УДК 351.865

Р. В. Лукьянчук,
соискатель Института законодательства Верховного Совета Украины (г. Киев)

ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

Данная статья посвящена анализу текущего состояния обеспечения кибернетической безопасности в Республике Казахстан. Регламентированы стратегические направления деятельности политического руководства Казахстана в сфере создания национальной системы обеспечения кибербезопасности. Проведен анализ актов законодательства Республики Казахстан, которые регулируют концептуальные основы обеспечения кибербезопасности. Детализированы направления усовершенствования законодательства с целью создания современного государственного механизма обеспечения кибербезопасности. Определены тенденции развития международного сотрудничества между Казахстаном и Украиной в сфере совместного реагирования на компьютерные инциденты при участии национальных команд (CERT).

Ключевые слова: *обеспечение кибербезопасности, информационная безопасность, кибератака, кибертерроризм, киберпреступность, информационное пространство, информационно-коммуникационные технологии, государственная техническая политика, государственный механизм обеспечения кибербезопасности.*

Аңдатпа

Бұл мақала Қазақстан Республикасында кибернетикалық қауіпсіздікті қамтамасыз етудің ағымдағы жағдайын талдауға арналған. Киберқауіпсіздікті қамтамасыз етудің ұлттық жүйесін құру саласында Қазақстанның саяси басшылығы қызметінің стратегиялық бағыттары регламенттелген. Қазақстан Республикасының киберқауіпсіздікті қамтамасыз етудің тұжырымдамалық негіздерін реттейтін заңнамалық актілеріне талдау жүргізілген. Кибер қауіпсіздікті қамтамасыз етудің қазіргі мемлекеттік тетіктерін құру мақсатында заңнаманы жетілдіру бағыттары жан-жақты талданған. Қазақстан мен Украина арасында ұлттық командалардың қатысуымен компьютерлік оқиғаларға бірлесіп ден қою (CERT) саласындағы халықаралық ынтымақтастықты дамыту үрдістері айқындалған.

Тірек сөздер: *киберқауіпсіздікті қамтамасыз ету, ақпараттық қауіпсіздік, кибершабуыл, кибертерроризм, киберқылмыстылық, ақпараттық кеңістік, ақпараттық-коммуникациялық технологиялар, мемлекеттік техникалық саясат, киберқауіпсіздікті қамтамасыз етудің мемлекеттік тетіктері.*

Abstract

This article is devoted to modern conditions of cyber security software in the Republic of Kazakhstan. The strategic directions of activity of the political leadership of Kazakhstan in sphere of national system of cyber security protection and its implement are determined. The legislative acts of the Republic of Kazakhstan, which are regulated the conceptual bases of cyber security protection are analyzed. The directions of improvement of state legislations to make modern mechanism of cyber security protection are detailed. Set the trend for developing of international cooperation between Kazakhstan and Ukraine to react for IT-incident together and with national CERT support.

Key words: *cyber security protection, information security, cyber attack, cyber terrorism, cybercrime, information space, information and communication technologies, public technical policy, public mechanism of cyber security protection.*

JEL codes: *Z10 General, Z18 Public Policy, O38 Government Policy, O32 Management of Technological Innovation and R&D.*

В современных условиях обеспечение кибернетической безопасности является одной из стратегических задач политического руководства большинства развитых государств. Динамическое развитие информационных технологий формирует новые угрозы и сценарии возможных силовых противостояний в киберпространстве. Сегодня в мировом масштабе наблюдается тенденция эволюции кибернетических атак – от простого блокирования работы Интернета и до активных мероприятий, направленных на уничтожение промышленных и критических государственных объектов информационной инфраструктуры, операционных систем.

Массовое внедрение и распространение доступных информационных передовых технологий создают благоприятные условия для посягательств и нападений как групп хакеров, так и отдельных государств на объекты национальной информационной инфраструктуры «третьих» стран, возникновения сбоев в работе государственных информационных ресурсов, что провоцирует подрыв информационного суверенитета «государства-мишени». Как свидетельствует международный опыт, целью кибернетических атак является нанесение масштабных финансово-экономических убытков, сбои в функционировании информационно-телекоммуникационных систем, что в совокупности негативно влияет на общее состояние как международной, так и национальной безопасности, одновременно провоцирует необходимость создания надежной защиты информационного пространства, государственных и коммерческих информационных ресурсов. Проблемным вопросом остается низкое качество услуг безопасности, предоставляемых поставщиками информационно-коммуникационных технологий (ИКТ), что осложняет и делает невозможной реализацию национальных и международных инициатив по противодействию и правовому реагированию на преступную деятельность, террористические акты и военную агрессию в кибернетическом пространстве.

В современном цивилизованном мире стремительно растет роль Интернета, который обладает серьезным потенциалом для повышения благосостояния населения и расширения доступа к информации. Однако в последнее время существует тенденция к увеличению угроз и снижению безопасности в киберпространстве. В частности, имеют место факты массового кибершпионажа как в США, так и в Азии и Европе. Поэтому вопрос о том, как в течение следующего десятилетия будет развиваться управление кибербезопасностью, имеет важное значение. Практически каждый политический или военный конфликт сопровождается противоборством в Интернете, при этом активно используется кибернетическое оружие. Враждебные действия в кибернетическом пространстве могут финансироваться как отдельными государствами, так и террористическими организациями, которые являются первым шагом к началу кибернетической войны. Международное и национальное кибернетическое пространство стало «параллельной вселенной», в которой преступники, а также террористы могут осуществлять кибератаки с высокой степенью безнаказанности.

Важным препятствием на пути борьбы с кибернетической преступностью является несовершенство существующих правовых механизмов. Нормативно-правовые акты, принимаемые как на государственном, так и на международном уровне, являются фундаментом, на котором строится глобальный механизм борьбы с кибернетическим терроризмом и кибернетической преступностью. Таким образом, усилия политического руководства государств необходимо сконцентрировать на максимальной реализации законодательных инициатив относительно обеспечения кибернетической безопасности, и Республика Казахстан не является здесь исключением.

Исследованию проблематики обеспечения информационной безопасности посвящены научные труды таких казахстанских ученых, как Н. А. Биекенов [1], Т. А. Дмитренко [2], А. Е. Жатканбаева [3], и других. При этом вопросы государственного управления процессами обеспечения кибернетической безопасности в Республике Казахстан на уровне научной проблемы указанные авторы не рассматривали, о чем свидетельствует актуальность тематической направленности подготовленной научной статьи.

Целью статьи является анализ правовых актов в контексте определения организационно-управленческих основ государственного обеспечения кибернетической безопасности на примере Республики Казахстан.

С момента провозглашения независимости Казахстан уверенно взял курс на интеграцию с мировым сообществом, в том числе и как активный участник построения информационного общества. По оценкам ведущих мировых экспертов, Казахстан занимает 18-е место в мире по количеству получаемого спама и 7-е по показателям опасности веб-серфинга, при этом до настоящего времени государственные информационные ресурсы не подвергались

политически мотивированным кибератакам, сходным с теми, что происходили в Польше в 2014 году или в Германии весной 2015 года, когда объектами посягательств стали интернет-ресурсы органов государственной власти указанных стран.

Именно поэтому в современных условиях ключевой задачей политического руководства Казахстана является создание единого развитого информационного пространства в глобальной сети казахстанского сегмента Интернета – Казнета, который представляет собой совокупность информационных сетевых ресурсов, информационно-телекоммуникационных систем, технологий их ведения и использования. Тенденции, связанные с информатизацией всех аспектов государственной и общественной жизни, объективно свидетельствуют, что существование современного независимого государства неразрывно связано с обеспечением информационной безопасности всех звеньев его государственных структур [4].

Именно органам государственного управления принадлежит ведущая роль в разработке и реализации перспективных национальных программ формирования и развития Казнета. Концепты государственной политики развития информационного пространства и обеспечения кибербезопасности Республики Казахстан сформированы в действующих положениях нормативно-правовых актов, с учетом основополагающих принципов международного права и необходимости защиты национальных интересов государства в информационной сфере. Анализ законодательства Республики Казахстан позволяет сделать вывод, что с целью создания адекватной информационной защиты государства необходимо обладать собственной интернет-инфраструктурой, медийной структурой, налаженной системой информационной пропаганды и ведения информационных войн.

