УДК/UDC 343.8

Криминологические аспекты классификации подходов обеспечения кибербезопасности развитых зарубежных государств

Ковалев Олег Геннадьевич
доктор юридических наук, кандидат психологических наук, профессор, академик РАЕН,
профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе
Псковский филиал Академии ФСИН России
г. Псков, Россия
e-mail: Okovalev66@gmail.com
ORCID: 0000-0002-7869-4925

Семенова Наталья Владиславовна
старший преподаватель кафедры гражданского права и процесса, судебный эксперт, член СУДЭКС
Псковский государственный университет
г. Псков, Россия
e-mail: natali_semenova@mail.ru
ORCID: 0000-0001-6458-9078

Скипидаров Артем Алексеевич
студент института права, экономики и управления
Псковский государственный университет
г. Псков, Россия
e-mail: temapskov@yandex.ru

Аннотация

В статье анализируются проблемы современной кибербезопасности и ее реализации в развитых зарубежных государствах. Предлагается авторское определение кибербезопасности на основе проведенного комплексного теоретико-эмпирического исследования. Установлено, что киберпреступниками, атакующими государственные, финансовые учреждения, оборонные, ресурсодобывающие, медицинские, туристические и другие компании и персональных пользователей, применяются разнообраз-

ные современные IT-технологии и программное обеспечение. Создание современной организационной структуры обеспечения кибербезопасности является приоритетной задачей органов государственной и исполнительной власти, бизнес-структур и общественных организаций, онлайн-сообществ. В целях использования опыта развитых зарубежных государств в данном направлении предложена классификация основных подходов в обеспечении кибербезопасности. Рассмотрен опыт реагирования различных государств на современные киберугрозы, разрешения киберситуаций различных уровней сложности.

Ключевые слова: кибербезопасность, развитые зарубежные государства, киберпреступники, IT-технологии, классификация, модели кибербезопасности, киберугрозы, киберситуации.

Criminological aspects of classification of approaches to ensuring cybersecurity in developed foreign countries

Kovalev Oleg Gennadyevich
Doctor of Law, professor, academician of the Russian Academy of Natural Sciences, professor of the Department of Organization of the Regime and Operetional-Search Activity in the Penal System
Pscov branch of the Academy of Federal Penitentiary Service of Russia
Pskov, Russia
e-mail: okovalev66@gmail.com
ORCID: 0000-0002-7869-4925

Semenova Natalya Vladislavovna
senior lecturer of the Department of Civil law and Procedure, forensic expert, member of SUDEX
Pskov State University
Pskov, Russia
e-mail: natali_semenova@mail.ru
ORCID: 0000-0001-6458-9078

Skipidarov Artyom Alekseyevich
student of the master's programme of the Institute of Law, Economics and Management
Pskov State University
Pskov, Russia
e-mail: temapskov@yandex.ru

Abstract

The article analyzes the problems of modern cybersecurity and its implementation in developed foreign countries. The author's definition of cybersecurity is proposed on the basis of a comprehensive theoretical and empirical study. It has been established that cybercriminals attacking government, financial institutions, defense, resource extraction, medical, tourism and other companies and personal users use a variety of modern IT technologies and software. The creation of a modern organizational structure for ensuring cybersecurity is a priority task for state and executive authorities, business structures and public organizations, online communities. In order to use the experience of developed foreign countries in this direction, a classification of the main approaches to ensuring cybersecurity is proposed. The experience of the response of various states to modern cyber threats, the resolution of cyber situations of various levels of complexity is considered.

Key words: cybersecurity, developed foreign countries, cybercriminals, IT technologies, a classification, models of cybersecurity, cyber threats, cyber situations.

Проблема современной кибербезопасности в условиях постоянно меняющегося и развивающегося киберпространства, роста киберпреступности, распространения киберугроз, совершения несанкционированных, криминальных кибератак на различные государственные учреждения, коммерческие организации, структуры и компании, факты кибертерроризма предполагают обеспечение кибербезопасности на высоком современном уровне.

За последние шесть лет киберпреступность в Российской Федерации выросла в 10 раз, ущерб от нее составил около 3 трлн рублей. Каждое пятое регистрируемое преступление совершается с использованием компьютерных технологий. По оценкам экспертов латентность в сфере digital преступности доходит до 85% [1].

Киберпреступниками, атакующими государственные, финансовые учреждения, оборонные, ресурсодобывающие, медицинские, туристические и другие компании и персональных пользователей применяются разнообразные современные IT-технологии и программное обеспечение.

В настоящее время кибербезопасность в Российской Федерации обеспечивают Генеральная прокуратура Российской Федерации, Министерство внутренних дел Российской Федерации, Следственный комитет Российской Федерации, Федеральная служба безопасности Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба охраны Российской Федерации, Росгвардия и Министерство юстиции Российской Федерации.

В связи с актуальностью данной проблемы учеными проводятся комплексные теоретико-эмпирические исследования правовых и организационных проблем обеспечения кибербезопасности, в т. ч. в правоохранительной, оборонной, банковской сферах, кибербезопасности в уголовно-исполнительной системе [2; 3].

Только в текущем году по результатам исследований опубликованы около 10 научных статей в различных изданиях, в т. ч. журналах, рецензируемых ВАК при Минобрнауки России.

Одним из промежуточных результатов изучения проблемы стало понимание киберпреступности как угрозы национальной безопасности современной России, необходимости выработки единой стратегии комплексного и системного противодействия киберугрозам, нормативно-правового регулирования, предупреждения и своевременного, адекватного реагирования на возникающие киберинциденты различной степени сложности со стороны специальных государственных органов, общественных организаций, бизнес-сообществ и граждан. Требуется создание современной организационной структуры обеспечения кибербезопасности, в т. ч. на объектах, наиболее подверженных риску кибератак со стороны киберпреступников и криминальных киберсообществ.

В этих целях может быть полезен опыт развитых зарубежных стран, которые уже длительное время весьма эффективно противодей-

ствуют киберпреступности, обеспечивают кибербезопасность на высоком профессиональном уровне.

Отметим, что существуют различные модели обеспечения кибербезопосности: североамериканская (США, Канада), европейская (страны Европейского Союза), китайская (КНР), турецкая (Турецкая Республика), модель стран юго-восточной Азии (Южная Корея, Сингапур, Индонезия и Малайзия), а также модель государств, ориентированных на национальную, государственную информационно-телекоммуникационную сеть «Интернет» (Республика Иран, КНДР). В рамках данной статьи рассмотрим некоторые из них с помощью методов сравнительного и контент-анализа, используя географический и организационно-экономический принципы обобщения и классификации полученных результатов.

Так называемая североамериканская модель организации кибербезопасности, которую используют США и Канада, начала активно развиваться после террористических атак 11 сентября 2001 г., показавших уязвимость национальной безопасности США, ее неспособность предотвращать угрозы и реагировать на них. В помощь уже существовавшим субъектам кибербезопасности (Федеральное бюро расследований, Центральное разведывательное управление, Министерство обороны, полиция, организации разведывательного сообщества) в кратчайшие сроки было создано Управление внутренней безопасности, статус которого вскоре был повышен до профильного министерства [4].

Отличительной чертой рассматриваемой модели является модернизация и создание новых организационных структур, подведомственных различным государственным правоохранительным, военным и разведывательным ведомствам, обменивающимся информацией о крупных киберинцидентах, координирующих совместную деятельность и финансируемых федеральным правительством.

Так, созданное в 2018 г. Агентство по кибербезопасности и безопасности инфраструктуры активно взаимодействует с Министерством юстиции, входящими в него Федеральным бюро расследований и Наци-

ональной объединенной рабочей группой по расследованиям киберпреступлений.

Министерство внутренней безопасности противодействует киберугрозам, разрешает киберинциденты с помощью Национального центра интеграции кибербезопасности и связи [5; 6].

Европейская модель направлена на реализацию утвержденной странами Европейского союза стратегии обеспечения кибербезопасности, осуществляемой на союзном и государственном уровнях. Данная модель отличается более продуманным и организованным комплексом мероприятий, проводимых в рассматриваемом контексте (разработкой концепции киберустойчивости организаций и объектов к киберинцидентам различного содержания, длительности и интенсивности, законодательным, организационным, методическим, материально-техническим, кадровым и финансовым сопровождением).

Активно осуществляется формирование в сознании граждан культуры кибербезопасности, алгоритмизации реагирования пользователей сети на возможные ухищрения, используемые киберпреступниками (фишинговые письма, программы-шифровальшики, программные вирусы и др.). В этих целях проводится системная разъяснительная работа, так называемые ежегодные месячники кибербезопасности, повышающие знания и навыки должностных лиц и граждан в сфере кибербезопасности.

Обеспечением кибербезопасности в соответствии с принятым в 2019 г. специальным законом занимаются не только специализированные государственные структуры в сфере IT-технологий (Агентство Европейского Союза по сетевой и информационной безопасности, осуществляющее информационно-аналитические и практические мероприятия по предупреждению, выявлению и разрешению киберинцидентов), но и общественные организации, онлайн-сообщества, бизнес-структуры, исследовательские и образовательные учреждения.

Зарекомендовал себя с положительной стороны созданный восемь лет назад Европейский центр киберпреступности, внесший значитель-

ный вклад в борьбу с этим криминальным явлением, его резонансными проявлениями на территории государств Евросоюза [7].

Следует обратить особое внимание на вопросы материально-технического обеспечения реализации стратегии кибербезопасности государств Европейского Союза в постпандемийный период, а также их финансирования, исчисляемого почти 2 млрд евро.

Так называемая турецкая модель кибербезопасности (Турецкая Республика) имеет комплексный, оборонно-наступательный характер, сочетает как оборонительные, так и активные наступательные действия, проведение тактических кибератак на упреждение возможной киберугрозы. Изучение проблемы показало, что Турецкая Республика больше других стран использовала при построении системы кибербезопасности опыт развитых государств в данном направлении с участием специалистов военного ведомства и гражданских экспертов. При этом правительством Турецкой Республики первостепенное внимание уделяется развитию и совершенствованию социального статуса и имиджа подразделений, участвующих в обеспечении кибербезопасности. Специальные подразделения объединены в структуру, состоящую из пяти основных департаментов: правоохранительного, военного, морского, космического и комплексной обороны. Перечисленные департаменты взаимодействуют с профильными министерствами и ведомствами в вопросах предупреждения и реагирования на возникающие киберугрозы, разрешения киберситуаций различной степени сложности. Проведенный сравнительный и контент-анализ показал, что Турецкой Республике в последние годы удалось создать масштабную, системную и устойчивую структуру кибербезопасности, организационно отличную от других развитых зарубежных стран использованием возможностей активно привлекаемых хакерских киберсообществ, а также хакеров-одиночек, принимающих участие в обеспечении национальной кибербезопасности Турецкой Республики. Государственными структурами применяется эффективная, простая и мобильная система нормативно-правового регулирования кибербезопасности государства.

Другим государством, принципиально отличающимся организацией и правовым регулированием кибербезопасности в условиях национальной информационно-телекоммуникационной сети «Интернет», является Республика Иран, где также находят активное применение различные программы фильтрации и блокировки интернет-страниц.

Иранская модель кибербезопасности базируется на идеологических принципах организации защиты от киберугроз и кибератак, функционировании «исламского интернета», не допускающего распространение враждебной для республики политической, культурной или религиозной информации.

Реализация проекта «национального интернета» состоит из трех основных этапов, осуществляемых в государстве, позволивших правительственным учреждениям использовать национальную сеть, а в исключительных случаях подключаться с помощью интернет-шлюза к всемирной информационно-телекоммуникационной сети «Интернет».

Другой особенностью защиты киберпространства Ирана от киберугроз и кибератак, влияющей на стратегию ее реализации, выявленной в ходе проведенного исследования, является высокая стоимость интернет-услуг, по которой в «антирейтинге» государств Республика Иран занимает восьмую позицию.

Также заслуживает внимания и изучения иранский опыт применения специальной идентификационной системы, функционирующей в режиме онлайн. Исследование организационных аспектов реализации кибербезопасности в Республике Иран показало, что система защиты киберпространства построена на сочетании использования возможностей и ресурсов государственных и негосударственных организаций и ведомств. Главным органом, координирующим сферу онлайн-коммуникаций, определяющим стратегию развития современных кибер и digital технологий, является Верховный совет по киберпространству. Постоянно действующими рабочими органами совета являются Национальный центр киберпространства, киберполиция, Корпус стражей исламской революции, ки-

берармия, Комитет по определению случаев криминального контента и Министерство информационных и телекоммуникационных технологий.

Таким образом, рассмотренные основные модели обеспечения кибербезопасности показывают приоритетность деятельности органов законодательной и исполнительной власти различных государств, институтов гражданского общества и бизнеса по созданию, внедрению и развитию современных форм и методов противодействия киберпреступности.

Список литературы

1. Ковалев О. Г., Семенова Н. А. Кибербезопасность современной России: теоретические и организационно-правовые аспекты // Столыпинский вестник. URL: https://stolypin-vestnik.ru/stolypinskij-vestnik-no-1-2021/ (дата обращения: 29.03.2021).

2. Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015. 325с.

3. Ковалев О. Г., Скипидаров А. А. Нормативно-правовое регулирование реализации стратегии кибербезопасности в государствах Европейского Союза // Столыпинский вестник. URL: https://stolypin-vestnik.ru/stolypinskij-vestnik-no-2-2021/ (дата обращения: 28.03.2021).

4. Creation of the Department of Homeland Security // Homeland Security. URL: http://www.dhs.gov/creation-department-homeland-security (дата обращения: 22.03.2021).

5. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (дата обращения: 24.03.2021).

6. Presidential Policy Directive - United States Cyber Incident Coordination // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (дата обращения: 24.03.2021).

7. European cybercrime centre - EC3 // Europol. URL: http://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата обращения: 12.02.2021).

References

1. Kovalev O. G., Semenova N. A. Cybersecurity of modern Russia: theoretical and organizational and legal aspects // Stolypin Vestnik. URL: https://stolypin-vestnik.ru/stolypinskij-vestnik-no-1-2021/ (date of access: 29.03.2021).

2. Bykov V. M., Cherkasov V. N. Crimes in the field of computer information: criminological, criminal-legal and criminalistic problems: monograph. M.: Jurlitinform, 2015. 325 p.

3. Kovalev O. G., Skipidarov A. A. Legal regulation of the implementation of the cybersecurity strategy in the states of the European Union // Stolypin bulletin. URL: https://stolypin-vestnik.ru/stolypinskij-vestnik-no-2-2021/ (date of access: 28.03.2021).

4. Creation of the Department of Homeland Security // Homeland Security. URL: http://www.dhs.gov/creation-department-homeland-security (date of access: 22.03.2021).

5. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (date of access: 03.24.2021).

6. Presidential Policy Directive - United States Cyber Incident Coordination // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (date of access: 24.03.2021).

7. European cybercrime center - EC3 // Europol. URL: http://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 12.02.2021).