КИБЕРБЕЗОПАСНОСТЬ СОВРЕМЕННОЙ РОССИИ: ТЕОРЕТИЧЕСКИЕ И ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ

CYBERSECURITY IN MODERN RUSSIA: THEORETICAL AND ORGANIZATIONAL AND LEGAL ASPECTS

УДК 343. 9

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

Семенова Н.В., преподаватель кафедры гражданского права и процесса Псковского государственного университета г. Псков.

Kovalev O. G., Okovalev66@gmail.com

Semenova N. V. natali_semenova@mail.ru

Аннотация

В статье рассматриваются теоретические и организационно-правовые аспекты кибербезопасности в современной России. Определено ее место и значение в общей системе национальной безопасности, влияние на обеспечение внутренней и внешней безопасности Российской Федерации. На основе статистических данных показана актуальность темы для различных отраслей знаний, и в первую очередь юридических, ее ярко выраженная прикладная направленность. Проведен сравнительный анализ мнений ученых по проблемным вопросам обеспечения кибербезопасности. На основании этого предложено авторское определение кибербезопасности, включающее в себя такие важные ее составные элементы какзащищенность

электронных систем, сетей, серверов, программных продуктов и персональных данных. Умышленное, тнесанкционированное, криминальное вмешательство посредством киберугроз, реализуемых с помощью киберпреступности, компьютерных атак и кибертерроризма. Проанализированы их содержание и особенности. Определены основные субъекты реализации кибербезопасности, предложены пути ее совершенствования.

Annotation

The article examines the theoretical and organizational and legal aspects of cybersecurity in modern Russia. Its place and significance in the general system of national security, its influence on ensuring the internal andexternal security of the Russian Federation are determined. At the state statistical service, the relevance of the topic for varios branches of knowledge, and primarily legal, is shown, its pronounced applied orientation. A comparative analysis of the opinions of scientists on the problematic issues of ensuring cybersecurity is carried out. Based on this, the authors definition of cybersecurity is proposed, which includes such essential components as the security of electronic systems, networks, servers, software products and personal data. Intentional, unauthorized, criminal interference through cyberthreats implemented through cybercrime, computer attacs, and cyberterrorism. Their content and features are analyzed. The main subjects of implementation of cybersecurity are definited, ways ofits improvement are offered.

Ключевые слова: кибербезопасность, внешняя и внутренняя безопасность, уровни защищенности, электронные сети, серверы, программные продукты, персональные данные, криминальное вмешательство, киберпреступность, компьютерная атака, кибертерроризм, субъекты кибербезопасности, теоретические, организационные, правовые, пути совершенствования.

Keywords: cybersecurity, the internal and external security, leveks of protection, electronic systems, networks, servers, software products, personal data, criminal interference, cybercrime, computer attac,cyberterrorism, subjects of

cybersecurity, theoretical , organizationa, legal, ways of improvement.

Постоянное, скачкообразное развитие IT технологий и киберпространства, их выраженный трансгенный характер предопределяют поиск новых защитных методик, техник и механизмов от различных угроз и негативных воздействий.

В последние годы наблюдается многократное возрастание угроз в современном киберпростарнстве, их ярко выраженная агрессивная направленность на внешнюю и внутреннюю безопасность Российской Федерации, значительный рост киберпреступлений, (почти на 90% ежегодно на протяжении последних 5 лет, а по преступлениям, связанным с использованием информации банковских карт граждан в 5 раз только в 2020 году).

Утечки данных по электронным сетям, включая персональные данные пользователей, компаний и корпораций, исчисляются в мировом масштабе десятками миллиардов случаев за последние три года. Ущерб при этом оценивается более чем в 2,5 трлн. долларов США ежегодно. Также многократно, до 170 млд. долларов США в год возрастают расходы компаний и организаций на кибербезопасность.

Обеспечение необходимого ее уровня является одной из приоритетных задач российского государства. Этому, в частности посвящена Доктрина информационной безопасности, принятая Указом Президента 05.12.2016 года, содержащая основные понятия в данной сфере, регламентирующая подходы, направления, средства и методы еереализации.

К стратегическим целям кибербезопасности относятся защита киберпространства Российской Федерации, ее суверенитета, обороноспособности, политической и социальной систем, территориальной целостности, а также прав и законных интересовграждан.

В условиях увеличения разведывательной активности организаций в отношении органов государственной и исполнительной власти, оборонных, промышленных, сырьевых предприятий, медицинских, страховых и туристических компаний РоссийскойФедерации, оказания психологического

воздействия, в том числе с элементами нейролингвистического программирования с использованием IT технологий, этнических, религиозных особенностей на массовое сознание для дестабилизации политическойситуации, обеспечение релевантной системы защиты выглядит крайненеобходимым.

Различные террористические и экстремистские организации также используют для своей криминальной пропаганды и вовлечения молодежи в преступную деятельность современные digital технологии,подрывая доверие к действующей власти, нарушая единство и территориальную целостность государства.

Существенное увеличение размера ущерба от компьютерных преступлений в России, исчисляемого несколькими трлн. рублей ежегодно, с ростом в геометрической прогрессии, наличие пробелов в законодательном и ведомственном регулировании, недостатки в организации скоординированного противодействия киберпреступности и обеспечения надлежащего уровня кибербезопасности, также предопределили выбор темы исследования, некоторые результаты которого приведены в данной статье.

Его методологической базой послужили основополагающиеположения отечественной юридической науки, сравнительно- правовой, статистический метод, методы системного и структурного анализа.

