ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В СТРАНАХ ЕВРОПЕЙСКОГО СОЮЗА

ORGANIZATIONAL PROBLEMS OF ENSURING CYBERSECURITY IN THE COUNTRIES OF THE EUROPEAN UNION

УДК 343. 9

Ковалев Олег Геннадьевич, доктор юридических наук, кандидат психологических наук, профессор, профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе Псковского филиала Академии ФСИН России г. Псков.

Скипидаров Артём Алексеевич, магистрант ФГБОУ ВО Псковского государственного университета, г. Псков.

Kovalev O. G., okovalev66@gmail.com

Skipidarov A. A., temapskov@yandex.ru

Аннотация

В статье рассматриваются геополитические, экономические, инфраструктурные и другие риски от киберугроз, различного рода кибератак, кибертерроризма увеличивающиеся в последние годы многократно.

Обращается внимание на необходимость объединения усилий международного сообщества в вопросах обеспечения кибербезопасности, передачи и использования информации о готовящихся киберугрозах и киберинцидентах.

Отмечается, что кибервымогательство становится все более распространенным видом криминальной деятельности отдельных лиц и организованных преступных кибергруппировок, использующих в своей противозаконной деятельности современные компьютерные средства,

технику и технологии. Более активное использование киберпреступниками при проведении кибератак на государственные и частные учреждения и компании программ-шифровальщиков. Описывается современная опасная негативная тенденция совмещения и замены кибершпионажа, кибершантажа и кибервымогательства уничтожением объектов инфраструктуры атакуемых структур.

Анализируются организационные проблемы обеспечения кибербезопасности в таких странах как Германия и Италия. Раскрываются особенности функционирования государственных органов указанных государств по реализации и координации кибербезопасности в военной и гражданской сферах.

Annotation

The article discusses the geopolitical, economic, infrastructural and other risks from cyber threats, various types of cyberattacks, and cyberterrorism, which have increased many times in recent years.

Attention is drawn to the need to unite the efforts of the international community in ensuring cybersecurity, the transfer and use of information about upcoming cyber threats and cyber incidents.

It is noted that cyber extortion is becoming an increasingly common type of criminal activity of individuals and organized criminal cyber groups that use modern computer tools, equipment and technologies in their illegal activities. Increased use of encryption software by cybercriminals in conducting cyberattacks on public and private institutions and companies. The article describes the current dangerous negative trend of combining and replacing cyber espionage, cyber-espionage and cyber-extortion with the destruction of infrastructure objects of the attacked structures.

The organizational problems of ensuring cybersecurity in such countries as Germany and Italy are analyzed. The features of the functioning of the state bodies of these states for the implementation and coordination of cybersecurity in the military and civil spheres are revealed.

Ключевые слова: кибербезопасность, инфраструктурные риски, киберугрозы, кибератаки, кибертерроризм, киберинциденты, кибервымогательство, организованные преступные кибергруппировки, программы-шифровальщики, кибершпионаж, кибершантаж, организационные проблемы, военная и гражданская сферы.

Keywords: cybersecurity, infrastructure risks, cyber threats, cyberattacks, cyberterrorism, cyber incidents, cyber extortion, organized criminal cyber groups, cryptographic programs, cyber espionage, cyberstalking, organizational problems, military and civilian spheres.

Обеспечение релевантной, устойчивой кибербезопасности является важной задачей государственных структур, организаций и сообществ, специализирующихся в данном направлении в развитых мировых государствах. В последнее время геополитические, экономические, инфраструктурные и другие риски от киберугроз, различного рода кибератак, кибертерроризма увеличиваются многократно. С каждым годом возрастают размеры финансовых и имиджевых убытков государственных учреждений, частных компаний и корпораций, от несанкционированного, криминального воздействия на их киберструктуры, компьютерные сети, сервера, программное обеспечение. Персональные пользователи также несут значительные материальные и моральные потери от подобного рода киберугроз.

Например, большими темпами растет спрос и продажи доступов к информации компаний, сетям и серверам которых получен незаконный доступ посредством спланированных и осуществленных хакерских атак. В мировом масштабе более чем в два раза возросли продажи данных краденных банковских карт. В России же, количество зарегистрированных преступлений, связанных с незаконным использованием информации банковских карт и других только за прошедший год, выросло в пять раз.

Кибервымогательство становится все более распространенным видом криминальной деятельности отдельных лиц и организованных преступных

кибергруппировок, использующих в своей противозаконной деятельности современные компьютерные средства, технику и технологии. В последние годы у киберпреступников приобрели большую популярность так называемые программы-шифровальщики, используя которые они осуществляют кибератаки на государственные и частные организации, учреждения и компании. Опасностью подобного рода атак является не только причинение значительных финансовых потерь, но и вывод из строя системы ее жизнедеятельности, поражения всей сопутствующей инфраструктуры.

