.B7.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.BD.D1.8B.D0.B5_.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC.D1.8B_.D1.83.D0.BF.D1.80.D0.B0.D0.B2.D0.BB.D0.B5.D0.BD.D0.B8.D1.8F_.D0.B2_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B8_.D0.B2.D0.B7.D0.BB.D0.B5.D1.82.D0.B5.D0.BB.D0.BE_.D0.BD.D0.B0_80.25 (дата обращения: 10.11.2022).

[2] См.: В Италии совершается 800 киберпреступлений в день // REGNUM. 2021. URL: https://regnum.ru/news/society/3407099.html (дата обращения: 10.11.2022).

[3] См.: Italy cyber security and cyber crime statistics (2020–2022) // comparitech.com. 2022. URL: https://www.comparitech.com/blog/information-security/italy-cyber-security-statistics/#Italy_has_announced_its_first-ever_National_Cyberse-curity_Strategy (дата обращения: 10.11.2022).

[4] См.: URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8#.D0.A1.D0.B0.D0.BC.D1.8B.D0.B5_.D1.80.D0.B0.D1.81.D0.BF.D1.80.D0.BE.D1.81.D1.82.D1.80.D0.B0.D0.BD.D0.B5.D0.BD.D0.BD.D1.8B.D0.B5_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.BF.D1.80.D0.B5.D1.81.D1.82.D1.83.D0.BF.D0.BB.D0.B5.D0.BD.D0.B8.D1.8F_.D0.B2_.D0.A1.D0.A8.D0.90_.D0.BD.D0.B0_.D0.BE.D0.B1.D1.89.D1.83.D1.8E_.D1.81.D1.83.D0.BC.D0.BC.D1.83_.D0.BF.D0.BE.D1.82.D0.B5.D1.80.D1.8C_.D0.B2_.244_.D0.BC.D0.BB.D1.80.D0.B4 (дата обращения: 10.11.2022).

преступлений велика и растет – от 7.9% в 2014 г. до 43% в 2020 г.[5]

Таким образом, проблема рассматриваемого вида преступлений масштабна, сложна и из-за свойств виртуального пространства должна решаться комплексно, на всех уровнях: международном, государственном, региональном, персональном. Если выделить государственный уровень, проблема противодействия данного вида правонарушений должна рассматриваться в различных аспектах: с точки зрения профилактики, предотвращения, пресечения и формирования санкционных механизмов. Однако в любом случае противодействие должно быть системным и иметь теоретический фундамент, иначе оно будет неэффективным. В сфере противодействия компьютерным преступлениям это, к сожалению, не всегда так: в силу специфики ИТ-отрасли законодатель должен реагировать оперативно, что иногда приводит к нарушению принципов уголовного закона при конструировании данных норм (например, при введении уголовной ответственности по ст. 207^1 и 207^2 УК РФ)[6]. Для исследований в таких случаях необходимо использование инструментов правовой политики, включая разработку комплекса приоритетов, целей и средств их реализации.

Поскольку информационные технологии развиваются достаточно быстро, многие из них (например, блокчейн, искусственный интеллект, интернет вещей) требуют формирования принципиально новых подходов к правовому регулированию. Отдельные страны, будучи лидерами в ИТ-сфере, столкнулись с некоторыми видами компьютерных преступлений раньше, чем другие, и, соответственно, имеют больший опыт – удачный и неудачный – в сфере вырабатывания новых юридических конструкций или приспособления старых. В силу сказанного выше представляется необходимым провести сравнительный анализ направлений совершенствования соответствующего сегмента законодательства в различных государствах (особенно в тех, которые являются признанными технологическими лидерами) – даже несмотря на то что проблема компьютерных правонарушений не решена ни в одном государстве, многие из них имеют опыт правового регулирования, полезный и при выстраивании данного сегмента правовой политики и в Российской Федерации.

Конечно, речь идет не об автоматическом применении существующих международно-правовых норм и простом заимствовании удачных конструкций (согласимся с мнением А.Н. Савенкова о неприемлемости такого подхода[7]), но вместе с тем отдельные конструкции по противодействию компьютерным правонарушениям могут быть использованы для правового регулирования виртуального пространства.

