Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407.

В целях реализации Указа Президента Республики Казахстан от 15 февраля 2017 года № 422 "О мерах по реализации Послания Главы государства народу Казахстана от 31 января 2017 года "Третья модернизация Казахстана: глобальная конкурентоспособность" Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ**:

1. Утвердить прилагаемую Концепцию кибербезопасности ("Киберщит Казахстана") (далее – Концепция).

2. Центральным государственным органам Республики Казахстан:

1) принять необходимые меры по реализации Концепции;

2) представлять раз в полугодие не позднее 10 числа месяца, следующего за отчетным полугодием, информацию в Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан о ходе реализации Концепции.

Сноска. Пункт 2 с изменением, внесенным постановлением Правительства РК от 17.03.2023 № 236 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Министерству цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан:

1) в трехмесячный срок разработать План мероприятий по реализации Концепции и в установленном законодательством порядке внести на рассмотрение в Правительство Республики Казахстан;

2) представлять два раза в год, к 25 июля и 25 января, сводную информацию о ходе реализации Концепции в Аппарат Правительства Республики Казахстан.

Сноска. Пункт 3 с изменениями, внесенными постановлением Правительства РК от 17.03.2023 № 236 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

4. Контроль за исполнением настоящего постановления возложить на Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

Сноска. Пункт 4 - в редакции постановления Правительства РК от 17.03.2023 № 236 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

5. Настоящее постановление вводится в действие со дня его подписания.

Премьер-Министр
Республики Казахстан *Б. Сагинтаев*

Утверждена
постановлением Правительства
Республики Казахстан
от 30 июня 2017 года № 407

КОНЦЕПЦИЯ
кибербезопасности ("Киберщит Казахстана")

Содержание

1. Введение

Концепция кибербезопасности ("Киберщит Казахстана") (далее – Концепция) разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира.

Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий (далее – ИКТ).

Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

При разработке Концепции изучен международный опыт в области формирования подходов к защите национальной информационно-коммуникационной инфраструктуры государств-лидеров в сфере разработки и использования

информационно-коммуникационных технологий, так и стран, стремящихся расширить сферу их применения для достижения целей социально-экономического развития.

Выполнение данной Концепции послужит дальнейшей модернизации казахстанского общества и станет вкладом Казахстана в реализацию Глобальной программы кибербезопасности ООН.

Термины и определения

Для целей настоящей Концепции под кибербезопасностью понимаются состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации.

Защита информации или электронных информационных ресурсов и информационных систем – комплекс физических, технических, программных, криптографических и административных мер, направленных на обеспечение информационной безопасности.

Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: конфиденциальность, целостность и доступность.

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

Если доступ к информации получает неуполномоченное лицо, происходят несанкционированный доступ или нарушение конфиденциальности.

Для некоторых видов защищаемых законом или владельцем типов информации конфиденциальность является одним из наиболее важных атрибутов (служебная информация, охраняемые законом виды тайн, персональные данные ограниченного доступа, например, сведения о клиентах банка, кредиторах, налоговые данные, сведения медицинских учреждений о состоянии здоровья пациентов и т. д.).

Целостность информации – способность информации (данных) сохраняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к нарушению целостности.

Особенно важна целостность данных, связанных с функционированием объектов критической информационно-коммуникационной инфраструктуры (например, автоматизированные системы управления воздушным движением, электро и энергоснабжения и так далее).

Доступность информации определяется способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам,

обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводят к потере доступности.

Доступность – важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиентов путем предоставления информационно-коммуникационных услуг (информационные системы продажи железнодорожных и авиационных билетов, банковских услуг, распространение продукции Интернет-ресурсами и электронными СМИ в Интернете). Ситуацию, когда уполномоченный пользователь не может получить доступ к определенным услугам (чаще всего сетевым), называют отказом в обслуживании.

В связи с развитием коммуникационных (сетевых технологий) также дополнительно выделяют еще два свойства информационной безопасности, связанные с личностью лица, управляющего или использующего информационную систему или электронный информационный ресурс с использованием сети удаленно: аутентичность и апеллируемость.

Аутентичность – возможность достоверно установить автора юридически значимого действия с информацией или сообщения в сфере оказания информационно-коммуникационных услуг, например, в электронной коммерции, когда используются электронно-цифровая подпись или иной способ аутентификации.

Апеллируемость (неотрекаемость) – возможность при отказе от авторства доказать, что автором действий с информацией в информационной системе или ресурсе является именно данный пользователь и никто другой путем регистрации совершаемых действий.

Аутентификация (установление подлинности) – проверка принадлежности к субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Идентификация – присвоение субъектам доступа к информационной системе или электронному ресурсу личного идентификатора, обеспечивающего установление подлинности и определение полномочий субъекта при его допуске в информационную систему, контроль полномочий в процессе сеанса работы и регистрацию действий.

Идентификация и аутентификация – основа современных программно-технических средств безопасности, так как любые ИКТ-услуги и сервисы в основном рассчитаны на обслуживание субъектов-пользователей.

Угроза информационной безопасности – потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или компоненты информационной системы или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей.

Наиболее распространенные угрозы информационной безопасности – это сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и так

далее), неправильное хранение архивных данных, нарушения прав доступа к данным, некорректная работа пользователей и обслуживающего персонала, потери информации (из-за несанкционированного доступа или инфицирования вредоносными программами – компьютерными вирусами).

Компьютерная атака – целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно–аппаратных средств (или протоколов межсетевого взаимодействия).

