ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56045— 2021/ ISO/IEC TS 27008:2019

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Рекомендации по оценке мер обеспечения информационной безопасности

(ISO/IEC TS 27008:2019, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 421-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TS 27008:2019 «Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности» (ISO/IEC TS 27008:2019 «Information technology — Security techniques — Guidelines for the assessment of information security controls», IDT).

ISO/IEC TS 27008 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВЗАМЕН ГОСТ Р 56045—2014/ISO/IEC TR 27008:2011

6 Некоторые положения международного документа, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Настоящий стандарт поддерживает определенный в ИСО/МЭК 27001 и ИСО/МЭК 27005 процесс менеджмента рисков системы менеджмента информационной безопасности (СМИБ), а также меры обеспечения информационной безопасности (ИБ), включенные в ИСО/МЭК 27002[1)].

Меры обеспечения ИБ должны соответствовать своему назначению (быть обоснованными и обеспечивающими решения задачи снижения рисков ИБ), быть действенными (правильно определенными, разработанными, реализованными, используемыми, управляемыми и поддерживаемыми) и эффективными (приносить организации чистую прибыль). В настоящем стандарте разъясняется порядок оценки мер обеспечения ИБ организации с учетом вышеуказанных и прочих задач, чтобы либо подтвердить, что они действительно соответствуют целям, действенны и эффективны (обеспечивают уверенность), либо определить необходимость изменений (возможности улучшения). Конечная цель состоит в том, чтобы меры обеспечения ИБ в достаточной степени снижали информационные риски, которые организация считает неприемлемыми и неизбежными, с разумными экономическими затратами и в соответствии с требованиями бизнеса. Настоящий стандарт обеспечивает необходимую гибкость определения необходимых оценок с учетом коммерческих целей и задач, политик и требований организации, известных угроз и уязвимостей ИБ, рабочих условий, зависимости от информационных систем и платформ, а также степени рисков, приемлемых для организации.

За рекомендациями по аудиту элементов систем менеджмента следует обращаться к ИСО/МЭК 27007, а по оценке соответствия СМИБ требованиям для сертификации — к ИСО/МЭК 27006[2)].

---

1) Здесь и далее речь идет об ИСО/МЭК 27000:2018; ИСО/МЭК 27001:2013, ИСО/МЭК 27002:2013.

2) Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Рекомендации по оценке мер обеспечения информационной безопасности

Information technology. Security techniques. Guidelines for the assessment of information security controls

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт предоставляет рекомендации по оценке реализации и функционирования мер обеспечения ИБ, включая оценку технического соответствия мер обеспечения ИБ информационных систем, согласно установленным в организации стандартам по ИБ.

В настоящем стандарте предлагаются инструкции по анализу и оценке мер обеспечения ИБ, используемых в рамках системы менеджмента ИБ, описание которой приводится в ИСО/МЭК 27001.

Настоящий стандарт применим для организаций всех видов и любых размеров, включая акционерные общества открытого и закрытого типов, государственные учреждения и некоммерческие организации, проводящие оценки ИБ и технического соответствия.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему):

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по управлению информационной безопасностью на основе ИСО/МЭК 27002 для облачных сервисов)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000.

ИСО и МЭК ведут терминологические базы данных для использования в стандартах по следующим адресам:

- Платформа просмотра ISO Online: доступна по адресу https://www.iso.org/obp;
- IEC Electropedia: доступна по адресу http://www.electropedia.org/.

4 Структура стандарта

Настоящий стандарт содержит описание процесса оценки мер обеспечения ИБ, включая оценку технического соответствия.

Издание официальное

В разделе 5 представлена вводная информация.

В разделе 6 представлен общий обзор оценок мер обеспечения ИБ.

В разделе 7 представлены методы оценок мер обеспечения ИБ.

В разделе 8 описан процесс оценки мер обеспечения ИБ.

В приложении А содержатся сведения о сборе предварительной информации.

В приложении В приведено практическое руководство по оценке технического соответствия ИБ.

В приложении С содержатся рекомендации по технической оценке облачных услуг.