В рамках исследования целесообразно обратиться к зарубежному законодательству.

Следует отметить, что нормативные правовые акты зарубежных государств обычно не дают нормативного определения понятия «киберпреступность»[8], так как оно представляет собой широкую категорию правонарушений, прямо или косвенно связанных с компьютерами и компьютерными сетями. Киберпреступления, как правило, определяются по средствам описания видов противоправной деятельности – чаще всего в уголовном законодательстве.

Так, в США основным механизмом судебного преследования за киберпреступления является Закон о компьютерном мошенничестве и злоупотреблениях 1986 (Computer Fraud and Abuse Act 1986[9], далее – CFAA), который запрещает: несанкционированный доступ (или превышение санкционированного доступа) к компьютеру и получение информации, связанной с национальной безопасностью; несанкционированный доступ (или превышение разрешенного доступа) к компьютеру, используемому в межгосударственной или внешней торговле; несанкционированный доступ к частному компьютеру, используемому правительством США; умышленный доступ к защищенному компьютеру без разрешения с целью мошенничества; повреждение компьютера умышленно или по неосторожности; торговля паролями; передача угроз вымогательства, в частности угроз повреждения защищаемого компьютера и угроз получения информации или нарушения конфиденциальности информации; кибервымогательство, связанное с требованием денег или имущества.

Италия как член Европейского Союза в 2001 г. подписала, а в 2008 г. ратифицировала Конвенцию Совета Европы о преступности в сфере компьютерной информации ETS от 23 ноября 2001 № 185 (The Budapest Convention (ETS No. 185)[10] (далее – Будапештская конвенция)[11]. В Будапештской конвенции определения киберпреступности тоже нет, есть перечисление видов киберпреступлений. По тому же пути идет и итальянский законодатель.

Согласно Будапештской конвенции к киберпреступлениям относятся: 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) правонарушения, связанные с использованием компьютерных средств: подлог с использованием компьютерных

---

[5] См.: Cybercrime as a share of total crimes in Singapore from 2014 to 2021 // Statista. 2022. URL: https://www.statista.com/statistics/1267252/singapore-cybercrime-as-share-of-total-crime/ (дата обращения: 30.08.2022).

[6] См.: *Пономаренко Е.В., Копшева К.О.* Соблюдение принципа справедливости и правил криминализации при установлении уголовной ответственности за распространение заведомо ложной общественно значимой информации: проблемные аспекты // Правовая политика и правовая жизнь. 2022. № 1. С. 187–192; *Грешнова Н.А., Ситник В.Н.* Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake)) // Вестник СГЮА. 2022. № 5. С. 182–189; и др.

[7] См.: *Савенков А.Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 6.

[8] *Кувшинова В.С.* Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 5–4. С. 53, 54; *Агаркова А.А., Синицына В.А.* Киберпреступность в современной России // Международный журнал гуманитарных и естественных наук. 2021. № 5–3. С. 13–16; *Чепрасова Ю.В., Шмарион П.В.* Основные направления противодействия киберпреступности // Вестник Воронежского ин-та МВД России. 2020. № 3. С. 256–262; *Пучков Д.В.* Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации // Правовая политика и правовая жизнь. 2019. № 1. С. 63–71; и др.

[9] См.: Congress.gov. URL: https://www.congress.gov/bill/99th-congress/house-bill/4718#:~: text=Computer%20Fraud%20and%20Abuse%20Act%20of%201986%20%2D%20Amends%20the%20Federal, the%20computer%20files%20of%20another

[10] См.: Будапештская конвенция: официальный сайт. 2022. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 10.11.2022).

[11] См.: Италия // Будапештская конвенция: официальный сайт. 2022. URL: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/Italy (дата обращения: 10.11.2022).

технологий, мошенничество с использованием компьютерных технологий; 3) правонарушения, связанные с содержанием данных: правонарушения, связанные с детской порнографией; 4) правонарушения, связанные с нарушением авторского права и смежных прав.