Заведующий сектором Отдела правоохранительной системы Администрации Президента Республики Казахстан, доктор юридических наук Н. А. Биекенов в своей научной публикации указывает, что высокие темпы развития в Казахстане информационно-коммуникационных технологий актуализируют вопросы защиты соответствующей инфраструктуры, поскольку ее повреждение или разрушение могут иметь значительные последствия для безопасности страны. Казахстан является частью более широкого киберпространства, в котором два главных соседа – Россия и Китай – особенно известны своим высоким уровнем киберпреступности. В 2011 году более трети мировых киберпреступлений, причинивших ущерб на $12,5 млрд, осуществлялись выходцами из Российской Федерации. Группы, вовлеченные в эту деятельность, все больше контролируются организованными преступными элементами. Китай, в свою очередь, является убежищем для киберпреступников, особенно для тех, кто участвует в экономических преступлениях [1].

Поэтому реализация мероприятий по укреплению кибербезопасности должна осуществляться на собственной программной платформе, поскольку в Казахстане используется импортное сетевое оборудование, которое обслуживается зарубежными вендорами дистанционно и может быть в любой момент отключено. Объективно весь серьёзный софт иностранных производителей, в частности, информация со смартфонов, планшетников и компьютеров Apple, посредством специальных программ в любое время доступны разведывательным службам США.

Марлен Ларюэль на страницах Аналитического обзора по Центральной Азии «Кибербезопасность в Центральной Азии: реальные угрозы, ложные предлоги?», опубликованного в июне 2012 года, утверждает, что Казахстан все чаще подвергается повседневным атакам на безопасность киберпространства. 85 % интернет-атак в Центральной Азии приходится именно на Казахстан, хотя при этом в стране осуществляется масштабная компьютеризация органов государственного управления (создание электронного правительства), крупного бизнеса, в частности, через Национальный научно-технологический холдинг «Парасат» (в который входят Kazsatnet, Казтелерадио, Казпочта, Национальный центр по информатизации) [5].

С целью развития национального информационного пространства, информационно-коммуникационной инфраструктуры в Республике Казахстан в 2013 году была принята

Государственная программа «Информационный Казахстан – 2020», утвержденная Указом Президента Республики Казахстан от 8 января 2013 года № 464 [6], фундаментальными задачами которой стали следующие: обеспечение эффективности системы государственного управления и доступности информационно-коммуникационной инфраструктуры; создание информационной среды для социально-экономического и культурного развития общества; развитие отечественного информационного пространства.

Реализация указанной программы предусматривает проведение активных мероприятий в информационной сфере Казахстана, результативность которых гарантирует: индекс «электронного правительства» (по методике ООН) в 2020 году в рейтинге первых 25 стран; обеспечение максимальной доступности информационно-коммуникационной инфраструктуры в домохозяйствах – 100 %; количество пользователей сети Интернет в 2020 году – 75 %; распространение эфирного цифрового телерадиовещания населения Казахстана – 95 % территории; доля сектора информационно-коммуникационных технологий в структуре ВВП страны – 4 %.

Таким образом, нормативно зафиксированы инициативы политического руководства Казахстана максимально развивать собственную информационно-коммуникационную инфраструктуру, гарантировать обеспечение как информационной, так и кибернетической безопасности страны.

Необходимо отметить, что положения Концепции информационной безопасности Республики Казахстан до 2016 года, утвержденной Указом Президента Республики Казахстан от 14 ноября 2011 года № 174 [7], определяют декларативные основы формирования национальной системы обеспечения информационной безопасности, реализации государственной технической политики в информационной сфере Республики Казахстан, направленные, в первую очередь, на создание благоприятных и оптимальных условий для хранения и защиты информации в киберпространстве; разработку, использование программно-аппаратных комплексов, развитие собственной системы защиты информации. Конечной целью реализации Концепции стало создание национальной системы обеспечения информационной безопасности, гарантирующей защиту национальных интересов Республики Казахстан в информационной сфере. Анализ положений Концепции позволяет определить направления государственного регулирования информационной безопасности: обеспечение активного участия страны в процессах создания, использования глобальных информационных сетей и систем (международное сотрудничество); развитие отечественного информационного пространства; совершенствование законодательства, регулирующего информационную сферу и т. д. Концепция основана на оценке текущей ситуации и определяет государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности и отвечает основным положениям Стратегии развития Республики Казахстан до 2030 года «Процветание, безопасность и улучшение благосостояния всех казахстанцев», в которой обеспечение информационной безопасности определено как долгосрочный приоритет национальной безопасности государства.

Реализация положений Концепции позволила внедрить оптимальную модель развития и регулирования казахстанского сегмента глобальной информационной сети Интернет, механизмов стимулирования производства позитивного содержательного контента, развития отечественных интернет-СМИ, модернизации телекоммуникационной инфраструктуры. Исходя из содержания указанного нормативно-правового акта, актуальной угрозой для Казахстана является нарастание в межгосударственных отношениях негативной тенденции использования информационного давления как действенного механизма глобальной конкуренции, а также использование различных средств информационной войны в киберпространстве. При этом активно используются методы блокирования интернет-СМИ путем проведения компьютерных атак.

Казахстан также является членом Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности, в соответствии с Законом

Республики Казахстан от 1 июня 2010 года «О ратификации Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» [8]. Исходя из анализа упомянутого акта, основными угрозами в информационной сфере, нейтрализация которых является ключевой задачей государств – членов ШОС, являются: масштабная разработка и применение информационного оружия, подготовка и ведение информационной войны; информационный терроризм, информационная преступность, использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств, угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур.

Еще в 2011 году, в ходе десятого саммита государств – членов ШОС, учитывая широкое использование информационно-коммуникационных сетей с целью распространения идеологии терроризма, сепаратизма, было принято решение о создании, по примеру США, подразделений кибервойск, и об установлении жесткого контроля над виртуальным пространством. Реализация указанных инициатив привела к созданию в рамках Шанхайской организации сотрудничества (ШОС) проекта о киберполиции.

По состоянию на 2015 год создание киберполиции в Казахстане было нивелировано руководством силовых структур, поскольку управление «К» криминальной полиции Республики Казахстан осуществляет мероприятия по предупреждению, выявлению, пресечению и раскрытию преступлений в сфере компьютерной информации, где объектом посягательства являются ЭВМ, их системы и сети (как носители информации), в том числе обеспечивают борьбу с киберпреступностью. В связи с чем создавать отдельный вид полиции или специальный орган в структуре МВД Казахстана не имеет смысла, поскольку это может привести к дублированию полномочий, что может негативно сказаться на результативности обеспечения кибербезопасности.

Анализ действующего законодательства Республики Казахстан в контексте обеспечения информационной безопасности характеризуется следующими модельными угрозами: возможные нарушения функционирования критически важных объектов информатизации; низкий уровень производства, внедрения и использования современных информационно-коммуникационных технологий; зависимость от импортных информационных технологий, использование которых может причинить ущерб национальным интересам; активизация международного информационного противоборства; внедрение технологий манипулирования информацией; недостаточно эффективная государственная политика информационного обеспечения; рост преступности, в том числе транснациональной, а также террористической деятельности с использованием информационно-коммуникационных технологий; попытки несанкционированного доступа извне к информационным ресурсам Республики Казахстан, приводящих к причинению ущерба ее национальным интересам; недостаточное развитие системы правового регулирования обеспечения национальной информационной сферы.

Так, правоохранительные органы Казахстана анонсируют увеличение количества преступлений в сфере информационных технологий: хакерство, электронные похищения, осуществление преступных связей через электронную почту, перевод преступных капиталов.

В современных условиях приоритетными направлениями совершенствования национальной системы обеспечения информационной безопасности в Республике Казахстан являются: развитие системы государственного управления информационной безопасностью, позволяющей обеспечить защищенность национальной информационной инфраструктуры и единого национального информационного пространства, разработка и реализация единой государственной технической политики в сфере обеспечения информационной безопасности, в т. ч. развитие и укрепление национальной системы защиты информации, развитие отечественного информационного пространства, совершенствование законодательства, регулирующего информационную сферу.

Поскольку составляющей информационной безопасности является именно кибернетическая безопасность, то ее обеспечение невозможно без реализации государственной технической политики, направленной на разработку и реализацию единых стандартов в области обеспечения требований к государственным и негосударственным информационным системам, ресурсам и поддерживающей их инфраструктуре; создание единой государственной системы мониторинга информационного пространства, создание Оперативного центра обеспечения информационной безопасности для координации усилий по защите критической инфраструктуры в сфере информационных технологий, развитие Единого шлюза доступа государственных органов к сети Интернет, Единой электронной почтовой системы для государственных органов, создание не менее двух территориально разнесенных центров хранения резервных баз данных государственных органов, развитие национальной системы идентификации в киберпространстве, проведение аттестации всех государственных информационных систем. В том числе актуальным направлением в современных условиях остается развитие системы государственного регулирования в области кибербезопасности, ее законодательное обеспечение, а также милитаризация кибертехнологий.

В 2011 году в Казахстане была создана Служба реагирования на компьютерные инциденты (KZ-CERT) при Министерстве связи и информации – единый центр для пользователей национальных информационных систем и сегмента сети Интернет, обеспечивающий сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователей по вопросам предотвращения угроз компьютерной безопасности. Деятельность KZ-CERT направлена на создание условий для безопасного использования информационно-коммуникационных технологий; своевременного выявления фактов атак на объекты государственной информационной инфраструктуры; обеспечения взаимодействия между консультантами и экспертами, работающими в сфере информационной безопасности; выявления уязвимых мест в компьютерных системах; развития международного сотрудничества в этой сфере.

Основной задачей KZ-CERT также является снижение уровня угроз информационной безопасности для пользователей казахстанского сегмента сети Интернет, оказание содействия казахстанским и зарубежным юридическим и физическим лицам при выявлении, предупреждении и пресечении противоправной деятельности, имеющей отношение к сетевым информационным ресурсам. KZ-CERT осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Казахстана. В компетенцию службы входит обработка следующих компьютерных инцидентов с целью их выявления и нейтрализации: атаки на узлы сетевой инфраструктуры и серверные ресурсы с целью нарушения их работоспособности (DoS (Denial of Service) и DDoS) и конфиденциальности информации; несанкционированный доступ к информационным ресурсам; распространение вредоносного программного обеспечения, незатребованной корреспонденции (спам); сканирование национальных информационных сетей и хостов; подбор и захват паролей и другой аутентификационной информации; взлом систем защиты информационных сетей, в том числе с внедрением вредоносных программ (сниффер, rootkit, keylogger и т. д.).

Одним из направлений работы KZ-CERT является профилактика правонарушений, связанных с киберпреступностью, в т. ч. противодействие ботнетам, проверка интернет-ресурсов на наличие уязвимостей и вредоносного кода, отслеживание хакерской активности и т. д. Функционирование KZ-CERT благоприятствует созданию условий для осуществления профилактики, выявления и нейтрализации атак на критические узлы и ресурсы национальной ИТ-инфраструктуры, имеющих целью нарушение их конфиденциальности, целостности и доступности.

Служба реагирования на компьютерные инциденты Казахстана (KZ-CERT) осуществляет такие мероприятия, как: оповещение, обработка инцидента, анализ инцидента, консультации по информационной безопасности. Оповещение являет собой оптимизацию объявлений

о новых угрозах на интернет-ресурсах (вирусах, атаках и других угрозах), сообщений об уязвимостях в аппаратном или программном обеспечении на сайте и по электронной почте. Обработка инцидента заключается в предоставлении рекомендаций по устранению угроз, минимизации их негативного воздействия и последствий киберинцидентов. Анализ включает в себя изучение всех доступных данных, вещественных доказательств, следов хакеров и взломщиков для определения масштабов повреждений, причины инцидента и принятия возможных ответных действий. В процессе проведения консультаций по информационной безопасности KZ-CERT осуществляет взаимодействие с правоохранительными органами, собственниками интернет-ресурсов, государственными органами, операторами связи и хостинг-провайдерами, а также с международными профильными организациями по вопросам информационной безопасности.