Нормативную основу исследования составили Конституция Российской Федерации, федеральные законы и другие нормативные правовые акты по теме.

Теоретическое изучение проблемы показало, что многие отечественные и зарубежные специалисты в области социальной инженерии, программирования, информатики, юриспруденции последние 15 лет все более активно исследуют различные аспекты кибербезопасности (компьютерной безопасности). Предлагают ее определения, различные классификации составляющих элементов, комплекс мер по совершенствованию и др.

Так, например, Ю.А. Родичев весьма подробно анализирует нормативно-правовую основу, международные и отечественные стандарты в сфере информационной безопасности [1].

В.В. Бондарев рассматривает законодательное регулирование информационной безопасности автоматизированных систем, основные киберугрозы, а также предлагает классификацию предупредительных мер в этом направлении[2].

В.М. Быков, Б.П. Смагоринский, В.Н. Черкасов исследовали кибербезопасность в контексте распространения и особенностейсовершения информационных преступлений, их криминологические, уголовно-правовые и криминалистические проблемы. Уделив при этом

первостепенное внимание характеристике и современным тенденциям киберпреступности, квалификации, а также выявлению, раскрытию и предупреждению преступлений в digital сфере [3].

Правовую основу кибербезопасности составляют Конституция Российской Федерации, выше названная Доктрина информационной безопасности, международные нормативные правовые документы, федеральные конституционные законы, федеральные законы, нормативные правовые акты Президента и Правительства Российской Федерации, федеральных министерств и ведомств, государственных органов местного самоуправления.

Проведенный сравнительный анализ различных подходов в изучении кибербезопасности, позволил сформулировать авторский вариант ее определения. Под кибербезопасностью понимается защищенность электронных систем, сетей, серверов, а также програмных продуктов и персональных данных от умышленного несанкционированного, криминального вмешательства посредством киберугроз, реализуемых с помощью киберпреступности, компьютерных атак и кибертерроризма.

В рассматриваемом контексте можно выделить три уровня защищенности: низкую, среднюю и высокую. Дифференциация по ним определяется использованием современных защитных IT технологий,

аппартных комплексов и программного обеспечения, позволяющих купировать и устранять организуемые криминальные атаки, в том числе с применением модифицированных вредоносных программ, компьютерных вирусов, а также предотвращать, своевременно реагировать и устранять киберугрозы и вызовы в современном киберпространстве.

Более детальное рассмотрение применения сил, средств и методов при организации кибербезопасности можно осуществлять в рамках отдельных ее элементов (безопасности сетей, приложений, информации, так называемой операционной безопасности).

Основными субъектами кибербезопасности в настоящее время являются должностные лица государственных органов, органов местного самоуправления, наделенных соответсвующими полномочиями, среди которых особо выделяются правоохранительные структуры, а также специальные службы (Генеральная прокуратура, Министерство внутренних дел, Следственный комитет, Федеральная служба безопасности, Министерство обороны, Федеральная служба охраны, Министерство юстиции Российской Федерации и подведомственная ему Федеральная служба исполнения наказаний, а также Росгвардия).

Перечисленные и другие субъекты кибербезопасности обеспечивают ее посредством правовых, организационных, технических, оперативно-розыскных, кадровых, разведывательных, контрразведывательных, научных, информационно-аналитическихмероприятий.

Таким образом, к основным направлениям совершенствования кибербезопасности и повышения ее эффективности можно отнести:

- использование современных защитных технологий, оборудования и комплексов, позволяющих поднять ее на высший уровень защищенности;
- повышение кадрового потенциала специалистов, способных решать сложные технические задачи по предотвращению, купированию и устранению современных киберугроз, их умений и профессионализма;
- скоординированную деятельность субъектов кибербезопасности по предупреждению, выявлению и раскрытию

киберпреступлений, компьютерных атак и кибертерроризма;

- опережающее законодательное регулирование, ведомственную нормативную правовую регламентацию института кибербезопасности, противодействие киберпреступности и кибертерроризму, ликвидацию правовых пробелов в максимально короткие сроки, в соответствии с потребностями правоприменительной практики в этой сфере;

- активное использование современных форм, средств и методов оперативно-розыскной деятельности, оперативно-розыскных мероприятий по обеспечению высшего уровня кибербезопасности и противодействия киберпреступности;

- использование опыта развитых зарубежных стран по организации кибербезопасности, противодействия киберугрозам, борьбы с кибертерроризмом и криминальными киберситуациями;

- тиражирование и внедрение в практическую деятельность опыта обеспечения кибербезопасности, накопленного ее субъектами в различных федеральных образованиях Российской Федерации;

- создание, развитие и совершенствование организационной и информационно-аналитической службы в субъектах кибербезопасности;

- организация всесторонних комплексных научных исследований проблем кибербезопасности, киберпреступности, кибер атак и кибертерроризма.

Литература

1. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. Спб., изд-во Питер, 2017. – 254с.; Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: международные и национальные стандарты / Учеб. пособие. Спб., изд-во Питер, 2019.-76с.

2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. М., Изд. МГТУ им Н.Э. Баумана, 2016.- 136с.

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

Literature

1. Rodichev Yu. A. Information security: regulatory and legal aspects. SPb., Pub. Pite, 2017. - 254p.; Rodichev Yu. A. Regulatory base and standards in the field of information security: international and national standards / Train. manual. SPb. Pub. Piter, 2019. - 76p.

2. Bondarev V.V. Introduction to information security of automated systems. M., Pub. MSTU N.E. Bauman, 2016.- 136p.

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