Более того, отмечается опасная негативная тенденция совмещения и даже замены кибершпионажа, кибершатнтажа и кибервымогательства уничтожением объектов инфраструктуры атакуемого учреждения, организации и компании.

Принято упоминать о более 500 кибератаках, совершенных в свыше 50 государствах в последнее время. Однако, учитывая данные исследований, показывающих что латентность преступлений в данной сфере может достигать 85%, а многие учреждения и компании предпочитают не заявлять о таких киберицидентах публично, эти цифры могут быть гораздо больше.

Второе место в мировом антирейтинге по количеству случаев кибервымогательства занимают компании, размещенные в государствах Европейского Союза, несмотря на наличие развитой и эффективной системы организации кибербезопасности.

С учетом актуальности темы, нами было проведено специальное теоретическое исследование правовых и организационных аспектов обеспечения кибербезопасности отдельных развитых европейских стран, накопленный опыт которых мог бы быть полезен для совершенствования кибербезопасности в Российской Федерации.

По справедливому высказыванию Президента России В.В. Путина, в целях обеспечения и поддержания необходимого уровня кибербезопасности необходимо развивать и совершенствовать систему международного обмена

информацией о киберугрозах, нейтрализовать которые возможно только совместными усилиями международного сообщества [1].

Используя методы сравнительного и факторного анализа, а также контент-анализа нормативных правовых и других литературных и информационных источников по теме, были определены и описаны основные подходы и модели организации кибербезопасности, ее правового регулирования и особенностей реализации. Определены направления и пути ее совершенствования.

Одной из наиболее успешной европейской страной в области правового регулирования и организации кибербезопасности является ФРГ, где с 2002 года эту деятельность в военной сфере и обороны осуществляет государственная организация стратегической разведки, а для защиты гражданских учреждений, организаций компаний и предприятий, десять лет назад был создан и активно развивается Национальный центр кибербезопасности, включенный в структуру головного офиса Федерального управления по информационной безопасности в Боне [2].

Необходимость его организации была обусловлена значительным ростом, начиная с 2005 года, количества кибератак на киберсистемы органов власти, коммерческие организации и предприятия а также появлением и распространением опасных компьютерных вирусов GhostNet и Stuxnet.

Во исполнение рекомендаций Федерального Правительства и Федерального управления по информационной безопасности, Национальный центр кибербезопасности осуществляет аналитическую работу по выявлению кибертерроризма и IT инцидентов, уязвимостей IT продуктов.

Данный центр объединяет и координирует усилия по кибербезопасности таких государственных органов как: Федерального ведомства по защите Конституции, Федеральной разведывательной службы, Федеральной полиции, Следственного управления, Таможни Германии, Бундесвера, Федерального управления гражданской защиты и помощи при стихийных бедствиях, и Федерального ведомства уголовной полиции, а также

сотрудничает с надзорными органами операторов критически важной инфраструктуры, в пределах определенных обязанностей и полномочий.

Указанное взаимодействие регламентируется соглашением о сотрудничестве перечисленных государственных структур [3]. Кроме того, указанный Национальный центр кибербезопасности ФРГ ориентирован на прямое сотрудничество с любыми институтами Европейского Союза, используя при этом возможности и ресурсы стран, входящих в его состав. При этом первостепенное внимание уделяется взаимодействию с Европейским агентством сетевой и информационной безопасности, а также с органами государств, специализирующимися на обеспечении кибербезопасности.

В числе задач центра особо выделяются профилактика, собирание, анализ и оценка информации о киберугрозах, а также раннее предупреждение кибератак, под которыми законодатель понимает умышленные действия, направленные против одной или нескольких киберсистем, осуществляемых посредством взлома их систем безопасности, а также краж личных данных пользователей, хакерских атак, распространения компьютерных вирусов, DOS-атак, атак на инфраструктуру интернета и другие [4].

Итальянский опыт организации кибербезопасности заключается в использовании американской модели киберкомандования. Он был нормативно закреплен в «Белой книге по обороне» в 2015 году [5].

Организованное два года спустя объединенное командование кибернетических операций было ориентировано на поэтапное достижение полной оперативной готовности противостоять киберугрозам и кибервойнам, реализуемых через компьютерные сети и реагированию на них в 2019 году [6].

