Об утверждении Методики проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности

Утративший силу

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 51/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 11 апреля 2018 года № 16744. Утратил силу приказом Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 15 июня 2019 года № 131/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования)

Сноска. Утратил силу приказом Министра цифрового развития, оборонной и аэрокосмической промышленности РК от 15.06.2019 № 131/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с подпунктом 6) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Методику проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности.

2. Признать утратившим силу приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 108 "Об утверждении Методики проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13236, опубликован 4 марта 2016 года в информационно-правовой системе "Әділет").

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

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

2) в течение десяти календарных дней со дня государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан направление его копии в бумажном и электронном виде 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) в течение десяти календарных дней после государственной регистрации настоящего приказа направление его копии на официальное опубликование в периодические печатные издания;

4) размещение настоящего приказа на интернет-ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

5) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства оборонной и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, согласно подпунктам 1), 2),3) и 4) настоящего пункта.

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

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

Министр оборонной и аэрокосмической промышленности Республики Казахстан *Б. Атамкулов*

Утверждена
приказом Министра оборонной
и аэрокосмической промышленности
Республики Казахстан
от 28 марта 2018 года № 51/НҚ

Методика проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности

Глава 1. Общие положения

1. Настоящая Методика проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса государственного органа на

соответствие требованиям информационной безопасности (далее – Методика) разработана в соответствии с подпунктом 6) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и Правилами проведения аттестации информационной системы, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности, утвержденными постановлением Правительства Республики Казахстан от 23 мая 2016 года № 298.

2. Настоящая Методика предназначена для проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности.

3. В настоящей Методике используются следующие определения и сокращения:

1) информационные активы – базы данных, системная документация, руководства пользователя, учетные материалы, процедуры эксплуатации или поддержки объекта аттестации, планы по обеспечению непрерывности функционирования информационного обеспечения и другая документация;

2) информационная система (далее – ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

3) аттестация информационной системы, информационно-коммуникационной платформы "электронного правительства" и интернет-ресурса государственного органа на соответствие требованиям информационной безопасности (далее – аттестация) – организационно-технические мероприятия по определению состояния защищенности объектов аттестации, а также их соответствия требованиям информационной безопасности;

4) техническая документация по информационной безопасности (далее – ТД по ИБ) – совокупность документов, разработанных в соответствии с едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – ЕТ) и регламентирующих общие требования, принципы и правила по обеспечению информационной безопасности объекта аттестации;

5) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных

информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

6) аутентификация – проверка принадлежности пользователю (субъекту доступа) предъявленного им идентификатора и подтверждение его подлинности;

7) объекты аттестации – информационная система, информационно-коммуникационная платформа "электронного правительства", интернет-ресурс;

8) инструментальное обследование компонентов инфраструктуры объекта аттестации – проведение сканирования посредством программного средства для удаленной или локальной диагностики каналов связи, узлов, серверов, рабочих станций, прикладного и системного программного обеспечения, баз данных и элементов сети на предмет выявления в них уязвимостей;

9) уязвимость – недостаток в программном обеспечении, обуславливающий возможность нарушения его работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном обеспечении;

10) аттестационное обследование – комплекс организационно-технических мероприятий направленных на изучение, анализ, оценку технической документации объекта аттестации, обследование состояния организации работ по выполнению требований информационной безопасности;

11) программное обеспечение (далее – ПО) – совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации;

12) комплекс средств защиты (далее – КСЗ) – совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения защиты средств вычислительной техники или информационных систем от несанкционированного доступа к информации;

13) физические активы – серверное оборудование, оборудование связи, магнитные носители и техническое оборудование, используемое в объекте аттестации.

4. Аттестационное обследование информационной системы, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа на соответствие требованиям информационной безопасности проводится в следующем порядке:

1) предварительное изучение структуры объекта аттестации;

2) изучение, анализ и оценка ТД по ИБ;

3) обследование состояния организации работ по выполнению требований ЕТ , стандартов СТ РК ИСО/МЭК 27001 "Информационные технологии. Методы и

средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (далее – СТ РК ИСО/МЭК 27001) СТ РК ИСО/МЭК 27002 "Методы обеспечения защиты. Свод правил по управлению защитой информации" (далее – СТ РК ИСО/МЭК 27002), и СТ РК ГОСТ Р 50739 " Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования" (далее – СТ РК ГОСТ Р 50739), в том числе инструментальное обследование объекта аттестации;

4) формирование акта аттестационного обследования.

Глава 2. Предварительное изучение структуры объекта аттестации

5. Предварительное изучение структуры объекта аттестации проводится с целью определения особенностей функционирования объекта аттестации и получения общей информации об аппаратно-программных средствах, локальной и корпоративной сети, технологиях и процедурах по защите информации, применяемых на аттестуемом объекте.

6. Процесс предварительного изучения структуры включает ознакомление со следующей технической документацией:

1) техническое задание на создание объекта аттестации;

2) общая функциональная и локальная схема объекта аттестации;

3) список программных и технических средств используемых в объекте аттестации;

4) договор на использование информационно-коммуникационных услуг (в случае, если объект аттестации использует информационно-коммуникационные услуги).

Глава 3. Изучение, анализ и оценка ТД по ИБ

7. Изучение, анализ и оценка ТД по ИБ проводится с целью определения полноты, актуальности и корректности требований по информационной безопасности на соответствие требованиям ЕТ, СТ РК ИСО/МЭК 27001 и СТ РК ИСО/МЭК 27002.

8. Изучению, анализу и оценке на соответствие требованиям информационной безопасности подвергаются следующие ТД по ИБ:

1) политика информационной безопасности (далее – Политика);

2) правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации (далее – Правила идентификации);

3) методика оценки рисков информационной безопасности (далее – Методика оценки рисков);

4) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации (далее – Правила по обеспечению непрерывной работы);

5) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения (далее – Правила инвентаризации);

6) правила проведения внутреннего аудита информационной безопасности (далее – Правила внутреннего аудита);

7) правила использования криптографических средств защиты информации (далее – Правила использования криптографических средств);

8) правила разграничения прав доступа к электронным ресурсам (далее – Правила разграничения доступа);

9) правил использования Интернет и электронной почты;

10) правила организации процедуры аутентификации;

11) правила организации антивирусного контроля;

12) правила использования мобильных устройств и носителей информации (далее – Правила использования мобильных устройств);

13) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов (далее – Правила организации физической защиты);

14) руководство администратора по сопровождению объекта аттестации (далее – Руководство администратора);

15) регламент резервного копирования и восстановления информации (далее – Регламент резервного копирования);

16) инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях (далее – Инструкция по внештатным ситуациям).

9. Каждый ТД по ИБ необходимо проверить на наличие листа ознакомления (в произвольной форме), его полноту и актуальность.

10. Результаты изучения, анализа и оценки ТД по ИБ фиксируются в акте аттестационного обследования.

Параграф 1. Изучение, анализ и оценка Политики

11. Изучение, анализ и оценка Политики проводится с целью определения полноты, актуальности и корректности основных положений Политики и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) основных целей и принципов Политики с раскрытием значимости ИБ как инструмента, обеспечивающего возможность совместного использования информации;

2) описания действий руководства по достижению целей по обеспечению ИБ;

3) описание наиболее существенных для государственного органа или организации политики безопасности, принципов, правил и требований;

4) требований в случае нарушения Политики;

5) общих определений и функции сотрудников в рамках управления ИБ;

6) требований к периодическому пересмотру Политики;

7) функции руководства по поддержанию вопросов обеспечения ИБ.

12. На основании результатов изучения, анализа и оценки Политики в акт аттестационного обследования заносится одно из следующих решений:

1) Политика соответствует требованиям ИБ – в случае наличия всех сведений , указанных в пункте 11 настоящей Методики, и их соответствия требованиям ИБ ;

2) Политика не соответствует требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 11 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 2. Изучение, анализ и оценка Правил идентификации

13. Изучение, анализ и оценка Правил идентификации проводится с целью определения полноты, актуальности и корректности основных положений Правил идентификации и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) порядка по проведению идентификации и классификации активов (информационные активы, физические активы и другие);

2) закрепление ответственных лиц за идентифицированные активы;

3) порядка составления и ведения реестра активов (с указанием класса актива, вида актива, значимость и владельца актива);

4) порядка маркировки активов в зависимости от их установленного класса, конфиденциальности, ценности и критичности;

5) выполнения требований на полноту сведений реестра активов.

14. На основании результатов изучения, анализа и оценки Правил идентификации в акт аттестационного обследования заносится одно из следующих решений:

1) Правила идентификации соответствуют требованиям ИБ – в случае наличия всех сведений указанных в пункте 13 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила идентификации не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 13 настоящей Методики , либо их не соответствия требованиям ИБ.

Параграф 3. Изучение, анализ и оценка Методики оценки рисков

15. Изучение, анализ и оценка Методики оценки рисков проводится с целью определения полноты, актуальности и корректности основных положений Методики оценки рисков и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) выбора методики оценки рисков, выполнение идентификации рисков;

2) описания методов по определению ценности и критичности информации;

3) описания порядка мониторинга, пересмотра и изменения рисков ИБ;

4) описания методов и последовательности по определению рисков информационной безопасности объекта аттестации;

5) описания метода и последовательности оценки выявленных рисков;

6) описания метода по обработке рисков;

7) описания метода и анализа угроз информационной безопасности и источники;

8) описания метода определения вероятности инцидента;

9) описания порядка обработки рисков с учетом корректировки, сохранение, избежание, разделение;

10) описания требований к периодичности пересмотра и переоценки рисков;

11) определения и оценку последствий в случае реализации риска;

12) определение ответственных лиц за ведение и обработку рисков;

13) описания порядка составления карты рисков;

14) описания порядка формирования плана обработки рисков по результатам оценки и анализа рисков.

16. На основании результатов изучения, анализа и оценки Методики оценки рисков в акт аттестационного обследования заносится одно из следующих решений:

1) Методика оценки рисков соответствует требованиям ИБ – в случае наличия всех сведений указанных в пункте 15 настоящей Методики, и их соответствия требованиям ИБ;

2) Методика оценки рисков не соответствует требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 15 настоящей Методики , либо их не соответствия требованиям ИБ.

Параграф 4. Изучение, анализ и оценка Правил по обеспечению непрерывной работы

17. Изучение, анализ и оценка Правил по обеспечению непрерывной работы проводится с целью определения полноты, актуальности и корректности основных положений Правил по обеспечению непрерывной работы и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) по идентификации событий, которые являются причиной прерывания процессов функционирования объекта аттестации (планирование должно сопровождаться оценкой рисков);

2) определения процессов обеспечения непрерывности работы активов, занесенных в реестр активов в случае их выхода из строя;

3) предусматривающих разработку плана обеспечения непрерывности работы активов, связанных со средствами обработки информации и их актуализация;

4) о порядке тестирования и обновления планов развития существующих процессов по непрерывности работы активов;

5) по назначению ответственных лиц за процессы функционирования объекта аттестации;

6) по проведению анализа плана мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов;

7) по разработке плана восстановления объекта аттестации;

8) способы размещения оборудования снижающий риск возникновения угроз, опасностей и возможностей несанкционированного доступа;

9) способы защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб;

10) требования периодичности технического обслуживания оборудования для обеспечения непрерывности функционирования, доступности и целостности.

18. На основании результатов изучения, анализа и оценки Правил по обеспечению непрерывной работы в акт аттестационного обследования заносится одно из следующих решений:

1) Правила по обеспечению непрерывной работы соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 17 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила по обеспечению непрерывной работы не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 17 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 5. Изучение, анализ и оценка Правил инвентаризации

19. Изучение, анализ и оценка Правил инвентаризации проводится с целью определения полноты, актуальности и корректности основных положений Правил инвентаризации и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований к идентификации средств вычислительной техники (далее – СВТ) с учетам их ценности и важности;

2) порядок оформления паспортов СВТ;

3) требований к периодичности проведения инвентаризации и паспортизации СВТ;

4) требований к утилизации и (или) списанию СВТ, телекоммуникационного оборудования и программного обеспечения, в том числе по утилизации устройств хранения данных и гарантированному уничтожению информации при повторном использования оборудования;

5) требований по назначению ответственных за инвентаризацию и паспортизацию СВТ;

6) требований к использованию, приобретению и учету лицензионного ПО.

20. На основании результатов изучения, анализа и оценки Правил инвентаризации в акт аттестационного обследования заносится одно из следующих решений:

1) Правила инвентаризации соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 19 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила инвентаризации не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 19 настоящей Методики , либо их не соответствия требованиям ИБ.

Параграф 6.Изучение, анализ и оценка Правил внутреннего аудита

21. Изучение, анализ и оценка Правил внутреннего аудита проводится с целью определения полноты, актуальности и корректности основных положений Правил внутреннего аудита и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) основных целей внутреннего аудита информационной безопасности;

2) требований по предоставлению доступа аудиторам;

3) требований к инструментальному аудиту;

4) требования по периодичности проведения внутреннего аудита;

5) требований к наличию и ведению плана - графика поэтапного проведения внутреннего аудита;

6) требования по порядку формирования рабочей группы по проведению внутреннего аудита;

7) требований по планированию, порядку и составу проведения аудита для объектов аттестации;

8) порядка и формы оформления результатов внутреннего аудита информационной безопасности.

22. На основании результатов изучения, анализа и оценки Правил внутреннего аудита в акт аттестационного обследования заносится одно из следующих решений:

1) Правила внутреннего аудита соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 21 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила внутреннего аудита не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 21 настоящей Методики , либо их не соответствия требованиям ИБ.

Параграф 7. Изучение, анализ и оценка Правил использования криптографических средств

23. Изучение, анализ и оценка Правил использования криптографических средств проводится с целью определения полноты, актуальности и корректности основных положений Правил использования криптографических средств и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) политики использования криптографических средств защиты информации в соответствии со СТ РК ИСО МЭК 27002;

2) требования к системе управления ключами;

3) требований по срокам активизации и дезактивации ключей;

4) требования по сертификату открытых ключей;

5) требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций в соответствии с заданием по безопасности.

24. На основании результатов изучения, анализа и оценки Порядка использования криптографических средств в акт аттестационного обследования заносится одно из следующих решений:

1) Правила использования криптографических средств соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 23 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила использования криптографических средств не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 23 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 8.Изучение, анализ и оценка Правил разграничения доступа

25. Изучение, анализ и оценка Правил разграничения доступа проводится с целью определения полноты, актуальности и корректности основных положений Правил разграничения доступа и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) описания стадии регистрации пользователей, с момента регистрации нового пользователя до снятия с регистрации пользователя;

2) описания перечня предоставляемых прав доступа к ресурсам;

3) описания порядка предоставления прав доступа;

4) требований по ведению учета всех зарегистрированных пользователей;

5) требований по проведению пересмотра прав доступа пользователей;

6) требований по ознакомлению пользователей о запрете разглашения либо передачи полученных идентификаторов;

7) описание требований по блокировке учетной записи.

26. На основании результатов изучения, анализа и оценки Правил разграничения доступа в акт аттестационного обследования заносится одно из следующих решений:

1) Правила разграничения доступа соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 25 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила разграничения доступа не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 25 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 9. Изучение, анализ и оценка Правил использования Интернет и электронной почты

27. Изучение, анализ и оценка Правил использования Интернет и электронной почты проводится с целью определения полноты, актуальности и корректности основных положений Правил использования Интернет и электронной почты и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) порядка использования электронной почты;

2) требования к оформлению электронного сообщения;

3) порядка и способов предоставления доступа в Интернет;

4) мониторинга и контроля доступа в Интернет;

5) требования об осуществлении электронного взаимодействия ведомственной электронной почты государственного органа с внешними электронными почтовыми системами только через единый шлюз электронной почты.

28. На основании результатов изучения, анализа и оценки Правил использования Интернет и электронной почты в акт аттестационного обследования заносится одно из следующих решений:

1) Правила использования Интернет и электронной почты соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 27 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила использования Интернет и электронной почты не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 27 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 10. Изучение, анализ и оценка Правил организации процедуры аутентификации

29. Изучение, анализ и оценка Правил организации аутентификации проводится с целью определения полноты, актуальности и корректности основных положений Правил организации аутентификации и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований по уведомлению пользователей о необходимости сохранения конфиденциальности вверенных им идентификаторов;

2) требований по уведомлению пользователей о запрете записи паролей, пин-кодов на бумаге, персональном компьютере или на переносных устройствах, если только не обеспечено безопасное их хранение;

3) описания порядка безопасного способа выдачи временных паролей;

4) описания требований к временным паролям;

5) требований о необходимости изменения идентифицирующих данных, при наличии любого признака возможности компрометации идентификатора;

6) требований по выбору качественных паролей;

7) описания требований по изменению парольной аутентификации через равные интервалы времени;

8) описания требований по смене временных паролей при первой регистрации в системе;

9) описания требований по запрету включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш.

30. На основании результатов изучения, анализа и оценки Правил организации аутентификации пользователей в акт аттестационного обследования заносится одно из следующих решений:

1) Правила организации аутентификации пользователей соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 29 настоящей Методики;

2) Правил организации аутентификации пользователей не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 29 настоящей Методики.

Параграф 11. Изучение, анализ и оценка Правил организации антивирусного контроля

31. Изучение, анализ и оценка Правил организации антивирусного контроля проводится с целью определения полноты, актуальности и корректности основных положений Правил организации антивирусного контроля и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований по использованию лицензионных антивирусных программных обеспечений.

2) требований по периодичности обновления антивирусных программных обеспечений;

3) требований для пользователей, по соблюдению информационной безопасности при использовании антивирусных программных обеспечений;

4) требований к веб-страницам на наличие вредоносного программного обеспечения;

5) требований по анализу всех файлов на носителях информации сомнительного или неавторизованного происхождения или файлов, полученных из общедоступных сетей, на наличие вирусов;

6) требований по анализу электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения

7) требований по организации мероприятий по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением;

8) описания процедур по восстановлению информации после вирусных атак.

32. На основании результатов изучения, анализа и оценки Правил организации антивирусного контроля в акт аттестационного обследования заносится одно из следующих решений:

1) Правила организации антивирусного контроля соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 31 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила организации антивирусного контроля не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 31 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 12. Изучение, анализ и оценка Правил использования мобильных устройств

33. Изучение, анализ и оценка Правил использования мобильных устройств проводится с целью определения полноты, актуальности и корректности основных положений Правила использования мобильных устройств и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований по анализу рисков в случае использования мобильных устройств за пределами организации;

2) требований по физической защите мобильных устройств и носителей информации;

3) требований по составлению перечня мобильных устройств, носителей информации и их маркировка;

4) требований к ведению журнала выдачи носителей информации.

5) порядка использования носителей информации;

6) порядка учета, хранения и обращения со съемными носителями персональных данных, и их утилизации;

7) требований к сотрудникам при использовании съемных носителей;

8) способов защиты мобильного оборудования, находящегося за пределами рабочего места, с учетом различных рисков работы за пределами организационных помещений;

9) порядка действий при выявлении фактов несанкционированных действий сотрудников при использовании, а также при утрате и уничтожении съемных носителей персональных данных.

34. На основании результатов изучения, анализа и оценки Правил использования мобильных устройств в акт аттестационного обследования заносится одно из следующих решений:

1) Правила использования мобильных устройств соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 33 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила использования мобильных устройств не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 33 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 13. Изучение, анализ и оценка Правил организации физической защиты

35. Изучение, анализ и оценка Правил организации физической защиты проводится с целью определения полноты, актуальности и корректности основных положений Правил организации физической защиты и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований к организации физической защиты серверного помещения в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

2) требований к организации контроля доступа в серверные помещения в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

3) требований по выполнению работ в серверном помещений в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

4) требований по безопасному размещению серверного оборудования в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

5) требований по организации вспомогательных услуг в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

6) требований по безопасному использованию кабельной сети в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

7) требований по безопасному техническому обслуживанию серверного оборудования в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

8) требований к безопасной утилизации или повторному использованию оборудования в соответствии с ЕТ и СТ РК ИСО/МЭК 27002;

9) требований к выносу/вносу оборудования в соответствии с ЕТ и СТ РК ИСО/МЭК 27002.

36. На основании результатов изучения, анализа и оценки Правил организации физической защиты в акт аттестационного обследования заносится одно из следующих решений:

1) Правила организации физической защиты соответствуют требованиям ИБ – в случае наличия всех сведений, указанных в пункте 35 настоящей Методики, и их соответствия требованиям ИБ;

2) Правила организации физической защиты не соответствуют требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 35 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 14. Изучение, анализ и оценка Руководства администратора

37. Изучение, анализ и оценка Руководства администратора проводится с целью определения полноты, актуальности и корректности основных положений Руководства администратора и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований к действиям администратора по основным типовым работам;

2) требования к действиям администратора при возникновении инцидентов, внештатных ситуаций, стихийных природно-климатических и техногенных воздействий;

3) порядок по установке, обновления и удаления ПО на серверах и рабочих станциях;

4) процедуры управления изменениями и анализа ПО в случае изменения системного ПО.

38. На основании результатов изучения, анализа и оценки Руководства администратора в акт аттестационного обследования заносится одно из следующих решений:

1) Руководство администратора соответствует требованиям ИБ – в случае наличия всех сведений, указанных в пункте 37 настоящей Методики, и их соответствия требованиям ИБ;

2) Руководство администратора не соответствует требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 37 настоящей Методики , либо их не соответствия требованиям ИБ.

Параграф 15. Изучение, анализ и оценка Регламента резервного копирования

39. Изучение, анализ и оценка Регламента резервного копирования проводится с целью определения полноты, актуальности и корректности основных положений Регламента резервного копирования и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) описания требований по составу информации, подлежащей резервному копированию;

2) определения объема резервного копирования;

3) описаний требований по размещению резервного оборудования, резервных копий и выбору места хранения резервных копий;

4) описаний требований по тестированию резервных копий и резервного оборудования;

5) описаний требований по размещению резервного серверного оборудования и ее физической защиты;

6) описаний процедур копирования информации и восстановления информации;

7) требования о периодичности резервирования информации и составлении графика резервного копирования;

8) требований по документированию процесса резервного копирования в части ведения реестра эталонных копий, реестра информационных ресурсов, подлежащих резервному копированию, журнала записи резервного копирования, журнала проверок резервных копий на восстановление, журнала учета электронных носителей резервной информации, журнала вноса/выноса электронных носителей резервной информации.

40. На основании результатов изучения, анализа и оценки Регламента резервного копирования в акт аттестационного обследования заносится одно из следующих решений:

1) Регламент резервного копирования соответствует требованиям ИБ – в случае наличия всех сведений, указанных в пункте 39 настоящей Методики, и их соответствия требованиям ИБ;

2) Регламент резервного копирования не соответствует требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 39 настоящей Методики, либо их не соответствия требованиям ИБ.

Параграф 16. Изучение, анализ и оценка Инструкции по внештатным ситуациям

41. Изучение, анализ и оценка Инструкции по внештатным ситуациям проводится с целью определения полноты, актуальности и корректности основных положений Инструкции по внештатным ситуация и заключается в проведении работ по определению наличия и качественной оценки следующих сведений:

1) требований по составлению перечня возможных внештатных или кризисных ситуаций, идентификация инцидентов по ИБ;

2) требование о назначении ответственных лиц за оповещение в случае инцидентов информационной безопасности;

3) порядок оповещения при возникновении внештатных ситуаций;

4) требования по принятию мер реагирования при возникновении инцидентов ИБ, внештатных (кризисных) ситуаций;

5) требования по разработке процедур восстановления работы в случае их остановки;

6) требования по осуществлению контроля за выполнением профилактических действий для предотвращения возникновения внештатных или кризисных ситуаций;

7) требований по расследованию случаев возникновения инцидентов и других внештатных ситуаций.

42. На основании результатов изучения, анализа и оценки Инструкции по внештатным ситуациям в акт аттестационного обследования заносится одно из следующих решений:

1) Инструкция по внештатным ситуациям соответствует требованиям ИБ – в случае наличия всех сведений, указанных в пункте 41 настоящей Методики, и их соответствия требованиям ИБ;

2) Инструкция по внештатным ситуациям не соответствует требованиям ИБ – в случае отсутствия одного и более сведений, указанных в пункте 41 настоящей Методики, либо их не соответствия требованиям ИБ.

Глава 4. Обследование состояния организации работ по выполнению требований ЕТ, стандартов СТ РК ИСО/МЭК 27001-2015 и СТ РК ИСО/МЭК 27002-2015, СТ РК ГОСТ Р 50739-2006, ТД по ИБ, в том числе инструментальное обследование объекта аттестации

43. Обследование состояние организации работ по выполнению требований ЕТ, стандартов СТ РК ИСО/МЭК 27001 и СТ РК ИСО/МЭК 27002, СТ РК ГОСТ Р 50739, ТД по ИБ в том числе инструментальное обследование объекта аттестации проводится с целью обследования и анализа:

1) положений Политики;

2) процессов по управлению информационной безопасностью;

3) организации управления активами;

4) обеспечения безопасности, связанной с персоналом;

5) физической защиты оборудования и безопасности окружающей среды;

6) обеспечения надлежащего и безопасного функционирования средств обработки информации;

7) организации управления доступом к информационным ресурсам;

8) процессов разработки, внедрения и обслуживания объектов аттестации;

9) организации управления инцидентами в области информационной безопасности;

10) управления непрерывности бизнеса;

11) степени соответствия правовым требованиям;

12) системы защиты от несанкционированного доступа к информации согласно СТ РК ГОСТ Р 50739.

44. Результаты обследования состояние организации работ по выполнению требований ЕТ, стандартов СТ РК ИСО/МЭК 27001 и СТ РК ИСО/МЭК 27002, СТ РК ГОСТ Р 50739, ТД по ИБ в том числе инструментальное обследование объекта аттестации фиксируются в акте аттестационного обследования.

Параграф 1. Обследование и анализ положений Политики

45. При обследовании и анализе положений Политики необходимо проверить :

1) одобрение руководством Политики, опубликование и доведение до сведения всех сотрудников и связанных внешних организаций;

2) понимание и принятие Политики сотрудниками организации;

3) периодический пересмотр Политики;

4) адекватность и выполнимость требований документов;

5) результаты анализа Политики через запланированные интервалы времени или в случае возникновения значительных изменений;

6) наличие ответственного лица за руководство разработкой, анализом Политики.

46. По итогам изучения и анализа положений Политики в акт аттестационного обследования заносится одно из следующих решений:

1) положение Политики соответствует требованиям ИБ – в случае выполнение пункта 45 настоящей Методики;

2) положение Политики не соответствует требованиям ИБ – в случае не выполнения одного и более подпунктов пункта 45 настоящей Методики.

Параграф 2. Обследование и анализ процессов по управлению информационной безопасностью

47. При обследовании и анализе процессов по управлению информационной безопасностью, необходимо осуществить обследование следующих процессов:

1) функционирование подразделения, ответственное за обеспечение информационной безопасности и (или) ответственное лицо за обеспечение информационной безопасности объекта аттестации;

2) функционирование органа (технический совет, рабочая группа по информационной безопасности) по вопросам информационной безопасности, с

участием высшего руководства организации, для обсуждения политик, рисков и других вопросов информационной безопасности;

3) проведение в организации регулярных совещаний руководства по вопросам координации действий по поддержанию режима безопасности;

4) разделение ролей и ответственности в области информационной безопасности между сотрудниками организации;

5) координация деятельности по вопросам ИБ внутри подразделений и между подразделениями государственного органа или организации;

6) внедрение идентификации рисков организации и средств обработки информации со стороны бизнес-процессов, затрагивающих сторонние организации (в случае если привлекаются сторонние организации);

7) соблюдение требований к безопасности перед предоставлением сторонним организациям права доступа к информации или активам организации (в случае если привлекаются сторонние организации);

8) соблюдение требований безопасности в соглашении со сторонней организацией, включающих доступ, обработку, передачу или управление информацией организации или средствами ее обработки (в случае если привлекаются сторонние организации).

48. На основании результатов обследования и анализа процессов по управлению информационной безопасностью в акт аттестационного обследования заносится одно из следующих решений:

1) процесс по управлению информационной безопасностью соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 47 настоящей Методики;

2) процесс по управлению информационной безопасностью не соответствует требованиям ИБ – в случае не выполнении подпунктов, указанных в пункте 47 настоящей Методики.

Параграф 3. Обследование и анализ организации управления активами

49. При обследовании и анализе организации управления активами необходимо осуществить обследование следующих процессов:

1) анализ идентификации, оформления и поддержки в рабочем состоянии инвентарной ведомости всех активов связанных с объектом аттестации;

2) определение степени владения организацией или государственного органа информации и активов, связанных со средствами обработки информации;

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

5) анализ классификации информации с точки зрения ее ценности, законодательных требований, чувствительности и критичности для организации;

6) маркировки и обращения с информацией в соответствии с принятой в организации схемой классификации и их исполнения.

50. На основании результатов обследовании и анализе процессов организации управления активами в акт аттестационного обследования заносится одно из следующих решений:

1) организация управления активами соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 49 настоящей Методики;

2) организация управления активами не соответствует требованиям ИБ – в случае не выполнения подпунктов пункта 49 настоящей Методики.

Параграф 4. Обследование и анализ обеспечения безопасности, связанной с персоналом

51. При обследовании и анализе обеспечения безопасности, связанной с персоналом необходимо обследовать:

1) функции персонала по обеспечению безопасности и исполнение закрепленных функций по ИБ в соответствии со СТ РК ИСО/МЭК 27002;

2) полноту требований по информационной безопасности устанавливаемых для сотрудников при приеме на работу в соответствии со СТ РК ИСО/МЭК 27002;

3) условия трудового договора в части информационной безопасности в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

4) соблюдение требования руководства о соблюдении безопасности в соответствии с установленными политиками и процедурами организации сотрудниками, подрядчиками и пользователями третьей стороны в соответствии со СТ РК ИСО/МЭК 27002;

5) осведомленность, обучение и переподготовку сотрудников в области информационной безопасности в соответствии со СТ РК ИСО/МЭК 27002;

6) наличие формализованного дисциплинарного процесса для сотрудников, нарушивших требования безопасности и его фактическое применение в соответствии со СТ РК ИСО/МЭК 27002;

7) наличие ответственности сотрудников при окончании срока или изменении условий трудоустройства в части информационной безопасности (возврат активов, аннулирование прав доступа) в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ.

52. На основании результатов обследования и анализа обеспечения безопасности, связанных с персоналом в акт аттестационного обследования заносится одно из следующих решений:

1) обеспечение безопасности, связанное с персоналом соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 51 настоящей Методики;

2) обеспечение безопасности, связанное с персоналом не соответствует требованиям ИБ – в случае невыполнения подпунктов пункта 51 настоящей Методики.

Параграф 5. Обследование и анализ физической защиты оборудования и безопасности окружающей среды

53. При обследовании и анализе физической защиты оборудования и безопасности окружающей среды необходимо осуществить обследование следующих процессов:

1) обеспечение физической защиты периметра и серверного помещения в соответствии со СТ РК ИСО/МЭК 27002;

2) организация контроля доступа в серверные помещения в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

3) организация защиты от внешних угроз в соответствии со СТ РК ИСО/МЭК 27002;

4) организация работ в серверных помещениях в соответствии со СТ РК ИСО /МЭК 27002;

5) обеспечение информационной безопасности при приеме и отгрузки материальных ценностей в зонах общественного доступа (если таковые имеются) в соответствии со СТ РК ИСО/МЭК 27002;

6) размещение оборудования (включая и то, что используется вне организации) для обеспечения защиты и информационной безопасности в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

7) обеспечение защиты от перебоев в подаче электроэнергии и других сбоев, связанных с отказом в обеспечении вспомогательных услуг в соответствии со СТ РК ИСО/МЭК 27002;

8) обеспечение информационной безопасности кабельной сети в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

9) обеспечение информационной безопасности при техническом обслуживании серверного оборудования в соответствии со СТ РК ИСО/МЭК 27002;

10) обеспечение информационной безопасности серверного оборудования, используемого вне серверного помещения в соответствии со СТ РК ИСО/МЭК 27002;

11) организация безопасной утилизации (списания) оборудования в соответствии со СТ РК ИСО/МЭК 27002.

54. На основании результатов обследования и анализа физической защиты оборудования и безопасности окружающей среды в акт аттестационного обследования заносится одно из следующих решений:

1) физическая защита оборудования и безопасности окружающей среды соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 53 настоящей Методики;

2) физическая защита оборудования и безопасности окружающей среды не соответствует требованиям ИБ – в случае не выполнения подпунктов пункта 53 настоящей Методики.

Параграф 6. Обследование и анализ обеспечения надлежащего и безопасного функционирования средств обработки информации

55. При обследовании и анализе обеспечения надлежащего и безопасного функционирования средств обработки информации необходимо осуществить обследование следующих процессов:

1) документальное оформление операционных процедур, ведение контроля изменений в объекте аттестации, разграничение обязанностей в объекте аттестации и разграничение средств разработки, тестирования и эксплуатации в соответствии со СТ РК ИСО/МЭК 27002;

2) соблюдение требований информационной безопасности при получение услуг от сторонних организации и (или) поставке услуг сторонним организациям в соответствии со СТ РК ИСО/МЭК 27002;

3) обеспечение информационной безопасности при управлении производительностью объектов аттестации в соответствии со СТ РК ИСО/МЭК 27002;

4) обеспечение безопасной защиты от вредоносного кода в соответствии со СТ РК ИСО/МЭК 27002;

5) соблюдение требований информационной безопасности при проведении процедур резервирования информации в объектах аттестации в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

6) обеспечение информационной безопасности при управлении сетью в соответствии со СТ РК ИСО/МЭК 27002;

7) исполнение требований к локальной и ведомственной (корпоративной) сети, установленных в ЕТ;

8) соблюдение информационной безопасности при работе с носителями информации (ленты, диски, флеш - накопители) в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

9) соблюдение информационной безопасности при обмене информации в соответствии со СТ ИСО/МЭК 27002;

10) обеспечения мониторинга информационной безопасности в объекта аттестации в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

11) обеспечение надлежащего и безопасного функционирования вычислительных ресурсов, реализующих технологии виртуализации и "облачных " вычислений в соответствии с требованиями ЕТ.

56. На основании результатов обследования и анализа обеспечения надлежащего и безопасного функционирования средств обработки информации в акт аттестационного обследования заносится одно из следующих решений:

1) обеспечение надлежащего и безопасного функционирования средств обработки информации соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 55 настоящей Методики

2) обеспечение надлежащего и безопасного функционирования средств обработки информации не соответствует требованиям ИБ – в случае не выполнения одно и более подпунктов пункта 55 настоящей Методики.

Параграф 7. Обследование и анализ организации управления доступом к информационным ресурсам

57. При обследовании и анализе организации управления доступа к информационным ресурсам необходимо обследовать следующие процессы:

1) обеспечение информационной безопасности по контролю доступа к информации и объекту аттестации в соответствии со СТ РК ИСО/МЭК 27002;

2) обеспечение информационной безопасности при управлении доступом пользователей в объекте аттестации в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

3) осведомление пользователей об их функциональных обязанностях по управлению доступом и их исполнение в соответствие со СТ РК ИСО/МЭК 27002 и ЕТ;

4) обеспечение информационной безопасности при предоставлении доступа сетевым сервисам в соответствии со СТ РК ИСО/МЭК 27002;

5) обеспечение информационной безопасности при предоставлении доступа к операционной системе в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

6) обеспечение контроля доступа к прикладным системам и информации в соответствии со СТ РК ИСО/МЭК 27002 и ЕТ;

7) соблюдение требований информационной безопасности при работе с переносными устройствами и работа в дистанционном режиме в соответствии со СТ РК ИСО МЭК 27002;

8) разделение сред опытной или промышленной эксплуатации ИС от сред разработки, тестирования или стендовых испытаний, с исполнением требовании установленных в ЕТ (для информационных систем);

9) обеспечение информационной безопасности интернет – ресурса в соответствии с ЕТ.

58. На основании результатов обследования и анализа организации управления доступа к информационным ресурсам в акт аттестационного обследования заносится одно из следующих решений:

1) организация управления доступа к информационным ресурсам соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 57 настоящей Методики;

2) организация управления доступа к информационным ресурсам не соответствует требованиям ИБ – в случае не выполнения одного и более подпунктов пункта 57 настоящей Методики.

Параграф 8. Обследование и анализ процессов разработки, внедрения и обслуживания объектов аттестации

59. При аттестационном обследовании и анализе процессов разработки, внедрения и обслуживание объектов аттестации необходимо обследовать:

1) обеспечение информационной безопасности на каждом этапе жизненного цикла в соответствии со СТ РК ИСО МЭК 27002;

2) обеспечение информационной безопасности при обработке данных в объекте аттестации в соответствии со СТ РК ИСО МЭК 27002;

3) корректность использования криптографических средств защиты информации в соответствии со СТ РК ИСО МЭК 27002;

4) обеспечение информационной безопасности системных файлов объекта аттестации в соответствии со СТ РК ИСО МЭК 27002;

5) обеспечение информационной безопасности в процессе разработки и внедрения объекта аттестации в соответствии со СТ РК ИСО МЭК 27002;

6) проведение работ по устранению, мониторингу уязвимостей объекта аттестации в соответствии со СТ РК ИСО МЭК 27002;

7) разделение сред опытной или промышленной эксплуатации ИС от сред разработки, тестирования или стендовых испытаний, с исполнением требований, установленных в ЕТ (для информационных систем);

8) обеспечение информационной безопасности интернет - ресурса в соответствии с ЕТ.

60. На основании результатов обследования и анализа процессов разработки, внедрения и обслуживание объектов аттестации в акт аттестационного обследования заносится одно из следующих решений:

1) процессы разработки, внедрения и обслуживания объектов аттестации соответствуют требованиям ИБ – в случае выполнения всех подпунктов пункта 59 настоящей Методики;

2) процессы разработки, внедрения и обслуживания объектов аттестации не соответствуют требованиям ИБ – в случае не выполнения подпунктов пункта 59 настоящей Методики.

Параграф 9. Обследование и анализ организации управления инцидентами в области информационной безопасности

61. При обследовании и анализе организации управления инцидентами в области информационной безопасности необходимо обследовать следующие процессы:

1) оповещение о случаях нарушения информационной безопасности, позволяющей обеспечить быстрое, результативное и последовательное реагирование на инциденты в области информационной безопасности в соответствии со СТ РК ИСО МЭК 27002;

2) назначение ответственности руководства в соответствии со СТ РК ИСО МЭК 27002;

3) мониторинг и регистрация инцидентов информационной безопасности, оперативность информирования об инцидентах в области информационной безопасности, процедуры составлению отчетов об инцидентах информационной безопасности в соответствии со СТ РК ИСО МЭК 27002;

4) сбор, сохранение и предоставление информации об инцидентах информационной безопасности на случай, если инцидент информационной безопасности может привести к судебному разбирательству в соответствии с СТ РК ИСО МЭК 27002;

5) регистрация событий, связанных с состоянием информационной безопасности и выявление нарушений путем анализа журналов событий в соответствие с ЕТ.

62. На основании результатов обследования и анализа организации управления инцидентами информационной безопасности в акт аттестационного обследования заносится одно из следующих решений:

1) организация управления инцидентами в области информационной безопасности соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 61 настоящей Методики;

2) организация управления инцидентами в области информационной безопасности не соответствует требованиям ИБ – в случае невыполнения подпунктов пункта 61 настоящей Методики.

Параграф 10. Обследование и анализ управления непрерывности бизнеса

63. При обследовании и анализе управления непрерывности бизнеса необходимо обследовать следующие процессы:

1) развитие и поддержки непрерывности бизнеса включающие в себя процессы по информационной безопасности в соответствии со СТ РК ИСО МЭК 27002;

2) идентификация событий, которые являются причиной прерывания бизнес-процессов в соответствии со СТ РК ИСО МЭК 27002;

3) реализация планов непрерывности бизнеса в соответствии со СТ РК ИСО МЭК 27002;

4) проведение тестирования, поддержки и пересмотра планов по обеспечению непрерывности бизнеса в соответствии со СТ РК ИСО МЭК 27002.

64. На основании результатов обследования и анализа управления непрерывности бизнеса в акт аттестационного обследования заносится одно из следующих решений:

1) управление непрерывностью бизнеса соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 63 настоящей Методики;

2) управление непрерывностью бизнеса не соответствует требованиям ИБ – в случае невыполнения подпунктов пункта 63 настоящей Методики.

Параграф 11. Обследование и анализ степени соответствия правовым требованиям

65. При обследовании и анализе степени соответствия правовым требованиям необходимо обследовать следующие процессы:

1) защита записей организации от потери, разрушения и фальсификации в соответствии с законодательными, другими обязательными, контрактными требованиями и бизнес – требованиями в соответствии со СТ РК ИСО МЭК 27002;

2) обеспечение информационной безопасности при переносе конфиденциальной персональной информации в соответствии со СТ РК ИСО МЭК 27002;

3) контроль нецелевого использования средств обработки информации в соответствии со СТ РК ИСО МЭК 27002;

4) проведение мероприятий по управлению техническими уязвимостями в ручную и (или) при помощи соответствующих инструментальных и программных средств в соответствии со СТ РК ИСО МЭК 27002;

5) применение мер по управлению и согласованию при проведении аудита информационной безопасности в соответствии со СТ РК ИСО МЭК 27002;

6) обеспечение информационной безопасности при доступе инструментальных средств аудита в соответствие со СТ РК ИСО МЭК 27002.

66. На основании результатов обследования и анализа степени соответствия правовым требованиям в акт аттестационного обследования заносится одно из следующих решений:

1) степень соответствия правовым требованиям соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 65 настоящей Методики;

2) степень соответствия правовым требованиям не соответствует требованиям ИБ – в случае не выполнении подпунктов пункта 65 настоящей Методики.

Параграф 12. Обследование и анализ системы защиты от несанкционированного доступа к информации согласно СТ РК ГОСТ Р 50739

67. При обследовании и анализе системы защиты от несанкционированного доступа к информации согласно СТ РК ГОСТ Р 50739 необходимо обследовать следующие процессы:

1) обеспечение защищенность информации при ее обработке в объекте аттестации от НСД в соответствии со СТ РК ГОСТ Р 50739;

2) реализация разграничения прав доступа показателями защищенности в соответствии со СТ РК ГОСТ Р 50739;

3) исполнение требовании к учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации в соответствии со СТ РК ГОСТ Р 50739;

4) исполнение требований к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету в соответствии со СТ РК ГОСТ Р 50739;

5) подробное и всестороннее описание комплексных средств защиты в соответствии со СТ РК ГОСТ Р 50739.

68. На основании результатов изучения и анализа объектов аттестации на соответствие требованиям защиты от несанкционированного доступа в акт аттестационного обследования заносится одно из следующих решений:

1) система защиты от несанкционированного доступа объекта аттестации согласно СТ РК ГОСТ Р 50739 соответствует требованиям ИБ – в случае выполнения всех подпунктов пункта 67 настоящей Методики;

2) система защиты от несанкционированного доступа объекта аттестации согласно СТ РК ГОСТ Р 50739 не соответствует требованиям защиты – в случае не выполнения подпунктов пункта 67 настоящей Методики.

Параграф 13. Инструментальное обследование объекта аттестации

69. Инструментальное обследование объекта аттестации проводится с целью выявления уязвимостей на объекте аттестации, в частности в системе защиты от внешнего и внутреннего проникновения, с помощью специализированного программного-аппаратного комплекса (далее – ПАК) на основании учетных записей для доступа к компонентам объекта аттестации, предоставленных заявителем.

70. Проведение инструментального обследования объекта аттестации включает в себя:

1) настройку ПАК (прописка учетной записи для проведения локальных и удаленных проверок, выбор режима инструментального обследования и т.п.);

2) запуск ПАК;

3) формирование и выдачу программного отчета, включающего в себя перечень выявленных уязвимостей с указанием их описания, количества и уровня;

4) экспертную оценку результатов инструментального обследования с учетом обоснования, представленного заявителем до формирования отчета, прилагаемого к акту аттестационного (дополнительного аттестационного) обследования.

71. На основании результатов инструментального обследования в акт аттестационного обследования заносится одно из следующих решений:

1) система защиты от внешнего и внутреннего проникновения соответствует требованиям ИБ – в случае отсутствия уязвимостей;

2) система защиты от внешнего и внутреннего проникновения не соответствует требованиям ИБ – в случае наличия уязвимостей.

Глава 5.Формирование Акта аттестационного обследования

72. Результаты аттестационного обследования оформляются в виде акта аттестационного обследования, который составляется по окончанию всех видов работ, входящих в аттестационное обследование, на основании полного комплекта проверочных листов по всем работам;

73. Акт аттестационного обследования составляется в произвольной форме и включает в себя:

1) результаты изучения, анализа и оценки ТД по ИБ;

2) отчет о состоянии организации работ по выполнению требований ЕТ, стандартов СТ РК ИСО/МЭК 27001 и СТ РК ИСО/МЭК 27002, СТ РК ГОСТ Р 50739, ТД по ИБ;

3) отчет по инструментальному обследованию объекта аттестации;

4) заключение по результатам всех видов работ аттестационного обследования и рекомендации по устранению несоответствий в случае их наличия.

74. Акт аттестационного обследования составляется в трех экземплярах, один из которых остается в государственной технической службе, а другие 2 экземпляра передаются в уполномоченный орган для уполномоченного органа и заявителя.