В рамках обеспечения профилактики правонарушений в сфере высоких технологий Службой оперативного реагирования Казахстана (KZ-CERT) осуществляется комплексное взаимодействие с Министерством внутренних дел республики. Так, в 2011 году были подписаны регламенты оперативного взаимодействия между Министерством связи и информации и Министерством внутренних дел, Комитетом национальной безопасности Казахстана по вопросам оперативного реагирования на какие-либо компьютерные инциденты, включая кибератаки. Также подписаны меморандумы о взаимном сотрудничестве в сфере информационной безопасности с Индийской (CERT-In), Армянской (CERT.AM), Азербайджанской (CERT.GOV.AZ), Румынской (CERT-RO), Латвийской (CERT.LV), Узбекской (UZ-CERT), Австралийской (CERT AUSTRALIA), Индонезийской (ID-CERT) службами реагирования на компьютерные инциденты. В июле 2012 года Казахстанская служба реагирования на компьютерные инциденты (KZ-CERT) стала членом рабочей группы по антифишингу APWG (Anti-Phishing Working Group), а в январе 2015 года вступила в Организацию исламского взаимодействия служб реагирования на компьютерные инциденты (OIC-CERT) на правах национальной службы реагирования.

С целью реализации мер по повышению доверия в сфере информационно-коммуникационных технологий (ИКТ) была подписана Декларация операторов связи и хостинг-провайдеров Республики Казахстан о безопасном Интернете. Данная декларация устанавливает основные принципы для эффективного исполнения законодательства Республики Казахстан, регулирующего отношения в сфере использования и улучшения координации действий операторов связи, а также хостинг-провайдеров, иных участников отношений, связанных с Интернетом, в том числе государственных органов и общественных организаций, патронирующих сферы безопасного использования ИКТ и ликвидации противоправного контента.

Для контроля за состоянием технологических процессов, связанных с информационной безопасностью, в Министерстве связи и информации Казахстана организована деятельность Центра мониторинга информационной безопасности «электронного правительства», основными задачами которого являются как выявление уязвимостей серверов «электронного правительства», так и регистрация, анализ событий и угроз информационной безопасности в компонентах «электронного правительства». Мониторинг состояния обеспечения информационной безопасности проводится на периодической основе с формированием соответствующих отчетов, а также с выработкой соответствующих рекомендаций по предупреждению и устранению возможных проблем и сбоев в системах защиты информационных систем. Выполнение этих рекомендаций позволяет существенно поднять уровень защищенности информационных систем инфраструктуры «электронного правительства» путем упреждающего устранения уязвимостей, которые могут быть использованы хакерами-злоумышленниками.

С целью определения перспективных направлений обеспечения кибербезопасности в Республике Казахстан 23 января 2014 года было проведено заседание Экспертного совета при Совете Безопасности Республики Казахстан, по результатам которого определены

ключевые вопросы развития киберпространства, осуществлен анализ современных рисков, связанных с развитием и внедрением кибертехнологий, детализированы подходы к обеспечению защищенности киберпространства страны, принято решение о милитаризации кибертехнологий. Также по итогам работы Экспертного совета при Совете Безопасности Республики Казахстан были уточнены фундаментальные задачи государственных органов и экспертного сообщества в сфере обеспечения кибербезопасности, одобрено решение о необходимости разработки Комплексного плана обеспечения кибербезопасности Республики Казахстан.

С 1 января 2016 года вступил в силу Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418 [9], который был принят с целью регулирования общественных отношений в сфере информатизации, определения направлений государственной поддержки развития информационно-коммуникационных технологий. Законом предусматривается внедрение сервисной модели информатизации, применение архитектурного подхода при автоматизации функций государственного управления, обеспечение безопасности при использовании информационно-коммуникационных технологий.

Глава 9 указанного законодательного акта регламентирует порядок и условия защиты объектов информатизации. Нормативно установлено, что защита объектов информационно-коммуникационной инфраструктуры осуществляется их собственниками, владельцами и пользователями, которые обязаны принимать меры, обеспечивающие: предотвращение несанкционированного доступа; своевременное обнаружение фактов несанкционированного доступа, если такой несанкционированный доступ не удалось предотвратить; минимизацию неблагоприятных последствий нарушения порядка доступа; недопущение несанкционированного воздействия на средства обработки и передачи электронных информационных ресурсов; оперативное восстановление электронных информационных ресурсов, модифицированных либо уничтоженных вследствие несанкционированного доступа к ним; незамедлительное информирование государственной технической службы о произошедшем инциденте информационной безопасности, за исключением собственников и (или) владельцев электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты; информационное взаимодействие с государственной технической службой по вопросам мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства»; предоставление доступа государственной технической службе к объектам информатизации «электронного правительства» и критически важным объектам информационно-коммуникационной инфраструктуры для проведения организационно-технических мероприятий, направленных на реализацию мониторинга обеспечения информационной безопасности.

Казахстан является стратегическим партнером Украины. По итогам визита Президента Украины П. Порошенко в Казахстан в октябре 2015 года было подписано Совместное заявление и План действий Казахстан – Украина до 2017 года, в которых определены ключевые направления двустороннего сотрудничества в следующих отраслях: топливно-энергетическая, сельскохозяйственная, транспортное, агропромышленное машиностроение, создание инфраструктурных объектов, авиационная, космическая, информационная и т. д.

К сожалению, до сих пор между Украиной и Казахстаном вопросы кооперации и взаимодействия между Службами реагирования на киберинциденты (CERT) с целью обмена опытом и информацией об угрозах и атаках в киберпространстве не урегулированы в формате двусторонних соглашений. Поэтому в современных условиях актуальным и перспективным направлением остается подписание Меморандума о сотрудничестве между Службами (CERT) Казахстана и Украины с целью максимальной защиты бинациональных информационных ресурсов, мониторинга и оперативного реагирования на угрозы как в национальном, так и международном киберпространстве.

Исходя из вышеуказанного, основным нормативно-правовым актом, который определяет концептуальные основы обеспечения кибербезопасности в Республике Казахстан остается

Концепция информационной безопасности Республики Казахстан до 2016 года, утвержденная Указом Президента Республики Казахстан от 14 ноября 2011 года № 174. Поскольку срок действия Концепции информационной безопасности имеет временные рамки и ограничен 2016 годом, то, с учетом изложенного, можно сделать вывод о необходимости разработки и принятия перспективной Концепции информационной безопасности Республики Казахстан на 2016–2020 годы, в положениях которой нужно определить стратегические задачи государственной политики в информационной сфере, тактические основы построения национальной системы кибербезопасности, с учетом существующих внутренних и внешних угроз, в том числе создание максимальной и надежной защищенности объектов критической информационной инфраструктуры, активизация международного сотрудничества в контексте оперативного реагирования на киберинциденты, обеспечение максимальной защиты государственных информационных ресурсов и телекоммуникационных систем от несанкционированного доступа и неправомерного использования, что предусматривает объединение усилий и комплексное взаимодействие между командами оперативного реагирования на киберинциденты Казахстана (KZ-CERT) и Украины (CERT-UA).

СПИСОК ЛИТЕРАТУРЫ

1 Биекенов Н. А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан [Электронный ресурс]- Режима доступа: http: // www.zakon.kz / 4627688-nekotorye-problemy-obespechenija.html.

2 Дмитренко Т. А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // Информационно-аналитический журнал «ANALYTIC». – 2003. – № 5. –С. 12–14.

3 Жатканбаева А. Е. Конституционно-правовые аспекты информационной безопасности в Республике Казахстан: монография. Министерство образования и науки РК. – Алматы: Комплекс, 2009. – 302 с.

4 Концепция формирования и развития единого информационного пространства казахстанского сегмента сети Интернет (Казнета) на 2008–2012 годы. Одобрена Постановлением Правительства Республики Казахстан от 17.04.2008 № 358 // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz.

5 Ларюэль М. Кибербезопасность в Центральной Азии: реальные угрозы, ложные предлоги? Аналитический обзор. – № 2. – 2012. [Электронный ресурс] – Режим доступа: http: // 037eabf.netsolhost.com/wordpress/wp-content/uploads/2013/10/Policy_Brief_2-RUS.pdf.

6 Государственная программа «Информационный Казахстан – 2020». Утверждена Указом Президента Республики Казахстан от 08.01.2013 № 464 // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz.

7 Концепция информационной безопасности Республики Казахстан до 2016 года. Утверждена Указом Президента Республики Казахстан от 14.11. 2011 № 174 // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz.

8 О ратификации Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: Закон Республики Казахстан от 01.06.2010 № 286 // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz.

9 Об информатизации: Закон Республики Казахстан от 24 ноября 2015 года № 418 // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz.

Дата поступления статьи в редакцию 02.12.2015