Деятельность указанного подразделения осуществляется в сфере киберзащиты и защиты киберсетей. В первом случае реализуется статическая и динамическая безопасность целостности сети и доступности информации совместно с другими подразделениями и структурами военного ведомства. Вторая связана с проведением экспертизы и оценки уязвимости киберсети, обеспечение быстрого и адекватного вмешательства с целью предотвращения

наступления негативных последствий и разрешения возникших киберинцидентов. В этих целях также предусмотрено специальное диагностическое тестирование систем не защищенность от несанкционированного проникновения.

Объединенное командование кибернетических операций подчиняется начальнику штаба обороны вооруженных сил и включает такие важные командно-штабные элементы как отдел персонала, экспериментальное оперативное подразделение, собирающее информацию о потенциальных киберпреступниках и киберугрозах, разрабатывающее и планирующее мероприятия противодействия угрозам и кибератакам, а также кибер-филиал специализированной образовательной организации.

Такая важная структура кибербезопасности Итальянской Республики как объединенное командование кибернетических операций обеспечивает поддержание на высоком организационно-методическом и техническом уровне проведение военных операций, планирует и проводит наступательные операции и выступает координирующим органом между итальянскими вооруженными силами и другими организациями и сообществами кибербезопасности.

Осуществлением внутригосударственной кибербезопасности занимается Департамент информационной безопасности, один из заместителей директора которого непосредственно ответственен за данное направление деятельности. Он координирует деятельность Объединенного командования кибернетических операций и государственной полиции, центра защиты критически важных объектов от преступлений против информатики, а также национальный центр информационной безопасности, с которым через специально организованные киберсети и киберинфраструктуры взаимодействуют другие федеральные министерства и департаменты.

Литература

1.Пленарное заседание международного конгресса по кибербезопасности / www.kremlin.ru [сайт]. – URL: http://www.kremlin.ru (дата обращения: 12.02.2021).

2.Ссылка: Комментарий к закону о Киберцентре / www.fr-online.de [сайт]. – URL: http://www.fr-online.de/politik/meinung/wahrlich-nicht-furchteinfloessend/-/1472602/8564624/-/index.html (дата обращения: 12.02.2021).

3.Ссылка: Стратегия федерального правительства по борьбе с интернет-преступностью - ответ федерального правительства Национального центра киберзащиты от 2 мая 2011 года / bundestag.de [сайт]. – URL: http://dip21.bundestag.de/dip21/btd/17/056/1705694.pdf. (дата обращения: 12.02.2021).

4.Ссылка: Стратегия Кибербезопасности Германии [сайт]. - URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf. (дата обращения: 12.02.2021)

5.Ссылка: Защита Италии от кибератак [сайт]. - URL: http://www.lastampa.it/2017/01/20/italia/cronache/ecco-come-litalia-vuole-proteggersi-dai-cyberattacchi-6v68j3xB6zX7BAT33rPpyI/pagina.html. (дата обращения: 12.02.2021).

6.Ссылка: Киберзащита: команда кибероперацій [сайт]. - URL: http://www.ilmattino.it/tecnologia/hitech/cyber_defence_entro_fine_anno_cominciera_ad_operare_comando_operazioni_cibernetiche-2573646.html. (дата обращения: 12.02.2021)

Literature

1.Plenary session of the International Congress on Cybersecurity. www.kremlin.ru [website]. – URL: http://www.kremlin.ru (accessed: 12.02.2021).

2.Link: Commentary on the Law on CyberCenter [website] / www.fr-online.de [сайт]. – URL: http://www.fr-online.de/politik/meinung/wahrlich-nicht-furchteinfloessend/-/1472602/8564624/-/index.html (accessed: 12.02.2021).

3.Link: Federal Government Strategy for Fighting Internet Crime - Federal Government Response to the National Cyber Defense Center on May 2, 2011 [website]. – URL: http://dip21.bundestag.de/dip21/btd/17/056/1705694.pdf. (accessed: 12.02.2021).

4.Link: German Cybersecurity Strategy [website]. - URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf. (accessed: 12.02.2021).

5.Link: Defending Italy Against Cyberattacks [website]. - URL: http://www.lastampa.it/2017/01/20/italia/cronache/ecco-come-litalia-vuole-proteggersi-dai-cyberattacchi-6v68j3xB6zX7BAT33rPpyI/pagina.html. (accessed: 12.02.2021).

6.Link: Cyber Defense: Cyber Operations Team [website]. - URL: http://www.ilmattino.it/tecnologia/hitech/cyber_defence_entro_fine_anno_cominc era_ad_operare_comando_operazioni_cibernetiche-2573646.html. (accessed: 12.02.2021).