Все иные термины приведены в значениях, используемых в Конституции Республики Казахстан, Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан "Об административных правонарушениях", законах Республики Казахстан " О национальной безопасности Республики Казахстан", "О государственных секретах", "О противодействии терроризму", "Об электронном документе и электронной цифровой подписи", "Об информатизации", "О техническом регулировании", "О разрешениях и уведомлениях", "О средствах массовой информации", "О связи", "О персональных данных и их защите", "О доступе к информации" и национальных технических стандартах.

2. 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 устраненная 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.

На сегодняшний день в учебные планы специальности "Системы информационной безопасности" кроме изучения прикладных дисциплин включены дисциплины, формирующие знания и навыки по прикладному программированию микропроцессорных систем и устройств, автоматизированному проектированию и разработке радиоэлектронных устройств, используемые в интегрированных системах безопасности.

Ведущими техническими высшими учебными заведениями страны преподаются дисциплины: "Прикладные инженерные программы", "Микропроцессоры и микропроцессорные системы", "Программирование и реализация встроенных систем".

Складывается практика проведения аналитических исследований, научно-исследовательских и опытно-конструкторских работ, организации профильных конференций и семинаров, что отражает растущий интерес общества, научных кругов и субъектов информатизации к различным аспектам деятельности в сфере информационной безопасности.

Проведенное Международным союзом электросвязи исследование "Глобальный индекс кибербезопасности" (далее – Глобальный индекс кибербезопасности), оценивающее правовую, техническую, организационную готовность и потенциал 195 стран, зафиксировало 23 групповое место Казахстана с индексом 0,176 из 29 групп стран.

Ключевые проблемы

1. В Республике Казахстан за период с 2010 по 2016 год плотность пользователей Интернета увеличилась с 36,1% до 75%, а количество пользователей мобильного Интернета с 3 миллионов 694 тысяч практически утроилось и достигло 10 миллионов 567 тысяч. Такое экспоненциальное увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов или вредоносного воздействия на технические средства.

Распространенность вредоносных программ для персональных компьютеров и мобильных устройств растет вместе с числом их пользователей. При этом подавляющее большинство пользователей не используют специализированное программное обеспечение для защиты своих персональных компьютеров, смартфонов, планшетов.

Этот фактор эксплуатируется "хакерами", что каждый день приводит к увеличению количества атак, нацеленных на заражение абонентских устройств вредоносным программным обеспечением.

В то время, как количество абонентских устройств, подключенных к Интернету, увеличивается и большинство пользователей продолжает игнорировать меры " цифровой гигиены" в отношении себя и принадлежащих им устройств, концепция " Интернета вещей" только усиливает проблему их безопасного использования.

Если традиционные электронные устройства, такие как персональные компьютеры и ноутбуки имеют возможности по установке и обновлению антивирусного программного обеспечения, то пользователи "Интернета вещей", часто даже не знают, как обезопасить их функционирование.

Такие устройства пока, в принципе, создаются без учета технологических рисков, что делает их потенциальными элементами вредоносных сетей, ("ботнет"), используемых для осуществления различных сетевых атак, направленных на потерю доступности информационных систем и влекущих для добросовестных пользователей отказ в обслуживании при оказании информационно-коммуникационных услуг.

Пренебрежение соображениями безопасности при использовании Интернет-ресурсов и социальных сетей ведет к повышенному риску для неприкосновенности частной жизни, несанкционированному использованию или модификации общедоступных персональных данных, а также разглашению персональных данных ограниченного доступа или их экстерриториальной доступности для преступных сообществ или разведывательных структур при их хранении на территории других государств.

Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в ее повышении у населения, работников сферы ИКТ и руководителей организаций создают питательную почву для развития правонарушений и преступлений в информационной сфере.

Отсутствие знаний о правовых ограничениях создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и смежных прав на программное обеспечение и влияющих на функционирование информационных ресурсов.

Таким образом, низкий уровень цифровой грамотности конечных пользователей в вопросах защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов (особенно "фишинговые" страницы поддельных интернет-магазинов и банков, распространение вирусных и "троянских" программ через "взломанные" сайты, скачивание нелицензионного ("пиратского") программного обеспечения) приводят к

тысячам случаев, когда граждане Республики Казахстан становятся жертвами, а принадлежащие им технические средства орудиями противоправного использования ИКТ.

2. Недостаточная осведомленность в методах защиты информации и низкая обеспеченность в системах информационной безопасности предприятий малого и среднего бизнеса, в том числе занятых в сфере оказания информационно-коммуникационных услуг, которые зачастую даже не могут оценить состояние принадлежащей информационно-коммуникационной инфраструктуры, приводят к большому количеству не анализируемых событий и инцидентов информационной безопасности, затрудняющих как профилактику технологических уязвимостей, так и борьбу с преступниками, использующими ИКТ как средство для совершения преступлений.

Кроме того, такие хозяйствующие субъекты представляют угрозу для других, в первую очередь, крупных предприятий или государственных органов и организаций, с которыми они работают в качестве партнеров или подрядчиков.

При этом, крупный частный и финансовый сектор склонен полагаться исключительно на собственные силы, недооценивая важность совместных усилий и отраслевых инициатив по формированию действительно безопасной среды операционной деятельности.

В тоже время низкая заинтересованность работодателей и отсутствие профессиональной конкуренции являются демотивирующим фактором для инициативного саморазвития практикующих специалистов в сфере информационной безопасности, а также создают предпосылки для занятия последних незаконными видами деятельности.

3. Существующая казахстанская модель школьного, средне-специального, высшего и послевузовского образования в области ИКТ, включая специализацию в сфере информационной безопасности, требует постоянного и тщательного анализа со стороны всех заинтересованных лиц (включая Министерство образования и науки Республики Казахстан, высшие учебные заведения и потенциальных работодателей) на предмет соответствия современным потребностям общества и тенденциям обеспечения безопасного развития информационных технологий в виду динамического развития данной области.

В частности, периодического пересмотра требуют образовательные и профессиональные стандарты, классификаторы специальностей, дисциплины, их контентное содержание и результаты обучения. Возникает необходимость разработки механизма, позволяющего более гибко реагировать на современные вызовы в области ИКТ. В виду того, что знания в данной области быстро устаревают, требуется периодическое подтверждение квалификации специалистов.

Из 93 высших учебных заведений, в которых готовят специалистов в сфере ИКТ, только 7 готовят специалистов по специальности "Системы информационной безопасности". Из 32439 студентов, обучавшихся в 2015-2016 годах, в указанных высших учебных заведениях только 362 (1,1%) обучались по специальности "Системы информационной безопасности", из них по государственному заказу 226 человек. Плановый выпуск в 2016 году составил 85 выпускников.

В 2016-2017 учебном году по государственному заказу на подготовку специалистов по специальности "Системы информационной безопасности" выделено 40 мест, 2014-2015 году – 60 мест, 2015-2016 году – 60 мест.

В этой связи будет уделено повышенное внимание на профориентационную работу по специальности "Системы информационной безопасности", в том числе обращено внимание абитуриентов на актуальность данной специальности, потребность специалистов данного профиля в индустрии.

Прием абитуриентов на обучение по специальности "Системы информационной безопасности" на коммерческой основе в недостаточной мере продвигается и рекламируется. Специальные дисциплины лишены наполнения, необходимого для применения выпускниками в специальных государственных органах после завершения обучения.

В учебных программах не учитываются требования к знаниям, умениям и навыкам профессионального стандарта "Специалист по информационной безопасности", утвержденного Национальной палатой предпринимателей "Атамекен" и основанного на отраслевой рамке квалификации.

Как следствие, в сфере ИКТ существует нехватка специалистов по информационной безопасности, как в государственном, так и частном секторе. Так в центральных государственных органах обеспеченность составляет всего 25%, в местных – 6%.

4. Отечественный сектор IT-отрасли не вносит существенного практического вклада в программу диверсификации национальной экономики (менее 5 процентов продуктов из используемых в государственном секторе имеют казахстанское происхождение), а культура кибербезопасности, в том числе производственная культура в сфере разработки и использования продуктов, не всегда является определяющей.

Несмотря на достигнутый высокий уровень информатизации сферы государственного управления, включая оборону и безопасность, широкое использование ИКТ в различных сферах жизни личности и общества, Казахстан как страна, пока, в значительной мере импортирует (заимствует) не только IT-технологии, но и готовые программные продукты, включая продукты обеспечения информационной безопасности в сфере информатизации и связи, что указывает с одной стороны на давление со стороны гигантов IT-индустрии, а с другой на недостаточность принимаемых усилий и мер по их рациональному замещению с опорой на собственные

силы в критически важных сферах разработок, от которых зависит обеспечение безопасности государства.

5. Меры, связанные с автоматизацией государственных функций и оказанием государственных услуг в электронной форме, а также продолжающаяся цифровизация доступа к информации о деятельности государственных органов несут в себе определенные риски.

Некачественные услуги и приложения, предоставляемые гражданам и частным организациям в рамках "электронного правительства", в том числе машиночитаемые открытые данные, могут привести к нарушению прав и законных интересов граждан.

Отклонения от установленных требований технических стандартов, вызванные низким уровнем производственной и эксплуатационной культуры, небрежность и халатность со стороны заказчиков и разработчиков решений на этапе создания, принцип остаточного финансирования обеспечения информационных систем системами защиты информации и контроля защищенности несут в себе высокие риски технологических сбоев.

Несвоевременное устранение владельцами информационных систем уязвимостей в программном обеспечении существенно увеличивает угрозы несанкционированного доступа.

Объем данных, обрабатываемых в государственном и частном секторах, растет, что приводит к необходимости выработки новых форм их хранения. В тоже время, такие формы хранения данных как облачное хранилище или использование онлайн-сервисов часто основываются операторами и поставщиками услуг на непрозрачных или не стандартизованных решениях, в том числе с точки зрения безопасности данных. При этом гармонизированные стандарты значительно отличаются от первоисточника из-за низкого качества их перевода и адаптации.

Ситуация усугубляется возможностью намеренного внедрения в программное обеспечение и телекоммуникационное оборудование не декларируемых функций (так называемых "бэкдоров"), которые не всегда могут быть выявлены на этапе сертификации, устранения уязвимостей в процессе эксплуатации или распознаны антивирусными программами и потому могут быть использованы для нарушения работы информационных систем и сетей телекоммуникаций.

6. Транснациональный и трансграничный характер многих продуктов ИКТ и международная связанность сетей телекоммуникаций общего пользования используются преступностью в целях совершения противоправных действий в отношении пользователей и операторов ИКТ-услуг и владельцев Интернет-ресурсов, размещенных в национальном сегменте, а также информационных систем, взаимодействующих с Интернетом.

Высокая латентность и зачастую международный характер таких преступлений повышают их общественную опасность. Ситуация усугубляется укоренившимися в

обществе стереотипами о безнаказанности так называемой "киберпреступности", ненужности принимаемых государством мер по укреплению сферы безопасного использования ИКТ, ограниченными возможностями органов правопорядка по привлечению к ответственности виновных в совершении высокотехнологичных преступлений, несмотря на развитые уголовно-правовые институты информационной безопасности.