5 Предпосылки

Меры обеспечения ИБ организации являются основными инструментами контроля неприемлемых информационных рисков и их снижения до допустимого для организации уровня.

Часть мер обеспечения ИБ организации обычно осуществляется путем реализации технических мер контроля и управления ИБ.

Технические меры обеспечения ИБ могут быть определены, документально оформлены, реализованы и поддерживаться в соответствии со стандартами, относящимися к ИБ. С течением времени на эффективность мер обеспечения ИБ и в конечном счете на применение в организации стандартов ИБ могут оказывать негативное влияние как внутренние факторы, такие как корректировки информационных систем, конфигурации функций безопасности и изменения окружающей среды информационных систем, так и внешние факторы, такие как совершенствование компьютерных атак. Оценка технического соответствия включена в ИСО/МЭК 27002 в качестве одной из мер обеспечения ИБ и осуществляется вручную и/или специальным образом с помощью автоматизированных инструментальных средств. Оценка технического соответствия может осуществляться лицами, выполняющими роль, не задействованную в осуществлении меры обеспечения ИБ (например, владельцем системы или персоналом, отвечающим за конкретные меры обеспечения ИБ), или внутренними или внешними специалистами по обеспечению ИБ.

Результат оценки технического соответствия определяется фактическим уровнем технического соответствия реализации ИБ в организации требованиям стандартов. Результат либо обеспечивает уверенность в том, что состояние технических мер обеспечения ИБ соответствует стандартам ИБ, либо, в противном случае, служит основой для совершенствования. В начале оценки должна быть четко установлена последовательность отчетности по аудиту и обеспечена целостность процесса отчетности. Необходимо принять меры, чтобы обеспечить:

- соответствующую компетенцию тех, кто выполняет оценку с самого начала (см. 6.2);
- получение соответствующими ответственными сторонами копии отчета об оценке технического соответствия непосредственно от аудиторов ИБ;
- невозможность получения несоответствующими или неуполномоченными сторонами копии отчета об оценке технического соответствия от аудиторов ИБ;
- возможность беспрепятственного выполнения работы аудиторами, проводящими оценку мер обеспечения ИБ в соответствии с принципами разделения обязанностей.

Оценка мер обеспечения ИБ, в особенности оценка технического соответствия, могут помочь организации:

- установить и понять степень серьезности потенциальных проблем или недостатков реализации и достаточности мер обеспечения ИБ, стандартов ИБ и, следовательно, технических мер обеспечения ИБ организации;
- установить и понять потенциальное влияние на организацию воздействия недостаточно смягченных угроз и уязвимостей ИБ;
- установить приоритеты в действиях по снижению рисков ИБ;
- подтвердить, что ранее выявленные или возникающие уязвимости и угрозы ИБ были должным образом устранены;
- поддерживать бюджетные решения в рамках инвестиционного процесса, а также другие управленческие решения, связанные с совершенствованием менеджмента ИБ организации.

6 Общая информация об оценках мер обеспечения информационной безопасности

6.1 Процесс оценки

6.1.1 Общие положения

Для объективной оценки мер обеспечения безопасности ИБ назначенные аудиторы ИБ должны быть хорошо подготовлены как в области мер обеспечения ИБ, так и в области тестирования, например, эксплуатации применимых инструментальных средств и технической цели тестирования. Приоритеты этапов работ по оценке мер обеспечения ИБ могут устанавливаться в соответствии с осознаваемыми рисками. Кроме того, этапы работ могут быть спланированы либо в соответствии с конкретными бизнес-процессами или системами, либо просто для последовательного охвата всех сфер, входящих в область оценки.

Конкретную оценку мер обеспечения ИБ аудиторы ИБ обычно начинают со сбора предварительной информации, рассмотрения планируемого объема и содержания работ, установления связи с руководителями и другими контактными лицами в соответствующих частях организации, а также расширения области оценки рисков для разработки документации с инструкциями по непосредственному проведению оценки. В приложениях А, В и С приведена дополнительная информация.

