Приложение

**ТРЕБОВАНИЯ**

**к защите информации, содержащейся в базах данных**

**государственных информационных систем**

**1. Общие положения**

1. Требования к защите информации, содержащейся в базах данных государственных информационных систем (далее – Требования), разработаны в соответствии с Законом Кыргызской Республики «Об электронном управлении» (далее – Закон об ЭУ) и определяют меры по защите информации в соответствии с Законом, а также в целом требования к использованию информационных технологий в государственных информационных системах и обеспечения безопасности информации, содержащейся в их базах данных.

2. Положения настоящих Требований обязательны для применения государственными органами, органами местного самоуправления, юридическими лицами с участием государства и/или муниципальных образований, а также организаций, финансируемых из республиканского и местных бюджетов, являющихся владельцами и/или операторами государственных/муниципальных информационных систем, а также иных элементов, входящих в состав государственной инфраструктуры электронного управления.

3. Положения Требований не распространяются на государственные информационные системы, содержащие в их базах данных информацию, отнесенную к государственным секретам в соответствии с законодательством Кыргызской Республики о государственных секретах, на сети телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи, информационные системы, не входящие в состав государственной инфраструктуры электронного управления.

4. В настоящих Требованиях используются следующие определения:

**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;

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

**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;

**кибербезопасность** – сохранение свойств целостности (которая может включать аутентичность и неотказуемость), доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий;

**техническая документация по обеспечению кибербезопасности (далее – ТД КБ)** – документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения целостности (включая аутентичность и неотказуемость), доступности и конфиденциальности информации, содержащейся в базах данных государственных информационных систем;

**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;

**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;

**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;

**рабочая станция** – стационарный или портативный компьютер в составе локальной сети, предназначенный для решения прикладных задач;

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

**кодированная связь** – защищенная связь с использованием документов и техники кодирования;

**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, средств биометрической идентификации);

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

**засекреченная связь** – защищенная связь с использованием засекречивающей аппаратуры;

**масштабируемость** – способность элемента государственной инфраструктуры электронного управления обеспечивать увеличение своей производительности по мере роста объема обрабатываемой информации и (или) количества одновременно работающих пользователей;

**журналирование событий** – процесс записи информации о происходящих программных или аппаратных событиях в журнал регистрации событий;

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

**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;

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

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

**правительственная связь** – специальная защищенная связь для нужд государственного управления;

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

**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;

**внутренний аудит информационной безопасности** – объективный, документированный процесс контроля качественных и количественных характеристик текущего состояния информационной безопасности элементов государственной инфраструктуры электронного управления, осуществляемый самой организацией (владельцем/оператором информационной системы) в своих интересах.

1. В настоящих Требованиях используются следующие сокращения:

АПК – аппаратно-программный комплекс;

ГИ ЭУ – государственная инфраструктура электронного управления;

ГИР/базовые ГИР – государственные информационные ресурсы;

ГО - государственный орган;

КБ – кибербезопасность;

ИС/ГИС – информационная система/государственная информационная система;

ИТ – информационные технологии;

КИИ - критическая информационная инфраструктура

ЛС - локальная сеть

ПО – программное обеспечение;

МСУ – органы местного самоуправления;

СПО – системное программное обеспечение;

ППО -  прикладное программное обеспечение;

ГО – государственный орган, его территориальные подразделения, осуществляющие полномочия владельца и/или оператора информационной системы;

СКЗИ – средства криптографической защиты информации;

СПП – сервисный программный продукт;

СЭМВ “Тундук” - система электронного межведомственного взаимодействия;

ТД КБ - техническая документация по кибербезопасности;

УГО – уполномоченный государственный орган в сфере информационных технологий и электронного управления (Государственный комитет информационных технологий и связи Кыргызской Республики)

ЭП – электронная подпись;

ЭУ – электронное управление.

**2. Требования к использованию информационных технологий**

**в государственных органах**

6. ГИ ЭУ представляет собой упорядоченную совокупность используемых в электронном управлении государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями и организациями информационных технологий и технических средств.

7. Создание, развитие и эксплуатация ГИ ЭУ осуществляются с учетом требований, предусмотренных Законом Кыргызской Республики «О государственных закупках».

Использование ИТ в ГО осуществляется в соответствии с Законом Кыргызской Республики «ОБ электронном управлении», с учетом требований к технико-экономическим обоснованиям, техническим спецификациям, техническим заданиям на закупку (модернизацию) ИС и ИТ для государственных и муниципальных органов, предприятий, учреждений, утверждаемых УГО, в соответствии с положительным заключением Межведомственной комиссии по координации информатизации (далее – Комиссия), вынесенным по итогам рассмотрения ведомственных проектов перехода к электронному управлению с учетом потребностей ГО, связанных с автоматизацией и оптимизацией деятельности ГО, а также с учетом Перечня технологий, изложенных в международных стандартах, для государственных информационных систем, использующих системы шифрования и средства криптографической защиты информации (СКЗИ), за исключением информации, отнесенной к государственным секретам, утверждаемого Правительством (Приложение 2).

8. ГО обеспечивает:

* + планирование затрат на информатизацию в соответствии с ГИ ЭУ, а также с учетом решений Комиссии, Совета по электронному управлению и развитию информационно-коммуникационных технологий при Правительстве Кыргызской Республики (далее - Совет);
	+ оказание государственных и муниципальных услуг в электронной форме с соблюдением настоящих Требований;
	+ размещение сведений о включении ИС, центров обработки данных, иных элементов в состав ГИЭУ, планах, процессах и бюджете в области ЭУ на портале электронных государственных услуг.

9. Развитие, эксплуатация ГИЭУ, включение в ее состав новых элементов осуществляется в соответствии с Законом «Об электронном управлении».

