Утверждены
постановлением Правительства
Республики Казахстан
от « 20 » декабря 2016 года
№ 832

Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности

Глава 1. Общие положения

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 от 24 ноября 2015 года «Об информатизации» (далее – Закон) и определяют требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

2. Положения ЕТ, относящиеся к сфере обеспечения информационной безопасности, обязательны для применения государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры.

3. Положения ЕТ не распространяются на:

1) отношения, возникающие при осуществлении Национальным Банком Республики Казахстан и организациями, входящими в его структуру, работ по созданию или развитию, эксплуатации интернет-ресурсов, информационных систем, не интегрируемых с объектами информационно-коммуникационной инфраструктуры «электронного правительства», локальных сетей и сетей телекоммуникаций, а также при проведении закупок товаров, работ и услуг в сфере информатизации;

2) информационные системы в защищенном исполнении, отнесенные к государственным секретам в соответствии с законодательством Республики Казахстан о государственных секретах, а также сети телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи.

4. Целью ЕТ является установление обязательных для исполнения требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности государственными органами,

органами местного самоуправления, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры.

5. Задачами ЕТ являются:

1) определение принципов организации и управления информатизацией государственных органов для решения текущих и стратегических задач государственного управления;

2) определение единых принципов обеспечения и управления информационной безопасностью объектов информатизации «электронного правительства»;

3) установление требований по унификации элементов информационно-коммуникационной инфраструктуры;

4) установление требований по структуризации информационно-коммуникационной инфраструктуры и организации серверных помещений;

5) установление обязательности применения рекомендаций стандартов в области информационно-коммуникационных технологий и информационной безопасности на всех этапах жизненного цикла объектов информатизации;

6) повышение уровня защищенности государственных и негосударственных электронных информационных ресурсов, программного обеспечения, информационных систем и поддерживающей их информационно-коммуникационной инфраструктуры.

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, реализующее 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) 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;

6) 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;

7) 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;

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

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

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

11) 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);

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

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

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

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

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

17) локальная сеть внешнего контура (далее – ЛС внешнего контура) – локальная сеть ГО, отнесенная к внешнему контуру телекоммуникационной

сети ГО, имеющая соединение с Интернетом, доступ к которому для ГО предоставляется операторами связи только через единый шлюз доступа к Интернету;

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

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

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

21) 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;

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

23) локальная сеть внутреннего контура (далее – ЛС внутреннего контура) – локальная сеть ГО, отнесенная к внутреннему контуру телекоммуникационной сети ГО, имеющая соединение с единой транспортной средой государственных органов;

24) 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;

25) 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.

7. Для целей настоящих ЕТ в них используются следующие сокращения:

1) АПК – аппаратно-программный комплекс;

2) ИБ – информационная безопасность;

3) ИС – информационная система;

4) ИКИ – информационно-коммуникационная инфраструктура;

5) ИКТ – информационно-коммуникационные технологии;

6) ПО – программное обеспечение;

7) МИО – местные исполнительные органы;

8) СПО – свободное программное обеспечение;

9) ЕШДИ – единый шлюз доступа к Интернету;

10) ИР – интернет-ресурс;

11) ГО – центральный исполнительный орган, государственный орган, непосредственно подчиненный и подотчетный Президенту Республики Казахстан, территориальные подразделения ведомства центрального исполнительного органа;

12) ЕТС ГО – единая транспортная среда государственных органов;

13) ЕПИР ГО – единая платформа интернет-ресурсов государственных органов;

14) СПП – сервисный программный продукт;

15) ЭИР – электронные информационные ресурсы;

16) ИКП ЭП – информационно–коммуникационная платформа «электронного правительства»;

17) ЭЦП – электронная цифровая подпись.

Глава 2. Требования к организации и управлению информатизацией и информационной безопасностью

Параграф 1. Требования к информатизации государственного органа

8. Информатизация ГО осуществляется в соответствии с архитектурой ГО, разрабатываемой и утверждаемой в порядке, предусмотренном статьями 23 и 24 Закона, а в случае ее отсутствия – в соответствии с положительным заключением экспертного совета в сфере информатизации, вынесенным по итогам рассмотрения запроса ГО о потребностях, связанных с автоматизацией и оптимизацией деятельности ГО.

9. ГО обеспечивает:

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

2) автоматизацию государственных функций и оказание вытекающих из них государственных услуг с соблюдением требований настоящих ЕТ;

3) размещение сведений об объектах информатизации, планах, процессах и бюджете в области информатизации на архитектурном портале «электронного правительства» в соответствии с правилами регистрации информационных систем государственных органов, учета сведений об объектах информатизации «электронного правительства» и размещения электронных копий технической документации объектов информатизации «электронного правительства», утверждаемыми уполномоченным органом в соответствии с подпунктом 30) статьи 7 Закона.

10. Развитие архитектуры «электронного правительства» осуществляется в соответствии с требованиями по развитию архитектуры «электронного правительства», утверждаемыми уполномоченным органом в соответствии с подпунктом 10) статьи 7 Закона.

11. При разработке типовой архитектуры «электронного акимата», утверждаемой в соответствии с подпунктом 18) статьи 7 Закона в части описания требований к информационно-коммуникационной инфраструктуре, МИО учитываются требования настоящих ЕТ.

12. При реализации сервисной модели информатизации в ГО и МИО руководствуются нормами правил реализации сервисной модели информатизации, требованиями по развитию архитектуры «электронного правительства», утверждаемыми уполномоченным органом в соответствии с подпунктами 4) и 10) статьи 7 Закона и требованиями настоящих ЕТ.

13. Обеспечение ГО и МИО товарами, работами, услугами в сфере информатизации осуществляется путем:

1) закупа, при наличии положительного заключения экспертного совета в сфере информатизации;

2) приобретения информационно-коммуникационной услуги из каталога ИК-услуг оператора ИК-инфраструктуры.

14. Реализацию задач в сфере информатизации в ГО или МИО обеспечивает подразделение информационных технологий, осуществляющее:

1) мониторинг и анализ применения ИКТ;

2) участие в мероприятиях по учету и анализу использования ИКТ-активов;

3) выработку предложений в стратегический план ГО по вопросам информатизации;

4) координацию работ по созданию, сопровождению и развитию объектов информатизации «электронного правительства»;

5) контроль за обеспечением поставщиками предусмотренного договорами уровня качества оказываемых услуг в сфере информатизации;

6) регистрацию ИС ГО или МИО на архитектурном портале «электронного правительства»;

7) размещение, актуализацию и контроль за сохранностью на архитектурном портале «электронного правительства» сведений об объектах информатизации ГО или МИО, эталонных копий ПО, исходных программных кодов (при их наличии), комплекса настроек лицензионного ПО, электронных копий технической документации объектов информатизации «электронного правительства»;

8) взаимодействие с сервисным интегратором, оператором, ГО, МИО и организациями в части реализации проектов в сфере информатизации при создании архитектуры ГО и реализации сервисной модели информатизации;

9) реализацию требований по ИБ.

15. Рабочее пространство в ГО и МИО организуется в соответствии с санитарно-эпидемиологическими требованиями к содержанию и эксплуатации жилых и других помещений, общественных зданий, утвержденными уполномоченным органом в сфере защиты прав потребителей и санитарно-эпидемиологического благополучия населения в соответствии с пунктом 6

статьи 144 Кодекса Республики Казахстан от 18 сентября 2009 года «О здоровье народа и системе здравоохранения».

16. Рабочее место служащего ГО и МИО оснащается с учетом его функциональных обязанностей и включает:

1) рабочую станцию или унифицированное рабочее место или терминальную систему с подключением к ЛС внутреннего контура ГО или МИО. Допускается оснащение рабочего места дополнительным монитором при необходимости;

2) комплект мультимедийного оборудования (наушники, микрофон и веб-камера) для работы с мультимедийными ЭИР или системой видеоконференц-связи при необходимости;

3) аппарат телефонной связи или IP-телефонии.