6.1.2 Предварительная информация

Предварительная информация может быть получена из различных источников, таких как:

- специальная литература, периодические издания, интернет, технические руководства, стандарты и политики технической безопасности организации, а также предварительные исследования общих рисков и мер обеспечения ИБ в данной области, конференции, семинары или форумы;
- результаты предыдущих оценок, тестирований и аудитов, частично или полностью относящихся к текущей области проверки и так или иначе выполненных аудиторами, проводящими проверку мер обеспечения ИБ (например, предварительные тесты безопасности, проведенные специалистами по обеспечению ИБ, могут дать обширные знания по безопасности основных прикладных систем);
- сведения о соответствующих инцидентах ИБ, ситуациях, близких к инцидентам, вопросах поддержки и изменениях, полученные от службы технической поддержки информационных технологий (ИТ), из процессов менеджмента изменений ИТ, процессов менеджмента инцидентов ИТ и из аналогичных источников;
- общие перечни контрольных проверок и договоров, касающихся проверки мер обеспечения ИБ и проводимых аудиторами или специалистами по ИБ с опытом работы в данной сфере.

Рекомендуется пересмотреть запланированные работы по оценке мер обеспечения ИБ с учетом предварительной информации особенно, если первоначальный план оценки был подготовлен несколько месяцев назад.

Например, дополнительные оценки могут выявить проблемы, которые заслуживают более глубокого изучения, или, наоборот, повысить уверенность в некоторых областях, что позволяет сосредоточить работу на чем-то другом.

Важная роль на раннем этапе оценки мер обеспечения ИБ отводится установлению контактов с руководителями и сотрудниками. После завершения процедуры оценки этот круг лиц должен ознакомиться с ее результатами и представить конструктивные предложения. Существенно повысить результативность и эффективность оценки мер обеспечения ИБ можно путем демонстрации лояльности к сотрудникам, а также обстоятельного разъяснения процесса оценки.

6.1.3 Контрольные списки оценки

Несмотря на то, что специалисты по-разному отражают результаты своей профессиональной деятельности в документации, как правило, при проведении оценки мер обеспечения ИБ используются стандартизованные процессы с соответствующими шаблонами рабочих документов, таких как контрольные списки оценки, внутренние опросные листы по средствам управления, графики тестирования, матрицы средств управления рисками и т. п.

Контрольный список оценки (или аналогичный документ) является основным документом по следующим причинам:

- отражает запланированные области работ по проведению оценки мер обеспечения ИБ, возможно даже с определенным уровнем детализации отдельных тестов для получения ожидаемых (или идеальных) результатов;
- содержит перечень работ, что обеспечивает уверенность в полном охвате планируемой области;

- необходимый для создания контрольного списка анализ в первую очередь подготавливает аудиторов, проводящих оценку мер обеспечения ИБ, к последующей практической деятельности по оценке, в то время как заполнение контрольного списка в процессе проведения оценки способствует развитию аналитического процесса, из которого можно будет получить данные для отчета о результатах оценки;

- обеспечивает основу для записи результатов предварительной оценки и работы на местах. Также в ходе оценки в него можно поместить, например, ссылку или комментарий о собранных свидетельствах;

- может быть проверен руководством аудита или другими аудиторами ИБ в рамках процесса обеспечения качества оценки;

- после завершения оценки (вместе со свидетельствами проверки) представляет собой достаточно подробную хронологическую запись выполненных работ по проверке и полученных результатов, которая может потребоваться для обоснования или подтверждения отчета по оценке, информирования руководства и для планирования будущих оценок.

Аудиторы ИБ должны с осторожностью использовать общие контрольные списки, составленные другими специалистами. Несмотря на возможную экономию времени, это может привести к утрате некоторых из вышеперечисленных преимуществ.

6.1.4 Проверка на месте

Проверка на месте по большей части состоит из последовательности тестов, проводимых аудиторами ИБ или по их поручению, с целью сбора свидетельств и их анализа, в том числе путем их сравнения с возможными или ожидаемыми результатами соответствующих обязательств выполнения требований, стандартов или более общих оценок передового опыта. Например, один из тестов в рамках проверки мер обеспечения ИБ может проверять наличие надлежащего антивирусного программного обеспечения на всех вычислительных платформах. При проведении подобных тестов зачастую используются методы выборки, поскольку для полномасштабного тестирования обычно недостаточно ресурсов. В зависимости от аудиторов и ситуаций ИБ используются разные методы выборки, которые могут включать в себя случайный выбор, стратифицированный выбор и другие более сложные методы статистической выборки (например, дополнительные выборки, если первоначальные результаты являются неудовлетворительными, для подтверждения степени слабости мер обеспечения ИБ). Более исчерпывающее тестирование, как правило, возможно в тех случаях, когда свидетельства можно собирать и проверять в электронном виде, например, используя запросы к базе данных проверок, собранных из систем или баз данных управления активами. Подход, основанный на выборочной оценке, должен, по крайней мере частично, определяться рисками, связанными с оцениваемой сферой деятельности.

Собранные в ходе оценки свидетельства должны отмечаться, упоминаться или вноситься в список рабочих документов оценки. Свидетельства оценки, наряду с анализом, выводами, рекомендациями по оценке и отчетами о результатах оценки, должны быть надлежащим образом защищены аудиторами, проводящими оценку мер обеспечения ИБ, потому что некоторые из них могут быть весьма конфиденциальными и/или ценными. Например, данные, извлекаемые из производственных баз данных в ходе оценки, должны быть защищены в той же степени, что и базы данных с использованием средств управления доступом, шифрования и т. д. Необходимо обеспечить строгий контроль инструментов автоматического просмотра, запросов, программ для извлечения данных и утилит и т. д. Аналогичным образом необходимо обеспечить общую физическую защиту печатных документов, подготовленных аудиторами ИБ или представляемых им. Такие документы должны храниться в местах, исключающих несанкционированный доступ к ним, во избежание раскрытия или изменения их содержания. В случае особенно чувствительных оценок риски, а следовательно, необходимые меры обеспечения ИБ должны быть идентифицированы и подготовлены на раннем этапе оценки.

Заполнив контрольный список оценки, проведя серию тестов и собеседований с соответствующими сторонами и собрав достаточное количество свидетельств, аудиторы ИБ должны иметь возможность изучить свидетельства, определить степень обработки рисков ИБ и проанализировать потенциальное влияние любых остаточных рисков. На этом этапе обычно составляется проект отчета о результатах оценки в произвольной форме, который проверяется с позиции оценки и обсуждается с руководством, особенно с руководством филиалов организации, отделов, функциональных подразделений или групп, непосредственно подпадающих под оценку, а также , возможно, и других затрагиваемых при этом подразделений организации.

Свидетельства должны быть рассмотрены беспристрастным образом, чтобы убедиться в следующем:

- имеется достаточное количество свидетельств оценки для того, чтобы обеспечить фактическую основу, подтверждающую все выводы оценки;

- все выводы и рекомендации имеют важное значение в области оценки, а несущественные вопросы исключены;

- свидетельства являются актуальными и действительны по отношению к системам и мерам обеспечения ИБ.

Если, исходя из выводов, планируется дальнейшая работа по оценке мер обеспечения ИБ, то это должно быть отмечено в отчете.

6.1.5 Процесс анализа

Процесс анализа, как и планирование оценки, по существу, основан на риске, хотя и располагает большей информацией благодаря свидетельствам, собранным во время оценочных действий. В то время как прямые оценки соответствия обычно могут давать ряд относительно простых результатов «пройдено/не пройдено» с достаточно очевидными рекомендациями, оценки ИБ часто формируют вопросы, требующие размышлений и обсуждений руководства до принятия решения о том, какие соответствующие меры (если таковые необходимы) будут предприняты. В некоторых случаях руководство может вынести решение о принятии некоторых рисков, идентифицированных в результате оценки ИБ. В других случаях оно может принять решение не выполнять рекомендации оценки в точности так, как они изложены. Это право руководства, и оно несет ответственность за свои решения. В этом случае аудиторы ИБ выполняют консультативную, неоперативную роль, но они оказывают значительное влияние и опираются на обоснованные методы оценки и фактические свидетельства.