10. Реализацию задач в сфере ЭУ в ГО обеспечивает подразделение информационных технологий, осуществляющее:

* + мониторинг и анализ применения ИКТ;
	+ участие в мероприятиях по учету и анализу использования ИКТ-активов;
	+ выработку предложений в планы ГО по вопросам внедрения ЭУ;
	+ координацию работ по созданию, сопровождению и развитию элементов ГИЭУ;
	+ контроль за обеспечением поставщиками предусмотренного договорами уровня качества оказываемых услуг в сфере ЭУ;
	+ регистрацию ИС ГО в Реестре ГИЭУ;
	+ размещение, актуализацию и контроль за сохранностью сведений об элементах ГИЭУ, эталонных копий ПО, исходных программных кодов (при их наличии), комплекса настроек лицензионного ПО, электронных копий технической документации элементов ГИЭУ;
	+ взаимодействие с УГО, операторами ИС, другими ГО, МСУ и организациями в части реализации проектов в сфере ЭУ;
	+ реализацию требований по КБ.

11. Рабочее пространство в ГО и МСУ организуется в соответствии с санитарно-эпидемиологическими требованиями к содержанию и эксплуатации жилых и других помещений, общественных зданий, в соответствии с требованиями законодательства КР.

12. Рабочее место служащего ГО и МСУ оснащается с учетом его функциональных обязанностей и включает:

* + рабочую станцию или унифицированное рабочее место или терминальную систему с подключением к ЛС внутреннего контура ГО или МСУ. Допускается оснащение рабочего места дополнительным монитором при необходимости;
	+ комплект мультимедийного оборудования (наушники, микрофон и веб-камера) при необходимости;
	+ аппарат телефонной связи или IP-телефонии.

      13. Для обеспечения КБ:

1) в ТД КБ определяются:

* + способы размещения рабочих станций служащих ГО или МСУ;
	+ 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 МСУ, 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 МСУ;

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

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

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

16. Для использования сервисов СЭМВ «Тундук» рабочая станция, подключенная к ЛС внутреннего контура ГО или МСУ, обеспечивается сетевым подключением к инфраструктуре СЭМВ «Тундук».

17. Обработка и хранение информации для служебного пользования ГО и МСУ, а также отнесенной к служебной тайне, осуществляются на рабочих станциях, подключенных к ЛС внутреннего контура ГО или МСУ и не имеющих подключения к Интернету.

18. Доступ к Интернету служащим ГО и МСУ предоставляется с рабочих станций, подключенных к ЛС внешнего контура ГО и МСУ, размещенных за пределами режимных помещений, определяемых в соответствии с Инструкцией по обеспечению режима секретности в Кыргызской Республике.

19. 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 Е1;
* использование операторов сотовой связи;
* использование услуг междугородной и международной связи.

20. Для проведения конференций, презентаций, совещаний, телемостов помещение (конференцзал) ГО и МСУ оснащается:

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

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

**3. Требования к организации кибербезопасности**

**в государственном органе**

21. В целях разграничения ответственности и функций в сфере обеспечения КБ подразделение КБ, являющееся структурным подразделением ГО или МСУ, обособленное от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов ЭУ, осуществляет:

* контроль исполнения требований ТД КБ;
* контроль за документальным оформлением КБ;
* контроль за управлением активами в части обеспечения КБ;
* контроль правомерности использования ПО;
* контроль за управлением рисками в сфере ИКТ;
* контроль за регистрацией событий КБ;
* проведение внутреннего аудита КБ;
* контроль за организацией внешнего аудита КБ;
* контроль за обеспечением непрерывности бизнес-процессов, использующих ИКТ;
* контроль соблюдения требований КБ при управлении персоналом;
* контроль за состоянием КБ элемента ГИЭУ.

  22. ТД КБ создается в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется ГО, МСУ или организация в своей деятельности.

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

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

23. Политика КБ ГО, МСУ или организации определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения КБ.

      24. В перечень документов в области обеспечения КБ также входят документы, детализирующие требования политики КБ ГО, МСУ или организации, рабочие формы, журналы, заявки, протоколы и другие документы, включая электронные, используемые для регистрации и подтверждения выполненных процедур и работ, в том числе:

* методика оценки рисков кибербезопасности;
* правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;
* правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;
* правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;
* правила проведения внутреннего аудита КБ;
* правила использования средств криптографической защиты информации;
* правила разграничения прав доступа к информационным ресурсам;
* правила использования Интернет и электронной почты;
* правила организации процедуры аутентификации;
* правила организации антивирусного контроля;
* правила использования мобильных устройств и носителей информации;
* правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов;
* каталог (перечень) угроз (рисков) КБ;
* план обработки угроз (рисков) КБ;
* регламент резервного копирования и восстановления информации;
* план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;
* руководство администратора по сопровождению объекта ГИ ЭУ/информационной инфраструктуры;
* инструкцию о порядке действий пользователей по реагированию на инциденты КБ и во внештатных (кризисных) ситуациях.
* журнал регистрации инцидентов КБ;
* журнал учета внештатных ситуаций;
* журнал посещения серверных помещений;
* отчет о проведении оценки уязвимости сетевых ресурсов;
* журнал регистрации и устранения уязвимостей ПО;
* журнал учета кабельных соединений;
* журнал учета резервных копий;
* журнал учета тестирования резервных копий;
* журнал учета изменений конфигурации оборудования;
* журнал тестирования и учета изменений СПО и ППО ИС;
* журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;
* журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.

Указанные документы должны быть разработаны в ГО, МСУ до 1 июля 2018 года.

      25. Для обеспечения защиты информационных активов проводятся:

1) инвентаризация активов;

* классификация и маркировка активов в соответствии с системой классификации, принятой в ГО, МСУ;
* закрепление активов за должностными лицами и определение меры их ответственности за реализацию мероприятий по управлению КБ активов;
* регламентация в ТД КБ порядка:
* использования и возврата активов;
* идентификации, классификации и маркировки активов.

      26. С целью управления рисками/угрозами в сфере КБ в ГО или МСУ осуществляются:

1) определение перечня угроз КБ в ИС при осуществлении ГО или МСУ соответствующих видов деятельности;

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

* выявление угроз КБ 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) КБ, включая оценку (переоценку) угроз (рисков), определение потенциального ущерба;

5) разработка и утверждение мероприятия по нейтрализации или снижению угроз (рисков) КБ.

      27. С целью контроля событий нарушений ИБ в ГО, МСУ 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 КБ, 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 кибербезопасности, защиты и безопасного функционирования элементов ГИЭУ, утверждаемыми УГО;

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 КБ.

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

* разрабатывается, тестируется и реализуется план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;
* доводится до сведения служащих ГО, МСУ или работников организации инструкция о порядке действий пользователей по реагированию на инциденты КБ и во внештатных (кризисных) ситуациях.

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

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

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

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

31. В ТД КБ определяется содержание процедур при увольнении служащих ГО, МСУ или работников организации, имеющих обязательства в области обеспечения КБ.

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

* включают физический и логический доступ, идентификаторы доступа, подписи, документацию, которая идентифицирует его как действующего служащего ГО, МСУ или работника организации;
* аннулируются после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора.

33. Кадровая служба организует и ведет учет прохождения служащими ГО, МСУ или работниками организаций обучения в сфере ЭУ и области обеспечения КБ.

     34. В целях обеспечения КБ при эксплуатации объектов ЭУ устанавливаются требования к:

* способам идентификации;
* применяемым СКЗИ;
* способам обеспечения доступности и отказоустойчивости;
* мониторингу обеспечения КБ, защиты и безопасного функционирования;
* применению средств и систем обеспечения КБ;
* регистрационным свидетельствам удостоверяющих центров.

35. C целью защиты информации для служебного пользования, конфиденциальной информации, специальных категорий персональных данных, содержащихся в базах данных ИС, применяются СКЗИ (программные или аппаратные) с параметрами согласно Техническим требованиям к средствам криптографической защиты информации, утверждаемыми Правительством, соответствующего уровня безопасности (Приложение 1).

36. Для обеспечения доступности и отказоустойчивости владельцами ИС обеспечиваются:

* наличие резервного собственного или арендованного серверного помещения;
* резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных.

37. ГО, МСУ осуществляют мониторинг:

* действий пользователей и персонала;
* использования средств обработки информации.

38. В ГО, МСУ в рамках осуществления мониторинга действий пользователей и персонала:

* при выявлении аномальной активности и злоумышленных действий пользователей эти действия регистрируются, блокируются и оперативно оповещается администратор;
* регистрируются и контролируются подразделением КБ действия обслуживающего персонала.

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

* определяются как инциденты КБ;
* учитываются в перечне угроз КБ;
* регистрируются в службе (подразделении) реагирования на компьютерные инциденты УГО и (или) уполномоченного государственного органа в сфере национальной безопасности.

40. На этапе опытной и промышленной эксплуатации элементов ГИЭУ используются средства и системы:

* обнаружения и предотвращения вредоносного кода;
* управления инцидентами и событиями КБ;
* обнаружения и предотвращения вторжений;
* мониторинга и управления информационной инфраструктурой ЭУ.

**4. Требования к информационным системам**

**государственных органов**

      41. Собственник и (или) владелец ИС:

* осуществляют идентификацию ИС, формируют и размещают описание метаданных (использования, описания, плана событий, хроники событий, отношений);
* регистрируют ИС, иной элемент ГИЭУ в Реестре государственной инфраструктуры электронного управления в соответствии с правилами и порядком, утвержденными УГО;
* поддерживают Реестр ГИЭУ в актуальном состоянии;
* осуществляют хранение ИС и метаданных; форму и способ хранения определяют самостоятельно.

42. Создание, развитие и эксплуатация государственной инфраструктуры электронного управления осуществляются с учетом требований, предусмотренных Законом Кыргызской Республики «О государственных закупках».

43. Создание, эксплуатация и поддержка сайтов ГО/МСУ в сети Интернет осуществляется с учетом требований по созданию и поддержке веб-сайтов государственных органов и органов местного самоуправления Кыргызской Республики, утверждаемых Правительством КР.

44. При списании ИС, ПО или СПП собственник и (или) владелец ИС обеспечивают сохранение структуры и содержания базы данных посредством встроенного функционала системы управления базы данных списываемой ИС с подготовкой инструкции по восстановлению ИС.    Способ хранения структуры и содержания базы данных определяется собственником самостоятельно.

45. ГО или МСУ при неиспользовании ИС обеспечивает ее передачу в архив в порядке, установленном Законом Кыргызской Республики «О Национальном архивном фонде Кыргызской Республики».

46. Перед началом опытной эксплуатации ИС разработчиком:

* для всех функциональных компонентов ИС создается набор тестов, сценариев тестирования и методика испытаний для проведения тестирования;
* осуществляются испытания ИС;
* для персонала ГО или МСУ осуществляется обязательное обучение, создание справочной системы и (или) инструкций по эксплуатации

47. Опытная эксплуатация ИС ГО или МСУ включает:

* документирование процедур проведения опытной эксплуатации;
* испытание на соответствие требованиям кибербезопасности;
* оптимизацию и устранение выявленных дефектов и недоработок с последующим их исправлением;
* оформление акта о завершении опытной эксплуатации ИС.

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

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

50. Предоставление УГО для учета и хранения разработанного ПО, исходных программных кодов (при наличии) и комплекса настроек лицензионного ПО ИС ГО или МСУ является обязательным и осуществляется в соответствии с порядком, определенным УГО.

