О внесении дополнений и изменений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности"

Постановление Правительства Республики Казахстан от 18 июня 2018 года № 355

Правительство Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности" (САПП Республики Казахстан, 2016 г., № 65, ст. 428) следующие дополнения и изменения:

в единых требованиях в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных указанным постановлением:

пункт 6 дополнить подпунктами 11-1) и 20-1) следующего содержания:

"11-1) кроссовое помещение – телекоммуникационное помещение, предназначенное для размещения соединительных, распределительных пунктов и устройств;";

"20-1) организация – государственное юридическое лицо, субъект квазигосударственного сектора, собственник и владелец негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственник и владелец критически важных объектов информационно-коммуникационной инфраструктуры;";

дополнить пунктом 8-1 следующего содержания:

"8-1. Сведения об архитектуре ГО передаются третьим лицам исключительно по согласованию с руководителями структурных подразделений по информационной безопасности и информационным технологиям ГО, либо лицами, их заменяющими, в соответствии с утвержденной политикой ИБ.";

подпункт 1) пункта 9 изложить в следующей редакции:

"1) планирование затрат на информатизацию и информационную безопасность в соответствии с утвержденной архитектурой ГО, а в случае ее отсутствия – согласно решениям экспертного совета в сфере информатизации;";

дополнить пунктом 25-1 следующего содержания:

"25-1. При организации доступа к Интернету из локальных сетей внешнего контура в обязательном порядке обеспечивается наличие антивирусных средств, обновлений операционных систем на рабочих станциях, подключенных к сети Интернет.";

пункты 29, 30 изложить в следующей редакции:

"29. При организации, обеспечении и управлении ИБ в ГО, МИО или организации необходимо руководствоваться положениями стандарта Республики Казахстан СТ РК ИСО/МЭК 27002-2015 "Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасностью".

30. В целях разграничения ответственности и функций в сфере обеспечения ИБ создается подразделение ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определяется должностное лицо, ответственное за обеспечение ИБ.

Требование настоящего пункта по созданию отдельного подразделения ИБ не распространяется на специальные государственные органы.

Подразделение ИБ или должностное лицо, ответственное за обеспечение ИБ, осуществляет:

1) контроль исполнения требований ТД ИБ;

2) контроль за документальным оформлением по ИБ;

3) контроль за управлением активами в части обеспечения ИБ;

4) контроль правомерности использования ПО;

5) контроль за управлением рисками в сфере ИКТ;

6) контроль за регистрацией событий ИБ;

7) проведение внутреннего аудита ИБ;

8) контроль за организацией внешнего аудита ИБ;

9) контроль за обеспечением непрерывности бизнес-процессов, использующих ИКТ ;

10) контроль соблюдения требований ИБ при управлении персоналом;

11) контроль за состоянием ИБ объекта информатизации "электронного правительства".";

часть вторую пункта 31 изложить в следующей редакции:

"ТД ИБ разрабатывается на казахском и русском языках, утверждается правовым актом ГО, МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации.";

пункт 35 изложить в следующей редакции:

"35. Перечень документов четвертого уровня включает рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения выполненных процедур и работ, в том числе:

1) журнал регистрации инцидентов ИБ и учета внештатных ситуаций;

2) журнал посещения серверных помещений;

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений;

5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;

6) журнал учета изменений конфигурации оборудования, тестирования и учета изменений СПО и ППО ИС, регистрации и устранения уязвимостей ПО;

7) журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;

8) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.";

подпункт 4) пункта 37 изложить в следующей редакции:

"4) формирование каталога угроз (рисков) ИБ, включающее:

оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ИСО/МЭК 27005-2013 "Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности";

определение потенциального ущерба;";

подпункты 4) и 5) пункта 38 изложить в следующей редакции:

"4) журналы регистрации событий хранятся в течение срока, указанного в ТД ИБ, но не менее трех лет и находятся в оперативном доступе не менее двух месяцев;

5) ведутся журналы регистрации событий создаваемого ПО в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, утверждаемых уполномоченным органом;";

пункт 43 изложить в следующей редакции:

"43. При увольнении или внесении изменений в условия трудового договора права доступа служащего ГО, МИО или работника организации к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего служащего ГО, МИО или работника организации, аннулируются после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора.";

пункт 45 изложить в следующей редакции:

"45. При инициировании создания или развития объектов информатизации первого и второго классов в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом в сфере информатизации в соответствии с подпунктом 11) статьи 7 Закона (далее – классификатор), а также конфиденциальных

ИС разрабатываются профили защиты для составных компонентов и задание по безопасности в соответствии с требованиями стандарта Республики Казахстан СТ РК ГОСТ Р ИСО/МЭК 15408-2006 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий".";

подпункт 1) пункта 46 изложить в следующей редакции:

"1) способам аутентификации;";

пункт 47 изложить в следующей редакции:

"47. При доступе к объектам информатизации первого и второго классов в соответствии с классификатором применяется многофакторная аутентификация, в том числе с использованием ЭЦП.";

дополнить пунктом 54-1 следующего содержания:

"54-1. Допускается применение в локальных сетях систем предотвращения утечки данных (DLP). При этом обеспечиваются:

визуальное уведомление пользователя о проводимом контроле действий;

получение письменного согласия пользователя на осуществление контроля его действий;

размещение центра управления и серверов системы предотвращения утечки данных в пределах локальной сети.";

дополнить пунктом 63-1 следующего содержания:

"63-1. Промышленная эксплуатация ИР ГО и МИО допускается при условии наличия акта с положительным результатом испытаний на соответствие требованиям информационной безопасности и аттестата соответствия требованиям информационной безопасности, за исключением случаев, предусмотренных статьей 66 Закона Республики Казахстан "Об информатизации.";

пункты 68 и 69 изложить в следующей редакции:

"68. Требования к создаваемому или развиваемому прикладному ПО ИС определяются в техническом задании, создаваемом в соответствии с требованиями стандарта Республики Казахстан СТ РК 34.015-2002 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы", настоящими ЕТ и правилами составления и рассмотрения технических заданий на создание или развитие информационных систем государственных органов, утверждаемыми уполномоченным органом по согласованию с уполномоченным органом в сфере обеспечения информационной безопасности.

69. Требования к создаваемому или развиваемому СПП определяются в задании на проектирование информационно-коммуникационной услуги, создаваемом в соответствии с настоящими ЕТ и правилами реализации сервисной модели информатизации, утверждаемыми уполномоченным органом.";

дополнить пунктом 69-1 следующего содержания:

"69-1. Промышленная эксплуатация сервисного программного продукта допускается при условии наличия акта с положительным результатом испытаний на соответствие требованиям информационной безопасности, протокола испытаний с целью оценки качества в соответствии с требованиями программной документации и действующих на территории Республики Казахстан стандартов в сфере информатизации и протокола экспертизы программной документации, за исключением случаев, предусмотренных статьей 66 Закона Республики Казахстан "Об информатизации".";

дополнить пунктом 90-1 следующего содержания:

"90-1. При реализации функций интеграционного взаимодействия объектов информатизации или компонентов объектов информации посредством шлюза, интеграционной шины, интеграционного компонента или интеграционного модуля обеспечиваются:

1) регистрация и проверка источников (точек подключений) запросов на легитимность;

2) проверка легитимности запросов по:

паролю или ЭЦП;

точке подключения;

наличию блокировки соединения;

разрешенным видам запросов, определенным в регламенте интеграционного взаимодействия;

разрешенной частоте запросов, определенной в регламенте интеграционного взаимодействия;

наличию в запросах признаков нарушений информационной безопасности;

наличию вредоносного кода по сигнатурам;

3) блокировка соединения при обнаружении нарушений в протоколах обмена сообщениями при:

отсутствии соединения в течение времени, определенного в регламенте интеграционного взаимодействия;

превышении разрешенной частоты запросов на время, определенное в регламенте интеграционного взаимодействия;

наличии в запросах признаков нарушений информационной безопасности;

превышении количества ошибок аутентификации, определенного в регламенте интеграционного взаимодействия;

выявлении аномальной активности пользователей;

выявлении попыток выгрузки массивов данных;

4) регулярная смена паролей соединения по времени действия, определенного в регламенте интеграционного взаимодействия;

5) замена логина соединения при выявлении инцидентов ИБ;

6) сокрытие адресации ЛС внутреннего контура;

7) журналирование событий, включающее:

регистрацию событий передачи/приема информационных сообщений;

регистрацию событий передачи/ получения файлов;

регистрацию событий передачи/получения служебных сообщений;

применение системы управления инцидентами и событиями ИБ для мониторинга журналов событий;

автоматизацию процедур анализа журналов событий на наличие событий ИБ;

хранение журналов событий на специализированном сервере логов, доступном для администраторов только для просмотра;

раздельное ведение журналов событий (при необходимости) по:

а) текущим суткам;

б) соединению (каналу связи);

в) государственному органу (юридическому лицу);

г) интегрируемым объектам информатизации;

8) предоставление сервиса синхронизации времени для интегрируемых объектов информатизации;

9) программно-аппаратная криптографическая защита соединений, осуществляемых через сети передачи данных;

10) хранение и передача паролей соединений в зашифрованном виде;

11) автоматизация оповещения об инцидентах ИБ ответственных лиц интегрируемых объектов информатизации.";

пункт 92 изложить в следующей редакции:

"92. Управление программно-аппаратным обеспечением ИС ГО и МИО осуществляется из ЛС внутреннего контура владельца ИС.

Программно-аппаратное обеспечение ИС ГО или МИО и негосударственных ИС, интегрируемых с ИС ГО или МИО, размещается на территории Республики Казахстан, за исключением случаев, связанных с межгосударственным информационным обменом , осуществляемым с использованием национального шлюза, в рамках международных договоров, ратифицированных Республикой Казахстан.";

дополнить пунктами 92-1 и 92-2 следующего содержания:

"92-1. Для организации работы ИС ГО и МИО допускается использование облачных сервисов (аппаратно-программные комплексы, ИС, предоставляющие ресурсы с использованием технологии виртуализации), центры управления и сервера которых физически размещены на территории Республики Казахстан.

92-2. Программно-аппаратное обеспечение ИС критически важных объектов информационно-коммуникационной инфраструктуры, содержащее персональные данные граждан Республики Казахстана, размещается на территории Республики Казахстан.";

пункт 99 изложить в следующей редакции:

"99. Выбор технологической платформы осуществляется с учетом приоритета оборудования с возможностью поддержки технологии виртуализации.";

дополнить пунктом 101-1 следующего содержания:

"101-1. Промышленная эксплуатация ИКП допускается при условии наличия акта с положительным результатом испытаний на соответствие требованиям информационной безопасности и аттестата соответствия требованиям информационной безопасности, за исключением случаев, предусмотренных статьей 66 Закона Республики Казахстан "Об информатизации".";

подпункт 1) пункта 116 изложить в следующей редакции:

"1) требования, предъявляемые в техническом задании на разработку (развитие) прикладного ПО ИС или задании на проектирование информационно-коммуникационной услуги, разработанном сервисным интегратором " электронного правительства";";

подпункт 4) пункта 128 изложить в следующей редакции:

"4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ ГО, МИО или организации используют услуги оператора ИКИ или другого оператора связи, имеющего зарезервированные каналы связи на оборудовании ЕШДИ;";

пункт 131 изложить в следующей редакции:

"131. Не допускается подключение к ЕТС ГО, локальной сети ГО или МИО, а также техническим средствам, входящим в состав ЕТС ГО, локальной сети ГО или МИО, устройств для организации удаленного доступа посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи, абонентских устройств сотовой связи и других беспроводных сетевых устройств. ";

пункт 140 изложить в следующей редакции:

"140. Требования, предусмотренные в подпунктах 10), 11) пункта 139 ЕТ, не предъявляются к ИС ГО и МИО, введенным в промышленную эксплуатацию до 1 января 2016 года и не подлежащим развитию до 1 января 2018 года.

Порядок информационного взаимодействия данных ИС ГО или МИО с негосударственными ИС определяется Правилами интеграции объектов информатизации "электронного правительства", утвержденными уполномоченным органом в сфере информатизации в соответствии с подпунктом 13) статьи 7 Закона.";

дополнить пунктом 163 следующего содержания:

"163. Распределительные устройства сетей телекоммуникаций размещаются в кроссовом помещении. Кроссовое помещение размещается ближе к центру обслуживаемой им рабочей области.

Размер кроссового помещения выбирается исходя из размера обслуживаемой рабочей области и устанавливаемого оборудования.

Помещение кроссового помещения должно соответствовать следующим требованиям:

наличие свободных служебных проходов для обслуживания оборудования;

отсутствие мощных источников электромагнитных помех (трансформаторов, электрических щитов, электродвигателей и прочее);

отсутствие труб и вентилей системы водоснабжения;

наличие систем пожарной безопасности;

отсутствие легко возгораемых материалов (деревянные стеллажи, картон, книги и прочее);

наличие отдельной линии электропитания от отдельного автомата для подключения шкафа по проекту;

наличие систем охранной сигнализации, контроля доступа;

наличие системы кондиционирования.".

2. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Премьер-Министр
Республики Казахстан *Б. Сагинтаев*