ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ОСОБЕННОСТИ ОРГАНИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ В США

LEGAL REGULATION AND FEATURES OF THE ORGANIZATION OF CYBERSECURITY IN THE UNITED STATES

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@ya.ru

Аннотация

В статье по результатам осуществляемого комплексного исследования правовых и организационных проблем современной кибербезопасности излагаются данные сравнительного анализа наиболее эффективных в этой сфере зарубежных государств. Рассматриваются правовое регулирование и особенности организации кибербезопасности в США, обладающей развитой системой выявления и реагирования на киберугрозы.

Анализируется организационная структура основных государственных органов, обеспечивающих кибербезопасность, вопросы их взаимодействия и координации. Освещаются основные нормативные правовые акты, регулирующие эту сферу деятельности, закрепляющие такие понятия как

кибербезопасность, киберугроза, киберинцедент, значительный киберинцедент, киберкоммуникации. Описываются правовые и организационные механизмы управления рисками кибербезопасности: идентификация, защита, обнаружение, реагирование и восстановление. Обосновывается актуальность и значение для совершенствования отечественной кибербезопасности понимания основных подходов, принципов организации, правового регулирования и научного сопровождения данного направления.

Annotation

Based on the results of a comprehensive study of the legal and organizational problems of modern cybersecurity, the article presents the data of a comparative analysis of the most effective foreign countries in this area. The article considers the legal regulation and features of the organization of cybersecurity in the United States, which has a developed system for detecting and responding to cybethreats. Analyzes the organizational structure of the established state bodies providing cybersecurity, issues of their interaction and coordination. The main normative legal acts regulating this sphere of activity, fixing such concepts as cybersecurity, cybethreat, cyberincident, significant cyberincident, cybercommunications are highlighted. The article describes the legal and organizational mechanisms for managing cybersecurity risks: identification, protection, detection, response and recovery. The article substantiates the relevance and importance of understanding the main campaigns, the principles of organization, legal regulation and scientific support of this area for improving domestic cybersecurity.

Ключевые слова: кибербезопасность, система выявления и реагирования, киберугроза, субъекты и объекты кибербезопасности, государственные органы, взаимодействие, координация, киберинцедент, значительный киберинцедент, киберкоммуникации, управление рисками, идентификация, защита, обнаружение, реагирование, восстановление.

Keywords: cybersecurity, detection and response system, cybethreat, subjects and objects of cybersecurity, government agencies, interaction, coordination, cyberincident, significant cyberinciden, cybercommunications, managing risks: identification, protection, detection, response, recovery.

Одним из путей совершенствования современной кибербезопасности Российской Федерации, обеспечения ее высокой эффективности является использование опыта развитых зарубежных стран в этом направлении, государственные структуры, организации и сообщества которых не случайно уделяют этой теме на протяжении последних десятилетий самое пристальное внимание.

Создаются и финансируются специальные подразделения и программы по защите кибербпространства, государственных учреждений, частных компаний и корпораций, персональных данных граждан. Осуществляются многочисленные научные, информационно-технические, организационно-правовые и другие исследования, активно внедряются в практическую деятельность современные аппаратные средства и комплексы.

С учетом изложенного, в рамках осуществляемого нами 4-х этапного комплексного исследования правовых и организационных проблем современной кибербезопасности, был проведен сравнительный анализ наиболее эффективных в этой сфере зарубежных систем.

Используя методы контент анализа зарубежной литературы и информационных источников, а также включенного наблюдения мы классифицировали развитые зарубежные страны, опыт которых по обеспечению кибербезопасности представляет наибольший интерес для отечественной науки и практики. В основу классификации были положены принципы наибольшей эффективности, а также географическо-политический и экономический.

В контексте изложенного представляет повышенный исследовательский интерес опыт организации и обеспечения кибербезопасности в Соединенных штатах Америки, странах Евросоюза, Китая, Юго-Восточной Азии (Южной Кореи, Сингапура и др.)

В США на протяжении длительного времени существовала исторически сложившаяся система субъектов – государственных органов, осуществлявших противодействие киберпреступности, компьютерным атакам и кибертерроризму, обеспечивавших кибербезопасность государства, коммерческих структур и граждан. В нее входили: Федеральное бюро расследований (ФБР), Центральное разведывательное управление(ЦРУ), министерство обороны, полиция а также организации разведывательного сообщества.

Серия терактов 11 сентября 2001 года показала, что в целом, система кибербезопасности находится на критически низком организационном и материально-техническом уровне, что послужило объективной причиной ее изменения, модернизации и совершенствования. В результате уже через 20 дней было создано Управление внутренней безопасности (Office of Homeland Security), на которое были возложены функции координации обеспечения национальной безопасности, взаимодействия в этой сфере с департаментами и службами, организациями и местными органами власти [1]. Спустя два года статус управления был повышен до Министерства внутренней безопасности (Department of Homeland Security).