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

       52. При промышленной эксплуатации ИС ГО или МСУ обеспечиваются:

* сохранность, защита, восстановление ИС в случае сбоя или повреждения;
* резервное копирование и контроль за своевременной актуализацией ИС;
* автоматизированный учет, сохранность и периодическое архивирование сведений об обращениях к ИС ГО или МСУ;
* мониторинг событий КБ ИС ГО или МСУ и передача его результатов в систему мониторинга обеспечения кибербезопасности службы (подразделения) реагирования на компьютерные инциденты УГО и (или) уполномоченного государственного органа в сфере безопасности;
* фиксация изменений в конфигурационных настройках ПО, серверного и телекоммуникационного оборудования;
* контроль и регулирование функциональных характеристик производительности;
* сопровождение ИС;
* техническая поддержка используемого лицензионного ПО ИС;
* 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;
* подключение пользователей к ИС, а также взаимодействие ИС осуществляется с использованием доменных имен.

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

* регламентации вопросов КБ в соглашениях на гарантийное обслуживание;
* управления рисками ИКТ в процессе гарантийного обслуживания.

54. После снятия ИС с эксплуатации ГО или МСУ сдает в ведомственный архив электронные документы, техническую документацию, журналы и архивированную базу данных снятой с эксплуатации ИС ГО или МСУ в соответствии с правилами приема, хранения, учета и использования документов, установленных Законом Кыргызской Республики «О Национальном архивном фонде Кыргызской Республики», нормативными правовыми актами в сфере архивного дела.

55. При поступлении заявки на прекращение эксплуатации ИС ГО или МСУ, УГО размещает соответствующие сведения в Реестре ГИЭУ.

56. Списание и (или) утилизация снятой с эксплуатации ИС ГО или МСУ осуществляются в соответствии с законодательством Кыргызской Республики о бухгалтерском учете и финансовой отчетности.  После списания ИС ГО или МСУ не используется.

57. Для обеспечения КБ:

1) на стадиях 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 элементы ГИЭУ, в том числе во время максимальных нагрузок;
* анализ влияния новой ИС на состояние КБ ГИЭУ;
* 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, из фазы тестирования в фазу опытной эксплуатации, 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.

**5. Требования к разрабатываемому или приобретаемому**

**прикладному программному обеспечению**

58. Требования к создаваемому или развиваемому прикладному ПО ИС определяются в техническом задании, создаваемом в соответствии с требованиями к технико-экономическим обоснованиям, техническим спецификациям, техническим заданиям на закупку (модернизацию) информационных систем и технологий для государственных и муниципальных органов, предприятий, учреждений, разрабатываемыми УГО.

      59. Разрабатываемое или приобретаемое готовое прикладное ПО:

* обеспечивает интерфейс пользователя, ввод, обработку и вывод данных на государственном, официальном и/или других языках при необходимости, с возможностью выбора пользователем языка интерфейса;
* учитывает требования: надежности; сопровождаемости; удобства использования; эффективности; универсальности; функциональности; кроссплатформенности;
* обеспечивает полнофункциональную поддержку технологии виртуализации;
* поддерживает кластеризацию;
* обеспечивается технической документацией по эксплуатации на государственном и официальном языках.

60. 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 КБ.

61. 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 КБ, 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.

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

63. Разработка прикладного ПО требует:

* учета особенностей, предусмотренных правилами реализации сервисной модели ГИЭУ;
* регламентации вопросов КБ в соглашениях на разработку ПО;
* управления рисками в процессе разработки прикладного ПО.

64. С целью обеспечения КБ:

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

* идентификации и аутентификации пользователей, при необходимости ЭП и регистрационных свидетельств;
* управления доступом;
* контроля целостности;
* журналирования действий пользователей, влияющих на КБ;
* защиты онлайновых транзакций;
* криптографической защиты информации с использованием СКЗИ соответствующего уровня при хранении, обработке;
* журналирования критичных событий ПО;

      2) в ТД КБ 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;

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

64. Мероприятия по контролю правомерности использования ПО определяются в ТД КБ, 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.

**6. Требования к технологической платформе**

      65. Выбор технологической платформы осуществляется с учетом приоритета оборудования, реализующего технологии виртуализации.        66. 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 или ресурсов;

3) совместимости:

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

67. ИС, включенные Реестр ГИ ЭУ, размещается на оборудовании, расположенном в серверном центре ГО.

    ГИ ЭУ обеспечивает:

* автоматизированное предоставление электронных услуг с единой точкой входа для их управления;
* виртуализацию вычислительных ресурсов серверного оборудования с использованием различных технологий;
* бесперебойное и отказоустойчивое функционирование предоставляемых электронных 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.

68. Для обеспечения КБ при использовании технологии виртуализации реализуются:

1) управление идентификацией, требующее:

* аутентификацию пользователей электронных услуг;
* 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 электронной услуги. Права доступа ограничиваются конкретными процедурами, определенными в ТД КБ 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 КБ, требующее:

* обязательности и регулярности процедур, определяемых в ТД КБ;
* 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 КБ;

5) регистрация событий КБ, требующая:

* журналирования действий администраторов;
* применения системы мониторинга инцидентов и событий КБ;
* оповещения на основе автоматического распознавания критического события или инцидента КБ;

6) управление инцидентами КБ, требующее:

* определения формального процесса обнаружения, выявления, оценки и порядка реагирования на инциденты КБ с актуализацией раз в полугодие;
* составления отчетов с периодичностью, определенной в ТД КБ, по результатам обнаружения, выявления, оценки и реагирования на инциденты КБ;
* уведомления ответственных лиц ГО, МСУ или организации об инцидентах КБ;
* регистрации инцидентов КБ в службе (подразделении) реагирования на компьютерные инциденты УГО и(или) уполномоченного государственного органа в сфере безопасности;

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 гипервизоров;
* физическое разделение сред эксплуатации от сред разработки и тестирования;
* определение в ТД КБ процедур управления изменениями для объектов информатизации;

8) определение в ТД КБ процедур восстановления после сбоев и отказов оборудования и ПО;

9) 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 c целью исключения доступа внешних пользователей к аппаратной части;
* логической изоляции между различными функциональными областями инфраструктуры среды виртуализации;
* физической изоляции между средами виртуализации ИС по уровню КБ.

