

**Об утверждении критериев оценки степени риска и проверочных листов в сфере информатизации в части обеспечения информационной безопасности**

Совместный приказ Заместителя Премьер-Министра Республики Казахстан - Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12. Зарегистрирован в Министерстве юстиции Республики Казахстан 6 февраля 2019 года № 18269.

      В соответствии с пунктом 3 статьи 141 и пунктом 1 статьи 143 Предпринимательского кодекса Республики Казахстан от 29 октября 2015 года, ПРИКАЗЫВАЕМ:

      1. Утвердить:

      1) Исключен совместным приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).  
      2) Исключен совместным приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).

      3) проверочный лист в сфере информатизации в части обеспечения информационной безопасности в отношении государственных юридических лиц, субъектов квазигосударственного сектора, собственников и владельцев негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственников и владельцев критически важных объектов информационно-коммуникационной инфраструктуры согласно приложению 3 к настоящему совместному приказу.

      Сноска. Пункт 1 с изменениями, внесенными совместным приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).

      2. Комитету по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

      1) государственную регистрацию настоящего совместного приказа в Министерстве юстиции Республики Казахстан;

      2) в течение десяти календарных дней со дня государственной регистрации настоящего совместного приказа направление его на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

      3) размещение копии настоящего совместного приказа на интернет - ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан.

      3. Контроль за исполнением настоящего совместного приказа возложить на курирующего вице-министра оборонной и аэрокосмической промышленности Республики Казахстан.

      4. Настоящий совместный приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

|  |  |
| --- | --- |
| *Заместитель Премьер-Министра*  *Республики Казахстан –*  *Министр оборонной и аэрокосмической*  *промышленности Республики Казахстан*  *\_\_\_\_\_\_\_\_\_\_\_\_* | *А. Жумагалиев* |
| *Министр национальной экономики*  *Республики Казахстан \_\_\_\_\_\_\_\_\_\_\_* | *Т. Сулейменов* |

      "СОГЛАСОВАН"

Комитет по правовой статистике

и специальным учетам

Генеральной прокуратуры

Республики Казахстан

|  |  |
| --- | --- |
|  | Приложение 1 к совместному приказу Заместителя Премьер-Министра Республики Казахстан – Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12 |

**Критерии оценки степени риска в сфере информатизации в части обеспечения информационной безопасности**

      Сноска. Приложение 1 утратило силу совместным приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).

|  |  |
| --- | --- |
|  | Приложение 2 к совместному приказу Заместителя Премьер-Министра Республики Казахстан – Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12 |

**Проверочный лист в сфере информатизации в части обеспечения информационной безопасности в отношении государственных и местных исполнительных органов**

      Сноска. Приложение 2 утратило силу совместным приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).

|  |  |
| --- | --- |
|  | Приложение 3 к совместному приказу Заместителя Премьер-Министра Республики Казахстан – Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12 |

      Сноска. Приложение 3 – в редакции совместного приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 20.01.2023 № 21/НҚ и Министра национальной экономики РК от 23.01.2023 № 8 (вводится в действие c 01.01.2023).

**Проверочный лист в сфере информатизации в части обеспечения информационной безопасности**  
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  
**в соответствии со статьей 138**

      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Предпринимательского кодекса Республики Казахстан

в отношении: государственных юридических лиц, субъектов

квазигосударственного сектора, собственников и владельцев негосударственных

информационных систем, интегрируемых с информационными системами

государственных органов или предназначенных для формирования государственных

электронных информационных ресурсов, а также собственников и владельцев

критически важных объектов информационно-коммуникационной инфраструктуры

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование однородной группы субъектов (объектов) контроля

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Государственный орган, назначивший проверку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Акт о назначении проверки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

№, дата

Наименование субъекта (объекта) контроля \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Индивидуальный идентификационный номер), бизнес-идентификационный номер

субъекта (объекта) контроля \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес места нахождения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| № | Перечень требований | Соответствует требованиям | Не соответствует требованиям |
| 1 | 2 | 3 | 4 |
| 1 | Соблюдение требования по осуществлению подключения локальных, ведомственных и корпоративных сетей телекоммуникаций государственных органов, местным исполнительным органом, государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцев критически важных объектов информационно-коммуникационной инфраструктуры (далее - ИКИ) к Интернету операторами связи через единый шлюз доступа к Интернету |  |  |
| 2 | Соблюдение требования по оповещению владельцем критически важных объектов информационно-коммуникационной инфраструктуры Национального координационного центра информационной безопасности об инцидентах информационной безопасности и о результатах реагирования на них |  |  |
| 3 | Соблюдение требования по применению средств:  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 |  |  |
| 4 | Соблюдение требования мониторинга обеспечения ИБ, защиты и безопасного функционирования при эксплуатации объектов информатизации |  |  |
| 5 | Наличие антивирусных средств, обновлений операционных систем на рабочих станциях, подключенных к сети Интернет при организации доступа к Интернету из локальных сетей внешнего контура |  |  |
| 6 | Наличие подразделения ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определение должностного лица, ответственного за обеспечение ИБ, с прохождением специализированных курсов в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата |  |  |
| 7 | Наличие и соответствие нормативно-технической документации (далее – ТД) по обеспечению ИБ, в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется государственные органы (далее - ГО), местным исполнительным органом (далее - МИО) или организация в своей деятельности.  ТД ИБ разрабатывается на казахском и русском языках, утверждается правовым актом ГО, МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации. ТД ИБ пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.  1. Политика ИБ ГО, МИО или организации является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ.  2. В перечень документов второго уровня входят документы, детализирующие требования политики ИБ ГО, МИО или организации, в том числе:  1) методика оценки рисков ИБ;  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 (далее - СКЗИ);  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.  3. 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.  4. Перечень документов четвертого уровня включает рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения выполненных процедур и работ, в том числе:  1) журнал регистрации инцидентов ИБ и учета внештатных ситуаций;  2) журнал посещения серверных помещений;  3) отчет о проведении оценки уязвимости сетевых ресурсов;  4) журнал учета кабельных соединений;  5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;  6) журнал учета изменений конфигурации оборудования, тестирования и учета изменений свободного программного обеспечения (далее - СПО) и прикладного программного обеспечения (далее - ППО) информационных систем (далее - ИС), регистрации и устранения уязвимостей программного обеспечения (далее - ПО);  7) журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;  8) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений |  |  |
| 8 | Соблюдение требования при доступе к объектам информатизации первого и второго классов в соответствии с классификатором по применению многофакторной аутентификации, в том числе с использованием электронной цифровой подписи |  |  |
| 9 | Соблюдение требования по внесению в должностные инструкции и (или) условия трудового договора функциональных обязанностей по обеспечению ИБ и обязательств по исполнению требований ТД ИБ служащих ГО, МИО или работников организации |  |  |
| 10 | Соблюдение требования по применению СКЗИ |  |  |
| 11 | Соблюдение требования по хранению, восстановлению государственных электронных информационных ресурсов, содержащихся в информационной системе, сохранности государственных электронных информационных ресурсов |  |  |
| 12 | Соблюдение требования для обеспечения ИБ информационных ресурсов (далее – ИБ ИР) по применению  систем управления содержимым (контентом), выполняющая:  санкционирование операций размещения, изменения и удаления в электронных информационных ресурсах (далее – 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 |  |  |
| 13 | Соблюдение требования по применению регистрационных свидетельств для проверки подлинности доменного имени и криптографической защиты содержимого сеанса связи с использованием СКЗИ при обеспечении ИБ ИР |  |  |
| 14 | Соблюдения требования по управлению идентификацией при использовании технологии виртуализации:  аутентификация клиентов информационно-коммуникационных 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 |  |  |
| 15 | Соблюдение требования по проведению аудита событий ИБ при использовании технологии виртуализации:  обязательность и регулярность 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 |  |  |
| 16 | Соблюдение требования регистрации событий ИБ при использовании технологии виртуализации:  журналирования действий администраторов;  применения системы мониторинга инцидентов и событий ИБ;  оповещения на основе автоматического распознавания критического события или инцидента ИБ |  |  |
| 17 | Соблюдение требования по исполнению процедур сетевого и системного администрирования:  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 |  |  |
| 18 | Соблюдение требования по обеспечению системы хранения данных системой резервного копирования |  |  |
| 19 | Соблюдение требования по применению программно-технических средств защиты информации, в том числе криптографического шифрования, с использованием СКЗИ при организации выделенного канала связи, объединяющего локальные сети |  |  |
| 20 | Соблюдение требования по исключению сопряжения ЛС внутреннего контура и ЛС внешнего контура между собой, за исключением организованных каналов связи с использованием СКЗИ |  |  |
| 21 | Соблюдение требовании по использованию  ведомственной электронной почты, службы мгновенных сообщений и иных сервисов; электронной почты, службы мгновенных сообщений и иных сервисов, центры управления и сервера которых физически размещены на территории Республики Казахстан, если иное не установлено уполномоченным органом, для осуществления оперативного информационного обмена в электронной форме служащими ГО, МИО и работниками государственных юридических лиц, субъектами квазигосударственного сектора, а также владельцами критически важных объектов информационно-коммуникационной инфраструктуры (далее - ИКИ) при исполнении ими служебных обязанностей |  |  |
| 22 | Наличие бесперебойного электропитания для активного оборудования локальных сетей |  |  |
| 23 | Соблюдение требования по физическому отключению неиспользуемых портов кабельной системы локальной сети от активного оборудования |  |  |
| 24 | Соблюдение требования по применению межсетевого экранирования |  |  |
| 25 | Наличие документирования при техническом сопровождении оборудования, установленного в серверном помещении:  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 |  |  |
| 26 | Наличие системы контроля и управления доступом в серверном помещении обеспечивающие 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 |  |  |
| 27 | Наличие в актуальном состоянии списка лиц, авторизованных для осуществления сопровождения объектов ИКИ, установленных в серверном помещении |  |  |
| 28 | Наличие системы обеспечения микроклимата в серверном помещении:  система обеспечения микроклимата включает системы кондиционирования, вентиляции и мониторинга микроклимата;  система кондиционирования воздуха обеспечивается резервированием;  электропитание кондиционеров серверного помещения осуществляется от системы гарантированного электропитания или системы бесперебойного электропитания;  системы кондиционирования и вентиляции отключаются автоматически по сигналу пожарной сигнализации |  |  |
| 29 | Наличие системы охранной сигнализации в серверном помещении:  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 |  |  |
| 30 | Наличие системы видеонаблюдения в серверном помещении:  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 |  |  |
| 31 | Наличие системы пожарной сигнализации в серверном помещении:  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 |  |  |
| 32 | Наличие системы пожаротушения в серверном помещении:  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;  оповещение о срабатывании системы пожаротушения выводится на табло, размещаемые внутри и снаружи помещения. |  |  |
| 33 | Наличие системы гарантированного электропитания в серверном помещении:  все источники электроэнергии подаются на автомат ввода резерва, осуществляющий автоматическое переключение на резервный ввод электропитания при прекращении, перерыве подачи электропитания на основном вводе;  система гарантированного электропитания предусматривает электроснабжение оборудования и систем серверного помещения через источники бесперебойного питания |  |  |
| 34 | Наличие системы заземления в серверном помещении:  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) |  |  |
| 35 | Отсутствие мощных источников электромагнитных помех (трансформаторов, электрических щитов, электродвигателей и прочее) в кроссовом помещении |  |  |
| 36 | Отсутствие труб и вентилей системы водоснабжения в кроссовом помещении |  |  |
| 37 | Наличие систем пожарной безопасности в кроссовом помещении |  |  |
| 38 | Отсутствие легко возгораемых материалов (деревянные стеллажи, картон, книги и прочее) в кроссовом помещении |  |  |
| 39 | Наличие в кроссовом помещении отдельной линии электропитания от отдельного автомата для подключения шкафа по проекту |  |  |
| 40 | Наличие в кроссовом помещении систем охранной сигнализации, контроля доступа |  |  |
| 41 | Наличие в кроссовом помещении системы кондиционирования |  |  |
| 42 | На этапе опытной и промышленной эксплуатации объектов информатизации используются средства и системы:  мониторинга и управления инцидентами и событиями ИБ информационной инфраструктурой;  обнаружения и предотвращения вторжений |  |  |
| 43 | Соблюдение требований по созданию собственного оперативного центра информационной безопасности и обеспечению его функционирования или приобретению услуг оперативного центра информационной безопасности у третьих лиц, а также взаимодействие его с Национальным координационным центром информационной безопасности |  |  |
| 44 | Соблюдение требования по размещению на Интернет-ресурсе с зарегистрированным доменным именем .KZ и (или) .ҚАЗ на аппаратно-программном комплексе, который расположен на территории Республики Казахстан.  Использование доменных имен .KZ и (или).ҚАЗ в пространстве казахстанского сегмента Интернета при передаче данных Интернет-ресурсами осуществляется с применением сертификатов безопасности |  |  |
| 45 | Соблюдение требования по проведению на регулярной основе инвентаризации серверного оборудования с проверкой его конфигурации |  |  |
| 46 | Соблюдение требований по приобретению товаров в целях реализации требований обеспечения ИБ для обороны страны и безопасности государства из реестра доверенного программного обеспечения и продукции электронной промышленности.  При этом, в случае отсутствия в реестре доверенного программного обеспечения и продукции электронной промышленности необходимой продукции, допускается приобретение товаров |  |  |
| 47 | Соблюдение требований по контролю событий нарушений ИБ в ГО, МИО или организации:  1) проведение мониторинга событий, связанных с нарушением ИБ, и анализ результатов мониторинга;  2) регистрация 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) обеспечение синхронизации времени журналов регистрации событий с инфраструктурой источника времени;  4) хранение журналов регистрации событий в течение срока, указанного в ТД ИБ, но не менее трех лет и находятся в оперативном доступе не менее двух месяцев;  5) ведение журналов регистрации событий  6) обеспечение защиты журналов регистрации событий от вмешательства и неавторизированного доступа. Не допущение наличие у системных администраторов полномочий на изменение, удаление и отключение журналов. Для конфиденциальных ИС требуются создание и ведение резервного хранилища журналов;  7) обеспечение внедрения формализованной процедуры информирования об инцидентах ИБ и реагирования на инциденты ИБ |  |  |
| 48 | Наличие соглашения, в котором устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение при привлечении сторонних организаций к обеспечению информационной безопасности ЭИР, ИС, ИКИ |  |  |
| 49 | Соблюдение требований при увольнении или внесении изменений в условия трудового договора права доступа служащего ГО, МИО или работника организации к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего служащего ГО, МИО или работника организации, аннулируются после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора |  |  |
| 50 | Соблюдение требования кадровой службой организации и ведения учета прохождения служащими ГО, МИО или работниками организаций обучения в сфере информатизации и области обеспечения ИБ |  |  |
| 51 | Соблюдение требования по регистрации в службе реагирования на компьютерные инциденты государственной технической службы событий, идентифицированных как критические для конфиденциальности, доступности и целостности  по результатам анализа мониторинга событий ИБ и анализа журнала событий |  |  |
| 52 | Соблюдение требования по проведению аудита ИБ не реже одного раз в год, владельцам критически важных объектов ИКИ, обрабатывающий данные, содержащие охраняемую законом тайну, за исключением банков второго уровня |  |  |
| 53 | Соблюдение требования при списании ИС, ПО или сервисного программного продукта по обеспечению сохранения структуры и содержания базы данных посредством встроенного функционала системы управления базы данных списываемой ИС с подготовкой инструкции по восстановлению ЭИР |  |  |
| 54 | Наличие акта с положительным результатом испытаний на соответствие требованиям ИБ |  |  |
| 55 | Соблюдение требования по обеспечению разрабатываемого или приобретаемого готового прикладного ПО  интерфейсом пользователя, ввод, обработку и вывод данных на казахском, русском и других языках, по необходимости, с возможностью выбора пользователем языка интерфейса |  |  |
| 56 | Соблюдение требования по осуществлению мониторинга:  действий пользователей и персонала;  использования средств обработки информации |  |  |
| 57 | Соблюдение требования по обеспечению разрабатываемого или приобретаемого готового прикладного ПО технической документацией по эксплуатации на казахском и русском языках |  |  |
| 58 | Соблюдение требования по обеспечению высокой доступности сервера встроенных систем:  1) горячей замены резервных вентиляторов, блоков питания, дисков и адаптеров ввода-вывода;  2) оповещения о критических событиях;  3) поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей |  |  |
| 59 | Наличие программного и аппаратного обеспечения гарантированного уничтожения информации при выводе из эксплуатации носителей информации, используемых в конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа |  |  |
| 60 | Наличие схемы локальной сети |  |  |
| 61 | Наличие в серверном помещении серверное оборудование аппаратно-программный комплекс и системы хранения данных |  |  |
| 62 | Соблюдение требования по расположению серверного помещения 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 |  |  |
| 63 | Наличие в серверном помещений фальшпола и (или) фальшпотолка для размещения кабельных систем и инженерных коммуникаций |  |  |
| 64 | Соблюдение требования по исключению через серверное помещение 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 |  |  |
| 65 | Соблюдение требования по расположению основных и резервных серверных помещений на безопасном расстоянии в удаленных друг от друга зданиях. Требования к резервным серверным помещениям идентичны требованиям к основным серверным помещениям |  |  |
| 66 | Соблюдение требования по исключению в серверном помещении размещения в одной виртуальной среде, одном серверном оборудовании, одном монтажном шкафу или стойке ЭИР, ИР, СПП, ИС, относящихся в соответствии с классификатором объектов информатизации первого класса с объектами информатизации второго и третьего класса |  |  |

      Должностное (ые) лицо (а)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

должность подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество (при наличии)

Руководитель субъекта контроля

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

должность подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество (при наличии)

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан