Акционерное общество «Товарная биржа «Эстау»

УТВЕРЖДЕНО

Президент АО «Товарная биржа «Эстау»

_____ Турсынова Бахытгуль Жарековна

«____» _____ 2024 г.

М. П.

Политика информационной безопасности Информационной системы «Электронная торговая система товарной биржи» ЭТСТБ.СМИБ.П.01.r01.21

г Астана
2024 г.

ЛИСТ СОГЛАСОВАНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	2	3	4	5

Содержание

1 Введение

Политика информационной безопасности ИС предназначена для определения целей и требований обеспечения информационной безопасности.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.

Настоящий документ отражает:

1. основные цели и принципы обеспечения ИБ 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 Организации политики безопасности, принципов, правил и требований;
4. требования к ответственности персонала в случае нарушения режима ИБ;
5. общие определения и конкретные обязанности сотрудников в рамках управления ИБ;
6. требования к периодическому пересмотру СМИБ;
7. обязательства руководства по поддержанию вопросов обеспечения ИБ;
8. ответственность руководства за обеспечение возможности выполнения сотрудниками и привлекаемыми со стороны исполнителями обязательств в отношении ИБ.

Настоящий документ отражает поддержку руководства Организации и определяет подход к управлению информационной безопасностью, который будет применяться в Организации. Данный документ включает следующие сведения:

a) определение информационной безопасности, ее общих целей и сферы действия, а также раскрытия значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации (Раздел «Введение»);

b) изложение целей и принципов информационной безопасности, в соответствии с решаемыми задачами, сформулированных руководством;

c) мероприятия по достижению целей и средства управления, в том числе структуры оценки рисков, а также управления рисками;

d) краткое объяснение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;
2) требования в отношении обучения вопросам безопасности;
3) управление непрерывностью бизнеса;
4) ответственность за нарушения политики безопасности;

e) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

f) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правил безопасности, которым должны следовать пользователи.

Настоящий документ должен быть доведен до сведения всех сотрудников в доступной и понятной форме. Факт ознакомления с документами СМИБ должен быть зарегистрирован в Журнале ознакомления, выдачи и возврата документации (по форме Приложения 2).

2 Область действия

Настоящий документ распространяется на всех сотрудников проекта, а также на сторонние организации и частные лица в мере, соответствующей договорным и/или лицензионным отношениям и/или другим видам договоренностей.

3 Нормативные ссылки

В настоящем документе используются материалы следующих документов:

3.1. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»;

3.2. Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите»;

3.3. Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи»;

3.4. Постановление Правительства Республики Казахстан от 12 ноября 2013 года № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач»;

3.5. Постановление Правительства Республики Казахстан от 3 сентября 2013 года № 909 «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных»;

3.6. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 5 июня 2019 года № 18795 «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности»;

3.7. Приказ и. о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 февраля 2016 года № 13349 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации»;

3.8. Приказ Министра информации и коммуникаций Республики Казахстан от 13 июня 2018 года № 263. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 июня 2018 года № 17141 «Об утверждении Правил проведения аудита информационных систем»;

3.9. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (далее – ЕТ);

3.10. Приказ и. о. Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 13 апреля 2018 года № 16756 «Об утверждении Правил проведения мониторинга выполнения единых требований в области информационно-

коммуникационных технологий и обеспечения информационной безопасности»;

3.11. СТ РК ISO/IEC 27000-2020 Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности Общий обзор и словарь;

3.12. СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования (далее – СТ РК ИСО/МЭК 27001-2015);

3.13. СТ РК ISO/IEC 27002-2015 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации (далее – СТ РК ИСО/МЭК 27002-2015);

3.14. СТ РК ISO/IEC 27003-2018 Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности Руководство;

3.15. СТ РК ISO/IEC 27005-2013 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности для связи между подразделениями и организациями;

3.16. СТ РК ISO/IEC 27010-2017 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности при коммуникациях между секторами и между организациями;

3.17. СТ РК ISO/IEC 27031-2013 Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса;

3.18. СТ РК ISO/IEC 27035-1-2017 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности Часть 1 Принципы менеджмента инцидентов;

3.19. СТ РК ISO/IEC 27035-2-2017 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности Часть 2 Руководящие указания по планированию и разработке реагирования на инциденты;

3.20. СТ РК ИСО/МЭК 13335-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий;

3.21. СТ РК ИСО/МЭК 13335-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий;

3.22. СТ РК ИСО/МЭК 13335-4-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой

информационных и коммуникационных технологий. Часть 4. Выбор защитных мер;

3.23. СТ РК ИСО/МЭК 13335-5-2008 Информационная технология Методы и средства обеспечения безопасности управление защитой информационных и коммуникационных технологий Часть 5 Руководство по управлению защитой сети;

3.24. СТ РК ИСО МЭК 31010-2010 Менеджмент риска. Методы оценки риска;

3.25. СТ РК ГОСТ Р 50739–2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

3.26. СТ РК 34.005–2002 Информационная технология. Основные термины и определения;

3.27. СТ РК 34.006–2002 Информационная технология. Базы данных. Основные термины и определения;

3.28. СТ РК 2190-2012 Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования;

3.29. СТ РК 2192-2012 Информационные технологии. Интернет-ресурс, интернет-портал, Интернет-портал. Общие описания;

3.30. СТ РК 2199-2012 Информационные технологии. Требования к безопасности Веб-приложений в государственных органах;

3.31. СТ РК 34.007–2002 Информационная технология. Телекоммуникационные сети. Основные термины и определения.

4 Применяемые термины и сокращения

В настоящем документе используются следующие термины и сокращения:

4.1. **Организация:** АО «Товарная биржа «Эстау».

4.2. **Руководство Организации (Первый руководитель Организации; Руководитель Организации):** Президент АО «Товарная биржа «Эстау».

4.3. **Ответственный сотрудник за обеспечение информационной безопасности (Ответственный сотрудник за обеспечение ИБ; Ответственный за обеспечение ИБ; СОИБ):** Сотрудник, отвечающий за контроль исполнения требований ИБ в Организации.

4.4. **Ответственный сотрудник по вопросам безопасности при работе с персоналом (СИБП):** Сотрудник, отвечающий за взаимодействие с ответственным за обеспечение ИБ, администраторами ИС, менеджером проекта и руководством Организации по вопросам безопасности при работе с персоналом.

4.5. **Операционные процедуры:** Действия, выполняемые персоналом в целях сопровождения, эксплуатации, обеспечения ИБ, технического обслуживания ИС, ЭИР.

4.6. **Политика (policy):** Намерения и направления, формально выраженные руководством [27002].

4.7. **Доступность (availability):** Свойство быть доступным и готовым к использованию по требованию авторизованного пользователя (сущности) [27001, ISO/IEC 13335-1].

4.8. **Интернет-ресурс (ИР)**: Электронный информационный ресурс, отображаемый в текстовом, графическом, аудиовизуальном или ином виде, размещаемый на аппаратно-программном комплексе, имеющий уникальный сетевой адрес и (или) доменное имя и функционирующий в Интернете [ET].

4.9. **Конфиденциальность (confidentiality):** Свойство, что информация становится недоступной и не раскрывается для неавторизованных пользователей, сущностей или процессов. [27001, ISO/IEC 13335-1].

4.10. **Менеджер проекта (МП):** Сотрудник Организации, отвечающий за управление проектом разработки, развития, сопровождения и поддержки ИС и/или ЭИР, ответственный за обеспечение надлежащей работы информационной системы в процессе эксплуатации и сопровождения ИС и/или ЭИР.

4.11. **Мобильный код:** Программный код, который можно перенести с одного компьютера на другой, а затем запускать автоматически для выполнения конкретной функции практически без взаимодействия с пользователем.

4.12. **Проприетарное программное обеспечение:** программное обеспечение, являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободного ПО (наличия

открытого программного кода недостаточно). Правообладатель проприетарного ПО сохраняет за собой монополию на его использование, копирование и модификацию, полностью или в существенных моментах. Обычно проприетарным называют любое несвободное ПО, включая полусвободное [Free Software Foundation (FSF)].

4.13. **Свободное программное обеспечение:** ПО удовлетворяющее следующим критериям [The Debian Free Software Guidelines (DFSG)]:

1) свободное распространение: лицензия не ограничивает распространение, каким бы то ни было лицам или организациям, не требует денежной компенсации;

2) исходные тексты: они должны присутствовать, и лицензия не должна ограничивать их распространение;

3) производные работы: лицензия должна разрешать создание и распространение производных работ от данного ПО на тех же условиях, как и оригинал;

4) целостность авторских исходных текстов: лицензия может запрещать распространение производных работ от исходных текстов, но в этом случае она должна разрешать свободное распространение патчей для исходного текста;

5) запрещается дискриминация людей или групп людей;

6) запрещается дискриминации по областям деятельности;

7) распространение лицензии: лицензия распространяется на любого, кто получил копию ПО;

8) лицензия не должна ограничивать другое ПО.

4.14. **Лицензионное программное обеспечение:** ПО, распространение, эксплуатация, использование, модификация, ребрендеринг и другие манипуляции контролируются и/или ограничиваются лицензионным соглашением.

4.15. **Администратор ИС (АИС, СА):** Ответственный сотрудник Организации или подрядной организации, назначенный выполнять работы по сопровождению ИС, и поддержанию среды эксплуатации ИС.

4.16. **Система менеджмента (управления) информационной безопасностью (СМИБ):** Часть общей системы управления Организацией, основанная на оценке бизнес-рисков и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности [27001].

4.17. **Сопровождение информационной системы:** Этап жизненного цикла информационной системы, на протяжении которого выполняются работы для обеспечения функционирования информационной системы, а также работы по изменению (модификации) ПО и документов информационной системы, вызванные возникшими проблемами или потребностями в модернизации или настройке.

4.18. **Целостность (integrity):** Свойство сохранения точности и полноты ресурсов. [27001, ISO/IEC 13335-1].

4.19. **Электронный информационный ресурс (ЭИР):** Информация, предоставленная в электронно-цифровой форме и содержащаяся на электронном носителе, Интернет-ресурсе и (или) в информационной системе [ЕТ].

4.20. **Электронная цифровая подпись (ЭЦП):** Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания [ЕТ].

4.21. **Эксплуатация информационной системы:** Этап жизненного цикла информационной системы, на протяжении которого информационная система используются в соответствии с её функциональным назначением и в соответствии с требованиями действующих документов Общества, а также осуществляются все необходимые действия по поддержке пользователей.

4.22. **Информационная система (ИС; Система):** Информационная система «Электронная торговая система товарной биржи».

4.23. **ОС:** Операционная система.

4.24. **ПО:** Программное обеспечение.

4.25. **ППО:** Прикладное программное обеспечение.

4.26. **ПП РК:** Постановление Правительства Республики Казахстан;

4.27. **ПИС, IPR:** Права на интеллектуальную собственность.

4.28. **СПО:** Системное программное обеспечение.

4.29. **БД:** База данных.

4.30. **СУБД:** Система управления базами данных.

4.31. **СП:** Сервер приложений.

4.32. **СК:** Серверная комната.

4.33. **ВП:** Веб-портал.

4.34. **ДМ:** Дисковый массив.

4.35. **РК:** Республика Казахстан.

4.36. **СКУД:** система контроля и управления доступом;

4.37. **СХД:** Система хранения данных.

4.38. **СЭ:** Сетевой экран.

4.39. **СЗИ:** Средства защиты информации.

4.40. **НУЦ РК, НУЦ:** Национальный удостоверяющий центр Республики Казахстан.

4.41. **ЭЦП:** Электронно-цифровая подпись.

4.42. **RSA (аббревиатура от фамилий Rivest, Shamir и Adleman):** криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

5 Цели и задачи Политики информационной безопасности

5.1.Цели

Главной целью, на достижение которой направлены все положения настоящего документа, является надежное обеспечение информационной безопасности информационных активов ИС.

Обеспечения информационной безопасности необходимо для минимизации ущерба от реализации угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИС.

Так же целью настоящего документа является обеспечить участие руководства Организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами Республики Казахстан.

В настоящем документе руководство Организации четко прописывает требования к обеспечению информационной безопасности, проявляя и поддерживая требования к информационной безопасности путем распространения настоящей политики информационной безопасности во всей организации и обязывая беспрекословное исполнение всех требований.

5.2.Задачи

Для достижения поставленных целей необходимо решить следующие задачи:

a) защита от вмешательства посторонних лиц в процесс функционирования ИС;

b) разграничение доступа зарегистрированных пользователей к информации, аппаратным, программным и криптографическим средствам защиты, используемым в ИС;

c) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

d) защита информации от несанкционированной модификации и искажения;

e) контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносных кодов, включая компьютерные вирусы;

f) обеспечение аутентификации пользователей ИС;

g) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба.

Владельцем Политики информационной безопасности является Организация.

5.3.Документирование политики информационной безопасности

Настоящий документ, содержит политику информационной безопасности, утверждается руководством Организации и доводится до

сведения всех сотрудников проекта, а также сторонних организаций и частных лиц в мере, соответствующей договорным и/или лицензионным отношениям и/или другим видам договоренностей с третьими лицами.

5.4.Пересмотр политики информационной безопасности

Настоящий документ подвергается анализу и пересмотру не реже одного раза в год или при возникновении существенных изменений, влияющих на соответствие требованиям стандартов, адекватности и эффективности применяемых мер обеспечения ИБ, выявленных в процессе внешнего или внутреннего аудита.

В ходе пересмотра следует оценить возможность улучшения положений политики информационной безопасности и процесса управления информационной безопасностью в соответствии с изменениями условий ведения бизнеса, законодательства, изменениями в организационной структуре или ИС, изменениями адекватной реальности и информационных угроз окружающей среды.

Ответственным лицом за контроль, реализацию, распространения, применения, исполнения, за развитие, оценку и пересмотр настоящего документа назначается сотрудник ответственный за обеспечение информационной безопасности.

Ответственный сотрудник за обеспечение информационной безопасности назначается приказом руководства Организации.

5.4.1. Процедура пересмотра политики информационной безопасности

Периодическая оценка и пересмотр настоящего документа производится согласно утвержденному графику по форме Приложения 1.

Оценка и пересмотр настоящего документа по результатам внешнего или внутреннего аудита производится по окончании всех мероприятий аудита.

Началом оценки и пересмотра настоящего документа является приказ руководства Организации об утверждении графика с указанием ответственных лиц за пересмотр разделов документа.

Ответственность за составление приказа и графика пересмотра возлагается на сотрудника ответственного за пересматриваемый документ.

В приказе должна быть отражена поддержка руководства Организации беспрепятственному улучшению Политики информационной безопасности, выделению финансовых и человеческих ресурсов для совершенствования обеспечения ИБ там, где это оправдано и необходимо.

Каждый ответственный за раздел документа сотрудник должен работать со своей копией документа.

По мере необходимости ответственный за пересматриваемый документ сотрудник созывает коллективные совещания всех заинтересованных сторон и обеспечивает им обратную связь. Председательство на совещаниях возлагается на ответственного за пересматриваемый документ сотрудника.

Результатом каждого совещания является протокол заседания, подписанный всеми участниками.

В случае если изменения одного раздела неизбежно влекут изменения других разделов, конфликтуют друг с другом или затрагивают политику информационной безопасности в целом, такие изменения должны согласовываться всеми ответственными за разделы документа сотрудниками.

Ответственный за пересматриваемый документ сотрудник должен проверять целостность требований, их непротиворечивость, соответствие принятым в РК законам стандартам после каждого принятого изменения.

Ответственный за пересматриваемый документ сотрудник и ответственные за пересмотр разделов документа должны учитывать следующие условия при принятии изменений в пересматриваемый документ:

a) при пересмотре политики информационной безопасности должны учитываться результаты пересмотра принципов управления организацией в целом;

b) жалобы и рекламации заинтересованных третьих сторон;

c) возможность улучшения положений политики информационной безопасности и процесса управления информационной безопасностью в соответствии с изменениями условий ведения бизнеса, доступности ресурсов, законодательства, изменениями в организационной структуре или информационной системе Организации;

d) существующие и вновь появившиеся угрозы и уязвимости информационной системы;

e) отчеты об инцидентах в области информационной безопасности (13.1);

f) рекомендации органов государственной власти (6.1.6);

g) результаты независимого аудита (6.1.8);

h) предпринятые необходимые корректирующие и предупреждающие действия (см. 6.1.8 и 15.2.1);

i) результаты предыдущих аудитов принципов управления;

j) процесс исполнения и соблюдения политики информационной безопасности.

Принятые на совещании изменения вносятся в режиме рецензирования в рабочую копию документа с отметкой о причине внесения изменений на полях и копии документа у ответственных сотрудников обновляется. Все принятые изменения и их причины сохраняются. Начальная копия документа и все промежуточные копии документа сохраняются у ответственного за пересматриваемый документ сотрудника.

Ответственный за пересматриваемый документ сотрудник отвечает за соблюдение сроков утвержденного графика. В случае нарушения сроков об этом должно быть уведомлено руководство Организации для принятия мер стимуляции процесса пересмотра. Выбор способов стимуляции процесса пересмотра находится в ответственности руководства Организации и должен соответствовать законодательству РК.

Вывод из пересмотра принципов управления должны включать в себя любые решения и действия, связанные с:

a) усовершенствованием подхода организации по управлению информационной безопасности и ее процессами;

b) улучшением целей и мероприятий по управлению информационной безопасностью;

c) усовершенствованием в распределении ресурсов и обязанностей.

По результатам совещания о принятия всех изменений, ответственный за пересматриваемый документ сотрудник направляет протокол совещания и результаты пересмотра с обоснованием всех принятых в документе изменений на согласование в порядке, установленном Организацией.

Согласующие стороны вправе запросить у ответственных за разделы пересматриваемого документа сотрудников дополнительных пояснений или корректировки внесенных изменений, если они обоснованы.

Пересмотренная политика информационной безопасности должна быть утверждена руководством организации.

6 Организация информационной безопасности

6.1. Внутренняя организация

Внутренняя структура Организации с выделенным сотрудником ответственным за обеспечение ИБ и отдельным подразделением ответственным за сопровождение ИС отражена в документе «Организационная структура».

Документы по ИБ создаются в соответствии с требованиями Приказа № 111/НҚ и ПП РК № 832 и в соответствии с требованиями СТ РК ISO/IEC 27001, СТ РК ISO/IEC 27002.

Документы по ИБ доводятся до сведения всех сотрудников проекта, а также сторонних организаций и частных лиц в мере, соответствующей договорным и/или лицензионным отношениям и/или другим видам договоренностей с третьими лицами. Документы по ИБ пересматриваются с целью анализа и актуализации, изложенной в них информации не реже одного раза в два года.

Настоящий документ является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ.

В перечень документов второго уровня входят документы, детализирующие требования настоящего документа, в том числе:

1) методика оценки рисков информационной безопасности;
2) правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;
3) правила проведения внутреннего аудита ИБ;
4) правила использования средств криптографической защиты информации;
5) правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам;
6) правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;
7) правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

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

1) каталог угроз (рисков) ИБ;
2) план обработки угроз (рисков) ИБ;
3) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

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

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

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 (ведется на стороне владельца серверных и кроссовых помещений);

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений (ведется на стороне владельца серверных и кроссовых помещений);

5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;

Ответственность за соблюдение требований настоящего документа и других документов по обеспечению ИБ возлагается на ответственного сотрудника Организации за обеспечение ИБ.

6.1.1. Обязанности руководства по обеспечению информационной безопасности

Настоящим документом руководство Организации утверждает требуемый уровень информационной безопасности ИС, который необходимо поддерживать, определяет механизмы управления информационной безопасностью и распределяет обязанности и ответственность персонала за ее обеспечение.

Руководство Организации выполняет следующие функции:

a) обеспечение целей информационной безопасности в соответствии с организационными требованиями и использование их в соответствующих процессах;

b) утверждает и контролирует пересмотр политики информационной безопасности ИС и других документов, требуемых для обеспечения информационной безопасности;

c) контролирует эффективность внедрения политики информационной безопасности;

d) выполняет управление и поддержку инициатив в области безопасности;

e) выделяет ресурсы (финансовые, материальные и человеческие) для обеспечения информационной безопасности;

f) распределяет основные обязанностей и ответственности в отношении информационной безопасности в Организации;

g) утверждает документы, планы и перечни (списки) по поддержке обеспечения информационной безопасности;

h) контролирует согласованность средств управления информационной безопасности в Организации (см. 6.1.2).

Для обеспечения необходимого уровня осведомленности сотрудников Организации руководство обеспечивает и контролирует обучение сотрудников в области информационной безопасности.

Для поддержания необходимого уровня осведомленности потребителей услуг Организации, зависящих от ИС и пользователей ИС, на сайте Организации имеется специальная рубрика со статьями, улучшающими понимание информационной безопасности и повышающих знания в этой области. Информация, обязательная к прочтению, отмечена красным цветом.

В случае необходимости по инициативе сотрудников организации или на собственное усмотрение руководство может проводить консультации у сторонних специалистов по информационной безопасности на платной или бесплатной основе.

Результаты консультаций должны документироваться в виде протоколов ответственными сотрудниками, в порядке установленными для обучения сотрудников организации и пользователей ИС.

Для того что бы обеспечить требуемый уровень информационной безопасности, а также для дальнейшего поддержания защищенности информации, информационных ресурсов, информационных систем, оборудования обработки, хранения и передачи информации и всей информационной инфраструктуры руководство Организации берет на себя обязанности и ответственность за обеспечение возможности выполнения работниками и привлекаемыми со стороны исполнителями обязательств в отношении ИБ.

Таким образом в случае возникновения ситуации при которой сотрудник Организации или привлекаемый со стороны исполнитель не может выполнить свои обязательства в рамках и в соответствии с требованиями документов регламентирующих обеспечение ИБ, руководство Организации принимает на себя обязательства исправить сложившуюся ситуацию в кротчайшие сроки и взять на себя ответственность за последствия такой ситуации.

6.1.2. Координация вопросов обеспечения информационной безопасности

Действия по обеспечению информационной безопасности координируются СОИБ и/или рабочей группой по ИБ.

Рабочая группа по ИБ создается приказом руководителя Организации при необходимости. Руководителем рабочей группы назначается СОИБ. В состав рабочей группы включаются ответственные сотрудники подразделений Организации и третьих сторон, отвечающие за обеспечение функционирование ИС в соответствии с установленными требованиями. Участники рабочей группы по ИБ должны иметь соответствующие функции и должностные обязанности, позволяющие поддерживать установленный режим информационной безопасности ИС.

Один раз в месяц (или по требованию руководства Организации или ответственного за обеспечение ИБ) в организации проводятся совещания рабочей группы по ИБ с участием руководства Организации по вопросам координации действий по поддержанию режима безопасности ИС. Совещания протоколируются и подписываются членами рабочей группы по ИБ.

Координация вопросов обеспечения информационной безопасности предусматривает сотрудничество между менеджерами, пользователями, администраторами, разработчиками приложений, аудиторами и сотрудниками безопасности, специалистами в области страхования и управления рисками, управления персоналом, менеджерами договоров, владельцами/распорядителями финансовыми и кадровыми ресурсами, а также обладать знаниями в правовых вопросах и управлении персоналом. Эта деятельность должна:

a) обеспечить безопасность работы, выполняемые в соответствии с политикой информационной безопасности;

b) определить способы обработки несоответствий;

c) согласовать конкретные методики и процедуры информационной безопасности, например, такие как оценка рисков, классификация информации с точки зрения требований безопасности;

d) выявить существенные изменения потенциальных угроз и подверженность информации и средств обработки информации к угрозам;

e) оценить адекватность и координировать внедрение конкретных мероприятий по управлению информационной безопасностью;

f) содействовать образованию сотрудников в области информационной безопасности, обучению и пониманию важности информационной безопасности в рамках всей организации;

g) оценить информацию, полученную в ходе мониторинга и пересмотра инцидентов информационной безопасности, и предпринять соответствующие меры по выявленным инцидентам.

6.1.3. Распределение обязанностей по обеспечению информационной безопасности

Настоящий документ устанавливает общие принципы и правила распределения функций и обязанностей, связанных с обеспечением информационной безопасности в организации. Политику следует, дополнять соответствующими инструкциями, правилами, планами, перечнями, графиками и журналами, являющимися неотъемлемой частью СМИБ и обязательными для исполнения руководством Организации, всеми сотрудниками проекта и третьими сторонами в соответствии с договорными обязательствами.

Ответственный за обеспечение ИБ может передавать свои полномочия по обеспечению безопасности кому-либо из сотрудников проекта или поставщикам услуг. Тем не менее, он остается ответственным за обеспечение

безопасности ИС и должен быть в состоянии определить, что любые переданные полномочия реализуются с соблюдением требований СМИБ.

В каждом документе составляющим СМИБ ИС четко прописаны обязанности и ответственность руководства Организации, ответственного за обеспечение ИБ, сотрудников проекта, пользователей и ответственных сотрудников третьих сторон и выполняются следующие правила:

a) активы и процессы (процедуры) безопасности, ИС, выделены и четко определены;

b) вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного ответственного сотрудника Организации (7.1.2);

c) уровни полномочий (авторизации) д ясно определены и документированы.

В случае временной нетрудоспособности СОИБ его права, обязанности и ответственность могут быть переданы другому сотруднику на усмотрение руководителя Организации. Передача прав, обязанностей и ответственности СОИБ закрепляется приказом руководителя Организации.

6.1.4. Процедура получения разрешения на использование средств обработки информации

Под новыми средствами обработки информации следует понимать программные, аппаратные, программно-аппаратные средства обработки данных приобретаемые, арендуемые или перенесенными с одного места использования на другое, переданные в использование новому сотруднику Организации или третьей стороне по договоренности.

При рассмотрении необходимости использования новых средств обработки информации, должны выполняться следующие требования:

a) одобрение использования новых средств обработки информации должно проходить до приобретения этих средств, на этапе составления технических спецификаций к договорам приобретения/аренды, при согласовании необходимо получить положительные отзывы от администраторов ИС, ответственного сотрудника по ИБ, менеджера ИС (для которой эти средства предусмотрены), в соответствии с должностными обязанностями;

b) аппаратные средства и программное обеспечение должны быть проверены на совместимость с другими компонентами информационной инфраструктуры Организации, результаты таких проверок должны быть оформленные в виде протоколов тестирования новых средств обработки информации;

c) в процессе тестирования новых средств обработки информации должно быть также определено соответствие функциональных возможностей выдвигаемым к ним требованиям, соответствие принятым в Организации нормам обеспечения ИБ;

d) средства обработки информации, передаваемые сотруднику, должны соответствовать его потребностям при исполнении своих должностных обязанностей;

e) сотрудник, принимающий средства обработки в пользование, должен использовать их строго в целях исполнения своих должностных обязанностей, и несет материальную ответственность за их сохранность;

f) использование личных средств обработки информации (например, ноутбуки, домашние компьютеры или иные портативные устройства) для обработки служебной информации в сети Организации запрещено;

g) использование мобильных устройств регулируется Правилами организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

6.1.5. Соглашения о соблюдении конфиденциальности

Настоящим документом руководство Организации определяет условия конфиденциальности и требования к соглашению о неразглашении информации в соответствии с целями защиты информации.

Соглашения о конфиденциальности или соглашения о неразглашении используются для уведомления о том, что информация является конфиденциальной или секретной. Соглашение составляется и заключается в соответствии с требованиями законодательства.

В организации могут быть использованы несколько форм соглашений о конфиденциальности и неразглашения информации (в отдельном документе или как часть договорных отношений):

a) соглашение с поставщиками;
b) соглашение с заказчиками;
c) соглашение с клиентами на договорной основе;
d) соглашение с клиентами на основе публичной оферты;
e) соглашение с партнерами.

На основании требований безопасности, принятых в Организации, могут возникнуть другие необходимости в заключении соглашения о конфиденциальности и неразглашении информации.

Соглашения о конфиденциальности и неразглашении информации защищают информацию ИС и ставят в известность подписавшие стороны о том, что они несут ответственность за защиту и использование информации, и ее использование и/или разглашение должно быть только в установленном порядке.

В соглашении о конфиденциальности и неразглашении информации необходимо указывать следующие сведения:

a) определение защищаемой информации (например, данные, защищаемые и ограниченные к распространению законами Республики Казахстан и (или) владельцами (собственниками), в том числе персональные данные, сведения, составляющие банковскую тайну, коммерческую (предпринимательскую) тайну, налоговую тайну, другие виды тайн);

b) ожидаемую продолжительность соглашения, включая случаи, когда требуется сохранить конфиденциальность на неопределенный срок;

c) необходимые действия в случае аннулирования соглашения;

d) обязанности и действия подписавших сторон, чтобы избежать утечки информации и предоставление подписанту доступ только к данным, безусловно необходимым ему для выполнения конкретной функции;

e) определение собственности предоставляемой информации с указанием владельца;

f) разрешение использования конфиденциальной информации, и права подписавшихся сторон на использование информации;

g) право на проведение аудита и мониторинга деятельности, связанной с конфиденциальной информацией владельцем информации или его уполномоченным представителем;

h) способы уведомлений и сообщений о несанкционированном разглашении или нарушении конфиденциальной предоставленной информации;

i) условия для сведений, которые могут быть возвращены или уничтожены при прекращении соглашения;

j) ожидаемые действия со стороны владельца переданной информации и подписанта, которые будут приняты в случае нарушения этого соглашения.

Соглашения о конфиденциальности и неразглашении информации должны соответствовать всем применяемым нормам законодательства (см. 15.1.1).

Сроки и порядок пересмотра требований в содержании соглашений о конфиденциальности и неразглашении информации устанавливается в соответствии с разделом 5.4 настоящего документа.

На СОИБ возлагается ответственность за контроль соблюдения требований в отношении заключения соглашений о конфиденциальности и неразглашении информации и контроль за соблюдением соответствующих соглашений со всеми сотрудниками Организации, а также подрядными организациями.

6.1.6. Взаимодействие с компетентными органами

В ответственность руководства Организации входит поддерживание контактов с представителями:

a) региональных правоохранительных органов:
   - Комитета национальной безопасности,
   - Прокуратуры,
   - Министерства внутренних дел;

b) региональных органов исполнительной власти:
   - Акимата,
   - Комитета государственных доходов.

c) региональных органов чрезвычайных ситуаций:
   - Министерства чрезвычайных ситуаций,

- службы реагирования на компьютерные инциденты (KZ-CERT),
- РГП «Государственная техническая служба»;

d) служб оказания срочной помощи:
- станций пожаротушения,
- пунктов оказания срочной медицинской помощи,
- газовых служб,
- аварийных служб электросети и водоснабжения.

e) поставщиков услуг и средств производства:
- поставщиков услуг юридической консультации,
- поставщиков каналов связи,
- поставщиков каналов электропитания,
- поставщиков водоснабжения,
- поставщиков средств контроля климата,
- поставщиков средств бесперебойного питания,
- поставщиков средств видеонаблюдения,
- поставщиков средств контроля и управления доступом,
- поставщиков технологических площадок,
- поставщиков серверного, клиентского и сетевого оборудования,
- исполнителей услуг охраны,
- исполнителей услуг, переданных на аутсорсинг.

f) клиентов для оповещения.

Ответственный за обеспечение ИБ сотрудник обязан держать в актуальном состоянии перечень контактов и информировать руководство Организации и других ответственных лиц в случае его изменения.

Поддержание таких контактов является обязательным для поддержки информационной безопасности, управления инцидентами (Раздел 13.2), непрерывности бизнеса и процесса планирования (Раздел 14).

Взаимодействие с регулирующими органами, также необходимы для прогнозирования и подготовки к предстоящим изменениям в законодательстве или правилах, которые должны соблюдаться Организацией.

Также на сайте Организации и/или на сайте ИС имеется специальная рубрика оповещения клиентов и пользователей о всех затрагивающих их интересы событиях. События, имеющие особую и чрезвычайную важность, отмечены красным цветом.

Для организации действий сотрудников проекта и пользователей разработана инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, определяющая ответственность и порядок взаимодействия во внештатных ситуациях и при обнаружении инцидента ИБ.

6.1.7. Взаимодействие с ассоциациями и профессиональными группами

В ответственность руководства Организации входит поддерживание контактов с профессиональными группами, ассоциациями и участвовать в

конференциях (форумах) специалистов в области информационной безопасности.

В связи с тем, что направление обеспечения информационной безопасности не является для Организации основным, руководство вправе ограничивать участие Организации на свое усмотрение.

Однако в обязательное участие должны войти все мероприятия, организовываемые уполномоченными государственными органами в сфере информатизации и обеспечения информационной безопасности.

Также сотрудники Организации могут вносить на рассмотрение руководства предложения об участии в мероприятиях с обоснованием пользы и эффективности его потенциальных результатов.

Дополнительно, руководство Организации не ограничивает и приветствует самостоятельное участие сотрудников в онлайн-семинарах, онлайн-вебинарах, интернет-форумах и выпуск собственных публикации на тему информационной безопасности, если таковые не нарушают соглашения о конфиденциальности и неразглашении информации.

Руководство Организации готово рассмотреть предложения членства в профессиональных группах по ИБ или участие в конференциях (форумах), и поддерживает аналогичное отношение к этой деятельности среди своих сотрудников, в первую очередь как средство для:

a) совершенствования знаний и навыков и соответствия новейшим требованиям в области информационной безопасности;

b) обеспечения полного понимания обстановки в области информационной безопасности;

c) получения своевременных предупреждений о тревожных сигналах, опасности и исправлений, касающиеся атак и уязвимостей;

d) получения доступа к специалистам за консультацией по вопросам информационной безопасности;

e) обмена информацией о новых технологиях, программных продуктах, угроз или уязвимостей;

f) организации адекватного реагирования на инциденты нарушения информационной безопасности (см. 13.2.1).

Помимо прочего руководством Организации могут рассматриваться предложения о совместных работах над проектами и заключении договорных отношений с целью улучшения сотрудничества и координации в вопросах безопасности, при соблюдении всех необходимых мер по строгому разграничению ответственности и соблюдении соглашений о конфиденциальности и неразглашении информации и норм законодательства РК.

6.1.8. Независимая[1] проверка (аудит) информационной безопасности

Требования к проверкам (аудитам) информационной безопасности изложены в Правилах проведения внутреннего аудита ИБ.

6.2. Обеспечение безопасности при наличии доступа сторонних организаций[2] к информационным системам

Необходимо обеспечивать безопасность информации и средств обработки информации Организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации.

Безопасность информации Организации и средств обработки информации не должна снижаться в результате доступа сторонних организаций к информационным системам.

Доступ к средствам обработки информации организации третьих сторон должен контролироваться. Все доступы сторонних организаций к информации и средствам обработки информации Организации должны быть авторизованы и фиксироваться, а представители сторонних организаций, имеющие доступ согласованы с руководством Организации и ответственным за обеспечение ИБ сотрудником.

Настоящим документом разделяются несколько классификаций доступа сторонних организаций и физических лиц:

1) классификация по целевому объекту:
   a) объект доступа – информация,
   b) объект доступа – средство обработки информации (одно и более),
   c) доступ к объекту технологического обеспечения информационной инфраструктуры Организации;
2) классификация по типу доступа:
   a) физический доступ,
   b) удаленный доступ;
3) классификация по географическому месту расположения субъекта и объекта доступа:
   a) из сети Организации к объекту в той же сети,
   b) из сети Организации к объекту за пределами сети Организации,
   c) из сторонней сети к объекту в сети Организации,
   d) из сторонней сети к объекту за пределами сети Организации;
4) классификация по защищенности каналов связи:
   a) доступ по защищенному каналу связи,
   b) доступ по незащищенному каналу связи;
5) классификация по цели доступа:

---

[1] В документах, регулирующих обеспечение ИБ проекта ИС слово «независимый» следует понимать, как независящий от проверяемого объекта, то есть аудитор проверяющий объект не имеет к нему отношения.

[2] В документах, регулирующих обеспечение ИБ проекта ИС словосочетание «сторонняя организация» следует понимать не только как стороннее юридическое лицо, но также как физическое лицо не имеющее прямое отношение к ИС или нанятое для выполнения конкретной работы на временной основе или стажера, временного консультанта и т.п.

a) потребление услуги,
b) предоставление услуги;

6) классификация по доверию к месту доступа субъекта:
a) доступ из доверенного места,
b) доступ из недоверенного места;

7) классификация по субъекту доступа:
a) доступ для клиентов (потребителей услуг Организации, не являющимися заказчиками разработки этих услуг),
b) доступ для заказчиков,
c) доступ для партнеров,
d) доступ для поставщиков услуг, оборудования.

Один и тот же доступ одного и того же субъекта может принадлежать разным классам в разных классификациях, но принадлежит только одному классу в рамках одной классификации.

Доступ сотрудников сторонних организаций к информации может осуществляться только по посредствам следующих классов доступа: 1) b); 2) a), b); 3) a), b), c); 4) a); 5) a), b); 6) a); 7) a), b), c), d).

Так же для определения доступа сторонней организации необходимо учитывать классификацию информации, как защищаемого объекта.

Доступ сторонних организаций к информации и средствам обработки информации Организации должен предоставляться с учетом соблюдения требований обязательств Организации в других договорных отношениях с соблюдением законодательства РК.

В случаях, когда возникает потребность в доступе третьей стороны, к информации организации и средствам обработки информации, а также в случае приобретения дополнительных услуг, программных продуктов или организации сервисного обслуживания средств обработки информации и других объектов технологического обеспечения, следует производить оценку риска, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью в соответствии с Методикой оценки рисков информационной безопасности.

Результаты такой оценки должны отражаться в документах, создаваемых для обоснования приобретения услуг, программных продуктов.

Обоснование потребности в доступе третьей стороны, к информации организации и средствам обработки информации должно быть оформлено в виде служебной записке на имя руководителя организации с обязательным согласованием СОИБ.

Все требования к доступу сторонней организации необходимо согласовывать с ответственным за обеспечение ИБ сотрудником, утверждать руководством Организации, отражать в договорных обязательствах третьей стороны и соглашении о конфиденциальности и неразглашении информации.

Ответственный за обеспечение ИБ обязан вести перечень предоставленных сторонним организациям и частным лицам доступов со ссылкой на соответствующие соглашения, в рамках которых эти доступы предоставлены.

6.2.1. Определение рисков, связанных со сторонними организациями

Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности Организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности в соответствии с Методикой оценки рисков информационной безопасности.

Там, где доступ сторонней организации к информации и средствам обработки, принадлежащим Организации, уже предоставлен следует производить регулярную переоценку рисков, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью в соответствии с Методикой оценки рисков информационной безопасности.

При определении рисков, связанных с доступом сторонней организации, Методика оценки рисков информационной безопасности учитывает следующие мероприятия:

a) необходимость доступа сторонней организации к средствам обработки информации;

b) тип доступа к информации и средствам обработки информации для сторонних организаций, например:

- физический доступ – к офисным помещениям, компьютерным комнатам, серверным;
- авторизованный (логический) доступ – к базам данных организации, информационным системам организации;

c) сетевое обеспечение связи между организацией и сетью сторонних организаций, например, постоянное подключение, удаленный доступ;

d) географическое месторасположение субъекта и объекта доступа, а также доверие к месту доступа субъекта;

e) значимость и чувствительность вовлеченной информации, и ее критичность для бизнес-операций;

f) меры управления по защите информации, не предназначенные для доступа сторонних организаций;

g) персонал сторонней организации, участвующий в обработке информации Организации;

h) организации, и персонал, имеющие авторизованный доступ, должны быть четко определены, проверены, согласованны с ответственным за обеспечение ИБ сотрудником и утверждены руководством Организации;

i) средства и элементы контроля, используемые сторонней организацией для хранения, обработки, совместного использования и обмена информацией должны быть проверены, согласованны с ответственным за обеспечение ИБ сотрудником и утверждены руководством Организации;

j) в рисках учитываются случаи предоставления доступа, не являющегося необходимым (требуемым) для сторонней организации и

получения сторонней организацией неточной или вводящей в заблуждение информации о доступе;

k) действия и процедуры для обработки инцидентов информационной безопасности и риск потенциальных повреждений, а также продолжение предоставления доступа сторонней организации, в случае инцидента нарушения информационной безопасности;

l) правовых и нормативных требований и других договорных обязательств, имеющих отношение к сторонней организации, которые должны быть приняты во внимание;

m) интересы любых других заинтересованных сторон могут быть затронуты в договоренности.

Доступ сторонних организаций к информации организации не должен осуществляться, пока не будут приняты меры по защите информации, подписаны договорные отношения, отражающие требования информационной безопасности к доступу и соглашение о конфиденциальности и неразглашении информации.

Все требования безопасности и внутренний контроль в результате работы со сторонними организациями, должны быть отражены в соглашениях со сторонними организациями (см. 6.2.2 и 6.2.3).

Необходимо, чтобы сторонняя организация ознакомилась со своими обязанностями, а также принимала на себя ответственность и обязательства, возникающих в результате получения доступа, обработки, совместного использования информации и средств обработки информации, принадлежащих Организации.

В случае предоставления доступа сторонним организациям, Организация оставляет за собой права контроля, управления, мониторинга, защиты, блокирования доступа на свое усмотрение.

Случаи с несколькими внешними заинтересованными сторонами должны быть документально закреплены, а ответственность сторон точно определена и идентифицирована.

Мероприятия по управлению информационной безопасностью, приведенные в Разделах 6.2.2 и 6.2.3 настоящего документа, должны применяться в различных комбинациях предоставления доступа сторонним организациям, такие как:

a) поставщики услуг, таких как услуг сети Интернет, телефонной связи, организации технического обслуживания и поддержки;

b) управление службы безопасности;

c) покупатели;

d) привлечение внешних средств и/или операций, например, систем информационных технологий, службы сбора данных, операции центра телефонного обслуживания;

e) аудиторы и консультанты по вопросам управления и бизнеса;

f) сотрудники, осуществляющие поддержку и сопровождение аппаратных средств и программного обеспечения;

g) сотрудники, осуществляющие уборку, обеспечивающие охрану и другие услуги;

h) стажеры и лица, работающие по временным трудовым соглашениям.

Такие соглашения должны способствовать снижению рисков, связанных со сторонними организациями и третьими лицами.

Участие других сторон в соглашениях со сторонними организациями должно быть четко оговорено и согласовано с руководством Организации и ответственным за обеспечение ИБ.

6.2.2. Процедура предоставления доступа сторонним организациям и частным лицам

Процесс рассмотрения возможности предоставления доступа инициируется в рамках заключения договорных отношений со сторонней организацией или физическим лицом, или официальным письмом сторонней организацией или физического лица с запросом о доступе.

Запрос о доступе должен быть обоснован и описан сторонней организацией или частным лицом. В запросе должны быть указаны сведения о лицах, которым будет предоставлен доступ.

Ответственным за сопровождение процесса рассмотрения возможности предоставления доступа сторонней организации или физическому лицу является ответственный за обеспечение ИБ сотрудник.

Ответственный за обеспечение ИБ сотрудник при участии ответственного за администрирование средства обработки информации или ИС, ответственного за помещение, к которому необходим доступ, ответственного менеджера ИС, ответственного разработчика, если доступ требуется к разрабатываемым ресурсам, программному коду или к архитектуре ИС, проверяет обоснованность запроса.

Далее ответственный за обеспечение ИБ, используя классификатор активов (Раздел 7), классификации видов доступа (п. 6.2), и другие утвержденные документы по обеспечению ИБ в Организации определяет необходимые меры по защите при доступе сторонней организации или физического лица.

Полученные результаты отражаются в соглашении (договор и соглашение о неразглашении) со сторонней организацией или частным лицом, согласуются с ответственными за актив сотрудниками и подписываются всеми участвующими в доступе сторонами.

Полученный документ заверяется подписью СОИБ утверждается руководителем Организации.

6.2.3. Рассмотрение вопросов безопасности при работе с клиентами

Перед предоставлением клиентам права доступа к информации или активам Организации необходимо определить и внедрить меры безопасности.

Перед предоставлением клиентам права доступа к любым активам организации (в зависимости от вида и степени доступа к данным, не все из них могут быть применены) учитываются следующие условия по решению вопросов безопасности:

a) защита активов, включая:

1) процедуры по защите активов организации, в том числе информации и программного обеспечения, а также управление известных уязвимостей;

2) процедуры для определения компрометации активов, например, вследствие потери или модификации данных;

3) целостность;

4) ограничения на копирование и раскрытие информации;

b) описание каждого предоставляемого продукта или услуги;

c) различные причины, требования и преимущества для доступа клиентам;

d) соглашения по управлению доступом, охватывающие:

1) разрешенные методы доступа, а также управление и использование уникального идентификатора, типа пользовательских ID и паролей;

2) процесс авторизации в отношении доступа и привилегий пользователей;

3) сведения о том, что любые неавторизованные доступы, запрещены;

4) процесс аннулирования прав доступа или прерывания связи между системами;

e) меры для отчетности, уведомления, а также изучение информации о неточностях (например, личные подробности), инцидентов нарушения информационной безопасности;

f) описание каждой предоставляемой услуги;

g) определение необходимого и неприемлемого обслуживания;

h) право мониторинга и аннулирования любых действий, связанные с активами организации;

i) соответствующие обязательства организации и заказчика;

j) обязательства относительно юридических вопросов, например, законодательства о защите данных с учетом различных национальных законодательств, особенно если контракт относится к сотрудничеству с организациями в других странах (15.1);

k) права интеллектуальной собственности (IPR) и авторские права (15.1.2), а также правовая защита любой совместной работы (6.1.5).

Требования безопасности, связанные с клиентами, обращающимися к активам Организации, могут измениться значительно в зависимости от средств обработки информации и информации, к которой обращаются.

6.2.4. Рассмотрение требований безопасности в соглашениях со сторонними организациями

Договорные отношения со сторонними организациями должны документально оформляться и содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации.

Такие соглашения должны быть согласованы с ответственными сотрудниками Организации: ответственным за обеспечение ИБ, ответственным за администрирование средства обработки информации, ответственным за помещение, к которому необходим доступ, ответственным менеджером ИС, ответственным разработчиком, если доступ требуется к разрабатываемым ресурсам, программному коду или к архитектуре ИС.

Письменное изложение договорных отношений должно составляться с целью, обеспечить уверенность в том, что нет никакого недопонимания между сторонами.

Для удовлетворения определенных требований безопасности следует учесть следующие положения, включаемые в соглашение (см. 6.2.1):

a) политику информационной безопасности;

b) защиту активов, включая:

1) процедуры по защите активов организации, в том числе информации и программного обеспечения;

2) любые необходимые способы ограничения физического доступа;

3) мероприятия по управлению информационной безопасностью для обеспечения защиты от вредоносного программного обеспечения (10.4.1);

4) процедуры для определения компрометации активов, например, вследствие потери или модификации данных;

5) мероприятия по обеспечению возвращения или уничтожения информации и активов по окончании соглашения или в установленное время в течение действия контракта;

6) конфиденциальность, целостность и доступность активов (2.1.5);

7) ограничения на копирование и раскрытие информации, предусмотренные в соглашении о конфиденциальности (6.1.5);

c) обучение пользователя и администратора методам и процедурам безопасности;

d) определение процесса информирования о возникающих проблемах в случае непредвиденных обстоятельств;

e) условия для перевода/приема/увольнения/замены персонала, в случае необходимости;

f) обязанности, касающиеся установки и сопровождения аппаратных средств и программного обеспечения;

g) четкая структура подотчетности и согласованные форматы предоставления отчётов;

h) четкий и определенный процесс управления изменениями;

i) соглашения по управлению доступом, охватывающие:

1) различные причины, требования и преимущества, необходимые для доступа сторонних лиц;

2) разрешенные методы доступа, а также управление и использование уникальных идентификаторов, типа пользовательских ID и паролей;

3) процесс авторизации в отношении доступа и привилегий пользователей;

4) требование актуализации списка лиц, имеющих право использовать предоставляемые услуги, а также соответствующего списка прав и привилегий.

5) сведения обо всех видах доступа, не авторизованные в четкой форме, являются запрещенными;

6) процесс аннулирования прав доступа или прерывания связи между системами;

j) процедуры отчетности, уведомления и расследования инцидентов нарушения информационной безопасности и выявления слабых звеньев системы безопасности;

k) описание предоставляемого продукта или услуги, а также описание информации, которые должны быть предоставлены вместе с безопасностью классификации (см. 7.2.1);

l) определение необходимого и неприемлемого уровня обслуживания;

m) определение поддающихся проверке критериев эффективности, их мониторинга и отчетности;

n) право мониторинга и аннулирования любых действий, связанные с активами организации;

o) право проводить проверки (аудит) договорных обязанностей или делегировать проведение такого аудита сторонней организации;

p) создание процесса реагирования для решения проблем;

q) требования непрерывности обслуживания, включая меры по обеспечению доступности и надежности в соответствии с бизнес-приоритетами организации;

r) соответствующие обязательства сторон в рамках контракта;

s) обязательства относительно юридических вопросов, например, законодательство о защите данных с учетом различных национальных законодательств, особенно если соглашение относится к сотрудничеству с организациями в других странах (15.1);

t) права интеллектуальной собственности (IPRs) и авторские права (15.1.2), а также правовая защита любой совместной работы (6.1.5);

u) привлечение третьей стороны вместе с субподрядчиками, а также обеспечения их безопасности;

v) в случае пересмотра/прекращения действия соглашения:

1) необходимо описать условия и ситуации пересмотра/прекращения действия соглашения, если любая из сторон пожелает прекратить отношения по действующему соглашению;

2) следует заключить повторное соглашение, если того требуют обстоятельства;

3) текущую документацию, содержащую списки активов, лицензии, соглашений или прав, относящиеся к ним следует пересматривать при пересмотре/прекращении действия соглашения.

Соглашения должны учитывать все выявленные риски и требования к безопасности (см. 6.2.1).

В случае привлечения сторонних организаций для выполнения особо ответственных задач (например, управления информационной безопасностью), в соглашении должны отражаться способы обеспечения сторонней организацией адекватной безопасности, как это определено оценкой рисков для этих задач, содержания и адаптации безопасности для выявления и решения с изменениями рисков.

Также в некоторых случаях может возникнуть потребность в переходном периоде, когда задача, передаваемая аутсорсеру, переходит под его ответственность частями. В таких ситуациях требуется составление четкого плана перехода с указанием зон ответственности каждой из сторон.

Во избежание задержек по предоставлению услуг со стороны третьих лиц, необходимо предусмотреть в соглашении сроки обработки.

В соглашениях с третьими лицами может быть и участие других сторон. Соглашения, согласно которым сторонней организации предоставляется доступ к информации, должны содержать прямое разрешение на назначение других правомочных сторон и условий для их доступа и участия.

Доступ, предоставленный сторонней организации не может быть делегирован третьей стороне. Такие случаи должны рассматриваться как доступ другой сторонней организации.

Прежде всего, соглашения должны быть подготовлены самой Организацией. При некоторых обстоятельствах, могут возникнуть ситуации, когда соглашение готовят и навязывают Организации со стороны третьих сторон. Организация должна обеспечить собственную безопасность и не воздействовать чрезмерным влиянием к требованиям сторонней организации, предусмотренных в этих соглашениях.

7 Управление активами

7.1.Ответственность за защиту активов организации

Все основные информационные активы ИС подлежат обязательному учету, за каждым активом закреплен ответственный сотрудник.

Ответственный за обеспечение ИБ должен составить и держать в актуальном состоянии перечень активов и ответственных за них сотрудников за поддержание соответствующих мероприятий по управлению информационной безопасностью в отношении вверенных им активам.

Осуществление мероприятий по управлению информационной безопасностью может быть делегировано от ответственного за актив другому лицу, закрепленному приказом руководства Организации, но ответственность должна оставаться за назначенным ответственным за актив сотрудником.

Процедуры, описывающие процесс управления активами:

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

7.1.1. Инвентаризация активов

Инвентаризация (учет) активов осуществляется в рамках финансово-бухгалтерского учета имущества Организации, в соответствии с утвержденными внутренними документами. В настоящем документе рассматривается только аспект инвентаризации тех активов, которые используются для обеспечения работы ИС.

Описываемый процесс инвентаризации активов может рассматриваться как расширение, либо дополнение к финансово-бухгалтерскому учету имущества Организации, проводится отдельно и никак не может его заменить.

Порядок проведения инвентаризации активов утвержден в Правилах идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации.

7.1.2. Ответственность за активы

Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного ответственного сотрудника Организации.

Ответственный сотрудник назначается по результатам инвентаризации активов и подписании обязательств материальной ответственности.

В ответственность сотрудника входит:

a) пересмотр и классификация подотчетной ему информации, активов;

b) определение и регулярный пересмотр доступа, с учетом принятых требований к управлению доступом;

c) контроль за поддержку, использованию и безопасность вверенных ему активов;

d) контроль соблюдения всех утвержденных в Организации требований, требований соглашений при совместном использовании со сторонними организациями и требований законодательства РК при использовании актива.

Ответственность может распространяться на:

a) производственный процесс;
b) определенный вид деятельности;
c) бизнес-приложения;
d) определенную группу данных;
e) защищаемые помещения;
f) технические средства (оборудование);
g) дистрибутивы программных средств;
h) системные утилиты и средства администрирования;
i) установленное программное обеспечение;
j) средства разработки, тестирования;
k) информацию;
l) закупаемую Организацией услугу (договор);
m) поставляемую Организацией услугу (договор);
n) ИС в целом.

Использование самого актива может быть поручено другим сотрудникам, например, персоналу, ежедневно работающему с активами, но ответственность за активы несет назначенный ответственный сотрудник.

Для простоты оперирования активы группируются. Активы, причисленные к одной группе, рассматриваются совместно, чтобы обеспечить выполнение определенной функции, как «услуги» или ИС в целом. В этом случае, ответственный сотрудник за оказание услуги или функционирования ИС несет ответственность за активы группы.

Ответственный сотрудник несет полную материальную ответственность за вверенные ему активы в соответствии с Трудовым, Административным Кодексом Республики Казахстан и другими нормативно-правовыми актами Республики Казахстан.

7.1.3. Приемлемое использование активов

Для обеспечения безопасного использования информации и активов Организации разработаны и утверждены руководством Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации.

Все сотрудники, подрядчики и пользователи сторонних организаций должны соблюдать режим информационной безопасности, утвержденный в Организации, в том числе:

a) правила для электронной почты и интернет-пользователей (10.8) описанные в Правилах организации антивирусного контроля, использования

мобильных устройств, носителей информации, Интернета и электронной почты;

b) рекомендации по использованию мобильных устройств, особенно для использования вне помещений организации (11.7.1) описанные в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

Сотрудники, подрядчики и пользователи сторонних организаций, использующие или имеющие доступ к активам организации, должны знать о существующих лимитах, установленных для их использования, связанными со средствами обработки информации и ресурсами. Они должны нести ответственность за их использование в соответствии с принятыми с Организацией соглашениями и законодательством РК.

Ответственность за соблюдение требований настоящего документа и требований, утвержденных в Организации документов по обеспечению ИБ в отношении безопасного использования активов, назначается СОИБ.

Ответственные за активы и группы активов (7.1.2) закрепляются в документе Перечень активов и ответственных за них сотрудников.

7.2.Классификация информации

Целью классификации информации ИС является обеспечение уверенности в том, что информационные активы защищены на надлежащем уровне.

В общем, классификация информации позволяет определить, как эта информация должна быть обработана и защищена.

Система классификации информации ИС изложена в Правилах идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации.

Процедура классификации и переклассификации информации ровно, как и всех активов выполняется в ходе инвентаризации, и как одно из корректирующих действий внутреннего аудита, но не реже одного раза в год. Результаты классификации должны учитываться в процессе предоставления доступа, в соответствии с заданной политикой контроля доступа.

7.2.1. Основные принципы классификации

Основные принципы классификации активов ИС изложены в Правилах идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации.

7.2.2. Маркировка и обработка информации

Для обеспечения использования принятой в Организации системы классификации разработаны и утверждены руководством Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации.

Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их

инвентаризации, относятся как к активам в физической, так и в электронной форме.

8 Правила безопасности, связанные с персоналом

8.1.Перед трудоустройством[3]

Настоящий раздел описывает требования к процедурам трудоустройства персонала, а также требования к контролю персонала партнеров и подрядных организаций.

Основная цель обеспечить уверенность в том, что сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации.

Ответственность за обеспечение безопасности каждой позиции штатного расписания должностей должна определяться заранее.

Все претенденты на трудоустройство должны быть заранее уведомлены об ответственность за обеспечение безопасности.

Требования, обязанности и ответственность за обеспечение безопасности сотрудников должны отражаться в должностных инструкциях.

Все кандидаты на работу, подрядчики и пользователи сторонней организации должны проходить тщательный отбор, особенно это касается должностей, предполагающих доступ к важной информации.

Для осуществления необходимого влияния на сторонние организации при выборе сотрудников, все требования относительно персонала выполняющего работы для Организации, должны быть отражены в договорных отношениях и подтверждаться соответствующими документами.

Все сотрудники и представители сторонних организаций, использующие средства обработки информации Организации, должны подписать соглашение о своих функциях и обязанностях в области информационной безопасности.

Все сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров обязаны соблюдать требования настоящего документа и других документов, регулирующих обеспечение информационной безопасности ИС.

8.1.1. Функции и обязанности персонала по обеспечению безопасности

Функции и обязанности персонала по обеспечению безопасности Организации, поставщиков товаров и услуг и партнеров в области безопасности должны быть определены и отражены в должностных инструкциях, договорных соглашениях в соответствии с требованиями информационной безопасности.

[3]Под словом «трудоустройство» (employment) следует понимать следующие ситуации: прием на работу (временную или постоянную), назначение на должность или перевод на другую должность, переоформление контрактов, аннулирование или временное прекращение каких-либо из этих ситуаций.

Функции и обязанности персонала по обеспечению безопасности должны содержать следующие требования:

a) внедрять и действовать в соответствии с политикой информационной безопасности (5.1);

b) защищать ресурсы от несанкционированного доступа, раскрытия, изменения, уничтожения или создания препятствий для их использования;

c) выполнять определенные в Организации процессы и мероприятия, связанные с безопасностью;

d) гарантировать выполнения обязанностей, порученных отдельным лицам при выполнении работ;

e) докладывать о событиях безопасности или других рисках безопасности.

Функции и обязанности персонала по обеспечению безопасности, должны быть сообщены кандидатам при приеме на работу, в ходе предварительного процесса трудоустройства.

Функции и обязанности персонала должны быть документированы в должностных инструкциях.

Функции и обязанности сотрудников партнеров и поставщиков товаров и услуг должны быть отражены в договорных отношениях.

Все сотрудники Организации, все работники нанятые по договору, сотрудники подрядных организаций и все пользователи ИС обязаны соблюдать требования настоящего документа и действующие документы регламентирующие требования к обеспечению ИБ.

Обязанности за осуществление контроля исполнения настоящего раздела возлагается на ответственного за обеспечение ИБ.

8.1.2. Проверка при приеме на работу

При приеме на работу сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров должна проводиться проверка в соответствии с порядком, установленным в Организации, с учетом требований бизнеса, характера информации, к которой будет осуществлен их доступ, и предполагаемых рисков.

При приеме на работу необходимо соблюдать конфиденциальность личных данных, в соответствии с действующим законодательством.

Проверка включает следующее:

a) оценка наличия положительных рекомендаций, в отношении деловых и личных качеств претендента;

b) проверка (на предмет полноты и точности) резюме претендента;

c) подтверждение заявляемого образования и профессиональных квалификаций;

d) независимая проверка подлинности документа, удостоверяющего личность (паспорт или заменяющего его документа).

Проверку проводит ответственный сотрудник отдела кадров привлекая там, где того требует компетентность, руководителя структурного

подразделения, на штатную позицию которого претендует кандидат, руководителя юридической службы и ответственного за обеспечение ИБ.

Аналогичный процесс проверки следует осуществлять для временного персонала и сотрудников поставщиков товаров и услуг.

В тех случаях, когда прием сотрудников осуществляется через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по проверке претендентов и процедурам уведомления, которым оно должно следовать, если проверка не была закончена или если результаты дают основания для сомнения или беспокойства.

Информация обо всех рассматриваемых кандидатах должна документироваться, результаты проверок должны быть оформлены в виде протоколов и заверены подписями ответственного сотрудника отдела кадров, руководителя структурного подразделения, на штатную позицию которого претендует кандидат, руководителя юридической службы и ответственного за обеспечение ИБ.

8.1.3. Условия трудового договора

Сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров должны согласовать и подписать условия трудового договора, в котором установлены их ответственность и ответственность Организации относительно информационной безопасности.

Принятие нового сотрудника производится на основании приказа руководителя Организации. Ответственный сотрудник отдела кадров выполняет инструктаж порядка приема на работу, отдельный этап которого определение должностных обязанностей и определения необходимых привилегий. Результаты запроса привилегий фиксируются в приказе о приеме на работу.

Приказ о приеме нового сотрудника направляется на исполнение СОИБ, менеджеру проекта ИС и администраторам ИС для выполнения процедур присвоения привилегий новому сотруднику в соответствии с его должностными обязанностями.

Сроки и условия трудового договора должны учитывать требования настоящего документа включая, но не ограничиваясь следующим:

a) для получения доступа к важной информации, все сотрудники, подрядчики и пользователи сторонних организаций, должны подписать соглашение о соблюдении конфиденциальности и неразглашении до предоставления доступа к средствам обработки информации;

b) ответственность и права сотрудников, подрядчиков и любых других пользователей, относительно законов об авторском праве или по защите данных (15.1.1 и 15.1.2);

c) ответственность за классификацию информации и управление активами организации, связанными с информационными системами и услугами, обрабатываемыми/используемыми сотрудниками, подрядчиками или пользователями сторонних организаций (7.2.1 и 10.7.3);

d) ответственность сотрудников Организации, сотрудников поставщиков товаров и услуг и сотрудников партнеров за обработку информации, полученную от других компаний или организаций;

e) ответственность Организации за обработку персональной информации, включая информацию, созданную в результате работы в организации (15.1.4);

f) ответственность распространяется и на работу вне помещений Организации, и вне рабочего времени, например, в случае исполнения работы на дому или в командировке (9.2.5 и 11.7.1);

g) договор должен отражать последствия для сотрудника в случае нарушения указанных требований (см. 8.2.3).

Договорные отношения между работодателем и работником должны оговаривать условия и правила пользования, касающиеся информационной безопасности с учетом характера и степени доступа к активам Организации, связанных с информационными системами и услугами.

Там, где необходимо, эта ответственность должна сохраняться и в течение определенного срока после увольнения с работы (8.3).

Поставщики товаров и услуг, партнеры должны в свою очередь ввести в контрактные соглашения от имени лица, вовлеченного в контракт требуемые условия обеспечения ИБ.

8.2.Работа по трудовому договору

Требования настоящего раздела должны обеспечивать уверенность в том, что сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих должностных обязанностей и для снижения риска человеческого фактора для информационной безопасности

В Организации должен поддерживаться адекватный уровень осведомленности, обучения и подготовки кадров в области информационной безопасности и правильное использование средств обработки информации, чтобы свести к минимуму возможные риски безопасности.

Также необходимо обеспечить применение дисциплинарной практики в процессе нарушения требований безопасности.

8.2.1. Обязанности руководства

Руководство Организации проявляет крайнюю заинтересованность в организации надежных механизмов обеспечения информационной безопасности всех бизнес-процессов предприятия и защиты интересов своих клиентов и сотрудников.

Настоящий документ является аккумуляцией поддерживаемого руководством Организации режима организации и обеспечения информационной безопасности.

Все сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров должны быть ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями в границах своей ответственности и компетентности.

Если сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров не осведомлены о своих обязанностях по обеспечению безопасности, то они могут причинить значительный ущерб организации. Мотивированный персонал может быть более надежным и привести к сокращению числа инцидентов нарушения информационной безопасности.

Лица, занимающие руководящие посты в Организации и не соответствующее занимаемой должности могут вызвать у персонала ощущение своей недооценки и привести к негативному воздействию на безопасность в Организации. Например, подобное несоответствие может привести к пренебрежению безопасностью сотрудниками или злоупотреблению активами организации.

В обязанности руководства входят обеспечение того, чтобы сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров:

a) были осведомлены об их обязанностях по обеспечению информационной безопасности, служебных функциях и обязанностях до предоставления доступа к конфиденциальной информации или информационным системам;

b) ознакомились с действующими документами по информационной безопасности в границах своей ответственности и компетентности;

c) были мотивированы для поддержания безопасности Организации;

d) достигли уровня информированности по вопросам безопасности, имеющие отношение к своим функциям и обязанностям в рамках Организации (см. 8.2.2);

e) соответствовали условиям трудовой деятельности, которая включает в себя политику информационной безопасности в Организации, а также соответствующие методы работы;

f) имели соответствующие навыки и квалификацию.

8.2.2. Осведомленность, обучение и переподготовка в области информационной безопасности

Ответственный за обеспечение ИБ должен составить, а руководство Организации утвердить График обучения и инструктажа сотрудников Организации (по форме Приложения 4) по вопросам информационной безопасности.

Внутреннее обучение и инструктаж проводится ответственным за обеспечение ИБ сотрудником Организации. Обучению подлежат все сотрудники Организации и, при необходимости, сотрудники поставщиков товаров и услуг и сотрудники партнеров в целях регулярного получения

информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций.

Обучение должно проводиться не реже одного раза в год, инструктаж – не реже двух раз в год.

По окончанию инструктажа сотрудник вносит запись в Журнал проведения обучения, инструктажа по информационной безопасности (по форме Приложения 9).

Обучение следует начинать с ознакомления политикой информационной безопасности в Организации до предоставления доступа к информации и услугам.

Обучение сотрудников должно обеспечить знание ими требований безопасности, ответственности в соответствии с законодательством, мероприятий по управлению информационной безопасностью, а также знание правильного использования средств обработки информации, например, процедур регистрации в системах, использования пакетов программ и информации относительно дисциплинарной практики (см. 8.2.3).

Деятельность по обучению и подготовки в области безопасности должна соответствовать функциям сотрудника, его ответственности и навыкам, а также должна содержаться информация об известных угрозах. Сотруднику в случае необходимости, следует обращаться за консультацией по вопросам ИБ к ответственному за обеспечение ИБ.

Ответственный за обеспечение ИБ должен проходить регулярные курсы повышения квалификации в специализированных обучающих центрах, а также обучение на практике в компетентных центрах, специализирующихся на организации и обеспечении информационной безопасности, не реже одного раза в три года с выдачей сертификата.

Результаты внутреннего обучения, инструктажа, курсов повышения квалификации должны быть отражены в Журнале проведения обучения, инструктажа по информационной безопасности и протоколах тестирования полученных знаний и навыков.

8.2.3. Дисциплинарная практика

Дисциплинарная практика должна применяться в качестве сдерживающего фактора для предотвращения нарушений политики и процедур по обеспечению информационной безопасности или любых других нарушений безопасности со стороны сотрудников, подрядчиков и сторонних организаций.

К сотрудникам, совершившим нарушение требований безопасности, применяется дисциплинарная практика, установленная в организации в соответствии с законодательством РК.

Применение дисциплинарной практики обеспечивает корректное и справедливое рассмотрение инцидента для сотрудников, которые подозреваются в серьезных или регулярных нарушениях требований безопасности.

Применение официальной дисциплинарной практики должно отражать позицию руководства Организации, принимающее во внимание такие факторы, как характер и степень тяжести нарушения и его воздействия на бизнес, было ли это нарушение совершено впервые или нарушалось неоднократно, получал ли нарушитель достаточное обучение, соответствующее законодательству, трудовому соглашению или другим факторам, по мере необходимости.

Дисциплинарное взыскание не должно применяться без предварительной проверки и сбора доказательств (см. 13.2.3).

Лицо, в отношении которого применилось дисциплинарное взыскание, вправе обжаловать решение руководства Организации в порядке и соответствии с законодательством РК.

В случаях серьезных проступков, применение дисциплинарной практики может повлечь снятие с занимаемой должности, лишение права доступа и привилегий, а также в случае необходимости, немедленного освобождения рабочего места.

8.3. Прекращение или изменение действия трудового договора[4]

В обязанности ответственного сотрудника отдела кадров входит уведомление сотрудников Организации (как минимум, СОИБ, менеджера проекта, администраторов ИС) об увольнении или изменении условий трудового договора в соответствии с установленным порядком.

В обязанности ответственного за обеспечение ИБ входит уведомление поставщиков товаров или услуг, партнеров об изменениях в режиме информационной безопасности Организации.

Ответственный сотрудник отдела кадров, выполняющий работы по приему, увольнению и смене обязанностей сотрудников Организации, обязан соблюдать требования настоящего документа.

Внутренние уведомления должны осуществляться по средствам официальной служебной переписки; уведомление внешних сторон – по средствам официальных писем.

8.3.1. Ответственность по окончании действия трудового договора

По окончании действия трудового договора должна быть четко определена и установлена ответственность выполнения процедур безопасности.

Информация об ответственности, по окончании действия трудового договора, должна включать текущие требования к безопасности и правовую ответственность, и при необходимости, обязанностей, содержащихся в соглашении о конфиденциальности (см. 6.1.5). А также сроки и условия трудового договора (8.1.3) должны действовать в течение определенного

[4]В контексте настоящего документа под словосочетаниями «окончании действия трудового договора», «увольнение сотрудника» следует понимать не только увольнение из Организации, но и смену позиции в штатном расписании должностей, изменение должности, изменение названия должности, изменение должностных обязанностей позиции в штатном расписании должностей.

периода времени после завершения срока работы сотрудников, подрядчиков или сотрудников партнеров.

Функции и обязанности обеспечения информационной безопасности должны оставаться в силе после прекращения работ, которые указаны в трудовых соглашениях сотрудников, подрядчиков или сотрудников сторонней организации.

Все изменения обязанностей или функций должны документироваться в трудовом договоре или должностных инструкциях, а также новые обязанности или функции должны контролироваться, как описано в 8.1.

В случае увольнения сотрудника Организации СОИБ должен сделать отметку в его обходном листе.

Ответственный за обеспечение ИБ обязан контролировать соблюдение режима ИБ при прекращении договорных обязательств и требуемый срок после этого.

Ответственный сотрудник отдела кадров обязан информировать ответственного за обеспечение ИБ, ответственного администратора ИС, менеджера проекта о прекращении договорных отношений с сотрудником Организации.

Менеджер проекта обязан информировать ответственного за обеспечение ИБ, ответственного администратора ИС о прекращении договорных отношений с поставщиком товаров или услуг в границах своего проекта.

Необходимо информировать сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров об изменениях в рабочем процессе и в работе с персоналом.

8.3.2. Возврат активов

По окончании действия договорных отношений с сотрудниками Организации, сотрудниками поставщиков товаров и услуг и сотрудниками партнеров все активы Организации, которые были переданы им для исполнения должностных обязанностей и/или в ответственное хранение должны быть возвращены по акту.

Ответственность за возврат материальных активов возлагается на материально-ответственное лицо. Ответственность за возврат информационных активов (программных средств, документации и т. п.), средств обеспечения безопасности (токены, ЭЦП, ID-карты, логины, пароли и т. п.) возлагается на ответственного за обеспечение ИБ.

Процесс увольнения, включая возвращение всех ранее выпущенных программ, служебных документов и оборудования должен быть, формализован и выполняется согласно установленным в Организации процедурам.

Ответственный за обеспечение ИБ должен удостоверится, чтобы вся защищаемая информация была передана Организации и надежно удалена с оборудования (см. 10.7.1), включая с личных средств обработки информации.

В случаях, когда увольняющийся сотрудник Организации, сотрудник поставщика товаров и услуг или сотрудник партнера не проявляет лояльность это должно быть задокументировано.

8.3.3. Аннулирование прав доступа

Права доступа к информации и средствам обработки информации сотрудников Организации, сотрудников поставщиков товаров и услуг и сотрудников партнеров должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение) или в случае смены должностных обязанностей.

По окончании действия трудового договора (увольнения), права доступа к отдельным активам, связанных с информационными системами и услугами должны быть пересмотрены. Ответственность за инвентаризацию, пересмотр, изменение и аннулирования прав доступа возлагается на ответственного за ИБ.

Права доступа, могут включать физический и логический доступ, ключи, идентификационные карты, средства обработки информации (см. 11.2.4), подписки, и удаления из всей документации, которая идентифицирует сотрудника в качестве действительного члена групп доступа.

Если уволившийся сотрудник Организации, сотрудник поставщика товаров и услуг и сотрудник партнера знает пароли для учетных записей, остающимися активными, то пароли должны быть изменены на момент прекращения или изменения работы, окончания действия трудового договора или соглашения.

Права доступа к информационным активам и средствам обработки информации должны быть сокращены или аннулированы, прежде чем действие трудового договора прекращается или изменяется в зависимости от оценки факторов риска, таких как:

a) является ли прекращение или изменение по инициативе сотрудника, или по инициативе руководства и какова причина прекращения;
b) текущие обязанности сотрудника;
c) ценность активов, доступных ему в настоящее время;
d) лояльность сотрудника к работодателю.

Если увольняющийся сотрудник является членом, каких-либо групп безопасности, при таких обстоятельствах, уволившиеся лица должны быть аннулированы из всех списков группового доступа, а также сотрудникам Организации, сотрудникам поставщиков товаров и услуг и сотрудникам партнеров рекомендуется не обмениваться информацией с увольняющимися лицами.

В случае прекращения действия трудового договора (увольнения) по инициативе руководства, недовольные сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров, могут преднамеренно повредить информацию или саботировать средства обработки информации.

Уволившиеся лица могут произвести попытку собрать информацию для будущего использования.

Ответственность за соблюдение требований безопасности при процедуре увольнения возлагается на ответственного за обеспечение ИБ.

9 Физическая защита и защита от воздействия окружающей среды

9.1. Охраняемые зоны

Для регламентации требований к механизмам предотвращения несанкционированного физического доступа, повреждения и воздействия на помещения и информацию проекта, утверждены Правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

Средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Контроль исполнения требований настоящего документа возлагается на ответственного за обеспечение ИБ.

9.1.1. Периметр физической безопасности

Требования к периметру физической безопасности изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.1.2. Контроль доступа в охраняемую зону

Требования к контролю доступа в охраняемую зону изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.1.3. Обеспечение безопасности зданий, производственных помещений и оборудования

Требования к обеспечению безопасности зданий, производственных помещений и оборудования изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.1.4. Защита от внешних угроз и угроз со стороны окружающей среды

Требования к защите от внешних угроз и угроз со стороны окружающей среды изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.1.5. Выполнение работ в охраняемых зонах

Требования к выполнению работ в охраняемых зонах изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.1.6. Зоны общественного доступа, приема и отгрузки материальных ценностей

Требования к зоне общественного доступа, приема и отгрузки материальных ценностей изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.2. Безопасность оборудования

Необходимо обеспечивать безопасность оборудования (включая и то, что используется вне организации), чтобы уменьшить риск неавторизованного доступа к данным, защитить их от потери или повреждения, или компрометации активов и нарушения непрерывности деятельности Организации.

Требования к безопасности оборудования изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

Контроль исполнения требований безопасности в отношении оборудования возлагается на ответственного за обеспечение ИБ.

9.2.1. Размещение и защита оборудования

Требования к размещению и защите оборудования изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.2.2. Вспомогательные услуги

Требования к управлению вспомогательными услугами изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.2.3. Безопасность кабельной сети

Требования к безопасности кабельной сети изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

Обязанность по осуществлению контроля исполнения настоящих требований возлагается на ответственного за обеспечение ИБ.

9.2.4. Техническое обслуживание оборудования

Требования к безопасности технического обслуживания оборудования изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.2.5. Обеспечение безопасности оборудования, используемого вне помещений организации

Требования к обеспечению безопасности оборудования, используемого вне помещений организации, изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

9.2.6. Безопасная утилизация (списание) или повторное использование оборудования

Требования к безопасности утилизации (списания) или повторного использования оборудования изложены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

9.2.7. Вынос имущества

Требования к процедуре выноса имущества изложены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

10 Управление передачей данных и операционной деятельностью

10.1. Операционные процедуры и обязанности

Все процессы, связанные с обработкой информации должны иметь формализованные процедуры, описывающие операционную деятельность участников процесса.

Все средства обработки информации должны быть снабжены формализованными операционными процедурами, а все лица, использующие эти средства, должны быть ознакомлены с соответствующими процедурами под роспись.

Обязанность по осуществлению контроля исполнения настоящих требований возлагается на ответственного за обеспечение ИБ.

10.1.1. Документальное оформление операционных процедур

С целью контроля исполнения требований ИБ, обеспечения преемственности, поддержания процесса улучшения все процессы операционной деятельности должны быть документированы в виде формализованных процедур.

Ответственный за обеспечение ИБ составляет и поддерживает в актуальном состоянии перечень операционных процедур по форме Приложения 4 Правил идентификации, классификации и маркировки активов.

Ответственными за разработку, поддержание в актуальном состоянии и исполнении операционных процедур назначаются:

– процедуры конфигурации ПО и средств обработки информации для обеспечения информационной безопасности – ответственный за обеспечение ИБ;

– процедуры сопровождения, поддержания эксплуатации – ответственный администратор ИС и/или ЭИР;

– процедуры учета активов, документирования проектов – менеджер проекта;

– процедуры, связанные с персоналом – ответственный за обеспечение ИБ.

Операционные процедуры должны документироваться, поддерживаться и быть доступными для авторизованных пользователей.

Обязанность по осуществлению контроля исполнения настоящих требований возлагается на ответственного за обеспечение ИБ

Операционные процедуры должны быть разработаны в отношении обслуживания систем обработки и обмена информацией, в частности процедуры запуска и безопасного завершения работы серверного оборудования и программного обеспечения, процедуры резервирования, текущего обслуживания и ремонта оборудования, обеспечения надлежащей безопасности помещений с компьютерным и коммуникационным

оборудованием, безопасности и обработки электронной почты и носителей информации.

Процедуры сопровождения, поддержания эксплуатации, обеспечения защиты, конфигурирования ИС и/или ЭИР должны содержать детальную инструкцию выполнения конкретного задания (работы) и включать:

a) обработку и управление информацией;

b) копирование (10.5);

c) определение требований в отношении графика выполнения заданий, включающих взаимосвязи между подразделениями Организации; время начала выполнения самого раннего задания и время завершения самого последнего задания;

d) обработку ошибок или других исключительных ситуаций, которые могут возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит (11.5.4);

e) необходимые контакты на случай неожиданных операционных и технических проблем;

f) специальные мероприятия по управлению выводом данных, например, в случае особых процедур применительно к выводу конфиденциальной информации, включая процедуры для безопасной утилизации выходных данных, не завершенных в процессе выполнения заданий (10.7.2 и 10.7.3);

g) перезапуск системы и процедуры восстановления в случае системных сбоев;

h) ведение журнала аудита и системного журнала регистрации (10.10).

Операционные процедуры, определяемые политикой безопасности, должны рассматриваться как официальные документы, документироваться и строго соблюдаться, а изменения к ним должны санкционироваться и утверждаться руководством Организации.

10.1.2. Контроль изменений

Допускается следующие процессы внесения изменений в ИС и/или ее части:

1) внедрение изменений исходного кода, полученных в результате работ по разработке, доработке и развитию ИС или ее части;

2) внедрение изменений исходного кода, выполненных с целью устранения уязвимостей;

3) внедрение изменений с целью устранения уязвимостей;

4) изменение версий и/или изменение компонент ИС;

5) изменение настроек ИС и/или ее компонент.

Процессы внесения изменений должны проводиться в соответствии с требованиями Политики безопасной разработки, доработки и развития ИС.

10.1.3. Разграничение обязанностей

Разграничение обязанностей – способ минимизации риска, нештатного использования средств обработки информации, вследствие ошибочных или

злонамеренных действий пользователей, и основной механизм идентификации лица выполнившего действия, приведшие к инциденту ИБ.

Обязанности и области ответственности должны быть строго разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации, или нецелесообразного использования активов организации.

Все планы, инструкции, организационные и операционные процедуры должны учитывать строгое разграничение обязанностей и области ответственности участвующих лиц. В каждом документе СМИБ должен присутствовать раздел с указанием ответственности за исполнение требований и контроль над исполнением требований. За каждым документом должен быть закреплен ответственный сотрудник за разработку, поддержание в актуальном состоянии и исполнение.

Непосредственно перед любым использованием всех активов Организации должна происходить аутентификация и авторизация. При выборе мер безопасности следует рассматривать возможность сговора.

В случаях, когда разделение обязанностей осуществить затруднительно, следует использовать средства контроля и мониторинга за действиями персонала.

10.1.4. Разграничение средств разработки, тестирования и эксплуатации

Ответственный за обеспечение ИБ должен составить, согласовать с заинтересованными сторонами, утвердить руководством Организации и поддерживать в актуальном состоянии перечни (по форме Приложения 4 Правил идентификации, классификации и маркировки активов):

- перечень разрешенного программного обеспечения;
- перечень системных утилит и средств администрирования;
- перечень средств разработки, тестирования.

Случаи использования неразрешенного ПО, средств администрирования и средств разработки, тестирования и эксплуатации должны выявляться в процессе аудита. К сотрудникам, допустившим несанкционированное использование, должны применяться меры дисциплинарного взыскания.

В целях обеспечения ИБ и отказоустойчивости ИС и ЭИР к эксплуатации допускаются только законченные релизы программного обеспечения.

В случае возникновения необходимости модификации программного кода ИС, процесс разработки и тестирования производится отдельно от эксплуатируемого экземпляра ИС. Внедрение новых доработок ПО производится в соответствии с требованиями Закона «Об информатизации».

10.2. Управление поставкой услуг лицами и/или сторонними организациями

Ответственный за обеспечение ИБ обязан поддерживать требуемый уровень информационной безопасности и оказания услуг (приобретаемые Организацией с целью обеспечения эксплуатации ИС) в соответствии с договорами об оказании услуг сторонними поставщиками (внешними лицами и/или организациями).

Ответственный за обеспечение ИБ должен осуществлять контроль над выполнением, соблюдением соглашений, и управлять изменениями в ИС, в СМИБ и в соглашениях с поставщиками услуг для того, чтобы оказываемые услуги удовлетворяли все требования к информационной безопасности, установленные утвержденными документами СМИБ.

Договорные отношения с поставщиками услуг должны включать описания режима информационной безопасности, требования по его соблюдению, описание границ доступа к информации всех участников, соглашение о конфиденциальности и неразглашении информации, требуемые средства обработки информации и другие сведения, затрагивающие информационную безопасность всех участников соглашения.

Там, где это необходимо в договорные соглашения должны включаться требования к непрерывности оказания услуг и/или поставки товаров. Эти требования могут быть выделены в отдельный документ, подписываемый всеми участниками соглашения, например, соглашение об уровне обслуживания (см. 14.1)

Для выполнения такого контроля руководства Организации поручает ответственному за обеспечение ИБ выполнять согласование характеристик услуг, приобретаемых с целью обеспечения эксплуатации ИС.

10.2.1. Оказание услуг

Ответственный за обеспечение ИБ обязан осуществлять контроль исполнения мер управления информационной безопасности, включенных в договор об оказании услуг сторонним организациям.

Договорные отношения с партнерами, клиентами должны включать описания режима информационной безопасности, требования по его соблюдению, описание границ доступа к информации всех участников, соглашение о конфиденциальности и неразглашении информации, требуемые средства обработки информации и другие сведения, затрагивающие информационную безопасность всех участников соглашения.

Там, где это необходимо в договорные соглашения должны включаться требования к непрерывности оказания услуг и/или поставки товаров. Эти требования могут быть выделены в отдельный документ, подписываемый всеми участниками соглашения, например, соглашение об уровне обслуживания (см. 14.1).

10.2.2. Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями

За каждой приобретаемой/оказываемой услугой или за каждым договором по приобретению/оказанию услуги должен быть назначен ответственный сотрудник Организации.

Ответственный сотрудник должен регулярно проводить мониторинг, аудит и анализ отчетов и актов, услуг за которые он отвечает.

Ответственный сотрудник отвечает за контроль соблюдения условий договорных соглашений, управление отношениями со сторонними организациями, и доводить до ответственного сотрудника за обеспечение ИБ сведения, относящиеся к аспекту информационной безопасности.

Ответственный за обеспечение ИБ должен:

a) следить за соблюдением требований информационной безопасности при приобретении/оказании услуг;

b) проверять достоверность отчетов приобретения/оказания услуг в отношении исполнения требований ИБ;

c) уведомлять заинтересованные стороны об инцидентах ИБ и предпринимать соответствующие действия при получении информации об инцидентах ИБ от сторонних организаций, выполнять консультации по ИБ;

d) проводить аудит и анализ услуг, отчетов о событиях безопасности, операционных проблем, неудач, отслеживания ошибок и сбоев, связанных с услугой;

e) устранение и решение любых выявленных проблем, связанных с ИБ.

Ответственный сотрудник за приобретаемую/оказываемую услугу и ответственный за обеспечение ИБ должны осуществлять тесное взаимодействие с целью быстрого реагирования на инциденты ИБ и незамедлительное применение корректирующих мер.

Там, где это необходимо количество ответственных за услугу сотрудников может быть увеличено, но их обязанности и области ответственности должны быть четко разграничены. Ответственные сотрудники за услуги назначаются приказом руководства Организации, сразу после подписания договорных отношений с приобретателем или поставщиком услуг.

Ответственный за услугу и ответственный за обеспечение ИБ, в границах своей ответственности, должны осуществлять мониторинг оказания услуги и предпринимать соответствующие меры с целью недопущения нарушения условий договорных отношений.

Поставщики и потребители услуг должны быть уведомлены о границах соей ответственности и обязанностях в рамках договорных отношений.

10.2.3. Изменения при оказании сторонними организациями услуг по обеспечению безопасности

Все изменения договорных отношений связанные с обеспечением ИБ должны быть согласованы с заинтересованными сторонами, документально оформлены и утверждены руководством Организации.

Изменения могут быть внесены в следствие:

a) усовершенствования СМИБ;

b) применения корректирующих мероприятий;

c) изменений рыночных условий приобретения/оказания услуг;

d) развитие новых инструментов и сред;

e) изменения физического расположения участников соглашения, мест оказания услуг;

f) изменение участников соглашения;

g) потребности применении иных компонент услуги или новых вариантов/версий услуги;

h) потребности использования новых технологий;

i) потребности применения новых решений для управления инцидентами информационной безопасности и повышения безопасности;

j) внесения изменений и обновления политики и процедур организации;

k) разработки новых программных приложений и систем;

l) усовершенствования текущих услуг;

m) осуществления изменений в Организации.

10.3. Планирование производительности и загрузки систем

Для обеспечения доступности данных, требуемой производительности и ресурсов систем для каждой ИС и/или ЭИР проводятся предварительные планирование и подготовка.

Для снижения риска перегрузки системы ответственным администратором проводится анализ предполагаемой ее нагрузки. Ответственный за планирование производительности и загрузки систем назначается решением рабочей группы по ИБ.

Требования к эксплуатации новых систем определятся настоящим документом и тестируются перед их приемкой и использованием.

Ответственность за исполнение требований в отношении процессов разработки, тестировании и приемки результатов возлагается на менеджера проекта.

10.3.1. Управление производительностью

Ответственный администратор должен осуществлять мониторинг, прогнозирование и корректировку потребности мощности ИС и/или ЭИР для обеспечения требуемой производительности.

Оценочными характеристиками выступают, как минимум (по всем вычислительным мощностям):

a) утилизация производительности центрального процессора;

b) утилизация объема оперативной памяти;
c) утилизация каналов связи;
d) утилизация объема хранилища данных;
e) количество подключенных сессий;
f) количество подключенных пользователей;
g) скорость подключения сессий;
h) корректность распределения вычислительных мощностей среди компонентов ИС;
i) частота и корректность высвобождение вычислительных мощностей.

Также должны регистрироваться оценочные характеристики свойственные для ИС и/или ЭИР.

Оценочные характеристики должны фиксироваться на всех аппаратных компонентах ИС и/или ЭИР включая серверное и активное сетевое оборудование.

Все оценочные характеристики должны регистрироваться и храниться на протяжении трех лет. Динамика изменений и тенденции в работе ИС и/или ЭИР должны быть выявлены и описаны в аналитическом отчете, предоставляемом два раза в год.

В заключительной части отчета должны содержаться выводы и прогнозы о производительности ИС и/или ЭИР о наличии или отсутствии необходимости модернизировать компоненты Системы, доработки исходного кода, корректировки настроек компонент, установки дополнительного ПО, расширению состава оценочных характеристик мониторинга, улучшению СМИБ необходимых для повышения доступности и эффективности ИС и/или ЭИР. При прогнозировании должны учитываться новые функциональные и системные требования, а также текущие планы и перспективные планы развития информационных технологий в Организации.

Отчет должен быть составлен ответственным администратором, согласован ответственным за обеспечение ИБ, менеджером проекта и утвержден руководством Организации.

Руководство Организации должно использовать эту информацию для идентификации/избежание потенциально узких мест, представляющих угрозу безопасности системы или пользовательским сервисам, угрозу отказа в обслуживании сервисов ИС в следствии непредвиденных/непредусмотренных нагрузок, а также с целью планирования соответствующих мероприятия по обеспечению информационной безопасности и улучшению надежности оказываемых сервисов.

Результатом рассмотрения отчета руководством Организации должно стать решение о составлении и исполнение плана разработки и применения корректирующих действий.

10.3.2. Приемка систем

Процесс разработки ИС и/или ЭИР является итерационным, разделенный на триплетные этапы «Разработка – Тестирование-Принятие/Непринятие». В случае непринятие результатов разработки после тестирования, этап разработки повторяется с целью исправления выявленных замечаний. Следующий этап может начаться только при положительных результатах тестирования предыдущего этапа разработки.

В процесс «Разработка – Тестирование – Принятие/Непринятие» должны привлекаться администраторы, ответственный за обеспечение ИБ представители конечных пользователей (или заказчика) и других заинтересованных сторон с целью обеспечения эффективной эксплуатации, разрабатываемой ИС и/или ЭИР.

Программа и методика тестирования должны быть изложены в соответствующих документах согласно требованиям стандартов, принятых в РК.

Требования, критерии оценки и функционал разрабатываемых, модернизируемых ИС и/или ЭИР должны быть описаны в программных/технических документах в соответствии с требованиями стандартов, действующих в РК

Критерии принятия новых и модернизированных информационных систем, новых версий программного обеспечения включают:

a) положительные результаты функционального тестирования;

b) положительные результаты тестирования механизмов обеспечения ИБ;

c) положительные результаты тестирования механизмов резервирования, восстановления и обеспечения непрерывной работы;

d) положительные результаты нагрузочного тестирования;

e) разработанные операционные процедуры (руководства, инструкции, памятки) по всем видам административных и пользовательских работ;

f) положительные результаты тестирования операционных процедур;

g) отсутствие неблагоприятного влияния применяемой системы или применяемого обновления на общую работу ИТ и информационную безопасность Организации;

h) проведение обучения пользователей и обслуживающего персонала и их тестирование, подготовка соответствующего образовательного материала;

i) тестирование эргономичности использования ИС и/или ЭИР.

Все результаты тестирования должны быть зафиксированные в протоколах. Протокола должны быть подписаны ответственным программистом, менеджером проекта, ответственным за обеспечение ИБ, представителем конечных пользователей (или заказчика), других заинтересованных сторон, руководством Организации.

Новые информационные системы, новые версии и обновления должны быть внедрены в производство только после прохождения официальной приемки в порядке, установленном законодательством РК. Результаты приемки должны быть зафиксированы в акте.

По письменной инициативе менеджера проекта или ответственного за обеспечение ИБ, но по согласованию с руководством Организации тестирование и/или приемка результатов разработки могут проводиться сторонними организациями с целью получения аккредитации, аттестата, протокола, сертификата или иного другого официального документа имеющего определенную законодательством РК силу.

10.4. Защита от вредоносного кода и мобильного кода

Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного кода, такого как компьютерные вирусы, сетевые «черви», «троянские кони» и логические бомбы.

Ответственный за обеспечение ИБ должен регулярно доводить до сотрудников Организации (в рамках инструктажа) и до пользователей (по средствам рассылки электронной почты или при помощи информационных каналов) сведения об опасности вредоносного кода, а ответственные администраторы должны обеспечить внедрение специальных средств контроля с целью обнаружения и/или предотвращения проникновения вредоносного кода и несанкционированного использования мобильного кода.

10.4.1. Меры защиты от вредоносного кода

Для обеспечения защиты от вредоносного кода в Организации утверждены Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

В Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты описаны меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также установлены требования к обеспечению соответствующего оповещения сотрудников Организации, партнеров, клиентов и пользователей ИС.

10.4.2. Меры защиты от мобильного кода

Использование мобильного кода разрешено только в виде скриптов для автоматизации функций администрирования и обеспечения ИБ.

Ответственный за обеспечение ИБ обязан составить перечень используемых системных утилит и средств администрирования (по форме Приложения 4 Правил идентификации, классификации и маркировки активов) и поддерживать его в актуальном состоянии. В перечне должно быть указано имя скрипта, источник, период проверки, проверочная сумма, ответственный за использование и проверку.

Обязанности за контроль настоящих требований, включая контроль проводимых проверок и запусков скриптов, возлагается на ответственного за обеспечение ИБ.

Мобильный код должен регулярно проверятся с целью подтверждения, что он не содержит вредоносного кода. В случае несовпадения зарегистрированной в перечне проверочной суммы с фактической суммой скрипта, ответственный сотрудник обязан остановить исполнение и все последующие запуски этого скрипта и сообщить об инциденте ИБ ответственному за обеспечение ИБ.

Ответственный за обеспечение ИБ обязан провести служебное расследование по факту инцидента ИБ. Причины инцидента должны быть выяснены и применены соответствующие корректирующие мероприятия.

Для защиты от мобильного кода, исполняющего несанкционированные действия выполняются следующие меры:

a) выполнение мобильного кода в логически изолированной среде;

b) блокирование любого использования мобильного кода неответственными лицами;

c) блокирование получения мобильного кода из неавторизованных источников;

d) защищенное хранение мобильного кода;

e) контроль ресурсов, используемых мобильным кодом;

f) контроль проверочных сумм для уникальной аутентификации мобильного кода.

К мобильному коду относятся скрипты (JavaScript, VBScript, Bash, sh, Perl, Python), Java-апплеты, элементы управления ActiveX, флэш-анимации, Shockwave и макросы, встроенные в файлы, обрабатываемые пакетом офисных программ.

При отсутствии необходимости в использовании мобильного кода в работе, его использование должно быть запрещено в настройках прокси-сервера, антивирусного шлюза, осуществляющего проверку веб-трафика и соответствующих приложений (веб-браузеров, пакетов офисных программ и т.д.).

В случае необходимости в использовании мобильного кода в работе необходимо соблюдать следующие меры защиты:

a) настройка приложений должна обеспечивать запуск мобильного кода только по явному разрешению пользователя;

b) необходимо разрешать запуск мобильного кода, полученного только от доверенных разработчиков;

c) в случае, если мобильный код подписан цифровой подписью разработчика, необходимо удостовериться, что цифровая подпись верна и регистрационное свидетельство (цифровой сертификат) является действующим;

d) при отсутствии уверенности в том, что мобильный код получен из доверенного источника, его запуск строго запрещен;

е) при наличии возможности, необходимо осуществить проверку мобильного кода на наличие деструктивных функций до его запуска.

10.5. Резервирование

С целью обеспечения адекватного управления процедурами резервирования и восстановления (14.1) в Организации утвержден Регламент резервного копирования и восстановления информации.

Обязанности по исполнению требований Регламента резервного копирования и восстановления информации возлагаются на ответственного администратора.

Обязанности по контролю исполнения требований Регламента резервного копирования и восстановления информации возлагаются на ответственного за обеспечение ИБ.

10.5.1. Резервное копирование

Средства резервного копирования и резервные копии, гарантируют восстановление всей необходимой информации и программного обеспечения после отказа носителей информации или аварии.

Средства резервирования регулярно тестируются для обеспечения уверенности в том, что они удовлетворяют требованиям планов по обеспечению непрерывности бизнеса (Раздел 14).

Для каждой резервной копии определен период хранения, а также учтены требования к архивным копиям долговременного хранения (15.1.3).

Регламент резервного копирования и восстановления информации содержит требования к регулярному созданию, тестированию резервных копий и средств администрирования, к порядку восстановления из резервных копий.

10.6. Управление безопасностью сети

Требования по информационной безопасности в отношении активов Организации, являющихся частью ИС, в равной степени распространяются на активы, составляющие сетевую инфраструктуру Организации, как внутри основного здания, так и за его пределами.

Обеспечение безопасности участков сетевой инфраструктуры, находящихся за пределами основного здания Организации требует особого внимания, в частности более частого контроля и аудита со стороны ответственного за обеспечение ИБ.

Информация, передаваемая по незащищённым и/или общедоступным каналам должна шифроваться и контролироваться ответственными сотрудниками Организации.

Обязанности по исполнения требований ИБ к сетевой инфраструктуре возлагаются на ответственного администратора.

Обязанности по контролю исполнения требований ИБ к сетевой инфраструктуре возлагаются на ответственного за обеспечение ИБ.

10.6.1. Средства контроля сети

Приказом руководства Организации или подрядной организации назначается ответственный администратор, в обязанности которого входит:

a) поддержание сетевой инфраструктуры ИС в рабочем состоянии;

b) инвентаризация и маркировка активов, входящих в сетевую инфраструктуру ИС;

c) настройка активного сетевого оборудования с целью недопущения утечек информации и несанкционированного доступа в сеть извне;

d) контроль доступа к ресурсам сети Интернет, получения и передача информации за пределы сетевой инфраструктуры ИС;

e) исполнение требований информационной безопасности в отношении активов, составляющих сетевую инфраструктуру Организации;

f) мониторинг активных компонентов сети и каналов связи;

g) мониторинг доступности сетевого и серверного оборудования;

h) мониторинг сервисов сети.

Мониторинг является основным внешним механизмом определения работоспособности сети и предоставляемых сервисов. Ответственный администратор, осуществляющий мониторинг компонентов сети составляет первую линию реагирования в случае отказа в обслуживании или недоступности сервисов.

В обязанности ответственного администратора входит адекватное и быстрое реагирование согласно Инструкции о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, в случаях затрагивающие непрерывность предоставления сервисов сети.

10.6.2. Безопасность сетевых сервисов

Требования к безопасности предоставляемых сервисов Организации или Организацией, а также непрерывность предоставления сервисов, должны быть четко описаны в договорных отношениях с поставщиками, подрядчиками, партнерами и заказчиками Организации.

Так же в договорных отношениях должны быть определены права заказчика на проведение аудита с целью определения качества и уровня безопасности потребляемых, предоставляемых сервисов.

Требования к обеспечению безопасности сетевой инфраструктуры Организации изложены в НТД по ИБ ИС.

НТД по ИС описывает:

a) технологии, применяемые для обеспечения безопасности сетевых услуг, таких как аутентификация, шифрование и контроль сетевых соединений;

b) технические параметры, необходимые для обеспечения соединения с сетью услуг в соответствии с уровнем безопасности и правилами сетевого соединения;

с) процедуры использования сервисной сети для ограничения доступа к сетевым услугам или приложениям, при необходимости.

10.7. Обращение с носителями информации

Документом, определяющим правила и порядок обращения с носителями информации, а также порядок проверки и защиту документов, компьютерных носителей информации (лент, дисков), данных ввода/вывода и системной документации от повреждения, воровства и неправомочного доступа, является Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

Обязанности по контролю исполнения требований ИБ настоящего раздела возлагаются на ответственного за обеспечение ИБ.

10.7.1. Управление съемными носителями информации

Для обеспечения ИБ в процессе управления съемными носителями информации утверждены Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

10.7.2. Утилизация носителей информации

Для обеспечения ИБ в процессе утилизации носителей информации утверждены организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

10.7.3. Процедуры обработки информации

Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования в процессе использования носителей информации утверждены Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

10.7.4. Безопасность системной документации

Документация, утверждённая в Организации, должна храниться в защищенном месте, предоставляться авторизованным сотрудникам согласно их функциональным обязанностям под роспись, выдача документации должна фиксироваться в Журнале ознакомления с документацией (по форме Приложения 2).

Требования к безопасности системной документации изложены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

10.8. Обмен информацией

Обмен информацией и программным обеспечением должен происходить на основе соглашений между организациями и соответствовать действующему законодательству (Раздел 15).

10.8.1. Политики и процедуры обмена информацией

Настоящий документ описывает требования и меры контроля к обеспечению защиты обмена информацией с клиентами, заказчиками, поставщиками услуг и партнерами Организации.

Любой процесс передачи информации должен контролироваться ответственными сотрудниками и подчиняться требованиям законов Республики Казахстан и утвержденным в Организации документам.

Обмен информацией может происходить с использованием различных средств связи, включая электронную и речевую связь, факсимильную и видеосвязь.

Обмен программными обеспечениями может происходить с использованием ряда различных носителей, включая скачивание из сети Интернет или приобретения у поставщиков, предоставляющих готовую продукцию.

Информация может быть перехвачена при обмене, нарушении политики и процедур использования средств связи, например, подслушивание при использовании мобильных телефонов в общественном месте, неправильных сообщений по электронной почте, прослушивание автоответчика, несанкционированного доступа к системам речевой связи, несанкционированном доступе к носителям информации или неправильной передачи сообщений на факсимильном аппарате.

Из-за перехвата информации могут быть нарушены бизнес-операции, а также при сбоях средств связи, их перегрузки или прерывания (10.3 и Раздел 14). Информация может быть под угрозой при доступе неавторизованных пользователей (Раздел 11).

Руководство Организации утверждает следующие меры для обеспечения безопасности передаваемой информации:

a) в случае необходимости передачи информации сотрудники Организации, должны проявлять бдительность и осторожность в процессе передачи информации; любая информации должна передаваться только авторизованным лицам с использованием доверенных средств передачи;

b) в Организации утверждены Правила организации антивирусного контроля для обнаружения и защиты от вредоносного кода, который передается путем использования электронных средств связи (10.4.1);

c) доступ к информации в виде вложенных файлов должен осуществляться с особой осторожностью только после проверки вложений на вредоносный код;

d) приемлемое использование электронных средств связи (см. 7.1.3) регулируется Правилами безопасного использования информации и активов, связанных со средствами обработки информации;

e) использование беспроводной связи, в роле локальной сети Организации запрещено; использование сотовой связи разрешено в границах ведения переговоров; подключение к глобальным сетям с использованием сотовой связи и передача с ее помощью информации запрещено;

f) сотрудникам, подрядчикам или любым другим работникам запрещается компрометировать Организацию, клиентов, заказчиков, поставщиков услуг и партнеров Организации, например, путем клеветы, домогательства, лицемерия, пересылки цепных писем («писем счастья»), несанкционированной покупки и т.д., выступать публично, давать интервью или публиковать какую-либо информацию от имени Организации без имеющегося на то официального документа;

g) Организация не занимается разработкой или реализацией средств криптографической защиты информации, являющиеся лицензируемыми видами деятельности; использование в организации электронно-цифровой подписи регулируется Законом Об электронном документе и электронной цифровой подписи; для защиты информации в процессе передачи данных используется стандартные протоколы с применением стойких ко взлому методов шифрования (https, sftp, ssh, RDP и др.) (см. 12.3, 15.1.6);

h) вся передаваемая информация, сохранение которой не требуется, должна уничтожаться;

i) сотрудники должны помнить, что нельзя оставлять важную или критическую информацию на печатающих устройствах, например, на копировальных машинах, принтерах, факсимильных аппаратах, так как эта информация может стать доступной для посторонних лиц;

j) автоматическая рассылка электронных писем, уведомлений, новостей Организации (а также публикация информации на официальном сайте Организации), разрешается только уполномоченным на это лицам, только с официального электронного почтового ящика и только адресатам, заранее подтвердившим свою подписку; подписчики имеют права отказаться от получения писем рассылки в любое время;

k) ответственный за обеспечение ИБ обязан уведомлять сотрудников (в рамках инструктажей) о необходимости принятия соответствующих мер предосторожности, например, для исключения подслушивания или перехвата информации при использовании телефонной связи:

1) лицами, находящимися в непосредственной близости, особенно при пользовании мобильными телефонами;

2) прослушивания телефонных переговоров путем физического доступа к трубке, телефонной линии или с использованием сканирующих приемников при применении аналоговых мобильных телефонов;

3) посторонними лицами со стороны адресата;

l) сотрудники не должны оставлять сообщений на автоответчиках, переадресация на которые произошла вследствие ошибки соединения, или автоответчиках операторов связи, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами;

m) ответственный за Обеспечение ИБ обязан напоминать сотрудникам (в рамках инструктажей) о возможных рисках, присущих факсимильным аппаратов и другим программируемым средствам передачи электронных сообщений, а именно:

1) несанкционированный доступ к встроенной памяти для поиска сообщений;

2) преднамеренное или случайное программирование аппаратов с целью передачи сообщений по определенным номерам;

3) отсылка документов и сообщений по неправильному номеру вследствие неправильного набора либо из-за использования неправильно сохраненного номера;

n) ответственный за Обеспечение ИБ обязан напоминать сотрудникам (в рамках инструктажей) о недопустимости сохранении персональных и служебных данных, такие как адреса электронной почты или другой личной информации, в программном обеспечении, чтобы избежать несанкционированных действий;

o) ответственный за Обеспечение ИБ обязан доводить до сведения сотрудников (в рамках инструктажей) о том, что современные печатные устройства снабжены памятью, и сохраняют страницы в случае дефекта бумаги или передачи, которые после устранения ошибки будут пропечатываться еще один раз. Кроме того, сотрудникам следует напомнить о том, что не следует вести конфиденциальные беседы в общественных местах, открытых офисах и в помещениях не предназначенных для этого.

10.8.2. Соглашения по обмену информацией

Любые соглашения по обмену информацией и программным обеспечением между Организацией и сторонними организациями должны быть официально оформлены и подписаны всеми участвующими сторонами.

В соглашениях необходимо отразить необходимость защиты и важность вовлеченной служебной информации.

Соглашения по обмену информацией должны учитывать следующие требования безопасности:

a) ответственный за обеспечение ИБ обязан контролировать процесс передачи и уведомлять о передаче, отправке, получении, составе и количестве информации;

b) отправитель и получатель должны быть авторизованы и заранее осведомлены о предстоящем процессе передачи;

c) процесс передачи информации должен журналироваться, все события, участники и объекты должны фиксироваться и прослеживаться;

d) минимальные технические требования по формированию и передаче информации должны быть официально зафиксированы и подписаны всеми участвующими сторонами;

e) в случае необходимости хранения информации после завершения совместных работ должны быть официально зафиксированы и подписаны условия депонирования полученной информации;

f) требования к курьерской службе должны быть официально зафиксированы;

g) ответственности и обязательства в случае потери данных должны быть официально зафиксированы;

h) система маркировки информации должна быть официально зафиксирована; применяемая маркировка должна гарантировать уверенность в том, что значение этой маркировки будет сразу же понятно и информация будет соответственно защищена;

i) маркировка информации, должна включать отметку с указанием определения владельцев информации и программного обеспечения; ответственным за защиту информации, при ее передаче возлагается на сотрудника, выполняющего процесс передачи; ответственность за учет авторских прав на программное обеспечение и аналогичные вопросы возлагается на менеджера проекта (см. 15.1.2 и 15.1.4); ответственность за контроль исполнения требований настоящего документа возлагается на ответственного за обеспечение ИБ;

j) технические требования в отношении записи и считывания информации и программного обеспечения должны быть официально зафиксированы и подписаны всеми участвующими сторонами;

k) любые специальные средства контроля, которые могут потребоваться для защиты важных объектов, например, криптографические ключи (12.3) должны быть официально зафиксированы и подписаны всеми участвующими сторонами.

Соглашения по обмену информацией должны учитывать требования утвержденных в Организации документов в отношении защиты физических носителей информации при транспортировке (см. 10.8.3), исполняться и поддерживаться.

10.8.3. Защита физических носителей информации при транспортировке

Информация может быть искажена или скомпрометирована вследствие несанкционированного доступа, неправильного использования или искажения во время физической транспортировки, например, при пересылке носителей информации по почте или через курьера.

Доступ к носителям информации должен быть только у авторизованных лиц. Использование носителей информации, хранение и транспортировка должны соответствовать требованиям производителя. Поврежденные носители информации должны утилизироваться в соответствии с установленными процедурами.

Для защиты информации во время их транспортировки между организациями, применяются следующие меры:

a) надежность перевозчиков и курьеров подтверждается сроком исполнения курьерской службы и закрепляется требованиями ответственности за транспортируемый объект;

b) договора курьерских услуг и услуг транспортировки согласуются с ответственным за обеспечение ИБ и подписываются руководством Организации;

c) непосредственно перед передачей транспортируемого объекта курьеру, курьер должен быть авторизован уполномоченными лицами курьерской службы;

d) упаковка должна быть достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при транспортировке, и соответствовать требованиям изготовителей носителей информации, защиту от каких-либо факторов окружающей среды, сокращающих эффективность восстановления носителя информации, таких как воздействие высокой температуры, влажности или электромагнитного поля;

e) специальные средства контроля следует применять, при необходимости, для защиты важной информации от неавторизованного раскрытия или модификации. Например:

1. использование запертых контейнеров;
2. личную доставку;
3. использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);
4. в исключительных случаях, разбивку отправления на несколько частей, пересылаемых различными маршрутами.

10.8.4. Электронный обмен сообщениями

Электронные обмены сообщениями, такие как электронная почта, мгновенные сообщения и электронный документооборот играют важную роль в бизнес-коммуникаций Организации. Однако электронные сообщения более подвержены риску по сравнению с бумажными системами связи.

Никакое электронное сообщение не может являться официальным документом, если оно не подписано электронно-цифровой подписью руководства Организации или официально уполномоченного им лица.

Сотрудникам разрешается обмениваться электронными сообщениями внутри Организации, с клиентами, заказчиками, поставщиками услуг и партнёрами только с применением протоколов шифрования «от точки к точке».

Все электронные сообщения, отправляемые во исполнение должностных обязанностей, должны быть подписаны фамилией, именем, отчеством, должностью, контактным телефоном отправителя, названием, адресом Организации и содержать предупредительный текст о конфиденциальности информации: «Данное сообщение (включая любые вложения) может содержать конфиденциальную информацию и быть предназначенным исключительно для лица или организации, которой оно адресовано.

Если Вы не являетесь надлежащим адресатом, то настоящим Вы уведомлены, что любое раскрытие, копирование, распространение или использование содержания этого сообщения строго запрещено.

Если Вы получили это сообщение по ошибке, пожалуйста, поставьте нас в известность об этом немедленно, ответив на это письмо, и затем удалите его из своей системы. Спасибо.».

Ответственный за обеспечение ИБ должен разъяснять сотрудникам (в рамках инструктажей) Организации вопросы безопасности электронных сообщений:

a) уязвимость сообщений по отношению к возможности от несанкционированного доступа или модификации, а также к отказу в обслуживании;

b) обеспечение правильных способов транспортировки сообщений;

c) общую ненадежность и уязвимость данной услуги;

d) правовые вопросы, например, требования в отношении электронных подписей;

e) обязательность получения предварительного разрешения у ответственного за обеспечение ИБ на использование внешних общественных услуг, таких как мгновенные файлы сообщения или совместное использование файлов;

f) обязательность процедуры аутентификации контроля доступа к общедоступным сетям и применению шифрования.

10.8.5. Системы бизнес-информации

Информационные системы обеспечивают возможность для быстрого распространения и совместного использования служебной информации путем использования сочетания возможностей документов, сервисов, переносных компьютеров, мобильных средств связи, почты, электронной почты, речевой связи, мультимедийных систем, сервисов доставки почтовых отправлений и факсов.

Для каждой интеграции информационных систем Организации должен быть разработан и утвержден регламент взаимодействия.

Регламент взаимодействия должен отражать:

a) известные уязвимости в административной системе и системе учета, где информацией пользуются между разными подразделениями организации;

b) оценку уязвимости информации при интеграции и методы обработки рисков;

c) механизмы взаимодействия, защиты, передачи, проверки целостности и гарантированной доставки информации;

d) классификацию информации интеграционного обмена с указанием способа защиты для каждого класса (7.2);

e) перечень персональных данных и разрешительные документы для их обработки;

f) места доступа к процессу обмена и категории сотрудников, подрядчиков или бизнес-партнеров, которые могут осуществляться к ним доступ (6.2 и 6.3);

g) ограничение определенных возможностей системы для определенных категорий пользователей;

h) идентификация статуса пользователей, например, служащих организации или подрядчиков;

i) сохранение и резервирование информации, содержащейся в системе (10.5.1);

j) требования к системе восстановления, месту размещения и обеспечению непрерывности (Раздел 14).

10.9. Услуги электронной торговли

Настоящий документ учитывает последствия безопасности, связанные с использованием услуг электронной торговли и транзакции в режиме реального времени (on-line), а также организационных мероприятий по управлению информационной безопасностью. Следует принимать во внимание целостность и доступность информации, проходящую по общедоступным сетям.

10.9.1. Электронная торговля

Организация не предоставляет услуг площадки электронной торговли. Организация учувствует в электронных торгах на официальных площадках государственных электронных закупках в соответствии с требованиями законодательства РК.

10.9.2. Транзакции в режиме реального времени (on-line)

Организация не оказывает услуг платформы для выполнения финансовых транзакций.

Финансовые транзакции, выполняемые самой Организацией во исполнения договорных и иных обязательств, проводятся посредствам банковских операций.

Информационная система использует в роле своего компонента транзакционную базу данных. Под транзакцией следует понимать группу последовательных операций с базой данных, которая представляет собой логическую единицу работы с данными. Транзакция может быть выполнена либо целиком и успешно, соблюдая целостность данных, безопасность, конфиденциальность, неизменность и независимо от параллельно идущих других транзакций, либо не выполнена вообще и тогда она не должна произвести никакого эффекта.

Средства, методы и механизмы обеспечения защиты транзакций соизмеряются с уровнем риска, связанным с каждой формой он-лайн транзакции.

Система управления базой данных настроена таким образом, чтобы информация, используемая в транзакциях в режиме реального времени (on-line), защищена от предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного воспроизведения транзакции.

Из соображений безопасности для онлайновой транзакции включено следующее:

a) использование электронных подписей каждой стороной, участвующей в транзакции;

b) подтверждения того, что:

1) учетные данные всех сторон, являются действительными и проверены;

2) транзакция остается конфиденциальной;

3) сохраняется конфиденциальности сведений всех заинтересованных сторон;

c) линии связи между всеми заинтересованными сторонами должны быть зашифрованы;

d) обеспечение согласованности протоколов, используемых для обмена данными между всеми заинтересованными сторонами;

e) обеспечение защиты данных базы, сведений о транзакции и расположение их в сетях, не имеющих прямого доступа из общественных сетей;

f) используемые механизмы подтверждения доверия к сертификатам и электронным подписям должны подчиняться требованиям законов Республики Казахстан.

Ответственный за обеспечение ИБ обязан следить за тем, чтобы транзакции соответствовали законам, правилам и нормам, установленным в юрисдикции, в которой транзакция производится, обрабатывается, завершается и/или хранится.

10.9.3. Общедоступная информация

Публикуемая для общественного пользования открытая информация должна быть защищена от неавторизованного изменения. Несанкционированная модификация опубликованной информации может нанести ущерб репутации Организации.

Информация для публичного доступа, например, информация на Web-сайте, доступная через Интернет, требует приведения в соответствие с законодательством и регулирующими нормами, под юрисдикцией которых находится система и осуществляется деятельность Организации.

Любая информация, требующая гарантии целостности должна подписываться электронно-цифровой подписью Организации (12.3). Соответствие цифровой подписи содержимому и актуальность цифровой подписи, должны проверяться перед публикацией информации или другим ее использованием.

Любой доступ к информации (в том числе и к открытой) должен фиксироваться для прослеживания получателя. Кроме того, все входящие данные, предоставленные в систему со стороны, должны быть проверены и одобрены.

Системы, предоставляющие возможность электронной публикации информации, обратной связи и непосредственного ввода информации,

должны находиться под надлежащим контролем, а вся публикуемая информация проходить соответствующую модерацию, чтобы:

a) полученная информация соответствовала законам Республики Казахстан (15.1.4);

b) информация, введенная в систему электронной публикации, обрабатывалась своевременно, полностью и точно;

c) важная информация была защищена в процессе ее сбора и хранения;

d) доступ к системе электронной публикации исключал бы возможность непреднамеренного доступа к сетям, с которыми она связана.

Ответственный за модерацию и контроль движения информации назначается приказом руководства Организации.

10.10. Мониторинг

Все события имеющие отношения к ИС и/или ЭИР должны прослеживаться с использованием электронных, бумажных журналов аудита и фиксирования мероприятий.

Ответственным за контроль соблюдения требований настоящего документа, является ответственный за обеспечение ИБ.

События, происходящие в процессе использования ИС и/или ЭИР должны регистрироваться. За каждым журналов должен быть назначен ответственный сотрудник Организации, отвечающий за его ведение.

Организация должна соблюдать все соответствующие правовые требования, предъявляемые к мониторингу и регистрации событий.

Процесс мониторинга позволяет проверять эффективность применяемых мероприятий по обеспечению информационной безопасности и подтверждать соответствие модели безопасности требованиям бизнеса.

10.10.1. Ведение журналов аудита

Механизмы ИС обеспечивают ведение и хранение в течение пяти лет журналов, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа.

В журналах должны фиксироваться:

a) идентификаторы пользователей;

b) даты и время входа и выхода и/или регистрации события в журнале;

c) тип события: информация, предупреждение, ошибка, отладка, сообщение функции ИБ, и др. по необходимости;

d) идентификатор источника события (например, терминала, модуля, подсистемы, сервера) и его местоположение (если возможно), его сетевой адрес;

e) записи успешных и отклоненных попыток операций (например, доступа к системе, создание объекта, запись в БД, подключения к портам управления и т. п.);

f) записи успешных и отклоненных попыток доступа к данным и другим ресурсам;

g) изменение конфигурации системы;
h) использование привилегий;
i) использование системных утилит и приложений;
j) доступ к файлам и типы доступа;
k) сетевые адреса и протоколы;
l) тревожные сигналы, подаваемые системой контроля доступа;
m) активации и деактивации систем защиты, таких как антивирусные системы и системы обнаружения вторжений.

В журналах аудита могут содержаться личные и конфиденциальные данные. В связи с этим любые журналы Организации подлежат защите и обеспечению конфиденциальности (см. также 15.1.4).

Системные администраторы не имеют разрешение на изменение, удаление или деактивацию журналов регистрации, изменение их собственных привилегий (см. 10.1.3).

10.10.2. Мониторинг использования средств обработки информации

Ответственный за обеспечение ИБ и администратор ИС обязаны осуществлять мониторинг журналов ИС и журналов систем автоматического реагирования на инциденты ИБ, если таковые используются.

В случае выявления инцидента ИБ сотрудники Проекта ИС, системные администраторы, ответственный за обеспечение ИБ должны соблюдать требования Инструкции о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, Правил по обеспечению непрерывной работы активов, связанных со средствами обработки информации и Плана мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации.

Регулярность мониторинга журналов определяется, разработанным ответственным за обеспечение ИБ и утвержденным руководством Организации, Планом мониторинга журналов регистрации (по форме Приложения 7). Сотрудники Организации должны соблюдать все соответствующие законодательные требования, применяемые к мониторинговой деятельности.

При мониторинге следует обращать внимание на:
a) авторизованный доступ, включая следующие детали:
1) пользовательский ID;
2) дату и время основных событий;
3) тип событий;
4) файлы, к которым был осуществлен доступ;
5) используемые программы/утилиты;
b) все привилегированные действия, такие как:
1) использование учетной записи супервизора;
2) запуск и остановка системы;
3) подсоединение/отсоединение устройства ввода/вывода;

c) попытки несанкционированного доступа, такие как:

1) неудавшиеся или отклоненные попытки пользователя;

2) неудавшиеся или отклоненные попытки доступа к данным и другим ресурсам;

3) нарушение политики доступа и уведомления сетевых шлюзов и систем сетевой защиты;

4) предупреждения от собственных систем обнаружения вторжений;

d) предупреждения или отказы системы, такие как:

1) консольные (терминальные) предупреждения или сообщения;

2) исключения, записанные в системные журналы регистрации;

3) предупредительные сигналы, связанные с управлением сетью;

4) оповещения, созданные системой управления доступом;

e) изменения или попытки изменения настроек безопасности системы и средств управления.

При разработке плана мониторинга журналов регистрации, частота рассмотрения результатов мониторинга должна определяться критичностью обрабатываемой информации. Должны быть рассмотрены факторы риска, в том числе:

a) критичность процессов приложений;

b) значимость, важность и критичность вовлеченной информации;

c) прошлый опыт несанкционированного проникновения в систему и ее неправильного использования, частота использования уязвимых мест;

d) степень взаимосвязи информационных систем организации с другими (особенно общедоступными) сетями;

e) регистрация деактивации средства.

Журналирование событий должно быть включено на рабочих станциях ответственного за обеспечение ИБ, менеджера проекта, администраторов, разработчиков для обеспечения уверенности в том, что они выполняют только те действия, на которые они были явно авторизованы.

Результаты мониторинга журналов заносятся в отчет по результатам внутреннего аудита (в рамках работ по аудиту) и в Журнал контроля, мониторинга обеспечения ИБ и проведения работ по информационной безопасности (по форме Приложения 10).

Для обеспечения непрерывной работы в режиме 24/7/365 СОИБ составляет, согласовывает с заинтересованными сторонами График круглосуточного дежурства ответственных администраторов ИС по форме согласно Приложения 8.

10.10.3. Защита информации журналов регистрации

Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства (внесения исправлений, удаления, отключения) и несанкционированного доступа.

Страницы бумажных журналов должны быть пронумерованы, прошнурованы и скреплены печатью. Строки должны вестись не прерывно, без пробелов, корректировка записей допускается только в присутствии

ответственного за ведение журнала, ответственного за обеспечение ИБ и скрепляться их подписями.

Доступ к электронным журналам должен быть ограничен и авторизован. При очистке журнала, в него должна вноситься запись о том «кто» и «когда» его очистил. Очистка журнала может производиться только ответственным за обеспечение ИБ. Внесение изменений в электронные журналы не допускается. Журналы событий ИС архивируются с использованием криптографической защиты.

Средства управления электронными журналами реализованы таким образом, чтобы обеспечить защиту от внесения несанкционированных изменений в отчеты и журналы, препятствованию работы оборудования и программного обеспечения создания отчетов и ведения журналов, в том числе:

a) изменение типов зарегистрированных сообщений;

b) редактирование или удаление файлов отчетов и записей журналов;

c) превышения вместимости носителей информации, на которых хранятся отчеты, в результате чего происходят сбои записи событий или перезапись последних зарегистрированных событий.

Системные журналы часто содержат информацию, значительный объем которой не представляет интереса с точки зрения мониторинга безопасности. Для облегчения идентификации существенных событий при мониторинге безопасности происходит автоматическое копирование соответствующих типов сообщений в отдельный журнал, а также используются системные утилиты и инструментальные средства аудита для подготовки к анализу данных.

10.10.4. Журналы регистрации действий администратора и оператора

Администратор ИС должен выполнять регистрацию своих действий в Журнале регистрации действий администратора (по форме Приложения 6).

Ответственный за обеспечение ИБ обязан проводить анализ действий администратора в соответствии с планом внутреннего аудита и планом мониторинга журналов регистрации проекта.

На серверном оборудовании ИС ведется автоматическая запись действий системных администраторов ИС. Ответственный за обеспечение ИБ должен проводить сверку записей Журнала регистрации действий администратора с журналом автоматической записи действий системных администраторов ИС в рамках мониторинга журналов регистрации проекта.

10.10.5. Регистрация неисправностей

Неисправности в работе программного обеспечения, серверного и сетевого оборудования ИС должны регистрироваться ответственными за них сотрудниками Организации в Журнале системно-технического обслуживания (по форме Приложения 5).

Обязанности за регистрацию сообщения пользователей о неисправностях, связанных с обработкой информации или системами связи в журнале жалоб и рекламаций возлагается на менеджера проекта.

Так же на менеджера проекта возлагается ответственность за контроль процесса исправления выявленных замечаний: принятие в обработку, разработка корректирующих мероприятий и плана их применения, отчет с результатами применения корректирующих мероприятий.

Менеджер проекта ИС и ответственный за ИБ обязаны осуществлять контроль работы по исправлению неисправностей и замечаний пользователей в процессе внутреннего аудита:

a) анализ неисправностей для обеспечения уверенности в том, что они были удовлетворительным образом устранены;

b) анализ предпринятых корректирующих мер, обеспечивающих уверенность в том, что мероприятия по управлению информационной безопасностью не были скомпрометированы (нарушены) и предпринятые действия надлежащим образом авторизованы.

10.10.6. Синхронизация часов

Правильная установка компьютерных часов важна для обеспечения точности заполнения журналов регистрации, которые могут потребоваться для расследований или как доказательство при судебных или и административных разбирательствах.

Некорректные метки времени в журналах регистрации могут затруднять такие расследования, а также приводить к сомнению в достоверности собранных доказательств. В качестве основных часов для систем регистрации событий используются следующие серверы времени *1.kz.pool.ntp.org, 1.asia.pool.ntp.org, 2.asia.pool.ntp.org*. Для поддержания синхронности всех серверов с основными часами используется протокол NTP.

Часы всех соответствующих систем обработки информации в пределах Организации и охраняемой зоны синхронизированы с помощью единого источника точного времени.

Интерпретация записей времени производится в соответствии с требованиями документов, прилагаемых производителем ПО и оборудования.

11 Контроль доступа

11.1. Бизнес-требования к контролю доступа

Доступ к информации и бизнес-процессам должен быть контролируемым с учетом требований бизнеса и безопасности

Требования к контролю доступа регламентированы в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.1.1. Политика контроля доступа

Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам и Матрицей доступа ИС однозначно определяют права и обязанности каждого пользователя и/или группы пользователей ИС.

Физический контроль доступа описан в Разделе 9. Пользователи ИС, сотрудники проекта, пользователи ИС и поставщики услуг обеспечения эксплуатации должны быть оповещены о необходимости выполнения требований в отношении доступа к ИС.

Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам и Руководство руководство администратора по сопровождению объекта информатизации, резервному копированию и восстановлению информации охватывают следующие аспекты:

a) требования к защите от НСД ИС;

b) идентификация всей информации СУБД ИС;

c) условия распространения информации и авторизации доступа, а также в отношении категорированной информации и требуемых уровней ее защиты (7.2);

d) выполнение требований классификации информации;

e) применяемое законодательство и любые договорные обязательства относительно защиты доступа к данным или сервисам (15.1);

f) стандартные роли пользователя для типовых обязанностей и функций;

g) управление правами доступа ответственными пользователями;

h) распределение обязанностей к контролю доступа, например, право доступа, авторизация доступа, администрирование доступа;

i) требования формализованной авторизации прав доступа (11.2.1);

j) требования периодического пересмотра прав доступа (11.2.4);

k) аннулирование прав доступа (8.3.3).

11.2. Управление доступом пользователей

Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам охватывают все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации

пользователей, которым больше не требуется доступ к информационным системам и сервисам.

Особое внимание уделено мероприятиям в отношении предоставления прав привилегированного доступа, с помощью которых пользователи могут обходить системные средства контроля.

11.2.1. Регистрация пользователей

Правила организации процедуры аутентификации и Руководство администратора по сопровождению ИС описывают формализованную процедуру регистрации и снятия с регистрации пользователей в отношении предоставления доступа к ИС.

11.2.2. Управление привилегиями

Предоставление и использование привилегий описывается в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

Формализованный процесс авторизации описан в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.2.3. Управление паролями пользователей

Управление паролями и парольной политикой определяется Правилами организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.2.4. Пересмотр прав доступа пользователей

Процедура пересмотра прав доступа пользователей описана в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.3. Ответственность пользователей

Ответственность пользователей описывается Правилами организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.3.1. Использование паролей

Пользователи должны соблюдать правила обеспечения безопасности при выборе и использовании паролей.

Все пользователи должны быть осведомлены о необходимости:

a) сохранения конфиденциальности паролей;

b) запрещения записи паролей на бумаге, на файле программного обеспечения или на переносных устройствах, если только не обеспечено безопасное их хранение;

c) изменения паролей всякий раз, при наличии любого признака возможной компрометации пароля;

d) выбора качественных паролей, которые:

1) не менее 6 символов длиной;

2) не подвержены легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например, имен, номеров телефонов, дат рождения и т.д.;

3) не уязвимы для атаки по словарю (т.е. не состоят из слов, включенных в словари);

4) содержат: строчные и прописные буквы латинского алфавита, цифры и символы $ # @;

e) изменения паролей каждые 30 дней, исключения повторного или цикличного использования старых паролей (пароли для привилегированных учетных записей должны меняться каждые 20 дней);

f) изменения временных паролей при первой регистрации в системе;

g) запрещения включения паролей в автоматизированный процесс регистрации, например, с использованием авто-сохранения браузером или скриптом;

h) исключения коллективного использования индивидуальных паролей;

i) не использовать один и тот же пароль для служебных и личных целей.

Пользователи обязаны уведомлять ответственного за обеспечение ИБ о потери, компрометации или забытых паролях ИС.

11.3.2. Оборудование, оставленное пользователем без присмотра

Требования к обеспечению безопасности оборудования, оставленного пользователем без присмотра, описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.3.3. Политика «чистого стола» и «чистого экрана»

Политика «чистого стола» и «чистого экрана» описана в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.3Б Политика использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам

11.3Б.1 Управление сетевой безопасностью

Цель настоящей политики: обеспечивать защиту информации в сетях Организации и в средствах обработки информации поддержки.

11.3Б.1.1 Сетевые средства управления

Для защиты от несанкционированного доступа к информации (передаваемой по сети), связанных с сетью услуг и самих компонентов сети необходимо использовать специализированные средства управления и контроля.

В частности, необходимо обеспечить соблюдение следующих требований:

a) соблюдение требований Правил использования сети интернет и электронной почты;

b) за каждый компонент сети (или за набор компонентов, например, за сеть в офисе, сеть в серверной и т. п.) должен быть назначен ответственный сотрудник (см. СТ РК 27002 пп. 6.1.2);

c) Для обеспечения конфиденциальности, целостность и доступности данных, передающихся по сетям (включая беспроводные сети) и защитить связанные системы/сервисы и обеспечить исполнение настоящего документа в целом (и требований п. 10 и п. 13.2 в частности) необходимо использовать специализированные средства управления и контроля. Обязательными средствами/функциями для защиты сети и передаваемых данных являются: IPS/IDS, потоковый антивирус, фильтр трафика по IP-адресу (источника и/или назначения), фильтрация по URL назначения, аутентификация/авторизация для доступа к настройкам оборудования и сервисам сети, журналирования событий, мониторинг состояния и доступности компонентов сети и сервисов, оповещение ответственных сотрудников об ошибках, подозрениях на инцидент ИБ и об инцидентах ИБ, организация точки подключения к VPN-сети (для удаленной работы сотрудников и/или удаленному подключению системных администраторов и СОИБ к средствам конфигурирования, мониторинга и журналирования и т. п.), шифрование трафика;

d) средства журналирования, средства мониторинга состояния и доступности компонентов сети и средства оповещения должны быть интегрированы, чтобы позволить делать запись, обнаружение действий (которые могут затронуть или относятся к информационной безопасности) и оповещение ответственных сотрудников;

e) на СОИБ возлагается ответственность координации управленческих действий и контроль соблюдения требований документов по ИБ, и ответственность за оптимизацию процессов обеспечения ИБ для гарантирования, что средства управления последовательно применяются через инфраструктуру обработки информации;

f) сервисы и компоненты сети должны быть однозначно идентифицированы подтверждены принятыми средствами (например, для доступа по средствам HTTPS, доступ должен быть подтвержден SSL-сертификатом выпущенными доверенным для Организации центром);

g) подключение сервисов к сети должно мониториться, журналироваться и быть ограниченным (обеспечивать минимально-необходимый набор привилегий для исполнения своих задач).

11.3Б.1.2 Безопасность сетевых служб (сервисов)

Настоящий документ включает и определяет механизмы безопасности, сервисное обслуживание и управленческие требования всех сетевых сервисов.

Приобретаемые услуги доступа к сети Интернет или подключения к частным сетям должны включать требования по информационной безопасности описанные в пп. 13.1.1 настоящего документа. Если такие меры

не могут быть предоставлены поставщиком подключения, то Организация должна самостоятельно обеспечить требуемый уровень информационной безопасности.

Сетевые службы включают предоставление связей, услуг частной сети и оценивают добавленные сети и решения для сетевой безопасности, которыми управляют, такие как брандмауэры и системы обнаружения вторжения. Эти услуги могут колебаться от простой неуправляемой полосы пропускания до сложных предложений с добавленной стоимостью.

Механизмы безопасности сетевых служб должны обеспечивать:

a) технологии, применяемые для безопасности сетевых служб, таких как идентификация, шифрование и сетевые средства управления связью;

b) технические параметры, требуемые для обеспеченной связи с сетевыми службами в соответствии с безопасностью и сетевыми правилами связи;

c) процедуры использования сетевой службы, чтобы ограничить доступ к сетевым службам или заявлениям, в случае необходимости.

11.3Б.1.3 Разделение в сетях

С целью обеспечения информационной безопасности там, где это повысит защищенность информации следует использовать разделение сетей.

В отношении компонентов информационных систем требуется обязательное разделение на компоненты доступные из внешних сетей (например, из Интернет или из сетей сторонних организация) и компонентов доступных только в корпоративной сети Организации (например, разделение на DMZ, и private network).

Беспроводные сети следует обязательно отделять от приватных сетей и использовать только для доступа к Интернет (изнутри Организации) или для доступа к точке подключения к безопасной сети (например, к точке подключения к VPN-соединению, которое обеспечивает необходимый уровень информационной безопасности) (см. СТ РК 27002 пп. 13.1.1).

Область действия беспроводных должна быть ограничена используя средства понижения мощности сигнала.

Для идентификации, шифрования и управления доступом к сети следует использовать надежные, современные, отвечающие установленным требованиям средства и технологии.

11.3Б.2 Информационная передача

Для поддержания безопасности информации, которая передается внутри организации и любому внешнему получателю необходимо соблюдать требования настоящего документа.

11.3Б.2.1 Информационная политика передачи и процедуры

Чтобы защитить передачу информации с помощью всех типов средств коммуникации, настоящая политика определяет обязательные требования к передаче, процедурам и средствам управления информацией.

Все процессы передачи информации должны соблюдать следующие требования:

a) чтобы защитить переданную информацию от перехвата, копирования, модификации, неправильного направления и разрушения необходимо соблюдение требований 13.1.1;

b) необходимо использовать потоковый антивирус для обнаружения и защиты от вредоносного программного обеспечения, которое может быть передано с помощью электронных средств связи (см. СТ РК 27002 пп. 12.2.1);

c) защита сообщенной электронной почты описана в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;

d) требования и рекомендации, обрисовывающие в общих чертах приемлемое использование средств для коммуникации изложены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;

e) сотрудники Организации, партнеры и подрядчики не должны компрометировать организацию, например, через клевету, преследование, олицетворение, отправление писем счастья, несанкционированную покупку, и т.д.;

f) требования к средствам криптографии изложены в Правила использования средств криптографической защиты информации (см. СТ РК 27002 пп. Раздел 10);

g) требования к деловой переписке, включая сообщения изложены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты, в соответствии с соответствующим национальным и местным законодательством и инструкциями;

h) требования к средствам управления и ограничения, связанных с использованием средств для коммуникации, например, автоматическим отправлением электронной почты к внешним почтовым адресам изложены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;

i) все сотрудники Организации, партнеры и подрядчики должны регулярно уведомляться о необходимости предпринимать меры предосторожности, чтобы не показать конфиденциальную информацию, а также об обязанности соблюдать требования настоящего документа;

j) сотрудники должны уточнять корректность адреса отправителя, чтобы предотвратить отправку информации случайным лицам;

k) сотрудники должны уведомлять в случае обнаружение неисправностей средств телекоммуникаций или о подозрении на нарушения требований информационной безопасности, а именно:

1) несанкционированный доступ к встроенным архивам сообщений, чтобы восстановить сообщения;

2) умышленное или случайное программирование машин, чтобы послать сообщения в определенные числа;

3) отправка документов и сообщений к неправильному числу или неправильному набору или использованием неправильного сохраненного числа.

Кроме того, персоналу нужно напомнить, что у них не должно быть конфиденциальных разговоров в общественных местах или по опасным каналам связи, открытым офисам и местам для собраний.

Информационные услуги по передаче должны выполнить любые соответствующие законные требования, принятые в Республике Казахстан (см. СТ РК 27002 пп. 18.1).

11.4. Контроль сетевого доступа

Доступ к серверам ИС, доступ сотрудников проекта к локальной сети и корпоративной сети регламентируется Правилами организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

Доступ сотрудников проекта к сети Интернет регламентируется Правилами организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты.

11.4.1. Политика в отношении использования сетевых услуг

Политика в отношении использования сетевых услуг регламентируется Правилами организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам.

11.4.2. Аутентификация пользователей для внешних соединений

Аутентификация удаленного доступа к серверам для их обслуживания достигается путем использования средств криптографии с использованием виртуальной частной сети (VPN).

Аутентификация серверов ИС происходит по их уникальному IP-адресу.

Сотрудникам проекта запрещено использовать беспроводные сети и мобильные технологии для доступа к сети проекта, сети Интернет и серверам ИС или другим сетям.

Сотрудникам проекта запрещено автоматизировать ввод паролей, ключей и других идентификаторов при подключении серверам ИС.

11.4.3. Идентификация оборудования в сетях

Идентификация оборудования при осуществлении доступа к нему описана в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.4.4. Защита диагностических и конфигурационных портов при удаленном доступе

Защита диагностических и конфигурационных портов при удаленном доступе описана в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.4.5. Принцип разделения в сетях

Принцип разделения в сетях описан в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам и технических документах к ИС.

11.4.6. Контроль сетевых соединений

Требования к процессу контроля сетевых соединений описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.4.7. Управление маршрутизацией сети

Требования к управлению маршрутизацией сети проекта и ИС описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5. Контроль доступа к операционной системе

Требования к контролю доступа к операционной системе в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.1. Безопасные процедуры регистрации с терминала

Требования к процедуре регистрации с терминала описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.2. Идентификация и аутентификация пользователя

Требования к идентификации и аутентификации пользователя описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.3. Система управления паролями

Требования к системе управления паролями описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.4. Использование системных утилит

Требования к обеспечению безопасности при использовании системных утилит описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.5. Периоды бездействия в сеансах связи

Требования к реакции компонентов ИС в периоды бездействия в сеансах связи описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.5.6. Ограничение времени соединения

Информационная система разработана таким образом что не допускает длительного бездействия канала соединения. Длительность интервала соединения без использования регулируется настройками ИС.

11.6. Контроль доступа к прикладным системам и информации

Контроль доступа к прикладным системам и информации описан в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.6.1. Ограничение доступа к информации

Пользователям ИС, включая персонал поддержки и эксплуатации, обеспечивается доступ к информации и функциям ИС в соответствии с Правилами организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.6.2. Изоляция систем, обрабатывающих важную информацию

Требования к изоляции систем, обрабатывающих важную информацию описаны в Правилах организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам .

11.7. Работа с переносными устройствами и работа в дистанционном режиме

Сотрудникам проекта разрешено работать только в защищаемых помещениях проекта:

a) в здании Организации;
b) в серверных помещениях проекта.

В качестве переносных устройств, для работы в защищаемых помещениях, разрешено использование только служебных средств обработки и хранения информации.

11.7.1. Работа с переносными устройствами и средствами связи

Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам устанавливают методы защиты информации и активов ИС от рисков при использовании средств связи и переносных устройств.

При использовании переносных устройств, например, ноутбуков, карманных компьютеров, переносных компьютеров и мобильных телефонов, необходимо принимать специальные меры противодействия компрометации служебной информации.

Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам , учитывают риски, связанные с работой с переносными устройствами.

Политика по ИБ и утвержденные документы по ИБ включают в себя требования по физической защите, контролю доступа, использованию средств и методов криптографии, резервированию и защите от вирусов. Документы по ИБ содержать правила и рекомендации по подсоединению мобильных средств к сетям, а также руководства по использованию этих средств.

Сотрудники проекта несут полную материальную ответственность за вверенные им средства вычислительной техники и несут ответственность в соответствии с требованиями законодательства РК за используемую ими информацию.

Для защиты от неавторизованного доступа или раскрытия информации, хранимой и обрабатываемой средствами вычислительной техники, необходимо использование средств и методов криптографии. Вся конфиденциальная информация электронном виде должна шифроваться персональным ключом получателя. Конфиденциальная информация на бумажном носителе должна транспортироваться в непрозрачном конверте средствами специализированной почты, несущей ответственность за конфиденциальность и сохранность отправлений в соответствии с требованиями законодательства РК.

Использование средств вычислительной техники для обработки служебной информации в общедоступных местах запрещено.

Средства и способы защиты от вредоносного программного обеспечения отражены в Правилах организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты .

Процесс, методы резервирования и защиты резервных копий отражены в Регламенте резервного копирования и восстановления информации.

Вычислительная сеть ИС и сотрудников проекта защищена межсетевым экраном. Удаленный доступ к серверам ИС осуществляется по зашифрованному каналу только после аутентификации пользователя.

На переносных устройствах запрещается хранить информацию с классом доступа выше открытой информации в незашифрованном виде.

Ответственный за обеспечение ИБ обязан информировать сотрудников проекта (в рамках инструктажа), использующих переносные устройства, о дополнительных рисках и необходимых мероприятиях обеспечения информационной безопасности, связанных с этим способом работы.

Сотрудникам проекта запрещено использовать беспроводные сети передачи данных и мобильные устройства для подключения к сети Интернет или другим сетям.

11.7.2. Работа в дистанционном режиме

Сотрудникам проекта разрешено работать только в защищаемых помещениях проекта:

a) в здании Организации;

b) в серверных помещениях проекта.

В качестве переносных устройств, для работы в защищаемых помещениях, разрешено использование только служебных средств обработки и хранения информации.

Защищаемые помещения должны отвечать установленным требованиям ИБ в соответствии с их назначением. Способы подключения и защиты передаваемой информации регламентируются НТД по ИБ.

Требования к обеспечению необходимого уровня информационной безопасности охватывают:

a) существующую физическую безопасность места работы в дистанционном режиме, с точки зрения безопасности здания и окружающей среды;

b) предлагаемое оборудование мест дистанционной работы;

c) требования к безопасности коммуникаций, исходя из потребности в удаленном доступе к внутренним системам, организации, важности информации, к которой будет осуществляться доступ, и которая будет передаваться по каналам связи, а также важность самих внутренних систем организации;

d) угрозу неавторизованного доступа к информации или ресурсам со стороны других лиц, имеющих доступ к месту дистанционной работы;

e) использование в домашних сетях требований или ограничений на конфигурацию беспроводных сетевых сервисов;

f) политику и процедуры для предотвращения споров о правах на интеллектуальную собственность разработанных на частное имущество;

g) доступ к частному оборудованию (для проверки безопасности компьютера или во время исследования), которые могут быть предотвращены законным путем;

h) лицензионные соглашения программного обеспечения, которые позволят организации стать ответственными за лицензирование программного обеспечения клиента на автоматизированных рабочих местах, принадлежавших конфиденциально сотрудникам, подрядчикам или пользователям сторонних организаций;

i) антивирусную защиту и систему сетевой защиты.

Мероприятия по обеспечению информационной безопасности в этих условиях включают:

a) обеспечение подходящим оборудованием и мебелью места дистанционной работы там, где использование оборудования, находящегося в частной собственности без контроля организации, не разрешается;

b) определение видов разрешенной работы, времени работы, классификацию, которая может храниться, а также определение внутренних

систем и услуг, доступ к которым авторизован лицу, работающему в дистанционном режиме;

c) обеспечение подходящим телекоммуникационным оборудованием, в том числе средствами обеспечения безопасности удаленного доступа;

d) физическую безопасность;

e) правила и руководства в отношении доступа третьих лиц;

f) обеспечение поддержки и обслуживания оборудования и программного обеспечения;

g) обеспечение защиты съемных носителей;

h) процедуры в отношении резервирования и непрерывности деятельности;

i) аудит и мониторинг безопасности;

j) аннулирование полномочий, отмену прав доступа и возвращение оборудования в случае прекращения работы в дистанционном режиме.

12 Разработка, внедрение и обслуживание информационных систем

12.1. Требования к безопасности информационных систем

12.1.1. Анализ и детализация требований безопасности

В настоящем документе, и в программных документах ИС произведен Анализ и детализация требований безопасности.

12.2. Правильная обработка данных в приложениях

12.2.1. Подтверждение корректности ввода данных

При вводе данных в формы ИС проводится проверка корректности ввода. Для этого применяются следующие мероприятия по обеспечению информационной безопасности:

a) проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;
2) недопустимых символов в полях данных;
3) отсутствующие или неполные данные;
4) превышение верхних и нижних пределов объема данных;
5) неавторизованные или противоречивые контрольные данные;

d) процедуры реагирования на ошибки, связанные с подтверждением данных;

e) процедуры проверки правдоподобия вводимых данных;

f) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;

g) создание журнала для регистрации действий, вовлеченных в процесс ввода данных (10.10.1).

12.2.2. Контроль обработки данных в системе

В силу специфики функциональных возможностей используемой в ИС СУБД, целостность введенных и хранимых данных в ИС проверяется встроенными механизмами контроля.

12.2.3. Целостность сообщений

В процессе обмена данными между пользователями, информация подписывается ответственными пользователями ЭЦП для обеспечения целостности информации в ИС.

12.2.4. Подтверждение достоверности выходных данных

Перед выводом данных ответственные сотрудники заказчика проводят согласование документов. Согласуемые документы подписываются ответственными пользователями ЭЦП для обеспечения целостности информации в ИС.

12.3. Криптографические средства защиты

Использование криптографических средств защиты описано в Правилах использования средств криптографической защиты информации.

12.3.1. Политика использования криптографических средств защиты

Требования к безопасности при использовании криптографических средств защиты изложены в Правилах использования средств криптографической защиты информации.

12.3.2. Управление ключами

Требования к процедурам управления ключами изложены в Правилах использования средств криптографической защиты информации.

12.4. Безопасность системных файлов

Доступ к системным файлам и исходным кодам программ контролируются, а мероприятия по поддержке проектов информационных технологий проводиться в соответствии с требованиями настоящих документов.

12.4.1. Контроль программного обеспечения, находящегося в промышленной эксплуатации

Для осуществления контроля программного обеспечения, находящегося в промышленной эксплуатации, используются внутренние средства операционной системы. Любые обновления ИС производятся системным администратором под контролем ответственного за обеспечение ИБ.

12.4.2. Защита данных тестирования системы

В случае выполнения работ по тестированию ИС, разворачиваются отдельные серверы. Для недопущения утечки информации на тестовых серверах используются фиктивные данные и ненастоящие учетные данные и пароли.

12.4.3. Контроль доступа к исходным кодам

Доступ к исходным кодам строго контролируется ответственным сотрудником за обеспечение ИБ. Изменение исходного кода ИС строго запрещено. Доработка ИС производится в соответствии с приказом руководителя организации.

12.5. Безопасность в процессах разработки и поддержки

12.5.1. Процедуры контроля изменений

Порядок управления изменениями в процессе разработки, доработки и развития ИС описана в Политике безопасной разработки, доработки и развития.

12.5.2. Технический анализ прикладных систем после внесения изменений в операционные системы

ИС находится на стадии эксплуатации. Внесение изменений в программный код модулей ИБ запрещен. Доработка ИС производится в соответствии с приказом руководителя организации.

12.5.3. Ограничения на внесение изменений в пакеты программ

ИС находится на стадии эксплуатации. Внесение изменений в программный код модулей ИБ запрещен. Доработка ИС производится в соответствии с приказом руководителя организации.

12.5.4. Утечка информации

Для предотвращения утечки информации выполняются следующие мероприятия:

a) ограничение доступа сотрудников проекта к ИС;
b) эксплуатация средств защиты сети;
c) надежное хранение резервных копий;
d) регулярный контроль персонала;
e) мониторинг использования ресурсов ИС.

12.5.5. Разработка программного обеспечения с привлечением сторонних организаций

В рамках проекта категорически запрещается привлекать сторонних разработчиков.

12.6. Управление техническими уязвимостями

Управление технической уязвимостью реализовано в эффективном, систематическом и повторяемом режиме с результатом измерений, принятых для подтверждения ее эффективности.

Целью процедур управления техническими уязвимостями является предотвращение эксплуатации ошибок программного кода, ошибок конфигурации программных и технических средств, и ошибок конфигурации средств защиты ИС.

12.6.1. Контроль технической уязвимости

Для качественного управления техническими уязвимостями необходимо выполнить инвентаризацию и классификацию активов ИС. Перечень активов должен содержать:

1) поставщика программного обеспечения;
2) номера версий;
3) установленное программное обеспечение;
4) место расположения;
5) ответственный сотрудник.

Мониторинг на наличие технических уязвимостей должен проводиться не одного раза в квартал (согласно Графику аудита информационной

безопасности) либо при подозрении на уязвимость. Ответственность за выполнение мониторинга и устранение технических уязвимостей возлагается на ответственного администратора.

Классификация уязвимостей по степени риска:

1) уязвимость низкого уровня – использование злоумышленником такой уязвимости не повлечет нарушение целостности, доступности и конфиденциальности информации ИС и не угрожает непрерывной работе ИС;

2) уязвимость среднего уровня – использование злоумышленником такой уязвимости не повлечет нарушение целостности, доступности и конфиденциальности информации ИС и однако угрожает непрерывной работе ИС;

3) уязвимость высокого уровня – использование злоумышленником такой уязвимости повлечет нарушение целостности, доступности и конфиденциальности информации ИС и угрожает непрерывной работе ИС;

Классификация уязвимостей по возможности устранения:

1) уязвимость, для устранения которой необходимо инициировать изменение исходного кода ИС или ее части;

2) уязвимость, для устранения которой необходим патч с обновлением с обновлениями от официального производителя/разработчика, но производитель/разработчик такой патч не выпустил;

3) уязвимость с имеющимся патчем от официального производителя/разработчика, внедрение которого не требует дополнительных обновлений компонентов ИС;

4) уязвимость с имеющимся патчем от официального производителя/разработчика, внедрение которого требует дополнительных обновлений компонентов ИС.

Неконтролируемая установка программного обеспечения на вычислительные устройства может привести к введению уязвимостей, а затем к утечке информации, потере целостности или другим инцидентам, связанным с информационной безопасностью, или к нарушению прав интеллектуальной собственности.

Для осуществления контроля появления новых уязвимостей в Организации утвержден перечень разрешенного к установке программного обеспечения. Сотрудники организации должны быть лишены привилегий самостоятельной установки нового программного обеспечения.

Процесс управления техническими уязвимостями должен регулярно контролироваться и оцениваться СОИБ в целях обеспечения его эффективности и действенности в рамках выполнения внутреннего аудита.

Ответственность за контроль проведения мониторинга и устранение технических уязвимостей, проведение анализа выявленных уязвимостей, определение причин и обстоятельств их появления, а также создание организационных условий для быстрого и эффективного их устранения возлагается на СОИБ.

Требования к процессу выявления технических уязвимостей

В целях качественного выявления и контроля уязвимостей используются специализированные сканеры, а также штатные средства операционной системы.

Для оперативного реагирования на обнаруженные уязвимости должны использоваться официальные источники информации от производителей оборудования и разработчиков используемых программных компонентов ИС.

СОИБ должен провести анализ выявленных и опубликованных уязвимостей с учетом

1) классификации по степени риска;
2) классификации возможности ее устранения;
3) приоритезации в процессе устранения;
4) сокращении сроков устранения уязвимостей;
5) влияния внедряемых изменений на разработку ИС;
6) влияния внедряемых изменений на параллельно внедряемые изменения исходного кода;
7) рисков внедрения патчей от официальных производителей;
8) влияние внедряемых изменений на среду эксплуатации;
9) разработки решений для минимизации рисков использования уязвимостей, которые невозможно устранить в кротчайшие сроки;
10) разработки/применения инструкций действия во внештатной ситуации и/или процедур обеспечения непрерывной работы ИС на случай использования не устранённой уязвимости;
11) порядка внедрения изменений.

Для уязвимостей без устранения, которых невозможно в кротчайшие сроки необходимо разработать методы минимизации рисков от их использования.

В случае появлении в официальных источниках информации о выявлении уязвимости, СОИБ должен оценить риск реализации угрозы при помощи новой уязвимости. Некоторый риск от уязвимости может быть компенсирован использованием иных средств обеспечения информационной безопасности.

По результатам анализа администратор ИС должен составить план устранения уязвимостей с четом:

1) сокращения сроков устранения уязвимостей;
2) подбора решения для устранения уязвимости;
3) разработки программы-методики испытаний выбранных решений;
4) порядка внедрения изменений;
5) влияния порядка внедрения одних изменений на порядок внедрения других;
6) влияние внедренных изменений на процесс внедрения изменений исходного кода;

7) тестирования выбранных решений и возможных дополнительных действий для из применения:

a). отключение служб или возможностей, связанных с уязвимостью;

b). адаптация или добавление элементов управления доступом, например брандмауэров, на сетевых границах;

c). усиление мониторинга для обнаружения фактических атак;

d). повышение осведомленности об уязвимости;

8) обязательств по обеспечению непрерывности работы ИС и/или минимизации времени простоя;

9) привлечения сторонних специалистов и/или подрядных организаций;

10) оповещения пользователей и других заинтересованных сторон;

11) подготовительных мероприятий к процессу тестирования и внедрения изменений.

План устранения изменений должен быть согласован с СОИБ, со всеми сторонами участвующими в эксплуатации сервисов ИС и утвержден руководством Организации, пользователи ИС должны быть уведомлены о (возможных) перебоях в работе сервисов ИС.

План устранения изменений может быть частью плана внедрения изменений рамках исполнения требований Политики безопасной разработки, доработки и развития.

Действия для устранения,
выявленных технических уязвимостей

Любые действия направленные на устранение выявленных технических уязвимостей должны быть запланированы, согласованы с СОИБ и руководством Организации, пользователи ИС должны быть уведомлены о (возможных) перебоях в работе сервисов, предоставляемых ИС.

Внедрение изменений направленных на устранение выявленных технических уязвимостей, повлекшие за собой изменение исходного кода, должны осуществляться в порядке, установленном Политикой безопасной разработки, доработки и развития ИС.

Внедрение изменений, направленных на устранение выявленных технических уязвимостей, в программных и/или технических средствах сторонних производителях/разработчиков должны проводиться строго в соответствии с рекомендациями производителя/разработчика в порядке, установленном Политикой безопасной разработки, доработки и развития ИС.

Все действия администраторов и СОИБ, направленные на устранение уязвимостей, должны фиксироваться в Журнале регистрации действий администратора и Журнале контроля, мониторинга обеспечения информационной безопасности (а также в Журнал системно-технического обслуживания если такое необходимо) и проведения работ по обеспечению информационной безопасности соответственно.

План внедрения изменений, направленных н устранение уязвимостей, должен учитывать результаты анализа и классификации уязвимостей.

Все изменения, направленные на устранение выявленных технических уязвимостей, должны быть протестированы в тестовой среде.

13 Управление инцидентами информационной безопасности

13.1. Оповещения о нарушениях и недостатках информационной безопасности

В Организации утверждена Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, служащая обеспечить оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность применения корректирующих действий.

На ответственного за обеспечение ИБ возлагается обязанность информировать, консультировать и вести разъяснительные работы с сотрудниками Организации, сотрудниками поставщиков товаров и услуг и сотрудниками партнеров о порядке действий в случае инцидентов по ИБ и во внештатных ситуациях.

Сотрудники Организации, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации должны немедленно сообщать о любых наблюдаемых или предполагаемых инцидентах ответственному за обеспечение ИБ.

13.1.1. Оповещение о случаях нарушения информационной безопасности

В Организации утверждена Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях, устанавливающая порядок информирования об инцидентах ИБ, а также порядок реагирования на инциденты, устанавливающая действия, которые должны быть предприняты после получения сообщения об инциденте ИБ.

Об инцидентах нарушения информационной безопасности необходимо информировать ответственного за обеспечение ИБ, менеджера проекта и руководство Организации.

13.1.2. Оповещение о недостатках безопасности

Сотрудники Организации, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в ИС или услугах в порядке, установленном в Инструкции о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

Для предотвращения нарушений информационной безопасности, сотрудники Организации, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации, должны сообщать незамедлительно о возможных причинах и недостатках ИБ для принятия решений.

13.2. Управление инцидентами информационной безопасности и его усовершенствование

Обязанность за управление инцидентами информационной безопасности и за усовершенствование этого процесса возлагается на ответственного за обеспечение ИБ.

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях определяет обязанности и порядок управления инцидентами ИБ для обеспечения быстрой и организованной реакции на нарушения информационной безопасности, а также описывает процесс непрерывного усовершенствования мониторинга, оценки, общего управления инцидентами информационной безопасности, и сбор доказательств.

13.2.1. Ответственность и процедуры

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях устанавливает ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности.

13.2.2. Извлечение уроков из инцидентов информационной безопасности

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях определяет механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности.

13.2.3. Сбор доказательств

В случае необходимости должен проводиться сбор доказательств инцидент информационной безопасности, который может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, а материалы представляться в соответствии с требованиями действующего законодательства РК, представителями компетентных органов.

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях описывает процедуру сбора доказательств.

13.2.3.1. Процедура сбора доказательств внутри организации

В случае необходимости представления и сбора доказательств в целях применения дисциплинарных мер, внутри организации ответственный за обеспечение ИБ инициирует процесс создания рабочей группы, разрабатывает и утверждает план работы группы.

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях описывает процедуру внутри организации.

14 Управление непрерывностью бизнеса

14.1. Вопросы информационной безопасности управления непрерывностью бизнеса

В рамках работ по обеспечению ИБ проводятся мероприятия управление непрерывностью бизнеса с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования предупреждающих и восстановительных мероприятий по управлению информационной безопасностью.

Необходимо, чтобы управление непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, ограничения последствий разрушительных инцидентов и обеспечения своевременного возобновления работы ИС.

Последствия от бедствий, нарушений безопасности и отказов в обслуживании анализируются. Разработаны и внедрены Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

Для оперативного реагирования и организации работ по недопущению перерывов в работе ИС разработан и утвержден План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации.

14.1.1. Включение информационной безопасности в процесс управления непрерывностью бизнеса

Для регламентирования порядка обеспечения непрерывной работы активов ИС разработаны и внедрены Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

14.1.2. Непрерывность бизнеса и оценка риска

Для регламентирования порядка обеспечения непрерывности бизнеса и оценки риска ИС разработаны и внедрены Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

14.1.3. Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность

Для оперативного реагирования и организации работ по недопущению перерывов в работе ИС разработан и утвержден План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации.

14.1.4. Структура планов обеспечения непрерывности бизнеса

План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации, определяет подход к непрерывности, подход к обеспечению информации и доступности информационной системы и ее безопасности. План непрерывности четко определять условия его реализации, а также должностных лиц, ответственных за выполнение каждого его пункта.

Требования к форме плана обеспечения непрерывной работы активов ИС отражены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

14.1.5. Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса

Требования к тестированию, поддержке и пересмотру планов по обеспечению непрерывности бизнеса отражены в Правилах организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

15 Соответствие требованиям

15.1. Соответствие правовым требованиям

Предотвращение любых нарушений норм уголовного и гражданского права, обязательных предписаний и регулирующих требований или договорных обязательств, а также требований безопасности является обязательным условием работы всех сотрудников и Организации в целом.

Проектирование, разработка, развитие, сопровождение, поддержка, эксплуатация, надлежащая работа ИС и/или ЭИР являются основными предметами обязательств Организации и регулируются нормативно-правовыми документами законодательства РК, договорами и лицензионными соглашениями, а также утвержденными требованиями безопасности.

15.1.1. Определение применимого законодательства

В ответственность менеджера проекта входит контролировать соблюдение юридических требований в отношении приобретаемых услуг и поставляемых услуг в рамках проекта.

Перечень юридических требований должен охватывать следующие нормативно-правовые акты законодательства РК и технические документы, действующие в РК:

a) в области авторского права;
b) в области лицензирования (продукции и/или деятельности);
c) в области информационной безопасности;
d) в области безопасности жизнедеятельности;
e) в области технического регулирования;
f) в области сертификации и подтверждения соответствия;
g) в области криптографической защиты;
h) в области использования ЭЦП;
i) соблюдение требований регламентов или нормативно-правовых документов уполномоченных государственных органов;
j) соблюдение требований стандартов по ИБ;
k) соблюдение требований стандартов разработки;
l) соблюдение требований стандартов сопровождения;
m) соблюдение требований стандартов эксплуатации;
n) соблюдение требований стандартов поддержки;
o) соблюдение требований стандартов оценки качества.

В виду ограниченной компетенции менеджера проекта руководство Организации поддерживает инициативу привлечение сторонних юридических консультантов, имеющих соответствующую квалификацию, в отношении конкретных юридических вопросов.

Требования в области обеспечения ИБ должны быть согласованы с ответственным за обеспечение ИБ.

Так же следует иметь в виду, что законодательные требования в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый за границу

государства), различаются в разных странах, что должно учитываться и контролироваться при согласовании соответствующих договоренностей

В соответствии с требованиями ЕТ мероприятия по контролю правомерности использования ПО проводятся не реже одного раза в год в рамках внутреннего аудита и включают в себя:

a) определение фактически используемого ПО;
b) определение прав на использование ПО;
c) сравнение фактически используемого ПО и имеющихся лицензий.

Все применяемые нормы законодательства, обязательные предписания, регулирующие требования и договорные обязательства, должны быть четко определены и документированы в пояснительной записке к проекту до подписания каких-либо обязательств. Пояснительная записка должна быть составлена менеджером проекта и доведена до сведений руководства Организации, всех причастных сторон и партнеров.

15.1.2. Права на интеллектуальную собственность (IPR)

Права интеллектуальной собственности распространяются на программное обеспечение, документы, проект, торговые марки, патенты, и лицензии исходного текста.

Программные продукты, являющиеся предметом собственности, поставляются в рамках лицензионного (или договора приобретения) соглашения, которое ограничивает использование определенными условиями, а также могут ограничивать копирование их с целью создания резервных копий. Ситуация с правом на интеллектуальную собственность (IPR) программного обеспечения, разработанного организацией, требует разъяснения персоналу.

Законодательные, регулирующие и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, эти ограничения могут содержать требования к использованию только тех материалов, которые или разработаны Организацией, или лицензированы, или предоставляются разработчиком для Организации.

Ответственный сотрудник за обеспечение ИБ обязан проконтролировать процесс осведомленности сотрудников Организации, о соблюдении авторских прав распространяемые на активы, а также включение требований о соблюдении прав на интеллектуальную собственность в договорные отношения с сотрудниками Организации.

Ответственный сотрудник за обеспечение ИБ должен составить, согласовать с заинтересованными сторонами и утвердить руководством Организации перечень программных активов ИС.

Сотрудники Организации, сотрудники поставщиков товаров и услуг и сотрудники партнеров должны быть уведомлены о запрете установки ПО не из перечня перечень разрешенного к установке и соответствующих мерах дисциплинарного взыскания в случае его нарушения.

Менеджер проекта отвечает за контроль соблюдения прав на интеллектуальную собственность в границах своего проекта. В частности, менеджер проекта должен выполнять следующие мероприятия для защиты любых материалов, являющихся интеллектуальной собственностью:

a) контроль строгого соблюдения требований авторского права сотрудниками Организации и подрядных организаций при использовании активов;

b) контроль отражения требований соблюдения авторского права в договорных отношениях, включая отношения с заказчиками, субподрядчиками, партнерами, поставщиками услуг;

c) обеспечение осведомленности сотрудников по вопросам авторского права на программное обеспечение принятых правил в отношении закупок, а также уведомление о применении дисциплинарных санкций к нарушителям;

d) ведение соответствующих регистров активов с требованиями защиты прав интеллектуальной собственности;

e) ведение подтверждений и доказательств собственности на лицензии, дистрибутивные диски, руководства и т.д.;

f) контроль над соблюдением ограничений максимального числа разрешенных пользователей программными продуктами;

g) регулярные проверки применения только авторизованного программного обеспечения и лицензированных продуктов;

h) реализация политики по обеспечению выполнения условий соответствующих лицензионных соглашений;

i) организация регулярного аудита.

Все сотрудники Организации обязаны исполнять следующие мероприятия для соблюдения прав на интеллектуальную собственность при выполнении своей деятельности:

a) строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов;

b) выполнение требований к утилизации или передачи программного обеспечения в другие организации в соответствии с действующим ЗРК и лицензионными соглашениями;

c) соблюдение ограничений получения из общедоступных сетей программного обеспечения и информации;

d) не дублирование, преобразовывая в другой формат; извлечение из коммерческих записей (пленка, аудио), кроме определенного разрешения в соответствии с законом об авторском праве;

e) не копирование полностью или частично книги, статьи, отчеты или другие документы, кроме разрешенного в соответствии с законом об авторском праве.

На СОИБ возлагается ответственность за контроль соблюдения сотрудниками настоящих требований.

15.1.3. Защита записей организации[5]

Требования настоящего документа распространяются только на записи, сделанные в рамках работ по проектированию, разработке, развитию, сопровождению, поддержки, эксплуатации, надлежащей работе ИС не распространяются на бухгалтерские записи, записи кадровой финансовой или других служб Организации.

Однако ответственный сотрудник за обеспечение ИБ должен принять во внимание необходимость учета записей физического доступа в помещения проекта, обеспечивающие функционирование ИС.

Важные записи организации необходимо защищать от утраты, разрушения и фальсификации. В отношении некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки бизнес-приложений.

В Организации действует следующая схема классификации записей:

Классификация по типу носителя:

a) на бумажном носителе;
b) на цифровом носителе.

Классификация по назначению:

a) рабочие данные;
b) операционные записи;
c) служебные записи.

Любые криптографические ключи, связанные с зашифрованными архивами или цифровыми подписями (12.3), хранятся безопасным способом и с доступом только авторизованным лицам.

Контроль за соблюдение настоящих требований возлагается на ответственного за обеспечение ИБ сотрудника Организации, ответственность за соблюдение настоящих требований возлагается на менеджера проекта.

Для некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки важных бизнес-приложений. Такие записи могут потребоваться как доказательства того, что Организация работает в рамках установленных законом норм или регулирующих требований, или с целью адекватной защиты от гражданского или уголовного преследования.

Выявление таки подшивок записей, их особая отметка, определение периода времени хранения и определение содержания данных должны быть установлены в соответствии с государственными законами, регулирующими требованиями или договорными отношениями Организации и возлагается на ответственного сотрудника за обеспечение ИБ.

---

[5]К записям могут относиться как сделанные на цифровом устройстве, так и сделанные вручную. В контексте настоящего подпункта слова «журнал», «подшивка» могут использоваться как синонимы. Например, «Журнал доступа в серверные помещения» это подшивка страниц с записями отметок входа и выхода в серверное помещение.

15.1.3.1. Работа с записями на бумажном носителе

Записи на бумажном носителе, должны подшиваться и заверяться подписью ответственного лица, ответственного за обеспечение ИБ сотрудника. В подшивке записи и страницы должны быть пронумерованы, а сами подшивки промаркированы. В подшивках записей не допускаются вставки пустых строк или страниц до последней по времени записи. В случае обнаружения пустых строк или страниц они должны быть перечеркнуты для недопущения фальсификации записей.

Передача подшивки записей в архив, утилизация производится по приказу руководства Организации и фиксируется актом при участии ответственного за подшивку, ответственного за обеспечение ИБ, ответственного архивариуса.

Сохранность записей на бумажном носителе должна осуществляться с учетом возможность снижения качества носителя, используемых для хранения данных. Среда хранения должна быть нормализирована для обеспечения сохранности сведений на бумажном носителе.

15.1.3.2. Работа с записями на цифровом носителе

В Организации допускается ведение электронных ручных записей там, где это упрощает рабочий процесс, но не в ущерб их безопасности, надежности, целостности, доступности, фиксированию и хранению.

Ведение электронных ручных записей допускается только с использованием специализированных программных средств, обладающих следующими возможностями:

a) поддержка принятой в Организации маркировки;
b) авторизацию пользователей;
c) параллельный доступ нескольких пользователей;
d) защиту от изменений;
e) шифрование записей;
f) защита канала передачи записей;
g) резервное копирование и восстановление;
h) архивирование;
i) электронно-цифровую подпись.

Записи, производимые компонентами ИС и/или ЭИР, должны храниться в соответствии с рекомендациями разработчиков этих продуктов, классифицироваться, архивироваться и утилизироваться в соответствии с требованиями настоящего документа, обеспечиваться защитой средствами среды компонентов ИС и/или ЭИР.

Архивирование электронных записей на цифровые носители относится к процессу резервного копирования информации, и должно выполняться в соответствии с требованиями Регламента резервного копирования и восстановления информации.

Маркировка архивированных записей должна удовлетворять требованиям настоящего документа. Каждый архив должен снабжаться текстовым документом с указанием:

a) источника записей и его кода;
b) название подшивки;
c) код подшивки (для маркировки записей);
d) ответственного лица за контроль ведения записей;
e) места хранения до архивации;
f) особая отметка;
g) класса хранимой информации;
h) лиц (или должностей Организации) имеющих доступ к подшивке;
i) ответственного за хранение;
j) период архивации;
k) место архивирования;
l) срока хранения в архиве;
m) способ утилизации.

Регламент резервного копирования и восстановления информации учитывает возможность снижения качества носителя, используемых для хранения данных, описывает процедуры по хранению и уходу за носителями данных в соответствии с рекомендациями изготовителя.

При использовании цифровых носителей данных Регламент резервного копирования и восстановления информации описывает процедуры проверки возможности доступа к данным (например, читаемость, как самих носителей, так и формата данных) в течение всего периода их хранения с целью защиты от потери вследствие будущих изменений в информационных технологиях.

Регламента резервного копирования и восстановления информации учитывает необходимость вывода всех требуемых записей в приемлемый период времени и в приемлемом формате, в зависимости от выполняемых требований.

Сохранность записей на цифровом носителе должна осуществляться с учетом возможности снижения качества носителей, используемых для хранения данных. Среда хранения должна быть нормализирована для обеспечения сохранности сведений на цифровом носителе в соответствии с требованиями производителя.

15.1.4. Защита данных и конфиденциальность персональной информации

Настоящий документ и все компоненты СМИБ Организации, направлены для обеспечения информационной безопасности Организации включая персональные данные. В процессе сбора, обработки, передачи, хранения персональной информации должны осуществляться требуемые технические и организационные меры для ее защиты:

a) шифрование;
b) защищенные каналы связи;
c) защищенные физические среды;
d) разграниченный авторизованный доступ;
e) защищенные среды функционирования;

f) прослеживаемая деятельность и персональная ответственность сотрудников Организации.

Ответственность за контроль исполнения требований по защите данных и конфиденциальность персональной информации возлагается на ответственного за обеспечение ИБ.

Защита данных и конфиденциальность персональной информации обеспечиваются в соответствии с требованиями:

a) нормативно-правовых актов РК;
b) договорных отношений;
c) оферт.

Ответственный за обеспечение ИБ должен следить за изменениями этих документов, доводить до сведений ответственных лиц о необходимости исполнять требования по ИБ и контролировать их исполнение.

Ответственный за обеспечение ИБ должен контролировать соблюдение законодательства в области ЭЦП и защиты персональных данных.

Ответственный за обеспечение ИБ должен проводить работы по соответствующему разъяснению менеджерам, пользователям и поставщикам услуг об их индивидуальной ответственности за обработку персональной информации, а также обязательности выполнения соответствующих мероприятий по обеспечению информационной безопасности.

Ответственный за обеспечение ИБ должен понимать принципы защиты данных, а также знать применяемые нормы законодательства в отношении защиты личных данных.

Средства обработки информации должны гарантировать разграничение доступа пользователей и администраторов к информации, а также требуемый уровень обеспечения ИБ.

15.1.5. Предотвращение нецелевого использования средств обработки информации

Для предотвращения нецелевого использования средств обработки информации проводится внутренний аудит (6.1.9) информационной безопасности Организации.

Контроль нецелевого использования средств обработки информации осуществляется ответственным за обеспечение ИБ в рамках внутреннего аудита, но не реже четырех раз в год. Установленная периодичность контроля должна быть отражена в График аудита информационной безопасности.

При обнаружении нецелевого использования средств обработки информации проводится внеплановая проверка использования средств обработки информации, о результатах которой докладывается Руководству организации для принятия соответствующих мер дисциплинарного воздействия, предусмотренных внутренними документами Организации и законодательством РК

Средства обработки информации Организации предназначены строго для достижения целей бизнеса, любое их использование не по назначению

влечет за собой наказания, предусмотренные внутренними документами Организации и законодательством РК.

Любое использование средств обработки информации для непроизводственных или неавторизованных целей, без одобрения руководства (6.1.4), расценивается как нецелевое.

Пользователи должны быть уведомлены о предстоящей процедуре аудита и о том, какие процедуры он включает.

При получении средств обработки информации сотрудник Организации должен быть ознакомлен под роспись с Инструкций пользователя по эксплуатации средств обработки информации и программного обеспечения.

При регистрации доступа к сети Организации или ИС на экране компьютера должно отражаться предупреждающее сообщение, указывающее, что пользователь запрашивает доступ в защищаемую среду, что неавторизованный доступ к ней запрещен, и он обязан соблюдать требования утвержденных документов по ИБ. Пользователь должен подтвердить это прочтение и реагировать соответствующим образом на него, чтобы продолжить процесс регистрации (11.5.1).

Сотрудники организации, подрядчики и пользователи сторонних организаций должны быть осведомлены о том, что во всех случаях они имеют право доступа только к тем данным, использование которых им разрешено.

Для автоматизации процесса аудит средств обработки информации, мониторинга их использования могут использоваться программные или аппаратные инструменты, если это будет обосновано и одобрено руководством Организации.

15.1.6. Регулирование использования средств криптографической защиты

Организация не занимается разработкой или реализацией средств криптографической защиты информации, являющиеся лицензируемыми видами деятельности.

Использование в организации электронно-цифровой подписи регулируется Законом Об электронном документе и электронной цифровой подписи.

Для защиты информации в процессе передачи данных используется стандартные протоколы с применением методов шифрования (https, sftp, ssh, RDP и др.).

15.2. Пересмотр политики безопасности и техническое соответствие требованиям безопасности

Безопасность информационных систем, необходимо регулярно анализировать и оценивать, с целью обеспечить соответствие систем, организационным политикам и стандартам безопасности.

Такой анализ (пересмотр) необходимо осуществлять в отношении соответствующих политик безопасности, а программные средства и информационные системы должны подвергаться аудиту на предмет соответствия этим политикам.

15.2.1. Соответствие политикам и стандартам безопасности

Процесс проверки соответствия политикам и стандартам безопасности входит в аудит ИБ (6.1.8).

Ответственный за обеспечение ИБ должен вести и поддерживать в актуальном состоянии Перечень законодательной и нормативной базы и утвержденных документов в области информационной безопасности с указанием бизнес процессов, которые должны соответствовать требованиям документов. Сами документы из перечня должны быть доступны и доведены до сотрудников Организации.

В процессе регулярных аудитов и оперативной деятельности ответственный за обеспечение ИБ должен дополнять перечень и уточнять в плоть до пунктов с требованиями к определенным бизнес-процессам Организации.

Руководители структурных подразделений и другие ответственные сотрудники Организации должны обеспечивать правильное выполнение всех процедур безопасности в пределах их зоны ответственности, на соответствие принятым политикам безопасности, стандартам безопасности и другим документам из перечня.

Если какое-либо несоответствие найдено в результате пересмотра СМИБ или в процессе работы, то руководители должны:

a) определить причины этого несоответствия;

b) оценить потребность в действиях, для обеспечения того, чтобы несоответствие не повторилось;

c) определить и провести соответствующие корректирующие меры;

d) провести анализ предпринятых корректирующих действий.

Результаты пересмотра и корректирующих действий, выполненных руководителями, должны быть зарегистрированы и записаны. Менеджеры проектов должны представлять отчет о результатах лицам, проводящим аудит (6.1.8).

Вопросы мониторинга использования систем рассмотрены в Разделе 10.10.

15.2.2. Проверка технического соответствия требованиям безопасности

Процесс проверки технического соответствия требованиям безопасности входит в аудит ИБ (6.1.8).

Регулярность аудита определяется графиком проведения аудитов.

Проверка технического соответствия должна осуществляться вручную (при помощи соответствующих инструментальных и программных средств, при необходимости) опытным системным администратором в присутствии ответственного за обеспечение ИБ или с помощью автоматизированного

пакета программ, который генерирует технический отчет для последующего анализа.

Мероприятия, увеличивающие риск отказа в работе, непреднамеренной остановки или компрометации безопасности ИС и/или ЭИР должны быть запланированы, документированы, повторяться не реже одного раза в два года и выполняться в тестовой среде с фиктивными данными.

Перед проведением проверки технического соответствия требованиям безопасности ответственный за обеспечение ИБ должен составить, согласовать и утвердить сценарий действий для проверки каждого требования подлежащего проверки.

Любая проверка технического соответствия должна выполняться только компетентными, авторизованными лицами под их наблюдением.

Проверка соответствия также включает тестирование на наличие попыток несанкционированного доступа к системе (проникновение), которое может быть выполнено независимыми экспертами, специально приглашенными по контракту для этого. Данное тестирование может быть полезным для обнаружения уязвимостей в системе и для проверки эффективности мер безопасности при предотвращении неавторизованного доступа вследствие этих уязвимостей.

Проверка технического соответствия включает испытания сред функционирования ИС и/или ЭИР для обеспечения уверенности в том, что мероприятия по обеспечению информационной безопасности функционирования аппаратных и программных средств были внедрены правильно. Этот тип проверки соответствия требует технической помощи специалиста.

15.3. Вопросы аудита информационных систем

Все требования к процедурам, инструментам и участникам аудита ИС отражены в Правилах проведения внутреннего аудита информационной безопасности ИС.

15.3.1. Меры управления аудитом информационных систем

Меры управления аудитом ИС отражены в Правилах проведения внутреннего аудита ИБ.

15.3.2. Защита инструментальных средств аудита информационных систем

Требования к защите инструментальных средств аудита информационных систем изложены в Правилах проведения внутреннего аудита ИБ.

16 Ответственность

Руководство Организации

a) контроль исполнения требований настоящего документа,
b) поддержание процессов обеспечения информационной безопасности.

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа.
b) обеспечение информационной безопасности.

Сотрудники проекта ИС:

a) исполнение требований настоящего документа.

В случае если действиями или бездействием сотрудник организации и/или пользователь нарушил требования настоящего документа (ровно как всех документов регламентирующих обеспечение информационной безопасности), руководство Организации имеет право применять практики административного наказания (в соответствии с ЗРК) и/или обратиться в суд для вынесения справедливого наказания и/или взыскания ущерба, нанесенного таким образом.

Приложение 1

График пересмотра Политики информационной безопасности
Информационной системы «Электронная торговая система товарной биржи»
на 2024 гг.
ЭТСТБ.СМИБ.П.01-01.r01.21

№	Раздел Политики информационной безопасности	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	17
1.	1 Введение																									СОИБ
2.	2 Область действия																									СОИБ
3.	3 Нормативные ссылки																									СОИБ
4.	4 Применяемые термины и сокращения																									СОИБ

Приложение 2

Журнал ознакомления, выдачи и возврата документации
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-02.r01.21

№ п/п	Ф. И. О	Должность	Перечень документов	Ознакомление, выдача, возврат	Дата и время.	Подпись
1	2	3	4	5	6	7

Приложение 3

Перечень сотрудников проекта
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-03-01.r01.21

№ п/п	Ф. И. О	Должность
1	**2**	**3**
1		Администратор
2		Администратор
3		Ответственный за обеспечение ИБ
4		Менеджер проекта

Перечень допущенных сотрудников в серверные помещения проекта
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-03-02.r01.21

№ п/п	Ф. И. О	Должность	Адрес защищаемого помещения
1	**2**	**3**	**4**
1		Администратор	
2		Администратор	
3		Ответственный за обеспечение ИБ	

Перечень допущенных сотрудников в рабочие помещения проекта
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-03-03.r01.21

№ п/п	Ф. И. О	Должность	Адрес защищаемого помещения
1	**2**	**3**	**4**
1		Администратор	
2		Администратор	
3		Ответственный за обеспечение ИБ	

Приложение 4

График обучения и инструктажа сотрудников
на 2024 гг.
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-04.r01.21

№ п/п	Ф. И. О	Должность	Наименование курсов	Период обучения	Форма проведения
1	2	3	4	5	6
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Приложение 5

Журнал системно-технического обслуживания
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-05.r01.21

№ п/п	Дата, время	Ф.И.О. исполнителя	Серверное, сетевое оборудование/программное обеспечение	Основание проведения работ	Выполняемые действия	Подпись
1	2	3	4	5	6	7

Приложение 6

Журнал регистрации действий администратора
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-06.r01.21

№ п/п	Дата, время	Ф.И.О. исполнителя Подпись	Учетная запись	Серверное, сетевое оборудование/программное обеспечение	Выполняемые действия	Результат (успешное или неуспешное завершение операции)
1	2	3	4	5	6	7

Приложение 7

План мониторинга журналов
на 2024 гг.
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-07.r01.21

№ п/п	Название журнала	Ф. И. О. ответственного сотрудника за мониторинг журнала	Интервал мониторинга
1	2	3	4
1.	Журналы операционной системы ОС		
2.	Журналы СУБД		
3.	Журнал автоматической записи действии системных администраторов ИС		
4.	Журналы ИС		
5.	Журнал ознакомления, выдачи и возврата документации		
6.	Журнал системно-технического обслуживания		
7.	Журнал регистрации действий администратора		
8.	Журнал проведения обучения, инструктажа по информационной безопасности		
9.	Журнал учета кабельных соединений		
10.	Матрица доступа к активам		
11.	Журнал учета съемных носителей информации и мобильных устройств		
12.	Журнал выдачи/возврата носителей информации и мобильных устройств		
13.	Журнал резервного копирования, восстановления, тестирования резервных копий и тестирования средств резервирования		
14.	Журнал инцидентов ИБ и учета внештатных ситуаций		

Приложение 8

График круглосуточного мониторинга
на 2024 гг.
Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-08.r01.21

Ф. И. О	Сентябрь	Октябрь	Ноябрь	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		1,3,5,7														

Приложение 9

Журнал проведения обучения, инструктажа по информационной безопасности Информационной системы «Электронная торговая система товарной биржи» ЭТСТБ.СМИБ.П.01-09.r01.21

№ п/п	Ф. И. О. сотрудника	Должность	Дата проведения	Тема	Подпись сотрудника
1	2	3	4	5	6
1.					
2.					

Приложение 10

Журнал контроля, мониторинга обеспечения ИБ и проведения работ по информационной безопасности Информационной системы «Электронная торговая система товарной биржи»
ЭТСТБ.СМИБ.П.01-10.r01.21

№ п/п	Ф. И. О. СОИБ	Дата (период) проведения	Действия	Результат	Подпись
1	2	3	4	5	6
1.					
2.					

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п./пп. документа	Дата замены	Номера страниц/ (операция: удалена, изменена, новая)		Всего листов (страниц) в документе	Рассылка документа (подразделения, группы, роли, должности и т. п.)	Ф. И. О. ответственного за документ	Роспись