7. **Требования к аппаратно-программному комплексу**

      69. Требования к конфигурации серверного оборудования АПК определяются в техническом задании на создание, закупку (модернизацию) информационных систем и технологий для государственных и муниципальных органов, предприятий, учреждений.

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

* с многопроцессорной архитектурой;
* позволяющих масштабировать ресурсы и увеличивать производительность;
* поддерживающих технологию виртуализации;
* включающих средства управления, изменения и перераспределения ресурсов;
* совместимых с используемой информационно-коммуникационной инфраструктурой.

71. Для обеспечения высокой доступности сервера применяются встроенные системы:

* горячей замены резервных вентиляторов, блоков питания, дисков и адаптеров ввода-вывода;
* динамической очистки и перераспределения страниц памяти;
* динамического перераспределения процессоров;
* оповещения о критических событиях;
* поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.

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

73. С целью обеспечения КБ на регулярной основе, определенной в ТД КБ, осуществляется инвентаризация серверного оборудования с проверкой его конфигурации.

74. Для обеспечения безопасности и качества обслуживания серверное оборудование АПК объектов ГИЭУ размещается только в серверном центре ГО в соответствии с требованиями к серверным помещениям, установленными в настоящих Требованиях.

75. Требования к системам хранения данных определяются в техническом задании на создание, закупку (модернизацию) информационных систем и технологий для государственных и муниципальных органов, предприятий, учреждений, и (или) технической спецификации на приобретение товаров, работ и услуг в сфере ЭУ.

76. Система хранения данных обеспечивает поддержку:

* единых средств для репликации данных;
* масштабируемости по объему хранения данных.

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

* сети хранения данных;
* системы хранения данных, поддерживающие систему виртуализации и (или) ярусного хранения данных.

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

* горячей замены резервных вентиляторов и блоков питания;
* горячей замены дисков и адаптеров ввода-вывода;
* оповещения о критических событиях;
* активных контроллеров (в количестве не менее двух);
* интерфейсов сети хранения данных (в количестве не менее двух портов на контроллер);
* поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.

79. Система хранения данных обеспечивается системой резервного копирования.

      80. Для обеспечения КБ, надежного хранения и возможности восстановления данных:

* применяется криптографическая защита хранимой служебной информации, конфиденциальной информации, специальных категорий персональных данных, содержащихся в базах данных ИС с использованием СКЗИ;
* используется выделенный сервер для защищенного хранения ключей шифрования по уровню безопасности не ниже уровня безопасности, используемых СКЗИ, установленного для криптографических ключей в Требованиях к СКЗИ;
* обеспечивается запись и испытание резервных копий в соответствии с регламентом резервного копирования, определенным в ТД КБ.

81. При выводе из эксплуатации носителей информации, используемых в ИС, содержащих в базах данных конфиденциальную информацию, специальные категории персональных данных, применяется программное и аппаратное обеспечение гарантированного уничтожения информации.

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

* требования, предъявляемые в техническом задании на разработку (модернизацию) прикладного ПО ИС или задании на проектирование СПП;
* соответствие типу операционных систем (клиентской или серверной);
* совместимость с используемым прикладным ПО;
* поддержка сетевых сервисов, функционирующих в сети телекоммуникаций;
* поддержка многозадачности;
* наличие средств получения и установки критичных обновлений и обновлений безопасности, выпускаемых производителем операционных систем;
* наличие средств диагностики, аудита и ведение журнала событий;
* поддержка технологий виртуализации.

      83. Приобретение системного ПО осуществляется с учетом приоритета:

* модели лицензирования, обеспечивающей снижение стоимости закупки, а также совокупной стоимости лицензии за период эксплуатации;
* ПО, обеспеченного технической поддержкой и сопровождением.

 84. С целью обеспечения КБ 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.

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

86. СПО предоставляется с открытым исходным кодом.

87. Используемое в ГО СПО дорабатывается с учетом поддержки форматов информационного взаимодействия через СЭМВ «Тундук».

88. Для обеспечения КБ при применении СПО:

* к использованию допускается СПО, поддерживаемое сообществом (ассоциацией) разработчиков СПО или прошедшее экспертизу и (или) сертификацию программного кода;
* сохраняются применявшиеся версии СПО.

**8. Требования к сетям телекоммуникаций**

89. Ведомственные (корпоративные) сети телекоммуникаций организуются путем объединения локальных сетей посредством выделенных собственных или арендованных каналов связи.

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

90. 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.

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

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

Управление оборудованием осуществляет оператор, предоставляющий выделенный канал.

      В настройках оборудования неиспользуемые порты блокируются.

      93. В целях обеспечения КБ:

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 МСУ между собой используются:

* средства разделения и изоляции информационных потоков;
* оборудование с компонентами, обеспечивающими КБ и безопасное управление;
* выделенные и интегрированные с оборудованием доступа межсетевые экраны, установленные в каждой точке подключения, с целью защиты периметра ГО.

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

4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей ГО или МСУ к Интернету использует услуги оператора связи, предоставившего подключение;

5) служащие ГО, МСУ и работники государственных организаций, предприятий, учреждений, а также владельцы стратегических объектов, объектов КИИ 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 ГО, его структурных и территориальных подразделений, МСУ размещается в доменных зонах gov.kg.

94. В ГО или МСУ допускается применение устройств для организации беспроводного доступа только к общедоступным ГИР, в местах, разрешенных для пребывания посетителей ГО или МСУ в "гостевой зоне".

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

96. Оператор ГИ ЭУ по заявкам ГО и МСУ осуществляет:

* распределение, регистрацию и перерегистрацию IP-адресов локальных сетей ГО и МСУ, подключенных к ГИЭУ, по заявкам ГО или МСУ;
* регистрацию доменных имен в доменных зонах Интернета gov.kg по заявкам ГО или МCУ;
* регистрацию доменных имен в сети ГИ ЭУ по заявкам ГО или МСУ;
* предоставление сервиса DNS в сети ГИЭУ.

97. ГО и МСУ ежегодно:

* запрашивают у УГО/оператора ГИЭУ перечень используемых на оборудовании ГИ ЭУ категорий интернет-ресурсов;
* выбирают из вышеуказанного перечня категории интернет-ресурсов, доступ к которым ограничивается для служащих ГО и МСУ, и составляют их список;
* направляют в УГО/оператору ГИЭУ вышеуказанный список и списки сетевых адресов информационно-коммуникационных сетей ГО и их территориальных подразделений, МСУ, получающих доступ к Интернету, для применения на оборудовании ГИЭУ.

98. УГО/оператор ГИЭУ осуществляет делегирование (обслуживание) доменных зон gov.kg с предоставлением сервиса в Интернете.

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

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

101. Все элементы кабельной системы подлежат маркировке. Все кабельные соединения регистрируются в журнале учета кабельных соединений.

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

103. Для обеспечения КБ:

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

2) разрабатывается и утверждается ТД КБ, 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, ГИС, содержащих специальные категории персональных данных, биометрические данные, 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 законодательством Кыргызской Республики;

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;
* физической защиты каналов передачи данных и сетевого оборудования;
* регистрации событий КБ;
* мониторинга и анализа сетевого трафика;
* управления сетью;

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

6) осуществляется взаимодействие локальных сетей центрального ГО и его территориальных подразделений между собой только через ГИЭУ, 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 МСУ между собой;

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

9) осуществляется соединение ЛС внешнего контура ГО и МСУ с Интернетом только через СЭМВ “Тундук”. Подключение к Интернету иным способом не допускается, за исключением специальных и правоохранительных ГО в оперативных целях.

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

Сервера инфраструктуры точного времени синхронизируются с сервером инфраструктуры точного времени верхнего уровня. Сервера инфраструктуры точного времени предоставляют доступ клиентам для синхронизации времени.

**9. Требования к системам бесперебойного функционирования технических средств и кибербезопасности**

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

105. 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.

106. 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.

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

108. 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.

109. 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.

110. Серверное помещение надежно защищается от внешнего электромагнитного излучения.

111. При размещении оборудования:

* обеспечивается исполнение правил технической эксплуатации электроустановок потребителей, утвержденных уполномоченным органом в сфере энергетики;
* обеспечивается исполнение требований поставщиков и (или) производителя оборудования к установке (монтажу), нагрузке на перекрытия и фальшпол, с учетом веса оборудования и коммуникаций;
* обеспечивается наличие свободных служебных проходов для обслуживания оборудования;
* учитывается организация воздушных потоков системы обеспечения микроклимата;
* учитывается организация системы фальшполов и фальшпотолков.

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

* обслуживание оборудования;
* устранение проблем, возникающих при работе аппаратно-программного обеспечения;
* факты сбоев и отказов, а также результаты восстановительных работ;
* послегарантийное обслуживание критически важного оборудования по истечении гарантийного срока обслуживания.

      Форма и способ документирования определяются самостоятельно.

113. Обслуживание критически важного оборудования выполняется сертифицированным техническим персоналом.

114. 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.

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

116. 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.

  117. С целью обеспечения КБ, отказоустойчивости и надежности функционирования:

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

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

3) серверное помещение оборудуется системами:

* контроля и управления доступом;
* обеспечения микроклимата;
* охранной сигнализации;
* видеонаблюдения;
* пожарной сигнализации;
* пожаротушения;
* гарантированного электропитания;
* заземления;

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

118. 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.

119. 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 200 С до 250 С 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.

120. 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.

121. 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

122. 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.

123. Система пожаротушения серверного помещения оборудуется автоматической установкой пожаротушения, независимой от системы пожаротушения здания.

Установка 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.

124. 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.

125. 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).

Приложение 1

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**к средствам криптографической защиты информации**

**Глава 1. Общие положения**

 1. Настоящий документ устанавливает общие технические требования к средствам криптографической защиты информации (далее – СКЗИ) как к технологически завершенным аппаратным, программным или аппаратно-программным средствам, независимо от страны производства и/или реализованных в СКЗИ алгоритмов криптографических преобразований, за исключением средств криптографической защиты информации, предназначенные в качестве основной меры защиты для сохранения конфиденциальности сведений, составляющих государственные секреты Кыргызской Республики.

 2. Настоящие Технические требования применяются для целей оценки соответствия средств криптографической защиты информации в порядке установленного настоящими техническими требованиями.

 3. СКЗИ предназначены для:

- сохранения конфиденциальности данных при помощи технологий криптографической защиты информации;

- аутентификации, в том числе контроля целостности данных, при помощи имитовставки и (или) электронной подписи;

- генерации, формирования, распределения ключей и (или) управления ключами.

 4. В настоящих Технических требованиях применяются следующие термины:

 **алгоритм криптографического преобразования** - набор конечного числа простых и однозначно определенных правил, зависящих от изменяемого параметра (ключа) и задающих последовательность выполнения операций для решения задачи криптографического преобразования;

**асимметричный алгоритм криптографического преобразования -** алгоритм криптографического преобразования, в котором прямое и обратное преобразования используют открытый и секретный ключи, взаимосвязанные таким образом, что вычислительно сложно определить секретный ключ из открытого ключа;

**аутентификация** - установление подлинности одного или нескольких аспектов информационного взаимодействия: сеанса связи, его времени, связывающихся сторон, передаваемых сообщений, источника данных, времени создания данных, содержания данных;

**доступность информации** - свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать;

**имитовставка** - строка бит фиксированной длины, полученная по определенному правилу из данных и ключа, добавленная к данным для обеспечения имитозащиты;

**имитозащита -** защита системы связи от навязывания ложных сообщений;

**информация -** сведения (сообщения, данные) независимо от формы их представления;

**ключ** СКЗИ - конкретное секретное или открытое (если специально указано) состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований;

**конфиденциальность информации** - свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право;

**криптографическая стойкость средства криптографической защиты информации -** вычислительная сложность метода (алгоритма) вскрытия криптографической защиты, наилучшего для данного средства криптографической защиты информации;

**криптографическое преобразование -** преобразование данных при помощи шифрования, выработки (проверки) имитовставки или формирования (проверки) электронной подписи;

**предварительное шифрование -** шифрование, технически реализованное отдельно от передачи зашифрованных данных по каналам связи;

**симметричный алгоритм криптографического преобразования -** алгоритм криптографического преобразования, в котором прямое и обратное преобразования используют один и тот же ключ или два ключа, каждый из которых легко вычисляется из другого;

**средство криптографической защиты** информации (СКЗИ) - средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;

**электронная подпись (ЭП) -** информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация;

**целостность информации** - свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

**Глава 2. Уровни безопасности СКЗИ**

 5. В зависимости от криптографической стойкости для СКЗИ устанавливаются 4 уровня безопасности:

 5.1. **СКЗИ первого уровня безопасности** предназначены для защиты информации, вред от разглашения или нарушения конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же СКЗИ (одних и тех же СКЗИ), не может быть причинен (не влечет негативных последствий в социальной, политической, международной, экономической, финансовой или иных областях деятельности) (коэффициент 0);

5.2. **СКЗИ второго уровня безопасности** предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же СКЗИ (одних и тех же СКЗИ) незначителен – менее 1 000 расчетных показателей (влечет незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), легко компенсируем оператором информационной системы и/или обладателем информации, которые могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств  (коэффициент 1);

5.3. **СКЗИ третьего уровня безопасности** предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же СКЗИ (одних и тех же СКЗИ), значителен – от 1 000 до 5 000 расчетных показателей (влечет умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), который может быть компенсирован оператором информационной системы и/или обладателем информации, которые могут выполнять хотя бы одну из возложенных на них функций (коэффициент 2);

5.4. **СКЗИ четвертого уровня безопасности** предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же СКЗИ (одних и тех же СКЗИ), является критическим – более 5 000 расчетных показателей (влечет существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), не может быть компенсирован оператором информационной системы и/или обладателем информации, которые не могут выполнять возложенные на них функции (коэффициент 3).

6. СКЗИ не могут быть признаны соответствующими первому, второму, третьему или четвертому уровню безопасности, если **вычислительная сложност**ь существующих алгоритмов вскрытия криптографической защиты, обеспечиваемой ими, составляет менее 250, 280, 2120 или 2160  возможных комбинаций для перебора соответственно.

**Глава 3. Общие технические требования к СКЗИ по уровням безопасности**

 7. Генерируемые СКЗИ ключи (кроме открытых ключей) должны представлять собой последовательности случайных чисел, формируемые с помощью физических генераторов шума (например, тепловых, диодных, радиационных, импульсных), либо последовательности псевдослучайных чисел, формируемые с использованием случайных событий (например, системных параметров ЭВМ, движений мыши, нажатий клавиатуры, состояния таймера).

8. СКЗИ, использующие распределение ключей по незащищенным каналам связи, должны обеспечивать криптографическую защиту ключей в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также навязывания ложных ключей.

8. Любой используемый СКЗИ ключ должен применяться только одним алгоритмом криптографического преобразования, например, только для шифрования или только для формирования электронной подписи.

9. Должна обеспечиваться защита от несанкционированного изменения СКЗИ, в том числе от модификации или подмены их элементов и модулей, с целью исключения влияния на криптографическую стойкость СКЗИ.

10. Техническая документация (конструкторская, технологическая и программная документация, в зависимости от вида СКЗИ) должна содержать полное описание реализованных в СКЗИ алгоритмов криптографических преобразований, генерации, формирования, распределения и управления ключами.

11. Если в СКЗИ реализованы алгоритмы криптографических преобразований, определенные государственными и межгосударственными стандартами или другими документами, действующими или применяемыми в Кыргызской Республики в установленном порядке, то в технической документации вместо их полного описания допускается делать ссылки на данные документы.

12. СКЗИ должны реализовывать алгоритмы криптографических преобразований в точном соответствии с их описанием, приведенным в технической документации.

13. В каждый комплект СКЗИ должна входить эксплуатационная документация, которая полно и адекватно описывает все возможные режимы их использования и содержит перечень всех организационных и технических мер, необходимых для обеспечения безопасности обрабатываемой информации, включая порядок и частоту смены ключей, порядок технического обслуживания СКЗИ и действия, которые необходимо предпринять для устранения ошибок оператора и других нештатных ситуаций, возможных во время эксплуатации, а также их последствий.

14. **Требования к СКЗИ первого уровня безопасности:**

14.1. Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 60 бит.

14.2. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 120 бит.

14.3. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 500 бит.

