О внесении изменений и дополнений 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 10 июня 2022 года № 383.

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" следующие изменения и дополнения:

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

пункт 1 изложить в следующей редакции:

"1. Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – ЕТ) разработаны в соответствии с подпунктом 3) статьи 6 Закона Республики Казахстан "Об информатизации" (далее – Закон) и определяют требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности.";

пункт 6 изложить в следующей редакции:

"6. Для целей настоящих ЕТ в них используются следующие определения:

1) маркировка актива, связанного со средствами обработки информации, – нанесение условных знаков, букв, цифр, графических знаков или надписей на актив с целью его дальнейшей идентификации (узнавания), указания его свойств и характеристик;

2) средство криптографической защиты информации (далее – СКЗИ) – программное обеспечение или аппаратно-программный комплекс, реализующие алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами шифрования;

3) активы, связанные со средствами обработки информации, (далее – актив) – материальный или нематериальный объект, который является информацией или содержит информацию, или служит для обработки, хранения, передачи информации и имеющий ценность для организации в интересах достижения целей и непрерывности ее деятельности;

4) техническая документация по информационной безопасности (далее –ТД ИБ) – документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения ИБ объектов информатизации и (или) организации;

5) мониторинг событий информационной безопасности (далее – мониторинг событий ИБ) – постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности;

6) масштабируемость – способность объекта информатизации обеспечивать возможность увеличения своей производительности по мере роста объема обрабатываемой информации и (или) количества одновременно работающих пользователей;

7) программный робот – программное обеспечение поисковой системы или системы мониторинга, выполняющее автоматически и (или) по заданному расписанию просмотр веб-страниц, считывающее и индексирующее их содержимое, следуя по ссылкам, найденным в веб-страницах;

8) не нагруженное (холодное) резервирование оборудования – использование подготовленного к работе и находящегося в неактивном режиме дополнительного серверного и телекоммуникационного оборудования, программного обеспечения с целью оперативного восстановления информационной системы или электронного информационного ресурса;

9) нагруженное (горячее) резервирование оборудования – использование дополнительного (избыточного) серверного и телекоммуникационного оборудования, программного обеспечения и поддержание их в активном режиме с целью гибкого и оперативного увеличения пропускной способности, надежности и отказоустойчивости информационной системы, электронного информационного ресурса;

10) рабочая станция – стационарный компьютер в составе локальной сети, предназначенный для решения прикладных задач;

11) системное программное обеспечение – совокупность программного обеспечения для обеспечения работы вычислительного оборудования;

12) интернет-браузер – прикладное программное обеспечение, предназначенное для визуального отображения содержания интернет-ресурсов и интерактивного взаимодействия с ним;

13) кодированная связь – защищенная связь с использованием документов и техники кодирования;

14) многофакторная аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);

15) кроссовое помещение – телекоммуникационное помещение, предназначенное для размещения соединительных, распределительных пунктов и устройств;

16) прикладное программное обеспечение (далее – ППО) – комплекс программного обеспечения для решения прикладной задачи определенного класса предметной области;

17) засекреченная связь – защищенная связь с использованием засекречивающей аппаратуры;

18) серверный центр государственных органов (далее – серверный центр ГО) – серверное помещение (центр обработки данных), собственником или владельцем которого является оператор информационно-коммуникационной инфраструктуры " электронного правительства", предназначенное для размещения объектов информатизации "электронного правительства";

19) журналирование событий – процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

20) серверное помещение (центр обработки данных) – помещение, предназначенное для размещения серверного, активного и пассивного сетевого (телекоммуникационного) оборудования и оборудования структурированных кабельных систем;

21) локальная сеть внешнего контура (далее – ЛС внешнего контура) – локальная сеть субъектов информатизации, определенных уполномоченным органом, отнесенная к внешнему контуру телекоммуникационной сети субъектов информатизации, имеющая соединение с Интернетом, доступ к которому для субъектов информатизации предоставляется операторами связи только через единый шлюз доступа к Интернету;

22) терминальная система – тонкий или нулевой клиент для работы с приложениями в терминальной среде либо программами - тонкими клиентами в клиент-серверной архитектуре;

23) инфраструктура источника времени – иерархически связанное серверное оборудование, использующее сетевой протокол синхронизации времени, выполняющее задачу синхронизации внутренних часов серверов, рабочих станций и телекоммуникационного оборудования;