7. Нагнетаемая отдельными странами милитаризация сферы ИКТ, трудности в доказывании причастности государств к использованию ИКТ в нарушение принципов международного права, вызванные в значительной степени стихийно сложившимся характером существующей международной системы управления Интернетом, сохраняющийся цифровой разрыв между странами препятствует формированию в мировом сообществе надежных международно-правовых инструментов предотвращения военного использования достижений в сфере информатизации и телекоммуникаций.

При этом по своей сути арсенал, используемый в военных целях, не отличается от арсенала программно-технических средств, используемых киберпреступностью, о чем свидетельствуют массовые случаи использования ИКТ в разведывательных, подрывных и иных целях, угрожающих поддержанию международного мира и безопасности.

Таким образом, Казахстан в сфере кибербезопасности испытывает такие серьезные угрозы как:

низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности;

нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;

непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

3. Международный опыт

Термин "кибербезопасность" и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

В тоже время на уровне ООН имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур", в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно-коммуникационных технологий в вопросах обеспечения (1) неприкосновенности частной жизни, (2) конфиденциальности , целостности и доступности информации в электронной форме, (3) защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно-техническими методами.

При этом многие страны не рассматривают в руководящих документах вопросы защиты от вредной или незаконной информации, распространяемой с использованием ИКТ в контексте понимания кибербезопасности из-за опасений в чрезмерном ограничении права на доступ и свободное распространение информации.

Отдельные страны рассматривают через призму кибербезопасности только неконтролируемое распространение в Интернете, как всемирной системе объединенных сетей телекоммуникаций и вычислительных ресурсов, электронных материалов, пропагандирующих терроризм, детскую порнографию и некоторые виды незаконной информации, в первую очередь, по причине технической сложности установления источника распространения такой информации.

При этом некоторые страны в оценке угроз и принимаемых в отношении них мер противодействия придерживаются понятия информационной безопасности применительно ко всем аспектам использования ИКТ, выстраивая соответствующую модель правового регулирования и системы государственного управления.

Так, например, стратегия Норвегии отмечает, что новые услуги и устройства предъявляют весьма высокие требования к компетенции простых пользователей. Но главная ответственность за обеспечение безопасности информации, систем и сетей возлагается на владельца или оператора. Такие работы должны быть частью ежедневной работы и финансироваться наряду с текущими операциями. Стоимость мер

по содействию информационной безопасности должна быть соразмерна оценке риска в отдельных сферах управления (глобальный индекс кибербезопасности составляет 0,735).

Эстония придает особое значение безопасности информационных систем. Рекомендуемые меры носят гражданский характер и основываются на правовом регулировании, обучении и сотрудничестве (глобальный индекс кибербезопасности составляет 0,706).

В основе стратегии Финляндии лежит понимание кибербезопасности как проблемы экономического характера, тесно связанной с развитием финского информационного общества (глобальный индекс кибербезопасности составляет 0,618).

Словакией обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества. Поэтому цель стратегии – служить прочным фундаментом для защиты информации. Стратегия направлена как на предотвращение угроз, так и на обеспечение готовности и устойчивости средств их предотвращения (глобальный индекс кибербезопасности составляет 0,618).

Ключевые цели стратегии кибербезопасности Чешской Республики включают в себя защиту информационно-коммуникационных систем от уязвимостей, которым эти системы подвергнуты, и уменьшение потенциального ущерба от атак на системы. Основной фокус стратегии приходится на проблемы свободного доступа к информационным сервисам, целостности и конфиденциальности данных в Чешской Республике (глобальный индекс кибербезопасности составляет 0,500).

Франция ориентируется на то, чтобы информационные системы были способны противостоять событиям, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации, делает упор на технические средства защиты информации, борьбу с киберпреступностью и установлением киберзащиты (глобальный индекс кибербезопасности составляет 0,588).

Стратегия Германии закладывает основу для безопасности критически важных информационных систем. Германия сосредоточена на предотвращении и уголовном преследовании кибератак, а также выхода из строя IT-оборудования, вызванного случайными факторами. Стратегия кибербезопасности Германии определяет уровень кибербезопасности, достигнутый суммой всех национальных и международных мер, принятых для защиты и доступа к информации и коммуникациям, целостности, достоверности и конфиденциальности данных в киберпространстве, а также укреплением германского технологического суверенитета и экономического потенциала во всем диапазоне основных стратегических IT-компетенций (глобальный индекс кибербезопасности составляет 0,706).

Программа развития электронной информационной безопасности Литвы ориентируется на определении целей и мероприятий, направленных на обеспечение

электронной информационной безопасности, развитие оборота электронной информации, а также обеспечение ее конфиденциальности, доступности и целостности в киберпространстве. Кроме того, стратегия Литвы направлена на защиту персональных данных, телекоммуникационных сетей, информационных систем и критически важных инфраструктур от нарушения безопасности и кибератак из-за пределов "электронного периметра" (глобальный индекс кибербезопасности составляет 0,441).

Нидерланды, с одной стороны, стремятся к безопасным и надежным информационно-коммуникационным системам, опасаясь серьезных нарушений в этих системах, а с другой стороны, признают необходимость свободы и открытости Интернет-пространства. В стратегии дается определение кибербезопасности. " Кибербезопасность – это защищенность от сбоев и неправильной эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация могут отрицательно повлиять на доступность и надежность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах" (глобальный индекс кибербезопасности составляет 0,676).

Стратегия безопасности ИКТ Австрии заключается в распространении интегральных подходов к безопасности, реализованных в системе "электронного правительства", к другим областям, включая те, которые должны быть созданы на транснациональном уровне в целях обеспечения долгосрочной жизнеспособности экономики Австрии (глобальный индекс кибербезопасности составляет 0,676).

Подход Великобритании направлен на развитие кибербезопасности. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно-телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Необходимо исключить риски типа кибератак преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики (глобальный индекс кибербезопасности составляет 0,706).

Национальная стратегия Швейцарии отмечает необходимость уменьшения влияния преобладающих интересов нескольких стран, участвующих в Интернет-индустрии, рассматривает применение описываемых в ней мер "в мирное время, и тем самым, явным образом исключает войны".

При этом отказоустойчивая военная инфраструктура рассматривается как важный элемент стратегического резерва для других субъектов в случае полномасштабного кризиса. Поскольку действующее законодательство в различных отраслях отражает кибер-аспекты существующих задач и обязанностей государственного и частного сектора, решение вопросов кибербезопасности в рамках единого специального кибер закона Швейцарии считается непригодным, так как "непрерывно адаптироваться к

изменениям должно действующее законодательство" (глобальный индекс кибербезопасности составляет 0,353).

Таким образом, в каждой стране национальное понимание кибербезопасности и ключевых приоритетов значительно различается.

Как следствие, различаются и подходы к составлению стратегий кибербезопасности . Тем не менее, руководящие документы, охватывающие вопросы кибербезопасности, как правило, предусматривают:

- построение государственной системы управления в сфере обеспечения кибербезопасности;

- определение соответствующего механизма (в основном общественно-государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур;

- определение необходимой политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения).

Как свидетельствует мировой опыт, полную защиту от ошибок в программном обеспечении или инцидентов информационной безопасности достигнуть невозможно, но путем осознанного ответственного поведения снизить их частоту и вероятность, обеспечить высокую скорость восстановления работоспособности информационных систем и ресурсов, чтобы не допустить разрушительных последствий, жизненно необходимо.

Координация этой сферы во многих странах в значительной степени выстраивается вокруг гражданского регулятора в области информационных технологий и связи (Агентство информационной безопасности KISA - Корея, Центр информационной безопасности Министерства информационных технологий – Республика Узбекистан, и др.), либо органа, ответственного за защиту и безопасность информации (Бюро безопасности информационной техники – Германия, Агентство безопасности информационных систем при Министерстве обороны – Франция, Агентство национальной безопасности Чехии, Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Служба специальной связи и защиты информации Украины. В Европейском союзе регулятором в этой сфере является Агентство информационной и сетевой безопасности).

4. Цели, задачи, ожидаемые результаты и период реализации

Целями Концепции являются достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

Задачи Концепции:

1. Формирование необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищенного телекоммуникационного оборудования.

2. Совершенствование правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами.

3. Создание высоко адаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры.

Ожидаемые результаты:

1) глобальный индекс кибербезопасности Казахстана к 2017 году составит 0,200, к 2018 году – 0,300, к 2019 году – 0,400, к 2020 году – 0,500, к 2021 году – 0,550, к 2022 году – 0,600;

2) повышение осведомленности об угрозах информационной безопасности к базовому периоду 2018 года в 2019 году – на 5%, в 2020 году – на 10%, в 2021 году – на 15%, в 2022 году – на 20%;

3) количество переподготовленных специалистов в сфере информационной безопасности в 2018 году – 300, в 2019 году – 500, в 2020 году – 600, в 2021 году – 700, в 2022 году – 800;

4) увеличение доли отечественных программных продуктов в сфере информатизации и связи, используемых в государственном и квазигосударственном секторах к базовому периоду 2017 года в 2018 году – на 10%, в 2019 году – на 20%, в 2020 году – 30%, в 2021 году – 40%, в 2022 году – 50%;

5) доля использования отечественных сертификатов безопасности при шифрованной передачи данных Интернет-ресурсами с доменом .KZ и .ҚАЗ в 2018 году составит 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, в 2022 году – 100%;

6) доля информационных систем государственных органов, негосударственных информационных систем, интегрируемых с государственными, информационных систем критически важных объектов информационно-коммуникационной

инфраструктуры, подключенных к центрам мониторинга информационной безопасности, в 2018 году – 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, к 2022 году – 100%.

Период реализации Концепции включает два этапа:

1) первый этап 2017-2018 годы;

2) второй этап 2019-2022 годы.

На первом этапе будут:

- сформирована развернутая правоприменительная практика соблюдения уже установленных требований в сфере обеспечения информационной безопасности, по результатам которого будут внесены необходимые изменения в законодательство;

- проведена ревизия образовательных программ и профессиональных стандартов, увеличено количество и качество подготавливаемых специалистов в области информационной безопасности, обеспечено повышение квалификации действующих работников, занятых в этой сфере;

- выстроена эффективная схема взаимодействия и кооперации между промышленностью и наукой в создании отечественных разработок, что создаст основу для развития национального и отраслевых оперативных центров информационной безопасности, что позволит на втором этапе обеспечить:

- ключевое участие казахстанских IT-компаний в обеспечении национальной информационно-коммуникационной инфраструктуры системами информационной безопасности;

- загрузку отечественных предприятий электронной промышленности заказами на приобретение государственными органами и квазигосударственным сектором телекоммуникационного оборудования, произведенного и прошедшего процедуры сертификации на соответствие требованиям информационной безопасности на территории страны.

5. Основные принципы и подходы

Основные принципы:

1) соблюдение прав, свобод и законных интересов физических лиц, а также прав и законных интересов юридических лиц;

2) обеспечение безопасности личности, общества и государства при применении информационно-коммуникационных технологий;

3) осуществление деятельности по информатизации на территории Республики Казахстан на основе единых стандартов, обеспечивающих надежность и управляемость объектов информатизации;

4) четкое разграничение полномочий государственных органов;

5) непрерывный мониторинг информационной безопасности объектов информационно-коммуникационной инфраструктуры;

6) интеграция системы обеспечения национальной безопасности с международными системами безопасности.