6 июня 2003 года на базе данного органа путем объединения Федерального Центра компьютерных инцидентов и Национальной системы коммуникаций было сформировано Национальное управление кибербезопасности (National Cyber Security Division). Оно сотрудничало с Администрацией Белого дома, Правительством, военными и разведывательными структурами, частными компаниями и корпорациями по

вопросам выявления и оценки рисков киберугроз и снижения уязвимости IT-инфраструктур перечисленных пользователей.

В 2007 году указанное подразделение было переименовано в управление национальной защиты и программ (NPPD), основной функцией которого стало обеспечение национальной безопасности посредством снижения и устранения киберугроз для национальной киберструктуры государства.

Через год, в марте 2008 в структуре Министерства внутренней безопасности был создан Национальный центр интеграции кибербезопасности и коммуникаций (NCCIC). Основными задачами которого были определены защита сетей и серверов, других правительственных киберкоммуникаций от несанкционированного воздействия. Также указанное подразделение наделялось широкими полномочиями по отслеживанию, сбору, анализу и передачи информации о киберсистемах Агенства национальной безопасности, Федерального бюро расследований и Министерства обороны США.

Более 10 лет указанная организационная структура является национальным центром кибернетической и коммуникационной информации, технической экспертизы и оперативной интеграции, функционирует в круглосуточном режиме ситуационной осведомленности, анализирует и реагирует на различные возникающие киберинциденты, в том числе криминального характера.

Рассматривая организационное построение и взаимодействие различных субъектов, осуществляющих кибербезопасность в США необходимо выделить Департамент инициатив по обеспечению национальной безопасности, координирующий усилия федерального правительства по обеспечению безопасности важнейших объектов инфраструктуры государства. Это ведомство в целях предотвращения киберугроз и нейтрализации их последствий осуществляет следующие мероприятия:

- создает технологически нейтральную структуру добровольной кибербезопасности;
- поощряет и стимулирует внедрение системы кибербезопасности во все ее потенциальные объекты;
- обеспечивает своевременность и качество обмена информацией о киберугрозах, увеличивая и детализируя его объем и содержание;
- реализует принцип обеспечения строгой защиты частной жизни и гражданских свобод при принятии любой законодательной и ведомственной инициативы по обеспечению безопасности критически важных объектов инфраструктуры;
- осуществляет постоянную, системную разработку ситуационной осведомленности в режиме реального времени с учетом физических и виртуальных (кибер) особенностей;
- изучает, предотвращает и устраняет каскадные последствия сбоев объектов инфраструктуры;
- анализирует и оценивает тенденции и динамику развития государственного и частного партнерства в вопросах обеспечения кибербезопасности, противодействия основным киберугрозам;
- обновляет и дополняет национальный план защиты объектов инфраструктуры;
- разрабатывает и реализует комплексные планы исследований и перспективного развития систем национальной безопасности. Ориентируясь при этом, в первую очередь, на исследования по совершенствованию кибербезопасности, проводимые Национальным институтом стандартов и технологий (NIST) для улучшения кибербезопасности критически важных объектов инфраструктуры.

Пересмотренная в апреле 2018 года структура указанного института, ориентируется на реализацию пяти основных функций управления рисками кибербезопасности: идентификацию, защиту, обнаружение, реагирование и восстановление.

16 ноября 2018 года было создано Агентство по кибербезопасности и безопасности инфраструктуры (Cybersecurity and Infrastructure Security Agency)[2]. Закон, регламентировавший создание названной структуры предусматривает также увеличение национального потенциала для защиты от кибератак, в том числе посредством повышения его финансирования, а также предусматривает первоочередную защиту федерального правительства, других департаментов и агентств.

Указанная структурная и организационная перестройка деятельности основных субъектов кибербезопасности в целях повышения их эффективности, сопровождалась также нормативным регулированием понятийного аппарата. Так, Закон о борьбе с терроризмом в США 2001года определил критически важные инфраструктуры государства, которые могут являться объектами кибербезопасности и отношении которых могут осуществляться киберугрозы и киберинциденты. К ним законодатель отнес жизненно важные системы и активы (физические и виртуальные), уничтожение или повреждение которых окажет разрушительное воздействие на национальную, экономическую и оборонную безопасность, здравоохранение и жизнедеятельность граждан [3].

Важной вехой в развитии и совершенствовании правового регулирования и организации современной системы кибербезопасности в США явилась Президентская директива от 26 июля 2016 года определившая основные алгоритмы по выявлению, рассмотрению и разрешению киберинцидентов, под которыми данный документ понимает также и криминальные инциденты или киберпреступность [4].

Весьма интересен в ней подход американских законодателей к трактовке центрального понятия кибербезопасности– киберинцидента, под которым понимается конкретное событие в компьютерной сети, угрожающее целостности, конфиденциальности или доступности компьютеров, информационных или коммуникационных систем, сетей и серверов, а также

физической или виртуальной инфраструктуры, контролируемой компьютерами или информационными системами, и находящейся в них информации.