17. Требования к унифицированному рабочему месту или терминальной системе ГО и МИО утверждаются уполномоченным органом.

18. При выборе закупаемых моделей рабочих станций необходимо руководствоваться следующими положениями:

1) аппаратные характеристики рабочих станций соответствуют либо превосходят системные требования, рекомендуемые разработчиком (производителем) используемого ПО;

2) для обеспечения общего уровня услуг унифицируются конфигурации рабочих станций;

3) для рабочих станций организуется централизованное автоматизированное распространение обновлений ПО;

4) для повышения качества и скорости администрирования количество различных аппаратно-программных конфигураций рабочих станций ограничивается тремя типами:

рабочая станция для работы с прикладным ПО;

рабочая станция повышенной мощности для работы с графическими пакетами, пакетами ПО моделирования и прочими. Используется для приложений с развитой графикой, высокими требованиями к производительности процессора, объемам оперативной памяти и видеоподсистем;

ноутбук для работы мобильных пользователей.

19. Для спецификации технических требований выделяются следующие ключевые параметры рабочих станций:

1) производительность, включающая в себя:

параметры быстродействия процессора;

необходимый объем оперативной памяти;

скорости внутренних шин передачи данных;

быстродействие графической подсистемы;

быстродействие устройств ввода/вывода;

параметры матрицы монитора;

2) надежность, обеспечиваемая за счет использования отказоустойчивых аппаратных средств и ПО, и определяется исходя из среднего времени безотказной работы;

3) масштабируемость, обеспечиваемая архитектурой и конструкцией персонального компьютера за счет возможности наращивания:

числа и производительности процессоров;

объемов оперативной и внешней памяти;

емкости встроенных накопителей.

20. Для обеспечения ИБ:

1) в ТД ИБ определяются:

способы размещения рабочих станций служащих ГО или МИО;

способы защиты рабочих станций от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб;

процедуры и периодичность технического обслуживания рабочих станций для обеспечения непрерывной доступности и целостности;

способы защиты рабочих станций мобильных пользователей, находящихся за пределами ГО или МИО, с учетом различных внешних рисков;

способы гарантированного уничтожения информации при повторном использовании рабочих станций или выводе из эксплуатации носителей информации;

правила выноса рабочих станций за пределы рабочего места;

2) на регулярной основе проводится учет рабочих станций с проверкой конфигураций;

3) установка и применение на рабочих станциях программных или аппаратных средств удаленного управления извне ЛС внутреннего контура исключается. Удаленное управление внутри ЛС внутреннего контура допускается в случаях, прямо предусмотренных в правовом акте ГО или МИО;

4) неиспользуемые порты ввода-вывода рабочих станций и мобильных компьютеров служащих ГО и МИО отключаются или блокируются, за исключением рабочих станций служащих подразделения ИБ.

21. Вопрос операций ввода-вывода с применением внешних электронных носителей информации на рабочих станциях служащих ГО и МИО регулируется в соответствии с политикой ИБ, принятой в ГО или МИО.

22. Для оптимизации размещения оборудования на рабочем месте служащего ГО и МИО допускается применение специализированного оборудования, обеспечивающего использование одной единицы монитора, ручного манипулятора (мышь) и клавиатуры для нескольких рабочих станций, без применения сетевых интерфейсов.

23. Для использования сервисов ИКП ЭП рабочая станция, подключенная к ЛС внутреннего контура ГО или МИО, обеспечивается сетевым подключением к инфраструктуре ИКП ЭП.

24. Обработка и хранение служебной информации ГО и МИО осуществляются на рабочих станциях, подключенных к ЛС внутреннего контура ГО или МИО и не имеющих подключения к Интернету.

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 обеспечению режима секретности в Республике Казахстан.

26. Сервис телефонной связи:

1) реализуется как на базе цифровых телефонных сетей общего пользования, так и с применением технологии IP-телефонии;

2) обеспечивает коммутацию пользователя с абонентами телефонных сетей по следующим каналам:

использование соединений абонентов через существующую локальную вычислительную сеть внутреннего и внешнего контура и ведомственную сеть передачи данных;

использование услуг связи оператора телефонной связи общего пользования по потоку E1;

использование операторов сотовой связи;

использование услуг междугородних и международных вызовов.

27. Для проведения конференций, презентаций, совещаний, телемостов конференцзал ГО и МИО оснащается:

1) конференцсистемой звукового усиления, включающей размещение на месте участника микрофона, громкоговорителя и светового индикатора запроса и выступления участника;

2) устройством ввода-вывода информации.

Для организации «телемоста» с географически распределенными участниками, находящимися в других городах или странах, конференцсистема по необходимости дополняется системой аудио- и видеоконференцсвязи оператора ИКИ ЭП.

28. Сервис печати:

1) реализуется посредством печатающего, копирующего и сканирующего оборудования, подключенного к локальной сети внутреннего контура ГО с использованием сетевого интерфейса либо прямого подключения к серверу печати;

2) обеспечивается программным обеспечением, реализующим:

централизованное управление пользователями и устройствами;

учет распечатываемых документов, а также копий, факсов, отправленных электронной почтой и сканирований по идентификационным номерам пользователей с возможностью распределения затрат между подразделениями и пользователями;

систему отчетов, графически иллюстрирующих активность печати, копирования и сканирования;

идентификацию пользователя до начала использования сервиса печати;

авторизацию служащего ГО на устройстве печати способами, регламентированными в ТД ИБ;

формирование очереди печати, осуществляющей печать посредством единой очереди печати с возможностью получения распечатанных документов на доступном устройстве печати.

Параграф 2. Требования к организации информационной безопасности

29. При организации, обеспечении и управлении ИБ в ГО, МИО или организации необходимо руководствоваться положениями стандарта Республики Казахстан СТ РК ИСО/МЭК 27002-2009 «Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации».

30. В целях разграничения ответственности и функций в сфере обеспечения ИБ подразделение ИБ, являющееся структурным подразделением ГО или МИО, обособленное от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, осуществляет:

1) контроль исполнения требований ТД ИБ;
2) контроль за документальным оформлением 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».

31. ТД ИБ создается в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется ГО, МИО или организация в своей деятельности.

ТД ИБ утверждается правовым актом ГО, МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации.

ТД ИБ пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.

32. Политика ИБ ГО, МИО или организации является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ.

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 и маркировки активов, связанных со средствами обработки информации;

3) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;

4) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

5) правила проведения внутреннего аудита ИБ;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к электронным информационным ресурсам;

8) правила использования Интернет и электронной почты;

9) правила организации процедуры аутентификации;

10) правила организации антивирусного контроля;

11) правила использования мобильных устройств и носителей информации;

12) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов.

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) регламент резервного копирования и восстановления информации;

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

5) руководство администратора по сопровождению объекта информатизации;

6) 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;

2) журнал учета внештатных ситуаций;

3) журнал посещения серверных помещений;

4) отчет о проведении оценки уязвимости сетевых ресурсов;

5) журнал регистрации и устранения уязвимостей ПО;

6) журнал учета кабельных соединений;

7) журнал учета резервных копий;

8) журнал учета тестирования резервных копий;

9) журнал учета изменений конфигурации оборудования;

10) журнал тестирования и учета изменений СПО и ППО ИС;

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

12) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.

Требования по содержанию документов третьего и четвертого уровней предусматриваются к ГО и МИО с 1 января 2017 года.

36. Для обеспечения защиты активов проводятся:

1) инвентаризация активов;

2) классификация и маркировка активов в соответствии с системой классификации, принятой в ГО, МИО;

3) закрепление активов за должностными лицами и определение меры их ответственности за реализацию мероприятий по управлению ИБ активов;

4) регламентация в ТД ИБ порядка:

использования и возврата активов;

идентификации, классификации и маркировки активов.

37. С целью управления рисками в сфере ИКТ в ГО или МИО осуществляются:

1) выбор методики оценки рисков в соответствии с рекомендациями стандарта Республики Казахстан СТ РК 31010-2010 «Менеджмент риска. Методы оценки риска» и разработка процедуры анализа рисков;

2) идентификация рисков в отношении перечня идентифицированных и классифицированных активов, включающая:

выявление угроз ИБ и их источников;

выявление уязвимостей, которые могут привести к реализации угроз;

определение каналов утечки информации;

формирование модели нарушителя;

3) выбор критериев принятия идентифицированных рисков;

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

оценку (переоценку) рисков идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК 13335-2008 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий»;

определение потенциального ущерба;

5) разработка и утверждение плана обработки угроз (рисков) ИБ, содержащего мероприятия по их нейтрализации или снижению.

38. С целью контроля событий нарушений ИБ в ГО, МИО или организации:

1) проводится мониторинг событий, связанных с нарушением ИБ, и анализ результатов мониторинга;

2) регистрируются события, связанные с состоянием ИБ, и выявляются нарушения путем анализа журналов событий, в том числе:

журналов событий операционных систем;

журналов событий систем управления базами данных;

журналов событий антивирусной защиты;

журналов событий прикладного ПО;

журналов событий телекоммуникационного оборудования;

журналов событий систем обнаружения и предотвращения атак;

журналов событий системы управления контентом;

3) обеспечивается синхронизация времени журналов регистрации событий с инфраструктурой источника времени;

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

5) ведутся журналы регистрации событий создаваемого ПО в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», утверждаемыми уполномоченным органом;

6) обеспечивается защита журналов регистрации событий от вмешательства и неавторизированного доступа. Не допускается наличие у системных администраторов полномочий на изменение, удаление и отключение журналов. Для конфиденциальных ИС требуются создание и ведение резервного хранилища журналов;

7) обеспечивается внедрение формализованной процедуры информирования об инцидентах ИБ и реагирования на инциденты ИБ.

39. С целью защиты критически важных процессов ГО, МИО или организации от внутренних и внешних угроз:

1) разрабатывается, тестируется и реализуется план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

2) доводится до сведения служащих ГО, МИО или работников организации инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации, подлежит регулярной актуализации.

40. Функциональные обязанности по обеспечению ИБ и обязательства по исполнению требований ТД ИБ служащих ГО, МИО или работников организации вносятся в должностные инструкции и (или) условия трудового договора.

Обязательства в области обеспечения ИБ, имеющие силу после прекращения действий трудового договора, закрепляются в трудовом договоре служащих ГО, МИО или работников организации.

41. В случае привлечения сторонних организаций к обеспечению информационной безопасности ЭИР, ИС, ИКИ, их собственник или владелец заключает соглашения, в которых устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение.

42. В ТД ИБ определяется содержание процедур при увольнении служащих ГО, МИО или работников организации, имеющих обязательства в области обеспечения ИБ.

43. При увольнении или внесении изменений в условия трудового договора права доступа служащего ГО, МИО или работника организации к информации и средствам обработки информации:

включают 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.

44. Кадровая служба организует и ведет учет прохождения служащими ГО, МИО или работниками организаций обучения в сфере информатизации и области обеспечения ИБ.

45. При инициировании создания или развития объектов информатизации первого и второго классов в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом 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 15408-2004 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

46. В целях обеспечения ИБ при эксплуатации объектов информатизации устанавливаются требования к:

1) способам идентификации;

2) применяемым СКЗИ;

3) способам обеспечения доступности и отказоустойчивости;

4) мониторингу обеспечения ИБ, защиты и безопасного функционирования;

5) применению средств и систем обеспечения ИБ;

6) регистрационным свидетельствам удостоверяющих центров.

47. С целью идентификации при доступе к объектам информатизации первого и второго классов в соответствии с классификатором применяется многофакторная аутентификация, в том числе с использованием ЭЦП.

48. С целью защиты служебной информации ограниченного распространения, конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа, применяются СКЗИ (программные или аппаратные) с параметрами, соответствующими требованиям к СКЗИ в соответствии со стандартом Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» для объектов информатизации:

первого класса в соответствии с классификатором – третьего уровня безопасности;

второго класса в соответствии с классификатором – второго уровня безопасности;

третьего класса в соответствии с классификатором – первого уровня безопасности.

49. Для обеспечения доступности и отказоустойчивости владельцами объектов информатизации ЭП обеспечиваются:

1) наличие резервного собственного или арендованного серверного помещения для объектов информатизации ЭП первого и второго классов в соответствии с классификатором;

2) резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП:

первого класса в соответствии с классификатором – нагруженное (горячее) в резервном серверном помещении;

второго класса в соответствии с классификатором – не нагруженное (холодное) в резервном серверном помещении;

третьего класса в соответствии с классификатором – хранение на складе в непосредственной близости от основного серверного помещения.

50. Объекты информатизации ЭП первого и второго классов в соответствии с классификатором подключаются к системе мониторинга обеспечения ИБ, защиты и безопасного функционирования не позднее одного года после их введения в промышленную эксплуатацию.

51. ГО, МИО осуществляют мониторинг:

действий пользователей и персонала;

использования средств обработки информации.

52. В ГО, МИО в рамках осуществления мониторинга действий пользователей и персонала:

1) при выявлении аномальной активности и злоумышленных действий пользователей эти действия:

регистрируются, блокируются и оперативно оповещается администратор для объектов информатизации ЭП первого класса в соответствии с классификатором;

регистрируются и блокируются для объектов информатизации ЭП второго класса в соответствии с классификатором;

регистрируются для объектов информатизации ЭП третьего класса в соответствии с классификатором;

2) регистрируются и контролируются подразделением ИБ действия обслуживающего персонала.

53. События ИБ, идентифицированные как критические для конфиденциальности, доступности и целостности, по результатам анализа мониторинга событий ИБ и анализа журнала событий:

1) определяются как инциденты ИБ;

2) учитываются в каталоге угроз (рисков) ИБ;

3) регистрируются в службе реагирования на компьютерные инциденты государственной технической службы.

54. На этапе опытной и промышленной эксплуатации объектов информатизации используются средства и системы:

обнаружения и предотвращения вредоносного кода;

управления инцидентами и событиями ИБ;

обнаружения и предотвращения вторжений;

мониторинга и управления информационной инфраструктурой.

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 СТ РК ИСО/МЭК 14888-1-2006 «Информационная технология. Методы защиты информации. Цифровые подписи с приложением. Часть 1. Общие положения», СТ РК ИСО/МЭК 14888-3-2006 «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».

56. Удостоверяющие центры Республики Казахстан, за исключением Корневого удостоверяющего центра Республики Казахстан, признаются в доверенных списках программных продуктов мировых производителей ПО путем аккредитации удостоверяющего центра в соответствии с правилами аккредитации удостоверяющих центров.

Удостоверяющие центры Республики Казахстан размещают свое регистрационное свидетельство в доверенной третьей стороне Республики Казахстан для обеспечения проверки ЭЦП граждан Республики Казахстан на территории иностранных государств.

Глава 3. Требования к объектам информатизации

Параграф 1. Требования к электронным информационным ресурсам и интернет-ресурсам

57. Собственник и (или) владелец ЭИР:

1) осуществляют идентификацию ЭИР, формируют и размещают описание метаданных (использования, описания, плана событий, хроники событий, отношений) при необходимости, в соответствии со стандартом Республики Казахстан СТ РК ИСО 23081-2-2010 «Информация и документация. Метаданные для управления записями. Часть 2. Вопросы концепции и реализации» в каталоге ЭИР, утверждаемом правовым актом ГО или организации;

2) определяют класс ЭИР в соответствии с правилами классификации объектов информатизации и классификатором объектов информатизации, утвержденными уполномоченным органом, и фиксируют класс ЭИР в технической документации и каталоге ЭИР;

3) поддерживают каталог ЭИР в актуальном состоянии;

4) осуществляют хранение ЭИР и его метаданных. Форму и способ хранения определяют самостоятельно.

58. Требования к созданию или развитию ИР определяются в технической спецификации на приобретение товаров, работ и услуг в сфере информатизации.

59. Собственник и (или) владелец ИР обеспечивают создание общедоступных ИР на казахском, русском и, по необходимости, на других языках, с возможностью выбора пользователем языка интерфейса.

60. Создание или развитие ИР осуществляется с учетом требований стандартов Республики Казахстан СТ РК 2190-2012 «Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования», СТ РК 2191-2012 «Информационные технологии. Доступность Интернет-ресурса для людей с ограниченными возможностями», 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».

61. Подготовка, размещение, актуализация ЭИР на ИР ГО или МИО осуществляются в соответствии с правилами информационного наполнения и требованиями к содержанию ИР ГО, утвержденными уполномоченным органом.

62. ИР центрального исполнительного органа, структурных и территориальных подразделений центрального исполнительного органа,

местного исполнительного органа размещается на ЕПИР ГО и регистрируется в доменных зонах gov.kz и мем.қаз**.**

ЕПИР ГО размещается на ИКП ЭП.

63. Управление ИР, размещение и актуализация ЭИР центрального исполнительного органа, структурных и территориальных подразделений центрального исполнительного органа, местного исполнительного органа осуществляются из внешнего контура локальной сети ИКИ ЭП оператором на основании заявки собственника и (или) владельца ИР.

64. При списании ИС, ПО или СПП собственник и (или) владелец ЭИР обеспечивают сохранение структуры и содержания базы данных посредством встроенного функционала системы управления базы данных списываемой ИС с подготовкой инструкции по восстановлению ЭИР.

Способ хранения структуры и содержания базы данных определяется собственником самостоятельно.

65. ГО или МИО при неиспользовании ЭИР обеспечивает его передачу в архив в порядке, установленном Законом Республики Казахстан от 22 декабря 1998 года «О национальном архивном фонде и архивах».

66. Для обеспечения ИБ ИР применяются:

1) регистрационные свидетельства для проверки подлинности доменного имени и криптографической защиты содержимого сеанса связи с использованием СКЗИ;

2) система управления содержимым (контентом), выполняющая:

санкционирование операций размещения, изменения и удаления ЭИР;

регистрацию авторства при размещении, изменении и удалении ЭИР;

проверку загружаемого ЭИР на наличие вредоносного кода;

аудит безопасности исполняемого кода и скриптов;

контроль целостности размещенного ЭИР;

ведение журнала изменений ЭИР;

мониторинг аномальной активности пользователей и программных роботов.

Параграф 2. Требования к разрабатываемому или приобретаемому прикладному программному обеспечению

67. На стадии инициирования создания или развития прикладного ПО определяется и фиксируется в проектной документации класс ПО в соответствии с правилами классификации объектов информатизации и классификатором объектов информатизации, утвержденными уполномоченным органом в соответствии с подпунктом 11) статьи 7 Закона.

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.

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

70. Требования к приобретаемому прикладному ПО определяются в технической спецификации на приобретение товаров, работ и услуг в сфере информатизации с учетом требований настоящих ЕТ.

71. Приобретение готового прикладного ПО осуществляется с учетом приоритета СПО при условии идентичности его характеристик с коммерческим ПО.

72. При формировании требований к разработке или приобретению ПО учитываются класс ЭИР и сведения каталога ЭИР.

73. Разрабатываемое или приобретаемое готовое прикладное ПО:

1) обеспечивает интерфейс пользователя, ввод, обработку и вывод данных на казахском, русском и других языках, по необходимости, с возможностью выбора пользователем языка интерфейса;

2) учитывает требования:

надежности;

сопровождаемости;

удобства использования;

эффективности;

универсальности;

функциональности;

кроссплатформенности;

3) обеспечивает полнофункциональную поддержку технологии виртуализации;

4) поддерживает кластеризацию;

5) обеспечивается технической документацией по эксплуатации на казахском и русском языках.

74. Создание (развитие) или приобретение ПО обеспечивается технической поддержкой и сопровождением.

Планирование, осуществление и документирование технической поддержки и сопровождения ПО проводится в соответствии со спецификациями изготовителя, поставщика или требованиями ТД ИБ.

75. Процесс создания (развития) прикладного ПО:

1) предусматривает:

создание информационной базы алгоритмов, исходных текстов и программных средств;

испытание и тестирование программных модулей;

типизацию алгоритмов, программ и средств ИБ, обеспечивающих информационную, технологическую и программную совместимость;

использование лицензионных инструментальных средств разработки;

2) включает процедуры приемки прикладного ПО, предусматривающие:

передачу разработчиком исходных текстов программ и других объектов, необходимых для создания прикладного ПО собственнику и (или) владельцу;

контрольную компиляцию переданных исходных текстов, с созданием полностью работоспособной версии прикладного ПО;

выполнение контрольного примера на данной версии ПО.

76. Контроль за авторизованными изменениями ПО и прав доступа к нему осуществляется с участием работников подразделения информационных технологий ГО или МИО.

77. Разработка прикладного ПО требует:

учета особенностей, предусмотренных правилами реализации сервисной модели информатизации;

регламентации вопросов ИБ в соглашениях на разработку ПО;

управления рисками в процессе разработки прикладного ПО.

78. С целью обеспечения ИБ:

1) на этапе разработки ПО учитываются рекомендации стандарта Республики Казахстан СТ РК ГОСТ Р 50739-2006 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;

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

идентификации и аутентификации пользователей, при необходимости ЭЦП и регистрационных свидетельств;

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;

3) в ТД ИБ определяются и применяются при эксплуатации:

правила установки, обновления и удаления ПО на серверах и рабочих станциях;

процедуры управления изменениями и анализа прикладного ПО, в случае изменения системного ПО;

4) лицензируемое ПО используется и приобретается только при условии наличия лицензии.

79. Мероприятия по контролю правомерности использования ПО определяются в ТД ИБ, проводятся не реже одного раза в год и включают в себя:

определение фактически используемого ПО;

определение прав на использование ПО;

сравнение фактически используемого ПО и имеющихся лицензий.

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 от 7 января 2003 года «Об электронном документе и электронной цифровой подписи».

Параграф 3. Требования к информационно-коммуникационной инфраструктуре

81. Требования к ИКИ формируются с учетом объектов, входящих в ее состав, согласно подпункту 25) статьи 1 Закона.

82. ЕТ устанавливает требования к следующим объектам ИКИ:

1) информационная система;

2) технологическая платформа;

3) аппаратно-программный комплекс;

4) сети телекоммуникаций;

5) системы бесперебойного функционирования технических средств и информационной безопасности.

Параграф 4. Требования к информационной системе

83. ИС ГО или МИО создается и развивается в порядке, определенном пунктом 1 статьи 39 Закона, а также учитываются требования статьи 38 Закона.

Обязательные требования к средствам обработки, хранения и резервного копирования ЭИР в ИС ГО или МИО определяются статьей 42 Закона.

84. Перед началом опытной эксплуатации разработчиком:

1) для всех функциональных компонентов ИС создается набор тестов, сценариев тестирования и методика испытаний для проведения тестирования;

2) осуществляются стендовые испытания ИС;

3) осуществляется для персонала:

ИС ГО или МИО первого класса в соответствии с классификатором обязательное обучение;

ИС ГО или МИО второго класса в соответствии с классификатором создание видео,- мультимедиа обучающих материалов;

ИС ГО или МИО третьего класса в соответствии с классификатором создание справочной системы и (или) инструкций по эксплуатации.

85. Опытная эксплуатация ИС ГО или МИО включает:

документирование процедур проведения опытной эксплуатации;

испытание на соответствие требованиям информационной безопасности;

оптимизацию и устранение выявленных дефектов и недоработок с последующим их исправлением;

оформление акта о завершении опытной эксплуатации ИС.

86. Перед вводом в промышленную эксплуатацию ИС в ГО, МИО или организации определяются, согласовываются, документально оформляются критерии приемки созданной ИС или новых версий и обновлений ИС.

87. Ввод в промышленную эксплуатацию ИС ГО или МИО осуществляется в соответствии с требованиями технической документации при условии положительного завершения опытной эксплуатации, наличия акта с положительным результатом испытаний на соответствие требованиям ИБ, аттестата соответствия требованиям ИБ и подписания акта о вводе в промышленную эксплуатацию ИС приемочной комиссией с участием представителей уполномоченного органа, заинтересованных ГО, МИО и организаций.

88. Предоставление сервисному интегратору «электронного правительства» для учета и хранения разработанного ПО, исходных программных кодов (при наличии) и комплекса настроек лицензионного ПО ИС ГО или МИО является обязательным и осуществляется в соответствии с порядком, определенным уполномоченным органом.

Модифицирование, разглашение и (или) использование исходных программных кодов, программных продуктов и ПО осуществляются по разрешению его собственника.

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) мониторинг событий ИБ ИС ГО или МИО и передача его результатов в систему мониторинга обеспечения информационной безопасности государственной технической службы;

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

6) контроль и регулирование функциональных характеристик производительности;

7) сопровождение ИС;

8) техническая поддержка используемого лицензионного ПО ИС;

9) 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;

10) подключение пользователей к ИС, а также взаимодействие ИС осуществляется с использованием доменных имен.

90. Интеграция ИС ГО или МИО, в том числе с ИС ГО и МИО, находящейся в опытной эксплуатации, осуществляется в соответствии с требованиями, определенными статьей 43 Закона.

Интеграция негосударственной ИС с ИС ГО или МИО осуществляется в соответствии с требованиями, определенными статьей 44 Закона.

91. Гарантийное обслуживание ИС на этапе промышленной эксплуатации с привлечением сторонних организаций требует:

регламентации вопросов ИБ в соглашениях на гарантийное обслуживание;

управления рисками ИКТ в процессе гарантийного обслуживания.

92. Управление программно-аппаратным обеспечением ИС ГО и МИО осуществляется из внутренней локальной сети 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, осуществляемого с использованием национального шлюза, в рамках международных договоров, ратифицированных Республикой Казахстан.

93. Собственник или владелец ИС ГО или МИО принимает решение о прекращении эксплуатации ИС в случае отсутствия необходимости ее дальнейшего использования.

О прекращении эксплуатации ИС ГО или МИО необходимо уведомить сервисного интегратора, с публикацией на архитектурном портале «электронного правительства» субъектов информатизации, чьи ИС интегрированы со снимаемой с эксплуатации ИС ГО или МИО, и ГО или МИО, являющихся пользователями данной ИС.

94. ГО или МИО составляет план снятия ИС ГО или МИО с эксплуатации и согласовывает его с ГО или МИО, являющимися пользователями ИС ГО или МИО.

95. После снятия ИС с эксплуатации ГО или МИО сдает 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 уполномоченным органом в сфере культуры в соответствии с подпунктом 2-4) статьи 18 Закона

Республики Казахстан от 22 декабря 1998 года «О национальном архивном фонде и архивах».

96. При поступлении заявки на прекращение эксплуатации ИС ГО или МИО сервисный интегратор аннулирует электронное свидетельство о регистрации ИС ГО или МИО и размещает соответствующие сведения на архитектурном портале «электронного правительства».

97. Списание и (или) утилизация снятой с эксплуатации ИС ГО или МИО осуществляются в соответствии с законодательством Республики Казахстан о бухгалтерском учете и финансовой отчетности.

В случае, если эксплуатация ИС ГО или МИО прекращена, но ИС ГО или МИО не списана в установленном порядке, то ИС ГО или МИО считается находящейся в консервации.

После списания ИС ГО или МИО не используется.

98. Для обеспечения ИБ:

1) на стадиях стендовых, приемо-сдаточных испытаний и тестовой эксплуатации осуществляются:

тестирование ПО ИС на основе разработанных комплексов тестов, настроенных на конкретные классы программ;

натурные испытания программ при экстремальных нагрузках с имитацией воздействия активных дефектов (стресс-тестирование);

тестирование ПО ИС с целью выявления возможных дефектов;

стендовые испытания ПО ИС для определения непреднамеренных программных ошибок проектирования, выявления потенциальных проблем для производительности;

выявление и устранение уязвимостей программного и аппаратного обеспечения;

отработка средств защиты от несанкционированного воздействия.

2) перед вводом ИС в опытную эксплуатацию требуется предусмотреть:

контроль неблагоприятного влияния новой ИС на функционирующие ИС и компоненты ИКИ ЭП, особенно во время максимальных нагрузок;

анализ влияния новой ИС на состояние ИБ ИКИ ЭП;

организацию подготовки персонала к эксплуатации новой ИС;

3) осуществляется разделение сред опытной или промышленной эксплуатации ИС от сред разработки, тестирования или стендовых испытаний. При этом реализуются следующие требования:

перевод ИС из фазы разработки в фазу тестирования фиксируется и документально оформляется;

перевод ИС из фазы тестирования в фазу опытной эксплуатации фиксируется и документально оформляется;

перевод ИС из фазы опытной эксплуатации в этап промышленной эксплуатации фиксируется и документально оформляется;

инструментальные средства разработки и испытываемое ПО ИС размещаются в разных доменах;

компиляторы, редакторы и другие инструментальные средства разработки в среде эксплуатации не размещаются или недоступны для использования из среды эксплуатации;

среда испытаний ИС соответствует среде эксплуатации в части аппаратно-программного обеспечения и архитектуры;

для испытываемых ИС не допускается использовать реальные учетные записи пользователей систем, находящихся в промышленной эксплуатации;

не подлежат копированию данные из ИС, находящихся в промышленной эксплуатации, в испытательную среду;

4) при выводе из эксплуатации ИС обеспечиваются:

архивирование информации, содержащейся в ИС;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей с оформлением соответствующего акта.

Параграф 5. Требования к технологической платформе

99. Выбор технологической платформы осуществляется с учетом приоритета оборудования, реализующего технологии виртуализации.

100. При выборе оборудования, реализующего технологию виртуализации, учитывается необходимость обеспечения следующей функциональности:

1) декомпозиции:

вычислительные ресурсы распределяются между виртуальными машинами;

множество приложений и операционных систем сосуществуют на одной физической вычислительной системе;

2) изоляции:

виртуальные машины полностью изолированы друг от друга, а аварийный отказ одной из них не оказывает влияния на остальные;

данные не передаются между виртуальными машинами и приложениями, за исключением случаев использования общих сетевых соединений;

3) совместимости:

приложениям и ОС предоставляются вычислительные ресурсы оборудования, реализующего технологию виртуализации.

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

ИКП ЭП обеспечивает:

автоматизированное предоставление ИК-услуг с единой точкой входа для их управления;

виртуализацию вычислительных ресурсов серверного оборудования с использованием различных технологий;

бесперебойное и отказоустойчивое функционирование предоставляемых ИК-услуг с коэффициентом использования не менее 98,7 %;

исключение единой точки отказа на логическом и физическом уровнях средствами используемого оборудования, телекоммуникаций и программного обеспечения;

разделение вычислительных ресурсов на аппаратном и программном уровнях.

Надежность виртуальной инфраструктуры обеспечивается встроенными средствами ПО технологии виртуализации и управления виртуальной средой.

102. Для обеспечения ИБ при использовании технологии виртуализации реализуются:

1) управление идентификацией, требующее:

аутентификацию клиентов ИК-услуг и привилегированных пользователей;

федеративной идентификации пользователей в пределах одной технологической платформы;

сохранения информации об аутентификации после удаления идентификатора пользователя;

применения средств контроля процедур назначения профилей полномочий пользователя;

2) управление доступом, требующее:

разделения полномочий администратора ИС и администратора среды виртуализации;

ограничения прав доступа администратора среды виртуализации к данным пользователя ИК-услуги. Права доступа ограничиваются конкретными процедурами, определенными в ТД ИБ и сервисном соглашении об обслуживании, и подлежат регулярной актуализации;

применения многофакторной аутентификации для привилегированных и критичных операций;

ограничения использования ролей со всеми полномочиями. Настройки профиля администратора ИС исключают получение доступа к компонентам среды виртуализации;

определения минимальных привилегий и реализацию модели ролевого управления доступом;

удаленного доступа посредством защищенного шлюза или списка разрешенных сетевых адресов отправителей;

3) управление ключами шифрования, требующее:

контроля ограничения доступа к данным о ключах шифрования СКЗИ;

контроля над организацией корневого каталога и подписки ключей;

блокирования скомпрометированных ключей и их надежного уничтожения;

4) проведение аудита событий ИБ, требующее:

обязательности и регулярности процедур, определяемых в ТД ИБ;

проведения процедур аудита для всех операционных систем, клиентских виртуальных машин, инфраструктуры сетевых компонентов;

ведения журнала регистрации событий и хранения в недоступной для администратора системе хранения;

проверки правильности работы системы ведения журнала регистрации событий;

определения длительности хранения журналов регистрации событий в ТД ИБ;

5) регистрация событий ИБ, требующая:

журналирования действий администраторов;

применения системы мониторинга инцидентов и событий ИБ;

оповещения на основе автоматического распознавания критического события или инцидента ИБ;

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;

регистрации инцидентов ИБ в Службе реагирования на компьютерные инциденты Государственной технической службы;

7) применение защитных мер аппаратных и программных компонентов инфраструктуры среды виртуализации, осуществляющих:

физическое отключение или блокирование неиспользуемых физических устройств (съемных накопителей, сетевых интерфейсов);

отключение неиспользуемых виртуальных устройств и сервисов;

мониторинг взаимодействия между гостевыми операционными системами;

контроль сопоставления виртуальных устройств физическим;

применение сертифицированных гипервизоров;

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

9) определение в ТД ИБ процедур управления изменениями для объектов информатизации;

10) определение в ТД ИБ процедур восстановления после сбоев и отказов оборудования и ПО;

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;

физической изоляции между средами виртуализации ЭИР и ИС различных классов по уровню ИБ.

Параграф 6. Требования к аппаратно-программному комплексу

103. Требования к конфигурации серверного оборудования АПК определяются в техническом задании на создание или развитие ИС и (или) технической спецификации на приобретение товаров, работ и услуг в сфере информатизации.

104. Выбор типовой конфигурации серверного оборудования АПК осуществляется с учетом обеспечения приоритета серверов:

1) с многопроцессорной архитектурой;

2) позволяющих масштабировать ресурсы и увеличивать производительность;

3) поддерживающих технологию виртуализации;

4) включающих средства управления, изменения и перераспределения ресурсов;

5) совместимых с используемой информационно-коммуникационной инфраструктурой.

105. Для обеспечения высокой доступности сервера применяются встроенные системы:

1) горячей замены резервных вентиляторов, блоков питания, дисков и адаптеров ввода-вывода;

2) динамической очистки и перераспределения страниц памяти;

3) динамического перераспределения процессоров;

4) оповещения о критических событиях;

5) поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.

106. Приобретаемое серверное оборудование обеспечивается технической поддержкой от производителя. Снимаемое с производства серверное оборудование не подлежит приобретению.

107. С целью обеспечения ИБ на регулярной основе, определенной в НТД ИБ, осуществляется инвентаризация серверного оборудования с проверкой его конфигурации.

108. Для обеспечения безопасности и качества обслуживания серверное оборудование АПК объектов информатизации:

первого класса размещается только в серверном центре ГО;

второго и третьего классов размещается в серверном центре ГО либо серверном помещении ГО или МИО, оборудованном в соответствии с требованиями к серверным помещениям, установленными в настоящих ЕТ.

109. Требования к системам хранения данных определяются в техническом задании на создание или развитие ИС и (или) технической спецификации на приобретение товаров, работ и услуг в сфере информатизации.

110. Система хранения данных обеспечивает поддержку:

единых средств для репликации данных;

масштабируемости по объему хранения данных.

111. Для высоконагруженных ИС, требующих высокой доступности, применяются:

1) сети хранения данных;

2) системы хранения данных, поддерживающие систему виртуализации и (или) ярусного хранения данных.

112. Для обеспечения высокой доступности системы хранения данных включают встроенные системы:

1) горячей замены резервных вентиляторов и блоков питания;

2) горячей замены дисков и адаптеров ввода-вывода;

3) оповещения о критических событиях;

4) активных контроллеров (в количестве не менее двух);

5) интерфейсов сети хранения данных (в количестве не менее двух портов на контроллер);

6) поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.

113. Система хранения данных обеспечивается системой резервного копирования.

114. Для обеспечения ИБ, надежного хранения и возможности восстановления данных:

1) применяется криптографическая защита хранимой служебной информации ограниченного распространения, информации конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа с использованием СКЗИ, в соответствии с пунктом 48 настоящих ЕТ;

2) используется выделенный сервер для защищенного хранения ключей шифрования по уровню безопасности не ниже уровня безопасности,

используемых СКЗИ, установленного для криптографических ключей в правилах использования криптографических средств защиты информации;

3) обеспечивается запись и испытание резервных копий в соответствии с регламентом резервного копирования, определенным в ТД ИБ.

115. При выводе из эксплуатации носителей информации, используемых в конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа, применяется программное и аппаратное обеспечение гарантированного уничтожения информации.

116. При выборе системного ПО серверного оборудования и рабочих станций учитываются:

1) требования, предъявляемые в техническом задании на разработку (развитие) прикладного ПО ИС или задании на проектирование СПП;

2) соответствие типу операционных систем (клиентской или серверной);

3) совместимость с используемым прикладным ПО;

4) поддержка сетевых сервисов, функционирующих в сети телекоммуникаций;

5) поддержка многозадачности;

6) наличие штатных средств получения и установки критичных обновлений и обновлений безопасности выпускаемых производителем операционных систем;

7) наличие средств диагностики, аудита и ведение журнала событий;

8) поддержка технологий виртуализации.

117. Приобретение системного ПО осуществляется с учетом приоритета:

1) модели лицензирования, обеспечивающей снижение стоимости закупки, а также совокупной стоимости лицензии за период эксплуатации;

2) ПО, обеспеченного технической поддержкой и сопровождением.

118. С целью обеспечения ИБ системное ПО обеспечивает возможность:

1) контроля доступа с применением:

идентификации, аутентификации и управления паролями пользователей;

регистрации успешных и неудавшихся доступов;

регистрации использования системных привилегий;

ограничения времени соединения, при необходимости, и блокировки сеанса по превышению лимита времени;

2) исключения для пользователей и ограничения для администраторов использования системных утилит, способных обходить средства контроля операционной системы.

119. СПО распространяется безвозмездно, без лицензионных ограничений, препятствующих использованию в ГО с соблюдением требований законодательства об авторском праве.

120. СПО предоставляется с открытым исходным кодом.

121. Используемое в ГО СПО дорабатывается с учетом поддержки форматов информационного взаимодействия через ШЭП.

122. Для обеспечения ИБ при применении СПО:

к использованию допускается СПО, поддерживаемое сообществом разработчиков СПО или прошедшее экспертизу и сертификацию программного кода;

сохраняются применявшиеся версии СПО.

Параграф 7. Требования к сетям телекоммуникаций

123. Ведомственные (корпоративные) сети телекоммуникаций организуются путем объединения локальных сетей, принадлежащих одному собственнику, посредством выделенных собственных или арендованных каналов связи.

Выделенные каналы связи, предназначенные для объединения локальных сетей, организовываются с использованием протоколов канального и сетевого уровней.

124. При организации ведомственной (корпоративной) сети путем объединения нескольких локальных сетей применяется радиальная или радиально-узловая топология сети. В узловых точках выделенные каналы подключаются к одному пограничному шлюзу. Каскадное (последовательное) подключение локальных сетей не используется.

125. При проектировании создается и при эксплуатации поддерживается в актуальном состоянии документированная схема ведомственной (корпоративной) сети телекоммуникаций.

126. Физический доступ к оборудованию для организации каналов связи имеет персонал, обслуживающий выделенный канал связи.

Управление оборудованием осуществляет оператор ИКИ ЭП, предоставляющий выделенный канал.

В настройках оборудования неиспользуемые порты блокируются.

127. Ввод в здание линий канала связи и их прокладка в здании осуществляются в соответствии с государственным нормативом СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования».

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 ГО или МИО 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.

При подключении сервера к ЕТС ГО и локальной сети безопасность обеспечивается посредством межсетевых экранов и отдельных шлюзов доступа, установленных в местах стыка с ЕТС ГО и локальной сетью;

4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей ГО или МИО к Интернету через ЕШДИ ГО или МИО использует услуги оператора ИКИ или другого оператора связи, имеющего собственные международные магистральные каналы связи в точке подключения ЕШДИ и зарезервированные каналы связи на оборудовании ЕШДИ;

5) служащие ГО, МИО и работники государственных организаций, субъектов квазигосударственного сектора, а также владельцев критически важных объектов ИКИ для осуществления оперативного информационного обмена (служебной переписки) в электронной форме при исполнении ими служебных обязанностей используют только ведомственные:

электронную почту;

службу мгновенных сообщений и иные сервисы.

Ведомственная электронная почта центрального исполнительного органа, структурных и территориальных подразделений центрального исполнительного органа, местного исполнительного органа размещается в доменных зонах gov.kz и мем.қаз.

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

129. Подключение ГО и МИО к ЕТС ГО осуществляется в соответствии с порядком подключения к ЕТС ГО и предоставления доступа к интранет-ресурсу ГО или МИО через ЕТС ГО, определяемым уполномоченным органом.

130. В ГО или МИО допускается применение устройств для организации беспроводного доступа только к общедоступным ЭИР «электронного

правительства» и местах, разрешенных для пребывания посетителей ГО или МИО в «гостевой зоне».

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

132. Оператор ИКИ ЭП по заявкам ГО и МИО осуществляет:

распределение, регистрацию и перерегистрацию IP-адресов локальных сетей ГО и МИО, подключенных к ЕТС ГО, по заявкам ГО или МИО;

регистрацию доменных имен в доменных зонах Интернета gov.kz и мем.қаз по заявкам ГО или МИО;

регистрацию доменных имен в сети ЕТС ГО по заявкам ГО или МИО;

предоставление сервиса DNS в сети ЕТС ГО.

133. ГО и МИО ежегодно:

1) запрашивают у государственной технической службы перечень используемых на оборудовании ЕШДИ категорий интернет-ресурсов;

2) выбирают из вышеуказанного перечня категории интернет-ресурсов, доступ к которым ограничивается для служащих ГО и МИО средствами ЕШДИ, и составляют их список;

3) направляют в государственную техническую службу вышеуказанный список и списки сетевых адресов информационно-коммуникационных сетей ГО и их территориальных подразделений, МИО, получающих доступ к Интернету, для применения на оборудовании ЕШДИ.

134. Государственная техническая служба осуществляет делегирование (обслуживание) доменных зон gov.kz и мем.қаз с предоставлением сервиса в Интернете.

135. Требования к создаваемой или развиваемой локальной сети определяются в технической спецификации на приобретение товаров, работ и услуг в сфере информатизации.

При проектировании кабельной системы локальной сети необходимо соблюдать требования государственного норматива СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования».

136. При проектировании создается документированная схема локальной сети, которая поддерживается в актуальном состоянии при эксплуатации.

137. Все элементы кабельной системы подлежат маркировке в соответствии с требованиями пункта 13.1.5 Государственного норматива СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования».

Все кабельные соединения регистрируются в журнале учета кабельных соединений.

138. Активное оборудование локальных сетей обеспечивается электропитанием от источников бесперебойного питания.

139. Для обеспечения ИБ:

1) неиспользуемые порты кабельной системы локальной сети физически отключаются от активного оборудования;

2) разрабатывается и утверждается ТД ИБ, включающая правила:

использования сетей и сетевых услуг;

подключения к международным (территориальным) сетям передачи данных;

подключения к Интернету и (или) сетям телекоммуникаций, сетям связи, имеющим выход в международные (территориальные) сети передачи данных;

использования беспроводного доступа к сетевым ресурсам;

3) служебная информация ограниченного распространения, информация конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа, не передается по незащищенным проводным каналам связи и радиоканалам, не оборудованным соответствующими СКЗИ.

Передача служебной информации ограниченного распространения производится с соблюдением специальных требований по защите информации ограниченного распространения, в соответствии с Правилами отнесения сведений к служебной информации ограниченного распространения и работы с ней, установленными Правительством Республики Казахстан;

4) применяются средства:

идентификации, аутентификации и управления доступом пользователей;

идентификации оборудования;

защиты диагностических и конфигурационных портов;

физического сегментирования локальной сети;

логического сегментирования локальной сети;

управления сетевыми соединениями;

межсетевого экранирования;

сокрытия внутреннего адресного пространства локальной сети;

контроля целостности данных, сообщений и конфигураций;

криптографической защиты информации в соответствии с пунктом 48 настоящих ЕТ;

физической защиты каналов передачи данных и сетевого оборудования;

регистрации событий ИБ;

мониторинга и анализа сетевого трафика;

управления сетью;

5) осуществляется взаимодействие локальных сетей ГО, а также МИО между собой только через ЕТС ГО, за исключением сетей телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи;

6) осуществляется взаимодействие локальных сетей центрального исполнительного государственного органа и его территориальных подразделений между собой только через ЕТС ГО, за исключением сетей

телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи;

7) исключаются сопряжение ЛС внутреннего контура и ЛС внешнего контура ГО, а также МИО между собой;

8) исключается подключение ЛС внутреннего контура ГО и МИО к Интернету;

9) осуществляется соединение ЛС внешнего контура ГО и МИО с Интернетом только через ЕШДИ. Подключение к Интернету иным способом не допускается, за исключением специальных и правоохранительных ГО в оперативных целях. Взаимодействие ВШЭП с Интернетом осуществляется через ЕШДИ;

10) размещается ИС ГО или МИО, реализующие информационное взаимодействие через Интернет, в выделенном сегменте ЛС внешнего контура ГО или МИО, и осуществляется взаимодействие с ИС ГО или МИО, размещенными в ЛС внутреннего контура ГО или МИО, через ВШЭП;

11) осуществляется информационное взаимодействие ИС, размещенных в Интернете, с ИС ГО или МИО, размещенными в ЛС внутреннего контура ГО или МИО, только через ВШЭП.

Функционирование ВШЭП осуществляется в соответствии с порядком, утвержденным уполномоченным органом в сфере информатизации;

12) сервера инфраструктуры источника времени верхнего уровня синхронизируются с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC(kz).

Сервера инфраструктуры точного времени синхронизируются с сервером инфраструктуры точного времени верхнего уровня

Сервера инфраструктуры точного времени предоставляют доступ клиентам для синхронизации времени.

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 шлюза электронного правительства, платежного шлюза «электронного правительства» с информационными системами, утвержденными уполномоченным органом в соответствии с подпунктом 13) статьи 7 Закона.

Параграф 8. Требования к системам бесперебойного функционирования технических средств и информационной безопасности

141. Серверное оборудование АПК и системы хранения данных размещаются в серверном помещении.

142. Серверное помещение располагается в отдельных, непроходных помещениях без оконных проемов. В случае наличия оконных проемов, они закрываются или заделываются негорючими материалами.

Для поверхности стен, потолков и пола применяются материалы, не выделяющие и не накапливающие пыль. Для напольного покрытия применяются материалы с антистатическими свойствами. Серверное помещение защищается от проникновения загрязняющих веществ.

Стены, двери, потолок, пол и перегородки серверного помещения обеспечивают герметичность помещения.

143. Двери серверного помещения составляют не менее 1,2 метра в ширину и 2,2 метра в высоту, открываются наружу или раздвигаются. Конструкция рамы двери не предусматривает порога и центральной стойки.

144. Серверное помещение оборудуется фальшполом и (или) фальшпотолком для размещения кабельных систем и инженерных коммуникаций.

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 на верхних этажах.

146. Монтаж коммуникационных каналов для прокладки силовых и слаботочных кабельных сетей здания выполняется в отдельных или разделенных перегородками кабельных лотках, коробах или трубах, разнесенных между собой. Слаботочные и силовые шкафы устанавливаются раздельно и закрываются на замок.

Прокладка кабелей через перекрытия, стены, перегородки осуществляется в отрезках несгораемых труб с герметизацией негорючими материалами.

147. Серверное помещение надежно защищается от внешнего электромагнитного излучения.

148. При размещении оборудования:

1) обеспечивается исполнение правил технической эксплутации электроустановок потребителей, утвержденных уполномоченным органом в сфере энергетики в соответствии с подпунктом 27) статьи 5 Закона Республики Казахстан от 9 июля 2004 года «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.

149. При техническом сопровождении оборудования, установленного в серверном помещении, документируются:

1) обслуживание оборудования;

2) устранение проблем, возникающих при работе аппаратно-программного обеспечения;

3) факты сбоев и отказов, а также результаты восстановительных работ;

4) послегарантийное обслуживание критически важного оборудования по истечении гарантийного срока обслуживания.

Форма и способ документирования определяются самостоятельно.

150. Обслуживание критически важного оборудования выполняется сертифицированным техническим персоналом.

151. В непосредственной близости от серверного помещения создается склад запасных частей для критически важного оборудования, содержащий запас комплектующих и оборудования для выполнения оперативной замены при проведении ремонтно-восстановительных работ.

152. Вмешательство в работу находящегося в эксплуатации оборудования возможно только с разрешения руководителя подразделения информационных технологий либо лица, его замещающего.

153. Основные и резервные серверные помещения располагаются на безопасном расстоянии в удаленных друг от друга зданиях. Требования к резервным серверным помещениям идентичны требованиям к основным серверным помещениям.

154. С целью обеспечения ИБ, отказоустойчивости и надежности функционирования:

1) в серверном помещении применяются способы расположения оборудования, обеспечивающие снижение рисков возникновения угроз, опасностей и возможностей несанкционированного доступа;

2) в серверном помещении исключается размещение в одной виртуальной среде, одном серверном оборудовании, одном монтажном шкафу или стойке ЭИР, ИР, СПП, ИС, относящихся в соответствии с классификатором объектов информатизации к разным классам;

3) поддерживается в актуальном состоянии список лиц, авторизованных для осуществления сопровождения объектов ИКИ, установленных в серверном помещении;

4) серверное помещение оборудуется системами:

контроля и управления доступом;

обеспечения микроклимата;

охранной сигнализации;

видеонаблюдения;

пожарной сигнализации;

пожаротушения;

гарантированного электропитания;

заземления;

5) отказоустойчивость инфраструктуры серверного помещения составляет не менее 99,7 %.

155. Система контроля и управления доступом обеспечивает санкционированный вход в серверное помещение и санкционированный выход из него. Преграждающие устройства и конструкция входной двери должны предотвращать возможность передачи идентификаторов доступа в обратном направлении через тамбур входной двери.

Устройство центрального управления системы контроля и управления доступом устанавливается в защищенных от доступа посторонних лиц отдельных служебных помещениях, помещении поста охраны. Доступ к программным средствам системы контроля и управления доступом, влияющим на режимы работы системы, со стороны персонала охраны исключить.

Электроснабжение системы контроля и управления доступом осуществляется от свободной группы щита дежурного освещения. Система контроля и управления доступом обеспечивается резервным электропитанием.

156. Система обеспечения микроклимата включает системы кондиционирования, вентиляции и мониторинга микроклимата. Системы обеспечения микроклимата серверного помещения не объединяются с другими системами микроклимата, установленными в здании.

Температура в серверном помещении поддерживается в диапазоне от 20℃ до 25℃ при относительной влажности от 45 % до 55 %.

Мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем. Система кондиционирования воздуха обеспечивается резервированием. Электропитание кондиционеров серверного помещения осуществляется от системы гарантированного электропитания или системы бесперебойного электропитания.

Система вентиляции обеспечивает приток свежего воздуха с фильтрацией и подогревом поступающего воздуха в зимний период. В серверном помещении давление создается избыточным для предотвращения поступления загрязненного воздуха из соседних помещений. На воздуховодах приточной и вытяжной вентиляций устанавливаются защитные клапаны, управляемые системой пожаротушения.

Системы кондиционирования и вентиляции отключаются автоматически по сигналу пожарной сигнализации.

Система мониторинга микроклимата контролирует климатические параметры в серверных шкафах и телекоммуникационных стойках:

температуру воздуха;

влажность воздуха;

запыленность воздуха;

скорость потока воздуха;

задымленность воздуха;

открытие (закрытие) дверей шкафов.

157. Система охранной сигнализации серверного помещения выполняется отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Контролю и охране подлежат все входы и выходы серверного помещения, а также внутренний объем серверного помещения. Система охранной сигнализации имеет собственный источник резервированного питания.

158. Расположение камер системы видеонаблюдения выбирается с учетом обеспечения контроля всех входов и выходов в серверное помещение, пространства и проходов возле оборудования. Угол обзора и разрешение камер должны обеспечить распознавание лиц. Изображение с камер выводится на отдельный пульт в помещение круглосуточной охраны

159. Система пожарной сигнализации серверного помещения выполняется отдельно от пожарной сигнализации здания. В серверном помещении устанавливаются два типа датчиков: температурные и дымовые.

Датчиками контролируются общее пространство серверного помещения и объемы, образованные фальшполом и (или) фальшпотолком. Сигналы оповещения системы пожарной сигнализации выводятся на пульт в помещение круглосуточной охраны.

160. Система пожаротушения серверного помещения оборудуется автоматической установкой газового пожаротушения, независимой от системы пожаротушения здания. В качестве огнегасителя в автоматической установке газового пожаротушения используется специальный нетоксичный газ. Порошковые и жидкостные огнегасители не используются. Установка газового пожаротушения размещается непосредственно в серверном помещении или вблизи него в специально оборудованном для этого шкафу. Запуск системы пожаротушения производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также ручных датчиков, расположенных у выхода из помещения. Время задержки выпуска огнегасителя составляет не более 30 с. Оповещение о срабатывании системы пожаротушения выводится на табло, размещаемые внутри и снаружи помещения. Система пожаротушения выдает команды на закрытие защитных клапанов системы вентиляции и отключение питания оборудования. Серверное помещение, оборудованное системой пожаротушения, оснащается вытяжной вентиляцией для удаления огнегасящего газа.

161. Система гарантированного электропитания предусматривает наличие двух вводов электропитания от разных источников внешнего электропитания на напряжение ~400/230В, частотой 50 Гц и автономного генератора. Все источники электроэнергии подаются на автомат ввода резерва, осуществляющий автоматическое переключение на резервный ввод электропитания при прекращении, перерыве подачи электропитания на основном вводе. Параметры линий электропитания и сечение жил определяются исходя из планируемой суммарной потребляемой мощности

оборудования и подсистем серверного помещения. Линии электропитания выполняются по пятипроводной схеме.

Система гарантированного электропитания предусматривает электроснабжение оборудования и систем серверного помещения через источники бесперебойного питания. Мощность и конфигурация источников бесперебойного питания рассчитываются с учетом всего запитываемого оборудования и запаса для перспективного развития. Время автономной работы от источников бесперебойного питания рассчитывается с учетом потребностей, а также необходимого времени для перехода на резервные линии и времени запуска генератора в рабочий режим.

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 Республики Казахстан от 9 июля 2004 года «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».