Для реализации задачи по формированию необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов, систем информационной безопасности и телекоммуникационного оборудования, устойчивых к вредоносному программно-техническому воздействию предлагается:

Формирование в обществе устойчивых представлений о "кибергигиене" и привитии высокой производственной культуры создания и использования ИКТ на всех этапах жизненного цикла программных продуктов, информационных систем, программного обеспечения, технологических платформ, информационной и сетевой инфраструктуры, поддерживающего оборудования.

Применение тренингов и обучающих практик по защите персональных данных и неприкосновенности частной жизни среди несовершеннолетних пользователей Интернета и их родителей.

Для профессионализации работников, ответственных за состояние информационной безопасности в государственных органах, и универсализации принимаемых ими мер соответствующим образом, адаптация профессиональных стандартов, а также расширение требований по практическим навыкам и техническим знаниям, улучшающим профили защиты и параметры контроля защищенности информационных ресурсов и систем.

Отведение важнейшей роли в реализации образовательных и исследовательских задач в сфере информационной безопасности высшими учебными заведениями Казахстана, что расширит технические возможности специальных государственных органов по обеспечению безопасности государства и повысит уровень аналитического и научно-исследовательского сопровождения мероприятий по реализации Концепции.

Решение задач по закладыванию и поддержанию высокого уровня профессиональной компетенции и технической готовности к противодействию киберпреступности путем привлечения научно-исследовательских организаций к участию в расследовании правоохранительными органами наиболее сложных киберпреступлений.

Для наращивания казахстанского потенциала в сфере научной, научно-технической и образовательной деятельности необходимо сосредоточиться на научно-исследовательских и опытно-конструкторских работах, обеспечить тесную связь учебного процесса с производственной деятельностью предприятий электронной промышленности, привести учебные программы в соответствие с отраслевыми профессиональными стандартами и современным уровнем развития технологий.

Предоставление приоритета исследованиям и собственной школе прикладной математики, по разработке средств криптографической защиты информации,

криптологии, разработок по программируемым логическим интегральным схемам, квантовой криптографии и разработке защиты систем передачи, обработки и хранения информации, а также систем информационной безопасности.

Преодоление проблемы не высокой востребованности отечественных разработок, т.к. кибербезопасность в конечном итоге зависит от уровня развития отечественной IT-отрасли и электронной промышленности. Одной из причин этого является отсутствие обязательности приоритетного использования их продукции в государственных органах.

Установление мер по их поддержке, в том числе через стимулирование государственно-частного партнерства повышения конкурентоспособности. Критериями должны стать соответствие требованиям локализации разработки и технической поддержки, наличие у поставщика исключительных прав интеллектуальной собственности на конструкторскую и техническую документацию программных продуктов и телекоммуникационного оборудования, а также наличие научно-производственной базы, необходимой для организации производства, гарантийного и послегарантийного обслуживания.

Проведение совместно с представителями отрасли постоянного анализа закупаемого в государственных органах и квазигосударственном секторе программном обеспечении и телекоммуникационного оборудования с целью определения перспектив их замещения на доверенные отечественные или иностранные образцы, прошедшие процедуры обязательной сертификации на соответствие требованиям информационной безопасности.

При уполномоченном органе по информационной безопасности образовать Совет по кибербезопасности, одной из главных задач которого должно стать рассмотрение актуальных вопросов по кибербезопасности, поддержание в актуальном состоянии руководящих документов, нормативно-правовой базы, содействие приоритетному использованию продукции отечественной электронной и софтверной промышленности, проведение публичной оценки общественно-значимых IT-проектов.

Установление постоянного прямого диалога с ведущими компаниями и предприятиями страны, образовательными и научными исследовательскими организациями, что позволит объединить усилия и придать системность и комплексность решению задач по обеспечению интегрированной кибербезопасности в наиболее значимых областях использования ИКТ.

Наряду с мониторингом, анализом защищенности государственных информационных систем и ресурсов, оказания содействия по безопасному использованию ИКТ в интересах граждан, дополнительным приоритетом государственной службы реагирования на компьютерные инциденты KZ-CERT определить популяризацию мер "кибергигиены".

Соизмеряясь со своими экономическими возможностями, собственникам и владельцам частных информационных систем стремиться к следованию стандартизованным процессам разработки, создания, испытаний и эксплуатации информационных систем, предусматривая необходимые меры по обеспечению их информационной безопасности. Способные выступить в качестве необходимого ориентира технические стандарты и другие нормативно-технические документы для этого имеются.

Для решения задачи по совершенствованию правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами предлагается:

Неукоснительное исполнение уже установленных законодательством и техническими стандартами требований по обеспечению информационной безопасности в государственном секторе, а также оперативное внесение в них необходимых изменений с учетом динамики развития технологий без ущерба для кибербезопасности.

Соблюдение установленных требований обеспечить действенными мерами государственного контроля.

Для полноценной оценки состояния защищенности объектов информатизации с учетом характера деятельности киберпреступников и иностранных технических компьютерных разведок, рассчитывающих на самоуспокоенность и небрежность со стороны владельцев информационных ресурсов и систем, необходимо стремиться к непрерывному мониторингу состояния информационных систем и ресурсов техническими средствами контроля защищенности и проведению работы по выявлению каналов утечки информации (уязвимостей, вирусов, троянских программ, недекларируемых функций и закладок).

