Лекция 12. Обеспечение информационной безопасности в системе упорядоченных свобод.

Анализ текущей ситуации

Характерная для последних десятилетий общемировая тенденция внедрения достижений информационно-коммуникационных технологий с темпами, существенно опережающими формирование культуры их использования, и укоренения общественных и производственных отношений, характерных для «информационного общества», в первую очередь, в вопросах обеспечения кибербезопасности, в Казахстане также находит свое подтверждение.

Тем не менее, начиная с 1998 года, когда было принято постановление Правительства Республики Казахстан от 31 декабря 1998 года № 1384 «О координации работ по формированию и развитию национальной информационной инфраструктуры, процессов информатизации и обеспечению информационной безопасности», было принято 3 новых редакции законов Республики Казахстан «Об информатизации» (2003, 2007, 2015 годы) и несколько специализированных законов Республики Казахстан о внесении в них соответствующих изменений по вопросам электронных форматов представления информации (данных) в том числе по вопросам информационно-коммуникационных сетей, «электронного правительства».

За прошедший период электронные информационные ресурсы и информационные системы введены в хозяйственный оборот наряду с другими видами имущественных активов, расширена сфера их рыночного использования.

Сфера автоматизации государственных услуг, рынок электронной коммерции и электронных платежей развиваются на принципах обеспечения безопасности личности, общества и государства при применении информационно-коммуникационных технологий, а также осуществления деятельности на основе единых стандартов, обеспечивающих надежность и управляемость объектов информатизации и связи.

С этапа становления вопросов информационной безопасности с учетом характера содержащейся информации дифференцированы правовые режимы общедоступных и конфиденциальных электронных информационных ресурсов и систем, установлены права и обязанности собственников, владельцев и пользователей по их защите.

Деятельность государственных органов и других субъектов по обеспечению информационной безопасности в области информатизации и связи осуществляется в соответствии с их отраслевой компетенцией, а также целями и задачами в предметных областях, связанных с использованием ИКТ (регулирование связи и информационных технологий, защита персональных данных, защита государственных секретов, противодействие деятельности иностранных технических разведок, оперативно-розыскная деятельность на сетях связи, расследование преступлений, совершаемых с использованием ИКТ и другие).

В целом, в Республике Казахстан организационно-правовые и технические основы системы мер по обеспечению информационной безопасности в области информатизации и связи (кибербезопасности) формировались и законодательно закреплялись как составляющие информационной безопасности и обеспечения безопасности информационного пространства и инфраструктуры связи в соответствии с Законом Республики Казахстан «О национальной безопасности».

В последние годы различные взаимоувязанные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение и развитие в Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан «Об административных правонарушениях», законах Республики Казахстан «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона Республики Казахстан «Об информатизации», вступившего в силу с 1 января 2016 года.

Ряд подзаконных актов, принятых в последнее время, еще не получил развернутой правоприменительной практики. В частности, постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (далее – Единые требования), представляющих собой кодификацию правовых и технических норм из национальных и гармонизированных стандартов. Документ подробно описывает процедуры и правила по использованию информационно-коммуникационных технологий при обработке защищаемых законом видов информации, содержит важные нормы по обеспечению технологической безопасности информационной инфраструктуры, информационных систем и ресурсов, программного обеспечения, технических средств на всех этапах их жизненного цикла.

На законодательном уровне регламентировано функционирование системы мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства», включающих в себя как государственные, так и негосударственные информационные системы, интегрируемые с государственными.

В Правилах проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», утвержденных приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66, заложены основные принципы взаимодействия между заинтересованными сторонами при технологических сбоях или признаках компьютерных атак, а также алгоритмы реагирования на возникающие события и инциденты информационной безопасности.

Центр мониторинга безопасности «электронного правительства» ежедневно выявляет не устраненные уязвимости, о чем для принятия мер направляет уведомления владельцам информационных систем, являющиеся его компонентами. Имеется положительная динамика выявляемых уязвимостей и принимаемых в отношении них мер. Так в 2014 году было выявлена 1241 не устранённая уязвимость, в 2015 – 469, в 2016 – 355.

Также постановлением Правительства Республики Казахстан от 8 сентября 2016 года № 529 утверждены Правила и критерии отнесения объектов к критически важным объектам информационно-коммуникационной инфраструктуры из числа особо важных государственных и стратегических объектов, а также объектов отраслей экономики, имеющих стратегическое значение.

На подобные объекты, вошедшие в перечень критически важных объектов информационно-коммуникационной инфраструктуры, распространяются Единые требования, а также необходимость участия в предусмотренных законодательством совместных мероприятиях по обеспечению мониторинга их информационной безопасности, защиты и безопасного функционирования, включая обязанность информирования об инцидентах информационной безопасности.

Совершенствуются процедуры введения информационных систем в промышленную эксплуатацию. В этой связи, законодательно дифференцированы меры

безопасности к информационным системам в зависимости от их отнесения к определенному классу, ограничен срок нахождения информационной системы в режиме опытной эксплуатации.

На соответствие требованиям информационной безопасности проведено более 500 аттестационных обследований государственных и негосударственных информационных систем, интегрируемых с государственными, по результатам которых выдано 199 аттестатов, являющихся основанием для введения в промышленную эксплуатацию. Оставшаяся часть информационных систем в соответствии с Законом Республики Казахстан «Об информатизации» должны быть аттестована до конца 2018 года.

С 1 января 2016 года информационные системы государственных органов, негосударственные информационные системы, интегрируемые с государственными информационными системами на этапе опытной эксплуатации, проходят испытания на соответствие требованиям информационной безопасности. Во время испытаний проверке подвергаются исходные коды, настройки функций безопасности, обследуется сетевое и серверное оборудование и осуществляется нагрузочное тестирование.

Результаты проведения испытаний отражаются в повышении защищенности и отказоустойчивости информационных систем, безопасности программного обеспечения информационных систем, снижении влияния факторов нарушений информационной безопасности информационных систем, внедрении механизмов контроля и мониторинга безопасности информационных систем.

Система технического регулирования предусматривает подтверждение соответствия программного обеспечения и телекоммуникационного оборудования, в том числе с определением случаев их обязательной сертификации при использовании в государственном секторе. В этих целях ежегодно актуализируется свод национальных и гармонизированных технических стандартов в сфере информационной безопасности, защиты информации, безопасности информационных технологий. В настоящее время это 68 технических стандартов.

Благодаря централизации подключения к Интернету через Единый шлюз доступа к Интернету государственных органов существенно снижены угрозы несанкционированного доступа и вредоносного воздействия на электронные информационные ресурсы государственных органов. На ежедневной основе фиксируется и отражается более 180 миллионов атак различного уровня.

Создана и совершенствуется система правовых, организационных, технических и криптографических мер защиты государственных секретов, обрабатываемых с использованием средств вычислительной техники.

Наиболее чувствительная для безопасности государства информация в электронной форме передается только через сети телекоммуникаций специального назначения, физически отделенные от Интернета и использующие криптографические средства защиты информации.

Подходы к обеспечению безопасности инфраструктуры связи и сетей телекоммуникаций общего пользования выстраиваются вокруг системы централизованного управления сетями телекоммуникаций, через возможности магистральных операторов связи, реализующих на пограничном оборудовании концепцию «электронной границы».

Национальный сегмент Интернета насчитывает более 120 тысяч Интернет-ресурсов в доменах .KZ и .ҚАЗ, в соответствии с законодательством физически размещаемых на территории Республики Казахстан. В целях оказания содействия владельцам и пользователям информационных ресурсов и систем по вопросам безопасного использования ИКТ с 2010 года функционирует национальная Служба

реагирования на компьютерные инциденты KZ-CERT. Служба является участником ряда международных организаций, в т.ч. FIRST (Forum of Incident Response and Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Организация исламского взаимодействия Служб реагирования на компьютерные инциденты).

Службой заключено 20 меморандумов о взаимопонимании и сотрудничестве с профильными структурами зарубежных стран, зафиксировано и обработано более 66 тысяч инцидентов информационной безопасности.

На казахстанском рынке появились первые отечественные компании, занимающиеся инструментальным аудитом по оценке защищенности (тестированием на проникновение) на соответствие требованиям информационной безопасности и специализирующиеся на исследовании обстоятельств, причин и условий инцидентов информационной безопасности, а также техническом исследовании вредоносного программного обеспечения. Разработаны первые отечественные средства антивирусной защиты.

В ряде национальных компаний и частных структурах существуют подразделения мониторинга технических событий и технологических процессов, которые в круглосуточном режиме ведут дежурство для оперативного реагирования на внештатные ситуации.

Законодательно определены цели сбора, обработки персональных данных граждан в электронном виде, а также порядок и меры по их защите. Законодательство регламентирует как процедуры их сбора исключительно с согласия граждан, так и уничтожения по их требованию операторами персональных данных, а также условия безопасного хранения персональных данных на территории страны и их трансграничной передачи.

Требования по безопасности банковских информационных систем обеспечиваются нормативно-правовыми актами Национального Банка Республики Казахстан с учетом отраслевых и международных требований по обеспечению безопасности информационных систем.

Новая редакция Уголовного кодекса Республики Казахстан, действующая с 2014 года, предусматривает отдельную главу, посвященную преступлениям, совершаемым в сфере информатизации и связи. С учетом квалифицирующих обстоятельств в ней содержится 38 составов преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций.

Кодекс Республики Казахстан «Об административных правонарушениях» также содержит ряд составов административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе на должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде нарушения требований по эксплуатации средств защиты электронных информационных ресурсов, невыполнения Единых требований, неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, мер по их защите.

Список использованной литературы:

1. Об утверждении концепции кибербезопасности ("Киберщит Казахстана"). URL: https://egov.kz/cms/ru/law/list/P1700000407