К значительным киберинцидентам законодатель относит тот (или их группу), который может нанести очевидный ущерб интересам национальной безопасности, международным отношениям или экономике государства, его общественным институтам и их доверию, гражданским свободам, общественному здоровью и безопасности американских граждан.
Ввиду того, что значительные киберинциденты предполагают обязательное участие в них государственного субъекта кибербезопасности, на Министерство юстиции возлагается руководящая и координирующая роль по их разрешению. Минюст США объединяет и направляет деятельность Федерального бюро расследований и Национальной объединенной рабочей группы по кибер-расследованиям на оптимальный алгоритм реагирования на киберугрозы.

Министерство внутренней безопасности действует при этом через Национальный центр интеграции кибербезопасности и связи, и также является важной федеральной структурой по реагированию на содержание и активы киберинцедента.

В то же время, Управление директора национальной разведки, используя возможности центра интеграции информации о киберугрозах является главным федеральным органом их разведывательного обеспечения, сопровождения и нейтрализации.

В частности, документ предусматривает принятие федеральным правительством государственных и частных мер по нейтрализации инцидентов. В особых случаях, алгоритм реагирования на них предполагает ответное реагирование более широкими мерами и действиями. При этом на министерства юстиции и внутренней безопасности возлагаются задачи по

поддержанию обновленной контактной информации в целях оказания помощи организациям, пострадавшим от киберинцидентов.

При этом федеральные структуры обязаны реагировать не только на непосредственные угрозы, но и на их содержание и последствия, организуя свою деятельность на принципах общей ответственности, уважения прав лиц, ставших объектами киберинцидентов, адекватности реагирования на киберугрозы и повлекшие инциденты, единства и согласованности действий государственных органов по их выявлению и разрешению.

Мероприятия реагирования на угрозы предполагают осуществление необходимых первоначальных и последующих следственных действий правоохранительных ведомств и органов национальной безопасности на территории пострадавшего субъекта. Такие действия могут включать сбор доказательств и разведданных; предоставление атрибуции; связывание однородных инцидентов в единую взаимосвязанную цепь; выявление всех пострадавших от инцидента лиц; определение алгоритма ассиметричного ответа на киберугрозы и криминальный характер киберинцидента; планирование мероприятий по устранению непосредственной угрозы а также содействие обмену информацией и координации с другими субъектами кибербезопасности и реагирования на возникающие киберугрозы.

Директива также определяет координирующие органы и их ответственность за эффективность реагирования на национальном и региональном уровнях. Так, транснациональное содержание Интернета, используемых коммуникационных инфраструктур, сетевых каналов передачи информации, серверов для ее хранения предполагает координацию действий государственных структур США с их союзниками и партнерами при разрешении инцидентов.

Таким образом, реализуемая в США система обеспечения кибербезопасности, начиная с готовности к противостоянию киберугрозам и

их купированию или устранению позволяют эффективно противостоять многочисленным киберинцидентам различной степени сложности.

Выстроенная и функционирующая система субъектов обеспечения кибербезопасности охватывает многие направления потенциальных киберугроз. Законодательное регулирование и научное обеспечение позволяют успешно справляться с широким спектром угроз и опасностей.

Изученный опыт обеспечения кибербезопасности в одном из наиболее развитом в этом направлении государстве, безусловно, может быть полезен отечественным ученым и практическим работникам в разработке перспективных научных исследований, методик и рекомендаций по совершенствованию правового и организационного обеспечения высшего уровня кибербезопасности в современной России.

Литература

1. Ссылка: www.dhs.gov [сайт]. – URL: http://www.dhs.gov/creation-department-homeland-security (дата обращения: 01.02.2021)

2. Ссылка: www.cisa.gov/about-cisa [сайт]. – URL: https://www.cisa.gov/about-cisa (дата обращения: 02.02.2021)

3. Закон о борьбе с терроризмом в США, 2001[сайт]. – URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (дата обращения: 03.02.2021)

4. obamawhitehouse.archives.gov [сайт]. – URL: http: obamawhitehouse.archives.gov //the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident(дата обращения: 02.02.2021)

Literature

1. Link: www.dhs.gov [website]. – URL: http://www.dhs.gov/creation-department-homeland-security (accessed: 01.02.2021)

2. Link: www.cisa.gov/about-cisa [website]. – URL: https://www.cisa.gov/about-cisa (accessed: 02.02.2021)

3. Закон о борьбе с терроризмом в США, 2001[website]. – URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (accessed: 03.02.2021)

4. Link: obamawhitehouse.archives.gov [website]. – URL: http: obamawhitehouse.archives.gov //the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident(accessed: 02.02.2021)