Такой подход позволит обеспечить сохранение возможности реализации государственных функций в случае чрезвычайных происшествий технологического, социального характера, вызванных инцидентами информационной безопасности, угрожающими национальной и общественной безопасности, а в случае чрезвычайного или военного положения возможности использования устойчивой информационно-коммуникационной инфраструктуры сил обеспечения национальной безопасности в интересах функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

Наряду с выстраиванием работы с объектами критической информационно-коммуникационной инфраструктуры из числа стратегических и особо важных государственных объектов, объектов стратегических отраслей экономики, пересмотреть критерий отнесения к критически важным объектам информационно-коммуникационной инфраструктуры с возможностью отнесения к

критически важным объектам, ориентированных на оказание информационно-коммуникационных услуг населению.

Распространять предупредительные и профилактические меры не только на государственные органы и собственников частных информационных систем, интегрируемых с государственными, но и на владельцев промышленных предприятий, финансовых организаций и других категорий объектов экономики, имеющих автоматизированные технологические процессы, нарушение которых может негативно сказаться на экономическом развитии страны.

На основе Единых требований и действующих Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства" предусмотреть разработку руководящих документов, служащих ориентиром не только для государственного сектора, но и для объектов, находящихся в частной собственности, в целях эффективной локализации и предотвращения реализации угроз в общенациональном масштабе.

В целях поддержания высокого доверия граждан и бизнеса к оказываемым государственными органами услугам на законодательном уровне для поставщиков программных продуктов, услуг связи и иной информационно-коммуникационной инфраструктуры выработать меры по информационной безопасности для указания в соглашениях, конкурсной документации и технических спецификациях к приобретаемым продуктам и решениям по обязательной технической поддержке закупаемых товаров и услуг в течение не менее трех лет.

Предусмотреть требования в сфере обеспечения безопасности автоматизированных систем управления технологическими процессами и телекоммуникационного оборудования сетей телекоммуникаций общего пользования. Особое внимание должно быть обращено на инфраструктуру в системах жизнеобеспечения населения, топливно-энергетическом секторе, инфраструктуре связи и других.

Существенно углубить понимание относительно устойчивости элементов критической инфраструктуры национального сегмента Интернета и центров обработки данных (дата-центров), аппаратно-программных комплексов, обеспечивающих функционирование общедоступных электронных информационных ресурсов (Интернет-ресурсов).

Обеспечение надежной идентификации, аутентификации и регистрации действий пользователей в соединении с мерами обеспечения конфиденциальности их персональных данных снижает риск наиболее распространенных угроз, связанных с аутентичностью пользователей информационных систем и общедоступных электронных ресурсов, включая аппаратно-программные комплексы электронных средств массовой информации. Это позволит исключить в национальном сегменте фальсификацию в сфере электронной коммерции, электронных платежей, банковской

деятельности и других информационно-коммуникационных услуг, оказываемых посредством Интернет-ресурсов.

Для создания высоко адаптированной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры предлагается:

Государственным органам и поставщикам услуг принять риск-ориентированный подход к безопасности, уделяя первоочередное внимание усилиям, которые обеспечивают наиболее высокий уровень надежности создаваемых информационных систем в нормальном и внештатном режимах и устойчивости их к умышленным сбоям.

Расширить взаимодействие между ведомственными и отраслевыми структурами мониторинга и реагирования на инциденты информационной безопасности для оказания содействия владельцам информационных ресурсов и систем и взаимного оповещения о возникающих угрозах. Их участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования, проектирования, разработки и эксплуатации отраслевых информационных систем и сетей и стать опорными точками, определяющими устойчивость всей информационно-коммуникационной инфраструктуры страны.

Специализация служб реагирования на инциденты информационной безопасности позволит расширить круг вовлеченных организаций и экспертов, что будет способствовать росту профессионализации работников, занятых в сфере информационной безопасности с учетом отраслевой специфики, и содействовать расширению рынка услуг аудита информационной безопасности для малого бизнеса, который часто не имеет возможности содержать квалифицированных специалистов в области IT и информационной безопасности.

Компьютерные атаки, запущенные из зарубежного пространства, максимально предотвращать на "электронной границе" - виртуальном периметре страны.

Руководящие документы Единой сети телекоммуникаций Республики Казахстан с учетом ее растущей уязвимости в результате конвергенции сетей телекоммуникаций и информационно-коммуникационных сетей и необходимости снижения объемов вредоносного трафика и своевременного блокирования операторами связи аномальной сетевой активности необходимо актуализировать.

Создание условий для эффективной борьбы с киберпреступностью путем постоянного повышения квалификации личного состава специализированных подразделений, расширения арсенала технических средств фиксации и криминалистических исследований "цифровых" доказательств.

Обеспечение кибербезопасности является задачей всех субъектов, деятельность которых связана с использованием ИКТ, поэтому сотрудничество в целях обеспечения

информационной безопасности будет способствовать защите интересов всех заинтересованных сторон.

Для объединения усилий при участии научного сообщества, частного сектора подготовить создание Национального координационного центра информационной безопасности, который в онлайн режиме будет обрабатывать информацию о состоянии защищенности "электронной границы", а также наиболее важных компонентов национальной информационной инфраструктуры и обеспечить обмен информацией, что позволит:

обеспечить гражданам и бизнесу доступ к квалифицированным оценкам угроз в сфере информационной безопасности и получению дополнительных знаний о том, как уменьшить негативное влияние от угроз использования уязвимостей в программном обеспечении и информационных и телекоммуникационных системах;

Министерству внутренних дел снизить количество и обеспечить высокую раскрываемость в значительной степени латентных преступлений, совершаемых с использованием информационных технологий;

государственным органам поддерживать высокий уровень отказоустойчивости и предупреждения возникновения технологических сбоев, а также своевременного устранения их последствий в инфраструктуре, входящей в состав "электронного правительства" и других государственных информационных систем и ресурсов;

собственникам критически важных объектов информационно-коммуникационной инфраструктуры получать своевременную информацию о возможном влиянии на безопасность принадлежащих им автоматизированных систем управления технологическими процессами;

Национальному Банку и банкам второго уровня получать дополнительную информацию об актуальных угрозах финансово-банковской системе.