Аудиторы ИБ должны предоставить проверяемой организации обоснованную уверенность в том, что мероприятия по ИБ (не все организации внедряют систему менеджмента) достигают поставленных целей. В результате оценки должен быть предоставлен отчет о разнице между реальностью и эталоном. Если эталоном является внутренняя политика, то она должна быть очень четкой. Для сравнения можно использовать критерии, перечисленные в приложении В. При аудиторской оценке мер обеспечения ИБ необходимо рассмотреть внутренние политики и процедуры. Недостающие важные критерии все же могут быть применены в организации неформально. Отсутствие критериев, идентифицированных как критические, может быть причиной потенциальных несоответствий.

6.2 Компетенции аудитора

Оценка мер обеспечения ИБ требует от аудитора объективного анализа и профессиональных навыков в сфере отчетности. В случаях, когда речь идет об оценке технического соответствия, требуется наличие дополнительных специальных навыков, включая детальные технические знания реализации политик безопасности в программных и аппаратных средствах, каналах связи и взаимосвязанных технических процессах. Аудиторы, проводящие оценку мер обеспечения ИБ, должны обладать следующими качествами:

- способностью оценки рисков информационных систем и архитектур безопасности, основанной на понимании концептуальных основ, лежащих в основе информационных систем;

- владением надлежащих практических приемов обеспечения ИБ, таких как меры обеспечения ИБ, представленные в ИСО/МЭК 27002 и других стандартах по безопасности, включая отраслевые стандарты;

- способностью к глубокому изучению сложной технической информации для идентификации любых существенных рисков и возможностей модернизации;

- прагматизмом в отношении практических ограничений оценок как ИБ, так и ИТ в целом;

- широкими и глубокими знаниями инструментов тестирования безопасности, операционных систем, системного администрирования, протоколов связи, а также методов безопасности приложений и методик тестирования;

- способностью проводить проверку соответствия требованиям физической безопасности;

- способностью понимать требования безопасности для социальной инженерии.

При этом рекомендуется:

- каждый специалист, которому поручается проведение оценки мер обеспечения ИБ, должен быть официально ознакомлен с основными принципами профессионального аудита в соответствии с ИСО 19011, такими как: этические нормы, независимость, объективность, конфиденциальность, ответственность, осмотрительность, получение полномочий для доступа к записям, функциям, имуществу, персоналу, информации с последующими обязательствами относительно надлежащего обращения и защиты полученных данных, элементов выводов и рекомендаций, а также процессов контроля исполнения;

- специалисты, которым поручается руководство проведением оценки ИБ, должны располагать подтвержденным профессиональным опытом в проведении технических оценок ИБ не менее трех лет.

Для оценки может быть создана группа проверки, состоящая из аудиторов, осуществляющих проверку мер обеспечения ИБ, и различных специалистов с соответствующей компетентностью. В случаях, когда специалистов с такими навыками или компетентностью в непосредственном распоряжении организации нет, должны быть рассмотрены риски и преимущества привлечения профильных внутриорганизационных или внешних специалистов и ресурсов для выполнения оценки в требуемом объеме.

Аудиторы ИБ также должны проверить, что служба и персонал, ответственные за информационную безопасность:

- доступны, достаточно осведомлены в области ИБ и своих конкретных задач;
- имеют в своем распоряжении необходимые ресурсы, например, время.

7 Методы проведения оценки мер обеспечения информационной безопасности

7.1 Обзор

Основу концепции оценки мер обеспечения ИБ составляют процедуры оценки, отчетность по оценке и контроль исполнения. Структура и содержание процедур проверки учитывают цели и методы проверки.

При проведении оценки мер обеспечения ИБ аудиторы могут использовать следующие четыре метода:

- анализ процессов;
- методы изучения;
- тестирование и валидация;
- методика выборочного исследования.

В 7.2—7.5 приводятся дополнительные сведения о каждом из методов оценки.

Для тестирования и валидации могут быть использованы ресурсоемкие автоматизированные инструменты. При планировании их использования следует учитывать возможное влияние таких инструментов на выполняемые операции, например, планирование выполнения оценок на непиковое время. Если часть оценки основана на таком инструментальном средстве, то аудиторы, проводящие оценку мер обеспечения ИБ, должны продемонстрировать или предоставить свидетельства того, что это инструментальное средство обеспечивает надежные результаты, которые подтверждают целостность инструмента.

Тестирование и валидация являются обязательными для следующих мер обеспечения ИБ, если они «частично работоспособны» или «полностью работоспособны»:

- В.2.5: Требование бизнеса по управлению доступом — ИСО/МЭК 27002 (подраздел 9.1);
- В.2.5: Процесс управления доступом пользователей — ИСО/МЭК 27002 (подраздел 9.2);
- В.2.5: Ответственность пользователей — ИСО/МЭК 27002 (подраздел 9.3);
- В.2.5: Управление доступом к системам и приложениям — ИСО/МЭК 27002 (подраздел 9.4);
- В.2.6: Криптографическая защита информации — ИСО/МЭК 27002 (пункт 10.1.1)[1)];
- В.2.8: Защита информации регистрационных журналов — ИСО/МЭК 27002 (пункт 12.4.2);
- В.2.9: Менеджмент информационной безопасности сетей — ИСО/МЭК 27002 (подраздел 13.1);
- В.2.10: Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования — ИСО/МЭК 27002 (пункт 14.1.2);
- В.2.10: Защита транзакций прикладных сервисов — ИСО/МЭК 27002 (пункт 14.1.3).

Методы оценки могут быть соответствующим образом комбинированы в зависимости от характера оценки и требуемого уровня достоверности. Оценка исследования, определяемая этим подходом, может быть следующего вида:

ПОВЕРХНОСТНАЯ ОЦЕНКА

— анализ процессов;

СРЕДНЯЯ ОЦЕНКА

— анализ процессов;

— изучение или тестирование на репрезентативной выборке;

[1)] Применение криптографических методов защиты информации осуществляется в соответствии с законодательством Российской Федерации.

ГЛУБОКАЯ ОЦЕНКА

— анализ процессов;

— изучение и тестирование на расширенной или исчерпывающей выборке.

7.2 Анализ процессов

7.2.1 Общая информация

Непосредственная оценка мер обеспечения ИБ, например изучение и тестирование, не всегда является возможной или достаточной для подтверждения пригодности для использования и эффективности. Более уместным или даже необходимым для оценки пригодности и эффективности мер обеспечения ИБ может быть анализ соответствующих процессов или операций на наличие свидетельств, подтверждающих, что они:

- теоретически задуманы с целью обеспечения желаемого эффекта управления;
- правильно реализованы;
- функционируют в соответствии с проектом;
- правильно администрируются, мониторятся и управляются;
- действительно обеспечивают предполагаемые эффекты обеспечения ИБ на практике.

Операционные и административные процессы определяют среду, в которой работают меры обеспечения ИБ, и обычно предоставляют свидетельства их работы в виде записей, регистраций в журналах и т. п. В частности, создание и обработка средствами ИБ таких данных, как оповещения, аварийные сигналы, события и отчеты об инцидентах, обычно свидетельствуют об их функциональности, но не являются достаточными для подтверждения их полной надежности и эффективности. Анализ связанных процессов и операций (например, процедуры оценки, наблюдение и/или интервьюирование задействованных людей) на практике наряду с тестами обеспечивает дополнительную гарантию подтверждения того, что данные, критерии или ситуации, которые должны приводить в действие меры обеспечения ИБ, выполняют эту функцию.

В ИСО 19011 (приложение В, подраздел В.2) описана методика проведения проверок документации.

В ИСО 19011 (приложение В, подраздел В.7) описана методика проведения опросов и интервью сотрудников.

7.3 Методы изучения

7.3.1 Общая информация

Изучение — это форма метода оценки, которая обеспечивает понимание, дает разъяснения или получает свидетельства посредством проверок, инспекций, оценок, наблюдений, исследований или анализа одного или нескольких объектов оценки. Цель оценки — определить наличие мер обеспечения ИБ, их функциональность, правильность, полноту и возможности их улучшения со временем.

Как правило, объектами оценки являются:

- механизмы (например, функциональности, заложенные в аппаратное обеспечение, программное и программно-аппаратное обеспечение, приложения, базы данных);
- процессы (например, системные операции, администрирование, управление, тренировочные мероприятия).

Типичными действиями аудитора ИБ являются:

- наблюдение за операциями резервного копирования системы и оценка результатов тренировочных мероприятий по планам действий в чрезвычайных ситуациях;
- наблюдение за процессами реагирования на инциденты;
- проверка, изучение или наблюдение за работой механизмов информационных технологий в аппаратном/программном обеспечении информационной системы;
- проверка, изучение и наблюдение за действиями по управлению изменениями, относящимися к информационной системе, и их регистрацией;
- проверка, изучение или наблюдение за мерами физической безопасности, связанными с работой информационной системы (например, наблюдение за безопасной транспортировкой и уничтожением ненужных конфиденциальных бумажных документов);
- оценка, изучение или наблюдение за конфигурацией информационной системы.

7.3.2 Процедурные меры обеспечения информационной безопасности

Наблюдение за всем спектром процессов без взаимодействия с ними (или с минимальным взаимодействием) может дать аудитору возможность быстро получить фактический материал о том, как

выполняются конкретные действия. В случаях редких или специфических событий для получения результатов могут использоваться дополнительные документально подтвержденные сведения.

7.3.3 Технические меры обеспечения информационной безопасности

Взаимодействие с объектом оценки (напрямую или через квалифицированного оператора) может позволить аудитору извлекать или непосредственно просматривать его параметры конфигурации, прогнозируя его поведение, без проведения фактического тестирования. Такой подход желателен при оценке критически важных объектов, работа которых может быть нарушена из-за применения методик тестирования или объектов, с которыми у оператора нет возможности взаимодействовать.

7.4 Тестирование и валидация

7.4.1 Общая информация

Метод тестирования и валидации — это метод оценки, при котором сравниваются фактические и ожидаемые рабочие показатели одного или нескольких объектов оценки в заданных условиях. Результаты оценки подтверждают наличие, эффективность, функциональность, правильность и полноту мер обеспечения ИБ и указывают на возможности их улучшения с течением времени.

Тестирование должно выполняться компетентными специалистами с соблюдением всех мер предосторожности. Необходимо учитывать возможное воздействие на рабочие процессы организации, а также заручиться поддержкой ее руководства до начала тестирования, рассмотреть возможность проведения тестов вне периодов обслуживания при малой загрузке или даже в хорошо воспроизведенной среде тестирования. Сбои или недоступность систем из-за тестирования могут оказать существенное воздействие на нормальную повседневную работу организации. Это может привести как к финансовым потерям, так и к ухудшению репутации организации. Поэтому особое внимание следует уделить планированию тестирования и формированию правильных договорных обязательств (включая и юридические аспекты).

Прежде чем сделать какие-либо выводы, аудитор ИБ должен тщательно исследовать ложноположительные и ложноотрицательные результаты тестирования.

Как правило, объектами оценки являются механизмы (например, аппаратное, программное и встроенное программное обеспечение) и процессы (например, системные операции, процедуры администрирования и управления, тренировочные мероприятия).

Типичными действиями аудитора ИБ могут быть:

- тестирование механизмов контроля доступа, идентификации, аутентификации и проверки;
- тестирование настроек конфигурации безопасности;
- тестирование устройств контроля физического доступа;
- тестирование ключевых компонентов информационной системы на проникновение;
- тестирование операций резервного копирования информационной системы;
- тестирование способности реагирования на инциденты;
- проверка возможностей плановых действий в чрезвычайных обстоятельствах;
- тестирование систем безопасности обнаружения, предупреждения и реакции на вторжения;
- проверка алгоритмов шифрования и механизмов хеширования;
- тестирование механизмов управления идентификаторами и привилегиями пользователей;
- тестирование механизмов авторизации;
- проверка каскадной устойчивости мер безопасности;
- валидация мониторинга и ведения журналов;
- проверка аспектов безопасности при разработке или приобретении приложений.