24) правительственная связь – специальная защищенная связь для нужд государственного управления;

25) 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;

26) федеративная идентификация – комплекс технологий, позволяющий использовать единое имя пользователя и аутентификационный идентификатор для доступа к электронным информационным ресурсам в системах и сетях, установивших доверительные отношения;

27) шифрованная связь – защищенная связь с использованием ручных шифров, шифровальных машин, аппаратуры линейного шифрования и специальных средств вычислительной техники;

28) локальная сеть внутреннего контура (далее – ЛС внутреннего контура) – локальная сеть субъектов информатизации, определенных уполномоченным органом, отнесенная к внутреннему контуру телекоммуникационной сети субъектов информатизации, имеющая соединение с единой транспортной средой государственных органов;

29) внешний шлюз "электронного правительства" (далее – ВШЭП) – подсистема шлюза "электронного правительства", предназначенная для обеспечения взаимодействия информационных систем, находящихся в ЕТС ГО с информационными системами, находящимися вне ЕТС ГО;

30) внутренний аудит информационной безопасности – объективный, документированный процесс контроля качественных и количественных характеристик текущего состояния информационной безопасности объектов информатизации в организации, осуществляемый самой организацией в своих интересах;

31) межсетевой экран – аппаратно-программный или программный комплекс, функционирующий в информационно-коммуникационной инфраструктуре, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами;

32) субъекты информатизации, определенные уполномоченным органом, – государственные органы, их подведомственные организации и органы местного самоуправления, а также иные субъекты информатизации, использующие единую транспортную среду государственных органов для взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных сетей.";

пункт 25 изложить в следующей редакции:

"25. Доступ к Интернету служащим ГО и МИО предоставляется с рабочих станций, подключенных к ЛС внешнего контура ГО и МИО, размещенных за пределами режимных помещений, определяемых в соответствии с Инструкцией по защите государственных секретов Республики Казахстан.";

пункт 29-1 изложить в следующей редакции:

"29-1. Приобретение товаров в целях реализации требований обеспечения ИБ для обороны страны и безопасности государства осуществляется из реестра доверенного программного обеспечения и продукции электронной промышленности в соответствии

с законодательством Республики Казахстан о государственных закупках, закупках отдельных субъектов квазигосударственного сектора.

При этом, в случае отсутствия в реестре доверенного программного обеспечения и продукции электронной промышленности необходимой продукции, допускается приобретение товаров в соответствии с законодательством Республики Казахстан о государственных закупках, закупках отдельных субъектов квазигосударственного сектора.";

пункт 50-1 изложить в следующей редакции:

"50-1. Собственники или владельцы негосударственных информационных систем, интегрируемых с информационными системами государственных органов, до интеграции с информационными системами государственных органов создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.

Владельцы критически важных объектов информационно-коммуникационной инфраструктуры создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан.

Собственники или владельцы критически важных объектов информационно-коммуникационной инфраструктуры, за исключением государственных органов, органов местного самоуправления, государственных юридических лиц, субъектов квазигосударственного сектора, в течение года со дня включения в перечень критически важных объектов информационно-коммуникационной инфраструктуры создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.";

пункт 54-1 изложить в следующей редакции:

"54-1. Для защиты объектов информатизации государственных органов применяются системы предотвращения утечки данных (DLP).

При этом обеспечиваются:

визуальное уведомление пользователя о проводимом контроле действий;

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

пункт 65 изложить в следующей редакции:

"65. ГО или МИО при неиспользовании ЭИР обеспечивает его передачу в архив в порядке, установленном Законом Республики Казахстан "О Национальном архивном фонде и архивах" (далее – Закон об архивах).";

пункт 80 изложить в следующей редакции:

"80. Прикладное ПО выполняет проверки подтверждения принадлежности и действительности открытого ключа ЭЦП и регистрационного свидетельства лица, подписавшего электронный документ, в соответствии с Правилами проверки подлинности электронной цифровой подписи, утвержденными уполномоченным органом в соответствии с подпунктом 10) пункта 1 статьи 5 Закона Республики Казахстан "Об электронном документе и электронной цифровой подписи".";

дополнить пунктом 87-1 следующего содержания:

"87-1. Испытания на соответствие требованиям информационной безопасности проводятся в соответствии со статьей 49 Закона.";

пункт 89 изложить в следующей редакции:

"89. При промышленной эксплуатации ИС ГО или МИО обеспечиваются:

1) сохранность, защита, восстановление ЭИР в случае сбоя или повреждения;

2) резервное копирование и контроль за своевременной актуализацией ЭИР;

3) автоматизированный учет, сохранность и периодическое архивирование сведений об обращениях к ИС ГО или МИО;

4) фиксация изменений в конфигурационных настройках ПО, серверного и телекоммуникационного оборудования;

5) контроль и регулирование функциональных характеристик производительности;

6) сопровождение ИС;

7) техническая поддержка используемого лицензионного ПО ИС;

8) гарантийное обслуживание разработчиком ИС, включающее устранение ошибок и недочетов ИС, выявленных в период гарантийного срока (Гарантийное обслуживание обеспечивается сроком не менее года со дня введения в промышленную эксплуатацию ИС);

9) подключение пользователей к ИС, а также взаимодействие ИС осуществляется с использованием доменных имен;

10) системно-техническое обслуживание;

11) сокращение (исключение) использования документов на бумажном носителе, а также требований по их представлению при осуществлении государственных функций и оказании государственных услуг.";

дополнить пунктом 92-4 следующего содержания:

"92-4. Собственники, владельцы и пользователи ИС ГО и МИО осуществляют наполнение, обеспечивают достоверность и актуальность ЭИР.";

пункт 95 изложить в следующей редакции:

"95. После снятия ИС с эксплуатации ГО или МИО сдают в ведомственный архив электронные документы, техническую документацию, журналы и архивированную базу данных снятой с эксплуатации ИС ГО или МИО в соответствии с Правилами приема, хранения, учета и использования документов Национального архивного фонда и других архивных документов ведомственными и частными архивами, утвержденными постановлением Правительства Республики Казахстан в соответствии с подпунктом 3) пункта 1-1 статьи 18 Закона об архивах.";

пункт 108 изложить в следующей редакции:

"108. Для обеспечения безопасности и качества обслуживания с оформлением договора совместных работ по ИБ в порядке, установленном законодательством Республики Казахстан, серверное оборудование АПК объектов информатизации ГО и МИО:

первого класса размещается только в серверном центре ГО;

второго и третьего классов размещается в серверном центре ГО, МИО или привлекаемого юридического лица, оборудованном в соответствии с требованиями к серверным помещениям, установленными в настоящих ЕТ, и имеющем в своем распоряжении оперативный центр информационной безопасности.";

дополнить пунктом 108-1 следующего содержания:

"108-1. Для обеспечения доступности и отказоустойчивости АПК объектов информатизации ГО и МИО резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных осуществляется с оформлением договора совместных работ по ИБ в порядке, установленном законодательством Республики Казахстан для объектов информатизации первого, второго и третьего классов в резервном серверном помещении ГО, МИО или привлекаемого юридического лица, оборудованном в соответствии с требованиями к серверным помещениям, установленными в настоящих ЕТ, и имеющем в своем распоряжении оперативный центр информационной безопасности.";

пункты 128 и 129 изложить в следующей редакции:

"128. В целях обеспечения ИБ:

1) при организации выделенного канала связи, объединяющего локальные сети, применяются программно-технические средства защиты информации, в том числе криптографического шифрования, с использованием СКЗИ;

2) выделенный канал связи подключается к локальной сети посредством пограничного шлюза с прописанными правилами маршрутизации и политиками безопасности. Пограничный шлюз обеспечивает следующий минимальный набор функций:

централизованную авторизацию узлов сети;

конфигурацию уровней привилегий администраторов;

протоколирование действий администраторов;

статическую трансляцию сетевых адресов;

защиту от сетевых атак;

контроль состояния физических и логических портов;

фильтрацию входящих и исходящих пакетов на каждом интерфейсе;

криптографическую защиту передаваемого трафика с использованием СКЗИ;

3) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей СИ между собой используются:

средства разделения и изоляции информационных потоков;

оборудование с компонентами, обеспечивающими ИБ и безопасное управление;

выделенные и интегрированные с оборудованием доступа межсетевые экраны, установленные в каждой точке подключения, с целью защиты периметра ЕТС ГО;

4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ ГО, МИО, государственные юридические лица, субъекты квазигосударственного сектора, а также владельцы критически важных объектов ИКИ используют услуги оператора ИКИ или другого оператора связи, имеющего зарезервированные каналы связи на оборудовании ЕШДИ.

Подключение ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ осуществляется в соответствии с Правилами функционирования единого шлюза доступа к Интернету, утвержденными уполномоченным органом в сфере обеспечения информационной безопасности;

5) служащие ГО, МИО и работники государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцы критически важных объектов ИКИ для осуществления оперативного информационного обмена в электронной форме при исполнении ими служебных обязанностей используют:

ведомственную электронную почту, службу мгновенных сообщений и иные сервисы;

электронную почту, службу мгновенных сообщений и иные сервисы, центры управления и серверы которых физически размещены на территории Республики Казахстан, если иное не установлено уполномоченным органом;

доступные облачные онлайн-сервисы видеоконференцсвязи в целях коммуникаций с иностранными физическими и юридическими лицами;

6) взаимодействие ведомственной электронной почты ГО и МИО с внешними электронными почтовыми системами осуществляется только через единый шлюз электронной почты;

7) служащие ГО, МИО и работники государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцы критически важных объектов ИКИ осуществляют доступ к ИР из ЛС внешнего контура только через ЕШДИ с использованием веб-обозревателя, являющегося СПО и соответствующего

требованиям Правил функционирования ЕШДИ, утвержденных уполномоченным органом в сфере обеспечения информационной безопасности;

8) служащими ГО, МИО и работниками государственных юридических лиц доступ к интернет-ресурсам осуществляется посредством интернет-браузера, дистрибутив которого имеет предустановленные регистрационные свидетельства национального удостоверяющего центра Республики Казахстан и корневого удостоверяющего центра Республики Казахстан.

129. Подключение СИ к ЕТС ГО осуществляется в соответствии с правилами подключения к ЕТС ГО и предоставления доступа к интранет-ресурсу через ЕТС ГО, определяемыми уполномоченным органом.";

пункт 148 изложить в следующей редакции:

"148. При размещении оборудования:

1) обеспечивается исполнение Правил технической эксплуатации электроустановок потребителей, утвержденных уполномоченным органом в сфере энергетики в соответствии с подпунктом 27) статьи 5 Закона Республики Казахстан "Об электроэнергетике" (далее – Закон об электроэнергетике);

2) обеспечивается исполнение требований поставщиков и (или) производителя оборудования к установке (монтажу), нагрузке на перекрытия и фальшпол, с учетом веса оборудования и коммуникаций;

3) обеспечивается наличие свободных служебных проходов для обслуживания оборудования;

4) учитывается организация воздушных потоков системы обеспечения микроклимата;

5) учитывается организация системы фальшполов и фальшпотолков.";

пункт 162 изложить в следующей редакции:

"162. Система заземления серверного помещения выполняется отдельно от защитного заземления здания. Все металлические части и конструкции серверного помещения заземляются с общей шиной заземления. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником, соединяемым с общей шиной заземления. Открытые токопроводящие части оборудования обработки информации должны быть соединены с главным заземляющим зажимом электроустановки.

Заземляющие проводники, соединяющие устройства защиты от перенапряжения с главной заземляющей шиной, должны быть самыми короткими и прямыми (без углов).

При построении и эксплуатации системы заземления необходимо руководствоваться:

Правилами устройства электроустановок, утвержденными приказом уполномоченного органа в сфере энергетики в соответствии с подпунктом 19) статьи 5 Закона об электроэнергетике;

стандартом Республики Казахстан СТ РК МЭК 60364-5-548-96 "Электроустановки зданий. Часть 5. Выбор и монтаж электрооборудования". Раздел 548 "Заземление устройства и системы уравнивания электрических потенциалов в электроустановках, содержащих оборудование обработки информации";

стандартом Республики Казахстан СТ РК МЭК 60364-7-707-84 "Электроустановки зданий. Часть 7. Требования к специальным электроустановкам". Раздел 707 " Заземление оборудования обработки информации";

стандартом Республики Казахстан СТ РК ГОСТ 12.1.030-81 "ССБТ. Электробезопасность. Защитное заземление, зануление";

стандартом Республики Казахстан СТ РК ГОСТ 464-79 "Заземление для стационарных установок проводной связи, радиорелейных станций, радиотрансляционных узлов проводного вещания и антенн систем коллективного приема телевидения. Нормы сопротивления".".

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

Премьер-Министр
Республики Казахстан *А. Смаилов*