Министерству обороны в рамках развития военной организации страны подготовить предложения по созданию системы по эффективной защите ведомственных информационных ресурсов, прогнозированию и своевременному выявлению компьютерных атак, проводить их оценку и классификацию на предмет угрозы военной безопасности государства.

На внешнеполитическом и внешнеэкономическом уровне последовательно продвигать национальные интересы Республики Казахстан, направленные на преодоление "цифрового" разрыва между участниками международного сообщества в информационной сфере, обозначив в качестве приоритетов реализацию инициатив по укреплению, на основе норм и принципов международного права, системы международной информационной безопасности.

В рамках двух и многосторонней дипломатии продолжить укреплять роль Казахстана в качестве сильного и последовательного партнера, выступающего против использования ИКТ в военных целях, следующего курсу открытости, укрепления мер

доверия в области международной информационной безопасности, при безусловном соблюдении суверенного равенства государств в выборе путей технологического развития. Ключевыми диалоговыми площадками должны стать международные, региональные и субрегиональные организации (ООН, ШОС, ЕАЭС, ОДКБ, СНГ и др.) с дальнейшим продвижением их инициатив в различных международных форматах.

Скоординированная реализация Концепции "Киберщит Казахстана" позволит существенно повысить место Казахстана в Глобальном индексе кибербезопасности и достигнуть к 2022 году индекса 0,600.

Необходимые ресурсы

На реализацию Концепции в 2017-2022 годах будут направлены средства государственного бюджета в рамках бюджетных программ заинтересованных государственных органов и предусмотренных в Плане реализации Государственной программы "Цифровой Казахстан 2020".

6. Перечень нормативных правовых актов, посредством которых предполагается реализация Концепции

В период реализации данной Концепции достижение поставленных целей и задач предполагается посредством следующих нормативных правовых актов:

1. Уголовный кодекс Республики Казахстан от 3 июля 2014 года.
2. Кодекс Республики Казахстан "Об административных правонарушениях" от 5 июля 2014 года.
3. Предпринимательский кодекс Республики Казахстан от 29 октября 2015 года.
4. Закон Республики Казахстан от 15 сентября 1994 года "Об оперативно-розыскной деятельности".
5. Закон Республики Казахстан от 31 августа 1995 года "О банках и банковской деятельности в Республике Казахстан".
6. Закон Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи".
7. Закон Республики Казахстан от 5 июля 2004 года "О связи".
8. Закон Республики Казахстан от 27 июля 2007 года "Об образовании".
9. Закон Республики Казахстан от 18 февраля 2011 года "О науке".
10. Закон Республики Казахстан от 6 января 2012 года "О национальной безопасности Республики Казахстан".
11. Закон Республики Казахстан от 21 мая 2013 года "О персональных данных и их защите".
12. Закон Республики Казахстан от 11 апреля 2014 года "О гражданской защите".
13. Закон Республики Казахстан от 16 мая 2014 года "О разрешениях и уведомлениях".
14. Закон Республики Казахстан от 24 ноября 2015 года "Об информатизации".

15. Закон Республики Казахстан от 4 декабря 2015 года "О государственных закупках".

16. Указ Президента Республики Казахстан от 8 января 2013 года № 464 "О Государственной программе "Информационный Казахстан – 2020" и внесении дополнения в Указ Президента Республики Казахстан от 19 марта 2010 года № 957 "Об утверждении Перечня государственных программ".

17. Постановление Правительства Республики Казахстан от 23 августа 2012 года № 1080 "Об утверждении государственных общеобязательных стандартов образования соответствующих уровней образования".

18. Постановление Правительства Республики Казахстан от 23 мая 2016 года № 298 "Об утверждении Правил проведения аттестации информационной системы, информационно-коммуникационной платформы "электронного правительства", Интернет-ресурса государственного органа на соответствие требованиям информационной безопасности".

19. Постановление Правительства Республики Казахстан от 8 сентября 2016 года № 529 "Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры".

20. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности".

21. Приказ Министра по инвестициям и развитию Республики Казахстан от 29 января 2015 года № 66 "Об утверждении Единых правил взаимодействия и централизованного управления сетями телекоммуникаций.

22. Приказ Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1240 "Об утверждении Правил выдачи сертификата безопасности"
.

23. Приказ Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1241 "Об утверждении Правил применения сертификата безопасности".

24. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 25 января 2016 года № 60 "Об утверждении Правил взаимодействия государственных органов по вопросам соблюдения требований законодательства Республики Казахстан в сетях телекоммуникаций".

25. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66 "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства".

26. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 63 "Об утверждении методики и правил проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы " электронного правительства", Интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности".

27. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 67 "Об утверждении Правил оказания услуг доступа к Интернету в пунктах общественного доступа к Интернету".

28. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 65 "Об утверждении Правил присоединения сетей операторов междугородной и международной связи к точке обмена Интернет-трафиком".

29. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 108 "Об утверждении Методики проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы "электронного правительства", Интернет-ресурса государственного органа на соответствие требованиям информационной безопасности".

30. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 118 "Об утверждении Правил регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета".