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 13 мая 2024 года № 372.

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 6 изложить в следующей редакции:

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

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

2) 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 имеет ценность для организации в интересах достижения целей и непрерывности ее деятельности;

3) 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;

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) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

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

7) система мониторинга обеспечения информационной безопасности – организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования информационно-коммуникационных технологий;

8) оперативный центр информационной безопасности – юридическое лицо или структурное подразделение юридического лица, осуществляющие деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

9) 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;

10) 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 на веб-страницах;

11) система предотвращения утечки данных (DLP) – средство защиты информации, предназначенное для предотвращения утечек электронных информационных ресурсов ограниченного доступа;

12) 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;

13) 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;

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

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

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

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

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

19) 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);

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

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

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

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

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

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

26) уязвимость – недостаток объекта информатизации, использование которого может привести к нарушению целостности и (или) конфиденциальности, и (или) доступности объекта информатизации;

27) прокси-сервер – промежуточный сервер, участвующий в интернет-соединении между компьютерами/серверами, через который происходит обмен информацией в целях ее защиты от сетевых атак;

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

29) регистрационное свидетельство (далее – цифровой сертификат) – электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан "Об электронном документе и электронной цифровой подписи";

30) 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;

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

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

33) 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;

34) 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;

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

36) 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;

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

38) 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;

39) единый репозиторий "электронного правительства" – хранилище исходных кодов и скомпонованных из них исполняемых кодов объектов информатизации " электронного правительства";

40) 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.";

пункт 13 изложить в следующей редакции:

"13. Обеспечение ГО и МИО товарами, работами и услугами в сфере информатизации осуществляется путем закупа с учетом заключения уполномоченного органа в сфере информатизации на представленные администраторами бюджетных программ расчеты расходов на государственные закупки товаров, работ и услуг в сфере информатизации, за исключением специальных государственных органов Республики Казахстан.";

подпункт 7) пункта 14 исключить;

пункты 14-1 и 15 изложить в следующей редакции:

"14-1. Собственники и (или) владельцы обеспечивают ввод в промышленную эксплуатацию объекта информатизации "электронного правительства" с использованием исполняемых кодов, скомпонованных из исходных кодов объектов информатизации "электронного правительства", переданных ему государственной технической службой в соответствии с правилами функционирования единого репозитория "электронного правительства".

15. Рабочее пространство в ГО и МИО организуется в соответствии с санитарными правилами "Санитарно-эпидемиологические требования к административным и жилым зданиям", утвержденными приказом Министра здравоохранения Республики Казахстан от 16 июня 2022 года № ҚР ДСМ-52 (зарегистрирован в Министерстве юстиции Республики Казахстан 20 июня 2022 года за № 28525).";

пункты 29, 29-1 и 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

ISO/IEC 27002-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью".

29-1. В целях реализации требований обеспечения информационной безопасности для обороны страны и безопасности государства осуществляется приобретение ПО и продукции электронной промышленности в виде товара и информационно-коммуникационной услуги из реестра доверенного программного обеспечения и продукции электронной промышленности в соответствии с Законом и законодательством Республики Казахстан о государственных закупках, закупках отдельных субъектов квазигосударственного сектора.

Реестр доверенного программного обеспечения и продукции электронной промышленности ведется уполномоченным органом в сфере электронной промышленности в соответствии с Правилами формирования и ведения реестра доверенного программного обеспечения и продукции электронной промышленности, а также критериями по включению программного обеспечения и продукции электронной промышленности в реестр доверенного программного обеспечения и продукции электронной промышленности, утвержденными уполномоченным органом в сфере электронной промышленности согласно пункту 7 статьи 7-6 Закона.

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

Собственники и владельцы программного обеспечения, включенного в реестр доверенного программного обеспечения и продукции электронной промышленности, обеспечивают ввод в промышленную эксплуатацию объекта информатизации " электронного правительства" с использованием исполняемых кодов, скомпонованных из исходных кодов объектов информатизации "электронного правительства", переданных ему государственной технической службой в соответствии с правилами функционирования единого репозитория "электронного правительства".

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.

Подразделение ИБ или должностное лицо, ответственное за обеспечение ИБ, осуществляют координацию работ по обеспечению ИБ и контроль за исполнением требований ИБ, определенных в ТД по ИБ.

Сотрудники, ответственные за обеспечение ИБ, проходят специализированные курсы в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата.";

пункты 33, 34 и 35 изложить в следующей редакции:

"33. В перечень документов второго уровня входят документы, детализирующие требования политики ИБ ГО, МИО или организации, в том числе:

1) методика оценки рисков информационной безопасности;

2) правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;

3) правила проведения внутреннего аудита ИБ;

4) правила использования средств криптографической защиты информации;

5) правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам;

6) правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;

7) правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

34. Документы третьего уровня содержат описание процессов и процедур обеспечения ИБ, в том числе:

1) каталог угроз (рисков) ИБ;

2) план обработки угроз (рисков) ИБ;

3) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

4) руководство администратора по сопровождению объекта информатизации, резервному копированию и восстановлению информации;

5) инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

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.";

в пункте 37:

подпункт 1) изложить в следующей редакции:

"1) выбор методики оценки рисков в соответствии с рекомендациями стандарта Республики Казахстан СТ РК 31010-2020 "Менеджмент риска. Методы оценки риска" и разработка процедуры анализа рисков;";

подпункт 4) изложить в следующей редакции:

"4) формирование каталога угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 27005-2022 "Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности";";

пункт 38 дополнить подпунктом 5-1) следующего содержания:

"5-1) обеспечивается подключение систем журналирования событий ИБ объектов информатизации "электронного правительства" к техническим средствам системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности по запросу государственной технической службы;";

дополнить пунктом 38-1) следующего содержания:

"38-1. ГО и МИО обеспечивают на постоянной основе физический доступ работникам Национального координационного центра информационной безопасности к объектам информатизации "электронного правительства" с предоставлением отдельных рабочих мест по запросу государственной технической службы в целях проведения работ по мониторингу обеспечения информационной безопасности и мониторингу событий информационной безопасности.";

пункт 40 изложить в следующей редакции:

"40. Функциональные обязанности по обеспечению ИБ и обязательства по исполнению требований ТД ИБ служащих ГО, МИО или работников организации вносятся в должностные инструкции.

Обязательства в области обеспечения ИБ, имеющие силу после прекращения действий трудового договора, закрепляются в трудовом договоре с работником организации.";

пункт 43 изложить в следующей редакции:

"43. При внесении изменений в условия трудового договора работника организации , ротации или продвижении по государственной службе служащего ГО, МИО, их увольнении права доступа 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.";

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 цифровых сертификатов.";

пункт 55 изложить в следующей редакции:

"55. Регистрационные свидетельства Корневого удостоверяющего центра Республики Казахстан подлежат признанию в доверенных списках программных

продуктов мировых производителей ПО для целей аутентификации в соответствии со стандартами Республики Казахстан СТ РК ИСО/МЭК 14888-1-2017 "Информационная технология. Методы защиты информации. Цифровые подписи с приложением. Часть 1. Общие положения", СТ РК ИСО/МЭК 14888-3-2017 "Методы защиты информации цифровые подписи с приложением. Часть 3. Механизмы, основанные на сертификате", ГОСТ Р ИСО/МЭК 9594-8-98 "Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации".";

пункт 60 изложить в следующей редакции:

"60. Создание или развитие ИР осуществляются с учетом требований стандартов Республики Казахстан СТ РК 2190-2012 "Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования", СТ РК 2191-2023 "Информационные технологии. Доступность веб-контента для лиц с инвалидностью", СТ РК 2192-2012 "Информационные технологии. Интернет-ресурс, интернет-портал, интранет-портал. Общие описания", СТ РК 2193-2012 " Информационные технологии. Рекомендуемая практика разработки мобильных веб-приложений", СТ РК 2199-2012 "Информационные технологии. Требования к безопасности веб-приложений в государственных органах".";

пункт 63-1 изложить в следующей редакции:

"63-1. Промышленная эксплуатация ИР ГО и МИО допускается при условии наличия протоколов испытаний с положительными результатами испытаний на соответствие требованиям информационной безопасности.";

дополнить пунктом 63-2 следующего содержания:

"63-2. В объектах информатизации ГО, МИО и организаций не допускается хранение ЭИР, содержащих персональные данные и используемых при автоматизации государственных функций и оказании вытекающих из них государственных услуг, после наступления даты достижения целей их сбора и обработки, собственниками или владельцами которых являются иные субъекты информатизации.";

подпункт 2) пункта 78 изложить в следующей редакции:

"2) требования к разрабатываемому или приобретаемому прикладному ПО предусматривают применение средств:

идентификации и аутентификации пользователей, при необходимости цифровых сертификатов;

управления доступом;

контроля целостности;

журналирования действий пользователей, влияющих на ИБ;

защиты онлайновых транзакций;

криптографической защиты информации с использованием СКЗИ конфиденциальных ИС при хранении, обработке;

журналирования критичных событий ПО;";

пункт 83 изложить в следующей редакции:

"83. Обязательные требования к средствам обработки, хранения и резервного копирования ЭИР в объектах информационно-коммуникационной инфраструктуры " электронного правительства" определяются статьей 42 Закона.";

пункт 87 изложить в следующей редакции:

"87. Ввод в промышленную эксплуатацию ИС ГО, МИО и организаций осуществляется в соответствии с требованиями технической документации при условии положительного завершения опытной эксплуатации, наличия протоколов испытаний с положительными результатами испытаний на соответствие требованиям информационной безопасности, подписания акта о вводе в промышленную эксплуатацию ИС приемочной комиссией с участием представителей уполномоченных органов в сферах информатизации и обеспечения информационной безопасности, заинтересованных ГО, МИО и организаций.";

пункт 88 изложить в следующей редакции:

"88. Ввод в промышленную эксплуатацию объекта информатизации "электронного правительства" осуществляется его собственником или владельцем только с использованием исполняемых кодов, скомпонованных из исходных кодов объектов информатизации "электронного правительства", переданных ему государственной технической службой в соответствии с правилами функционирования единого репозитория "электронного правительства".";

пункт 95 изложить в следующей редакции:

"95. После снятия с эксплуатации объекта информатизации "электронного правительства" электронные информационные ресурсы, техническая документация и исходные программные коды подлежат передаче в архив в соответствии с законодательством Республики Казахстан.";

пункт 98-1 изложить в следующей редакции:

"98-1. На информационную систему критически важных объектов ИКИ также распространяются требования стандарта Республики Казахстан СТ РК IEC/PAS 62443-3-2017 "Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.";

пункты 101 и 101-1 изложить в следующей редакции:

"101. ИКП ЭП размещается на оборудовании, расположенном в серверном центре ГО.

101-1. Промышленная эксплуатация ИКП ЭП допускается при условии наличия протоколов испытаний с положительными результатами испытаний на соответствие требованиям информационной безопасности.";

в пункте 102:

подпункт 6) изложить в следующей редакции:

"6) управление инцидентами ИБ, требующее:

определения формального процесса обнаружения, выявления, оценки и порядка реагирования на инциденты ИБ с актуализацией раз в полугодие;

составления отчетов с периодичностью, определенной в ТД ИБ, по результатам обнаружения, выявления, оценки и реагирования на инциденты ИБ;

уведомления ответственных лиц ГО, МИО или организации об инцидентах ИБ;

передачи информации об инцидентах ИБ в Национальный координационный центр информационной безопасности;";

подпункт 8) изложить в следующей редакции:

"8) разделение сред эксплуатации от сред разработки и тестирования;";

подпункт 11) изложить в следующей редакции:

"11) исполнение процедур сетевого и системного администрирования, требующее:

обеспечения сохранности образов виртуальных машин, контроля целостности операционной системы, приложений, сетевой конфигурации, ПО и данных ГО или организации на наличие вредоносных сигнатур;

отделения аппаратной платформы от операционной системы виртуальной машины с целью исключения доступа внешних пользователей к аппаратной части;

логической изоляции между различными функциональными областями инфраструктуры среды виртуализации.";

в пункте 128:

подпункт 4) изложить в следующей редакции:

"4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ ГО государственные юридические лица, субъекты квазигосударственного сектора, а также собственники или владельцы критически важных объектов ИКИ, за исключением объектов среднего образования сельских населенных пунктов, использующих спутниковые (космические) каналы связи для доступа к Интернету, используют услуги оператора 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;";

подпункт 7) изложить в следующей редакции:

"7) служащие ГО, МИО и работники государственных юридических лиц, субъектов квазигосударственного сектора, а также собственники или владельцы критически важных объектов ИКИ, за исключением объектов среднего образования сельских населенных пунктов, использующих спутниковые (космические) каналы связи для доступа к Интернету, 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;";

подпункт 134-1 изложить в следующей редакции;

"134-1. Государственная техническая служба применяет на оборудовании ЕШДИ политику блокировки следующих категорий ИР и ПО (по умолчанию):

VPN;

удаленный доступ;

p2p;

игровые ресурсы;

неизвестные приложения, не входящие по умолчанию в перечень категорий ИР и ПО;

вредоносные ИР и ПО.";

в пункте 139:

подпункт 9) изложить в следующей редакции:

"9) осуществляется соединение ЛС внешнего контура СИ с Интернетом только через ЕШДИ. Подключение к Интернету иным способом не допускается, за исключением объектов среднего образования сельских населенных пунктов, использующих спутниковые (космические) каналы связи для доступа к Интернету, специальных и правоохранительных ГО в оперативных целях. Взаимодействие ВШЭП с Интернетом осуществляется через ЕШДИ;";

дополнить подпунктом 10-1) следующего содержания:

"10-1) при использовании в ЛС внутреннего контура объектов информатизации, размещенных в Интернете, или ЛС внешнего контура ГО, МИО или организации, которые не подключены посредством ВШЭП, используется экранированная подсеть, соответствующая следующим требованиям:

подсеть ограничена со стороны Интернета и ЛС внутреннего контура отдельными межсетевыми экранами с функциями обнаружения и предотвращения вторжений, а также преобразования внешних сетевых адресов для сокрытия внутренних сетевых адресов;

все подключения из ЛС внешнего контура, Интернета и ЛС внутреннего контура осуществляются исключительно на компьютер, размещенный вне экранированной подсети, который выполняет обработку сетевого трафика на всех уровнях сетевых протоколов, включая прикладной уровень без возможности перенаправления сетевого трафика по иному маршруту, отличающемуся от изначального;

не допускается сохранение запросов и ответов, а также свободное использование на рабочих станциях доступов к общедоступным ресурсам Интернета через прокси-сервер ;";

заголовок параграфа 8 изложить в следующей редакции:

"Параграф 8. Требования к системам бесперебойного функционирования технических средств и информационной безопасности, а также серверным помещениям (центрам обработки данных)";

пункт 145 изложить в следующей редакции:

"145. Через серверное помещение исключается прохождение любых транзитных коммуникаций. Трассы обычного и пожарного водоснабжения, отопления и канализации выносятся за пределы серверного помещения и не размещаются над серверным помещением в пределах одного этажа.

При необходимости размещения пожарных гидрантов над серверным помещением оборудуется сухотрубная система пожаротушения с устройством гидроизоляции перекрытия и организуется водоотвод над серверным помещением.";

пункт 162 изложить в следующей редакции:

"162. Система рабочего заземления серверного помещения выполняется отдельно от защитного заземления здания. Все металлические части и конструкции серверного помещения заземляются 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 ГОСТ Р 50571.21-2009 "Электроустановки зданий. Часть 5. Выбор и монтаж электрооборудования. Раздел 548. "Заземляющие устройства и системы уравнивания электрических потенциалов в электроустановках, содержащих оборудование обработки информации";

стандартом Республики Казахстан СТ РК ГОСТ Р 50571.22-2006 "Электроустановки зданий. Часть 7. Требования к специальным электроустановкам". Раздел 707. " Заземление оборудования обработки информации";

стандартом Республики Казахстан ГОСТ 12.1.030-81 "Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление";

стандартом Республики Казахстан 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 *О. Бектенов*