14.4. Длина вычисляемого СКЗИ хэш-кода должна быть не менее 120 бит.

14.5. Длина формируемой СКЗИ ЭП должна быть не менее 120 бит.

14.6. Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,50 ± 0,03).

**15. Требования к СКЗИ второго уровня безопасности:**

15.1. Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 100 бит.

15.2. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 160 бит.

15.3. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 1500 бит.

15.4. Длина вычисляемого СКЗИ хэш-кода должна быть не менее 160 бит.

15.5. Длина формируемой СКЗИ ЭП должна быть не менее 200 бит.

15.6. Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,50 ± 0,01).

15.7. СКЗИ должны реализовывать процедуры вычисления и проверки контрольной информации о ключах в целях предотвращения использования случайно искаженных на этапе распределения и загрузки ключей с вероятностью не менее 0,9999.

15.8. При предварительном шифровании СКЗИ должны реализовывать процедуры вычисления и проверки контрольной информации о шифруемых данных в целях выявления случайно искаженных зашифрованных данных с вероятностью не менее 0,9999.

15.9. СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования.

**16. Требования к СКЗИ третьего уровня безопасности:**

16.1. Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 150 бит.

15.2. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 250 бит.

16.3. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 4000 бит.

16.4. Длина вычисляемого СКЗИ хэш-кода должна быть не менее 250 бит.

16.5. Длина формируемой СКЗИ ЭП должна быть не менее 300 бит.

16.6. Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,500 ± 0,003), при этом ключи должны быть последовательностями случайных чисел и формироваться с помощью физических генераторов шума.

16.7. СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭП для ключей в целях предотвращения использования случайно или умышленно искаженных на этапе распределения и загрузки ключей с вероятностью не менее 0,999999.

16.8. При предварительном шифровании СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭП для шифруемых данных в целях выявления случайно или умышленно искаженных зашифрованных данных с вероятностью не менее 0,999999.

16.9. СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования и других нештатных ситуациях.

16.10 СКЗИ должны обеспечивать иерархическую криптографическую защиту ключей на этапе их распределения и управления в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также навязывания ложных ключей, или эксплуатационная документация СКЗИ должна содержать организационные и технические меры по обеспечению защиты от данных угроз.

16.11. Реализуемые СКЗИ штатные процедуры удаления (уничтожения) ключей должны гарантировать невозможность их восстановления.

**17. Требования к СКЗИ четвертого уровня безопасности:**

17.1. Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 200 бит.

17.2. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 400 бит.

17.3. Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 8000 бит.

17.4. Длина вычисляемого СКЗИ хэш-кода должна быть не менее 400 бит.

17.5. Длина формируемой СКЗИ ЭП должна быть не менее 400 бит.

17.6. Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,500 ± 0,001), при этом ключи должны быть последовательностями случайных чисел и формироваться с помощью физических генераторов шума.

17.7. СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭП для ключей в целях предотвращения использования случайно или умышленно искаженных на этапе распределения и загрузки ключей, с вероятностью не менее 0,999999999.

17.8. СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭП для шифруемых данных в целях выявления случайно или умышленно искаженных зашифрованных данных с вероятностью не менее 0,999999999.

17.9. СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования и других нештатных ситуациях, предотвращать транзит через себя открытых данных в область хранения, распределения и последующей обработки зашифрованных данных.

17.10. СКЗИ должны обеспечивать иерархическую криптографическую защиту ключей на этапе их распределения и управления в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также от навязывания ложных ключей.

17.11. Реализуемые СКЗИ штатные процедуры удаления (уничтожения) ключей должны гарантировать невозможность их восстановления. Если СКЗИ не реализуют указанных процедур, то эти процедуры гарантированного удаления (уничтожения) ключей (кроме открытых ключей) должны быть реализованы техническими средствами, поставляемыми в комплекте с СКЗИ.

Приложение 2

**ПЕРЕЧЕНЬ**

**технологий, изложенных в международных стандартах, для государственных информационных систем, использующих системы шифрования и средства криптографической защиты информации (СКЗИ), за исключением информации, отнесенной к государственным секретам**

1. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.»;
2. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки ЭЦП.»;
3. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования.»;
4. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры
5. ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров
6. ГОСТ 34.310-2004 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
7. ГОСТ 34.311-2004 «Информационная технология. Криптографическая защита информации. Функция хеширования»;
8. RFC 3647 Certificate Policy and Certification Practices Framework (серии международных стандартов IETF);
9. RFC 5280 из серии международных стандартов IETF (регулирующий требования к структуре регистрационных свидетельств и списку отозванных регистрационных свидетельств)
10. RFC 3280 из серии международных стандартов IETF (Certificate and Certificate Revocation List (CRL) Profile)
11. RFC 1422 из серии международных стандартов IETF
12. RFC 3029 Data Validation and Certification Server Protocols серии международных стандартов I ETF
13. Серия стандартов ITU-T Х.500 версии 3 (ITU-T X.509, ITU-T X.501)
14. RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
15. RFC 5816 - update of RFC 3161
16. RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
17. RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2
18. RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1
19. (RFC 4033, RFC 4034, RFC 4035) DNSSEC
20. Associated Signature Containers (ASiC) (ETSI EN 319 162-1 V1.1.1 (2016-04)
21. XML Advanced Electronic Signatures ETSI EN 319 132-1 V1.1.0
22. RFC 4253 SSH
23. RFC 3447 - (PKCS) #1: RSA Cryptography Specifications Version 2.1
24. ISO/IEC 18033-3:2005 для AES
25. ISO/IES 10118-3 для SHA-1, SHA-256, SHA-384, SHA-512
26. RFC 2104 HMAC (для имитовставок)
27. ISO/IEC 9797-1 CMAC, CBC-MAC (для имитовставок)
28. ISO/IEC 14888-3:2016