В Сингапуре основным нормативным правовым актом в рассматриваемой области является уголовный Акт о злоупотреблениях в компьютерных сетях и кибербезопасности (Computer Misuse and Cybersecurity Act 1993[12] (далее – CMA), изменения внесены в 2017 г.), но непосредственного определения понятия «киберпреступность» в нем также не содержится, однако на сайте Национального совета по предупреждению преступности Сингапура (National crime prevention council, www.ncpc.org.sg) можно обнаружить определение киберпреступлений как преступных деяний, связанных с использованием компьютеров, в том числе: получение несанкционированного доступа к компьютеру для просмотра, изменения или уничтожения его данных; совершение преступлений с использованием Интернета в качестве средства массовой информации (например, сексуальные преступления, вымогательство, торговля наркотиками, мошенничество на онлайн-аукционах, порнография); получение несанкционированного доступа к компьютеру в своих целях (для совершения преступления); похищение номеров кредитных карт или информации о личности; мошенничество через сеть Интернет[13].

Приведенную дефиницию конечно нельзя считать нормативной, но она дает представление о подходах к определению киберпреступлений органами государственной власти и в совокупности с описаниями действий в случае, если гражданин стал жертвой компьютерного преступления, является примером правового информирования населения относительно официальной позиции органов государственного управления по данному вопросу.

Законодательство Российской Федерации идет в целом по тому же пути, однако не давая дефиницию понятия компьютерных преступлений, зарубежный законодатель определяет их составы более подробно. Кроме того, можно отметить, что в исследуемых странах, как в Уголовном кодексе РФ, есть тенденция выделять нормы уголовного права в данной области в единый документ, т.е. обособлять. Но перечень составов в гл. 28 УК РФ узкий и включает неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации; нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети Интернет и сетей связи общего пользования (ст. 274^1). Однако есть ст. 207^3 (фактически статья об уголовном наказании за «фейки» (недостоверные новости) о Вооруженных Силах РФ), ст. 159^3 (мошенничество с использованием электронных средств платежа) и др. То есть нормы обнаруживаются по всему Уголовному кодексу РФ, и понимание того, что относится к компьютерным преступлениям, получить сложно. Поэтому в рамках рассматриваемого сегмента правовой политики представляется необходимым в качестве приоритета выделить изменение уголовного законодательства в части систематизации и уточнения составов компьютерных преступлений и переструктурированию гл. 28 УК РФ.

Что касается профилактики киберпреступлений, то анализ законодательства зарубежных стран показывает, что данное направление описывается и задается в стратегических документах.

Так, в мае 2022 г. итальянское правительство в рамках действующей Национальной стратегии кибербезопасности в период до 2026 г. поставило в общей сложности 82 цели[14].

План реализации начинается с указания источников денежных средств для содействия инновациям и кибербезопасности (налоговые льготы для компаний; создание национального налогового льготного района для строительства Национального парка кибербезопасности и ряда узлов по всей Италии; выделение 623 млн евро из Национального плана восстановления и устойчивости на инновации и кибербезопасность и др.). Интересно, что в стратегии отсутствует направление по работе с населением в целях повышения его цифровой грамотности, что можно считать минусом итальянского подхода к профилактике киберпреступности.

Данный вывод подтверждается опытом Сингапура, сделавшего упор в своем развитии на технологии и человеческий потенциал,– здесь законодательные механизмы профилактики киберпреступлений также представлены стратегическими документами, но выбран подход, основанный на повышении цифровой грамотности населения. Аргументация выбора данного подхода следующая: неосведомленность или поверхностное отношение к кибербезопасности среди конечных пользователей может быть слабым местом даже самых безопасных систем. Стратегия кибербезопасности Сингапура 2021 г. (The Singapore Cybersecurity Strategy 2021) предусматривает расширение возможностей киберискушенного населения относительно «здорового цифрового образа жизни»: предполагается в сотрудничестве с бизнес-структурами повысить осведомленность, изменить отношение к кибербезопасности и содействовать внедрению передовой киберпрактики. Кроме того, во исполнение данных положений правительство Сингапура организует целевые информационные мероприятия с охватом отдельных групп населения (студенты, работающие взрослые, пожилые люди). Помимо повышения осведомленности правительство страны планирует поддерживать и поощрять частных лиц и предприятия при организации их защиты.

В Сингапуре существует орган государственной власти, обеспечивающий координацию действий по профилактике киберпреступлений, – Агентство кибербезопасности Сингапура (далее – CSA). Портал CSA Go Safe Online предоставляет действенные советы и подсказки для населения и предприятий по организации защиты от киберпреступлений. Предполагается также запустить добровольный знак доверия SG Cyber Safe и знак кибергигиены для предприятий, что позволит предприятиям иметь четкое представление об уровне их кибербезопасности; рекомендовано обучение сотрудников навыкам обеспечения кибербезопасности; использование ресурсов и наборов инструментов для

[12] См.: Singapore Government Agency Website. Singapore Statutes Online. 2022. URL: https://sso.agc.gov.sg/Act/CMA1993? ProvIds=P1II-&usg=AOvVaw0fMUimAxMx1hlg83bdcQQE (дата обращения: 26.11.2022).

[13] См.: Cybercrime // National crime prevention council. 2022. URL: https://www.ncpc.org.sg/cybercrime.html (дата обращения: 18.11.2022).

[14] См.: Italy unveils its first-ever national cybersecurity strategy // decode39.com. 2022. URL: https://decode39.com/3459/italy-national-cybersecurity-strategy/ (дата обращения: 10.11.2022).

повышения осведомленности о кибербезопасности в организации, разработанных CSA.

Для владельцев критической инфраструктуры Стратегией кибербезопасности Сингапура 2021 г. в качестве профилактики предписано: придерживаться риск-ориентированного подхода к кибербезопасности; использование цепочки поставок объектов критической инфраструктуры; использование системы компетенций кибербезопасности Operational Technology (OT) в качестве инструмента для создания процессов и структур для управления кибербезопасностью.

Учитывая другую форму организации правовой системы в США, здесь присутствует и другой подход к профилактике киберпреступлений. Безусловно, есть и стратегические документы (например, Киберстратегия ФБР[15]), но они ориентированы скорее на реагирование на киберинциденты, чем на профилактику. Тем не менее там описан основной подход к профилактике – обеспечить неотвратимость наказания за кибернарушения.

На уровне штатов, где проблема стоит достаточно остро в силу многочисленности совершаемых атак, направленных на объекты социальной сферы (школы, колледжи, медицинские учреждения и др.), подход к профилактике киберпреступлений другой. В 2022 г. по крайней мере 40 штатов и Пуэрто-Рико представили или рассмотрели более 250 законопроектов или резолюций, которые в значительной степени касаются кибербезопасности[16]. Среди предлагаемых изменений есть и положения профилактического характера, направленные на: обеспечение требований от государственных учреждений проводить обучение сотрудников кибербезопасности; разрабатку формальных политик, стандартов и практик информационной безопасности; обеспечение обязательного обучения сотрудников; установление обязанности сообщать об инцидентах в области безопасности, включая атаки программ-вымогателей; обеспечение финансирования программ и практик кибербезопасности в государственных учреждениях, местных органах власти и школах; разработку или поддержку программ и стимулов для обучения для сотрудников негосударственных организаций по кибербезопасности.

Таким образом, законодательные механизмы профилактики компьютерных преступлений в зарубежных странах представлены стратегическими документами.

В Российской Федерации действует Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646[17] (далее – Доктрина). Конечно, за шесть лет Доктрина частично утратила свою актуальность, особенно на фоне текущей геополитической обстановки. В частности, в Доктрине мало внимания уделено внутригосударственному уровню и личностному уровню защиты от кибератак. Представляется, что при формировании новой Доктрины стоит ориентироваться на опыт Сингапура, предполагающий повышение осведомленности разных групп населения, изменение отношения к кибербезопасности и содействие внедрению передовой киберпрактики защиты.

Киберпреступления имеют специфические характеристики, которые усложняют процесс их обнаружения[18], поэтому механизмы реагирования в зарубежных государствах связаны с существованием групп реагирования на киберинциденты.

Так, в Италии есть несколько групп реагирования на компьютерные чрезвычайные ситуации (CERT), которые охватывают государственный и частный секторы, а также граждан.

В Сингапуре на базе CSA для борьбы с атаками на объекты критической инфраструктуры существуют группы реагирования на инциденты, которые готовы расследовать, сдерживать и устранять кибератаки.

В США у ФБР есть специально обученные киберотряды в каждом из 56 полевых офисов. Группа быстрого реагирования Cyber Action Team может быть развернута по всей стране в течение нескольких часов для реагирования на крупные инциденты.

Кроме того, международные стандарты информационной безопасности (ISO 27001) требуют от организаций разработки планов управления реагированием на киберинциденты.

В зарубежных странах в качестве меры реагирования предусмотрена обязанность организаций уведомлять о компьютерных инцидентах соответствующие органы: введенная в действие в итальянском законодательстве, как и в других государствах Евросоюза, Директива NIS предусматривает для всех компаний и организаций, предоставляющих основные услуги (энергетика, транспорт, банки, цифровая инфраструктура, здравоохранение и т.д.), обязанность уведомлять о компьютерных инцидентах отраслевой национальный орган; если произошла утечка личных данных, организация обязана сообщить об этом их владельцам; в Сингапуре организации, которые относятся к владельцам объектов критической инфраструктуры, имеют установленную уголовным законом (CMA) обязанность сообщать об инцидентах в соответствующие органы (разные по отраслям для разных объектов), для прочих организаций CMA предусмотрена обязанность сообщать об инцидентах в Сингапурскую группу реагирования на компьютерные чрезвычайные ситуации, а в случае несанкционированного доступа к компьютерным системам организации необходимо подать заявление в полицию; в США в марте 2022 г. было принято соответствующее законодательство (Закон об отчетности о важных киберинцидентах в отношении критически важной киберструктуры, Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA[19]), согласно которому организации критической инфраструктуры обязаны сообщать о важных киберинцидентах (технические детали находятся в стадии разработки).

Интересная модель есть в Сингапуре: организации, которые относятся к владельцам объектов критической инфраструктуры, обязаны проводить регулярные проверки и оценки рисков для уязвимостей кибербезопасности,

[15] См.: The Cyber Threat // FBI. 2022. URL: https://www.fbi.gov/investigate/cyber (дата обращения: 10.11.2022).

[16] См.: Cybersecurity Legislation 2022 // The NCSL Foundation for State Legislatures. 2022. URL: https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2022637922035.aspx (дата обращения: 10.11.2022).

[17] См.: СЗ РФ. 2016. № 50, ст. 7074.

[18] См.: *Мордвинов К.В., Удавихина У.А.* Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1. С. 83–88.

[19] См.: Cybersecurity laws and regulations USA // Iclg.com. 2022. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (дата обращения: 20.11.2022).

причем за несоблюдение этих обязательств законодательством предусмотрены значительные уголовные санкции[20].

Имеющиеся практики в законодательствах различных государств позволяют не только обеспечить высокую степень защиты, но и собирать статистическую информацию для дальнейших научных разработок механизмов защиты и реагирования на киберинциденты.

Что касается ситуации в Российской Федерации, то Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации была утверждена Президентом РФ еще 12 декабря 2014 г.[21], однако специальные подразделения по борьбе с киберпреступлениями в структуре МВД России и Прокуратуры РФ были созданы только в 2020 г., и представляется, что в текущей ситуации их для оперативного реагирования недостаточно. Обязанность сообщать о киберинцидентах законодательством не закреплена; механизмы сертификации критически важных информационных систем не отработаны. Хотя начало данной работе положено Указом Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[22], законодателю и правоприменителям предстоит еще много работы по формированию эффективной системы реагирования на киберинциденты, для чего необходимо использовать опыт стран, где разработки систем реагирования уже ведутся.

Санкционная политика в исследуемых государствах отличается, что обусловлено общими правовыми традициями.

Например, в Сингапуре законодательство о киберпреступлениях продолжает политику жесткого правового регулирования, когда даже небольшие правонарушения влекут серьезные последствия: в частности, для большинства компьютерных киберпреступлений (взлом компьютерных систем и / или повреждение веб-сайтов, распространение вредоносного программного обеспечения, DDOS атаки, мошенничество с использованием компьютерных технологий, неправомерное использование компьютера, нарушение авторских прав, кража личных данных, мошенничество с идентификацией, распространение недостоверной информации) характерны уголовно-правовые санкции, предусматривающие штрафы и лишение свободы. За отдельные виды компьютерных правонарушений могут быть предусмотрены иные меры воздействия: например, за нарушение авторских прав используются гражданско-правовые санкции, а за кражу личных данных и распространение недостоверной информации – административно-правовые.

В отличие от законодательства Сингапура в странах Европейского Союза, в том числе в Италии, виды применяемых мер за компьютерные правонарушения разнообразнее, т.е. количество составов киберпреступлений меньше. Тем не менее большинство санкций носит уголовно-правовой характер, так как это предусматривает Будапештская конвенция (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование компьютерных устройств, правонарушения, связанные с использованием компьютерных средств, правонарушения, связанные с нарушением авторского права и смежных прав, а также раскрытие информации, составляющей одну из тайн, кража личных данных, ограничения на содержание цифровых ресурсов), но могут применяться и административно-правовые (противозаконный доступ, воздействие на данные, воздействие на функционирование системы, противозаконное использование компьютерных устройств, правонарушения, связанные с использованием компьютерных средств, кража личных данных, ограничения на содержание цифровых ресурсов), гражданско-правовые (правонарушения, связанные с нарушением авторского права и смежных прав, а также раскрытие информации, составляющей одну из тайн) и иные (воздействие на функционирование системы, блокировка информационных ресурсов) меры.

В США на федеральном уровне CFAA предусматривает как уголовные, так и гражданские наказания (которые в уголовном контексте могут варьироваться от 10 до 20 лет лишения свободы за некоторые преступления с отягчающими обстоятельствами, с наказаниями за преступления без отягчающих обстоятельств, перечисленными ниже). Кроме того, есть еще законодательство, касающееся киберпреступлений, включая Закон о защите электронных коммуникаций (Electronic Communications Privacy Act of 1986, ECPA)[23], который обеспечивает уголовные санкции для защиты сообщений при хранении и передаче, включая преднамеренный перехват электронных сообщений в пути с некоторыми исключениями, доступными для правоохранительных органов, поставщиков услуг и других лиц. Закон об экономическом шпионаже от 1996 г.[24] и др. являются дополнительными источниками потенциальных уголовных и гражданских санкций. В дополнение к федеральным законам многие штаты приняли законы, запрещающие взлом и другие киберпреступления, некоторые из которых шире, чем федеральные законы. Меры предусмотрены в том числе и уголовные. Например, уголовный закон штата Нью-Йорк запрещает сознательное использование компьютера с целью получения доступа к компьютерным материалам (посягательство на компьютер), с наказанием в виде лишения свободы на срок до четырех лет[25].

Защита персональных данных в зарубежных странах предусматривает в основном административные санкции в виде больших штрафов.

Зарубежное законодательство предусматривает и санкции за противозаконное использование компьютерных устройств (в том числе распространение, продажу или предложение к продаже оборудования, программного обеспечения и других инструментов для совершения киберпреступлений или использование ИТ-систем без разрешения ее владельца на предмет уязвимости, а также любую другую деятельность, которая неблагоприятно сказывается или угрожает целостности, конфиденциальности или доступности компьютерной системы), включая достаточно развернутое описание того, что подразумевается под компьютерными устройствами.

---

[20] См.: Сравнительный анализ подходов к регулированию критической информационной инфраструктуры // internetpolicy.kg. 2020. 1 мар. URL: http://internetpolicy.kg/wp-content/uploads/2020/03 (дата обращения: 20.11.2022).

[21] См.: Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document131/ (дата обращения: 20.11.2022).

[22] См.: СЗ РФ. 2022. № 18, ст. 3058.

[23] См.: H.R.4952 – Electronic Communications Privacy Act of 1986 // Congress.gov. URL: https://www.congress.gov/bill/99th-congress/house-bill/4952 (дата обращения: 20.12.2022).

[24] См.: H. Rept. 104–788 – ECONOMIC ESPIONAGE ACT OF 1996 // Congress.gov. https://www.congress.gov/congressional-report/104th-congress/house-report/788/1 (дата обращения: 20.12.2022).

[25] См.: Cybersecurity laws and regulations USA // Iclg.com. 2022. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (дата обращения: 20.11.2022).

И все же, несмотря на слишком строгие санкции, законодательство Сингапура в исследуемой сфере отличается максимальной степенью проработки. В частности, основной Закон о киберпреступлениях (CMA): описывает круг субъектов (любое лицо, независимо от национальности и гражданства, как в Сингапуре, так и за его пределами, при условии, если обвиняемый, компьютерная программа или данные находились в Сингапуре в момент совершения преступления и / или преступление причиняет и / или создает риск вреда для Сингапура[26]); задает терминологический аппарат, что позволяет избежать сложностей при толковании законодательства в ходе судебных разбирательств; определяет основания для наступления ответственности (чаще всего связано с отсутствием полномочий у правонарушителя) и составы преступлений, позволяющие охватить максимальное количество противоправных деяний; вводит понятие «инструменты для взлома» с максимально широким определением таких инструментов, как устройства или компьютерные программы, которые можно использовать для совершения киберпреступлений; при этом, чтобы положение не стало всеобъемлющим, запрет применяется только в том случае, если инструменты получены с намерением совершить киберпреступление (обвинитель должен будет доказать такие намерения).

Ранее отмечалось, что в российском законодательстве составы преступлений не представлены в одном месте, а имеющихся дефиниций недостаточно, что приводит к сложностям в судебной практике.

* * *

Таким образом, сфера противодействия преступлениям, совершаемым с использованием информационных технологий, нуждается в новых подходах, т.е. требуется использование инструментов правовой политики. При выстраивании системы приоритетов последней имеет смысл обратить внимание на опыт отдельных стран – лидеров в сфере информационных технологий. Среди перспективных направлений совершенствования правовой системы на основе проведенного анализа можно выделить: структурирование видов компьютерных преступлений в Уголовном кодексе РФ и уточнение составов (включение, например, санкций за противозаконное использование компьютерных устройств); формирование новой Доктрины информационной безопасности с ориентацией на опыт Сингапура (повышение осведомленности разных групп населения, изменение отношения к кибербезопасности и содействие внедрению передовой киберпрактики защиты); создание специальных групп реагирования на киберинциденты, а также введение законодательно закрепленных обязанностей для организаций (минимально только для объектов критической инфраструктуры) уведомлять о компьютерных инцидентах соответствующие органы (при разработке соответствующих методических документов, определяющих время для сообщения, его состав и порядок действий) и проводить регулярные проверки и оценки рисков для уязвимостей кибербезопасности; дальнейшая разработка терминологического аппарата, позволяющего избежать сложностей при толковании соответствующего сегмента законодательства в ходе судебных разбирательств.

[26] См.: Data protection and cybersecurity laws in Singapore // CMS. 2021. 19 February. URL: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/singapore (дата обращения: 20.11.2022).

СПИСОК ЛИТЕРАТУРЫ

1. *Агаркова А.А., Синицына В.А.* Киберпреступность в современной России // Международный журнал гуманитарных и естественных наук. 2021. № 5–3. С. 13–16.
2. *Грешнова Н.А., Ситник В.Н.* Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake)) // Вестник СГЮА. 2022. № 5. С. 182–189.
3. *Кувшинова В.С.* Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 5–4. С. 53, 54.
4. *Мордвинов К.В., Удавихина У.А.* Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1. С. 83–88.
5. *Пономаренко Е.В., Копшева К.О.* Соблюдение принципа справедливости и правил криминализации при установлении уголовной ответственности за распространение заведомо ложной общественно значимой информации: проблемные аспекты // Правовая политика и правовая жизнь. 2022. № 1. С. 187–192.
6. *Пучков Д.В.* Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации // Правовая политика и правовая жизнь. 2019. № 1. С. 63–71.
7. *Савенков А.Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 6.
8. Сравнительный анализ подходов к регулированию критической информационной инфраструктуры // internetpolicy.kg. 2020. 1 мар. URL: http://internetpolicy.kg/wp-content/uploads/2020/03 (дата обращения: 20.11.2022).
9. *Чепрасова Ю.В., Шмарион П.В.* Основные направления противодействия киберпреступности // Вестник Воронежского ин-та МВД России. 2020. № 3. С. 256–262.

REFERENCES

1. *Agarkova A.A., Sinitsyna V.A.* Cybercrime in modern Russia // International Journal of Humanities and Natural Sciences. 2021. No. 5–3. P. 13–16 (in Russ.).
2. *Greshnova N.A., Sitnik V.N.* Ensuring public interest in the context of digitalization: problems of Criminal Law in Russia (on the example of deepfake technology) // Herald of the Saratov State Law Academy. 2022. No. 5. P. 182–189 (in Russ.).
3. *Kuvshinova V.S.* Criminological characteristics of cybercrime // International Journal of the Humanities and Natural Sciences. 2020. No. 5–4. P. 53, 54 (in Russ.).
4. *Mordvinov K.V., Udavihina U.A.* Cybercrime in Russia: Current Challenges and Successful Practices in Combating Cybercrime // Theoretical and Applied Jurisprudence. 2022. No. 1. P. 83–88 (in Russ.).
5. *Ponomarenko E.V., Kopsheva K.O.* Compliance with the principle of justice and the rules of criminalization when establishing criminal liability for the dissemination of knowingly false socially significant information: problematic aspects // Legal Policy and Legal Life. 2022. No. 1. P. 187–192 (in Russ.).
6. *Puchkov D.V.* The state of criminal law regulation of cybercrimes in the criminal legislation of the Russian Federation // Legal Policy and Legal Life. 2019. No. 1. P. 63–71 (in Russ.).
7. *Savenkov A.N.* Counteracting cybercrime in the financial and credit sphere as a vector for ensuring global security // State and Law. 2017. No. 10. P. 6 (in Russ.).

8. Comparative analysis of approaches to the regulation of critical information infrastructure // internetpolicy.kg. March 1, 2020 URL: http://internetpolicy.kg/wp-content/uploads/2020/03 (accessed: 20.11.2022) (in Russ.).

9. *Cheprasova Yu. V., Shmarion P. V.* The main directions of combating cybercrime // Herald of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2020. No. 3. P. 256–262 (in Russ.).

Сведения об авторах

СОКОЛОВ Александр Юрьевич –
доктор юридических наук, профессор,
директор Саратовского филиала
Института государства и права
Российской академии наук;
410028 г. Саратов, ул. Чернышевского, д. 135
ORCID: 0000-0003-3350-7775

СОЛДАТКИНА Оксана Леонидовна –
кандидат юридических наук,
старший научный сотрудник
Саратовского филиала
Института государства и права
Российской академии наук;
410028 г. Саратов, ул. Чернышевского, д. 135
ORCID: 0000-0002-9955-4083

Authors' information

SOKOLOV Aleksandr Yu. –
Doctor of Law, Professor,
Director of the Saratov Branch
of the Institute of State and Law
of the Russian Academy of Sciences;
135 Chernyshevsky str., 410028 Saratov, Russia

SOLDATKINA Oksana L. –
PhD in Law,
Senior Researcher, Saratov Branch
of the Institute of State and Law
of the Russian Academy of Sciences,
135 Chernyshevsky str., 410028 Saratov, Russia