7.4.2 Тестирование слепым методом

Аудитор, проводящий оценку мер обеспечения ИБ, тестирует объект оценки без каких-либо предварительных знаний его дополнительных характеристик, помимо общедоступных. Объект подготавливается к оценке лицом, заблаговременно знающим все детали оценки. Слепая оценка в основном осуществляется на основе навыков аудитора, проводящего оценку мер обеспечения ИБ. Объем и глубина слепой оценки могут быть настолько обширными, насколько позволяют знания и работоспособность аудитора, проводящего оценку мер обеспечения ИБ. Таким образом, это тестирование имеет ограниченное применение при оценках безопасности и его следует избегать. Его обычно называют «этичным хакерством».

7.4.3 Тестирование двойным слепым методом

Аудитор, проводящий оценку мер обеспечения ИБ, тестирует объект оценки без каких-либо предварительных знаний его дополнительных характеристик, помимо общедоступных. Аудитор заранее не

сообщает об области оценки или используемых тестах. При двойной слепой оценке тестируется подготовленность объекта оценки к неизвестным параметрам оценки.

7.4.4 Тестирование методом серого ящика

Аудитор, проводящий оценку мер обеспечения ИБ, тестирует объект оценки, располагая ограниченным знанием о его защите и активах, но полным знанием о доступных тестах. Объект подготавливается к оценке лицом, заблаговременно знающим все детали оценки. Оценка методом серого ящика осуществляется на основе навыков аудитора, проводящего оценку мер обеспечения ИБ. Основным свойством этого тестирования является результативность. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему оценку мер обеспечения ИБ, перед тестированием, а также от надлежащих знаний аудитора. Таким образом, это тестирование имеет ограниченное применение при оценках безопасности и его следует избегать. Этот вид тестирования часто называют «тестированием уязвимостей», и оно чаще всего инициируется объектом как «мероприятие по оценке самого себя».

7.4.5 Тестирование методом двойного серого ящика

Аудитор, проводящий оценку мер обеспечения ИБ, тестирует объект оценки, располагая ограниченным знанием о его защите и активах, но полным знанием о доступных тестах. Аудитор заранее сообщает об области и сроках оценки, но не о тестах. Оценка методом двойного серого ящика тестирует подготовленность объекта к неизвестным параметрам оценки. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему оценку мер обеспечения ИБ, и объекту оценки перед тестированием, а также от применяемых знаний аудитора, проводящего оценку мер обеспечения ИБ.

7.4.6 Тестирование тандемным методом

Аудитор, проводящий оценку мер обеспечения ИБ, и объект оценки подготавливаются к оценке. Для обоих заранее известны все детали оценки. При тандемном методе тестируется защита, меры обеспечения ИБ объекта. Однако при использовании данного метода не может осуществляться тестирование подготовленности объекта к неизвестным параметрам оценки. Основным свойством данного тестирования является доскональность, поскольку аудитор, проводящий оценку мер обеспечения ИБ, имеет полное представление обо всех тестах и ответных действиях. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему оценку мер обеспечения ИБ, перед тестированием, а также от надлежащих знаний аудитора. Это тестирование часто называют «внутренней оценкой», и аудитор, проводящий оценку мер обеспечения ИБ, часто играет активную роль в общем процессе обеспечения безопасности.

7.4.7 Инверсионный метод

Аудитор, проводящий оценку мер обеспечения ИБ, тестирует объект оценки, располагая полным знанием о его процессах и операционной безопасности, однако объекту оценки ничего не сообщается о том, что, как или когда будет тестировать аудитор. Основным свойством этого тестирования является оценка подготовленности объекта к неизвестным параметрам и направлениям оценки. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему оценку мер обеспечения ИБ, а также от надлежащих знаний и творческого подхода аудитора. Это тестирование часто называют «Red Team Assessment».

7.5 Методика выборочного исследования

7.5.1 Общая информация

В ИСО 19011 (см. приложение В, В.3) приведены рекомендации по проведению выборки.

7.5.2 Репрезентативная выборка

При оценке мер обеспечения ИБ может использоваться репрезентативная выборка объектов проверки (по их типу и количеству в пределах данного типа), обеспечивающая уровень покрытия, необходимый для определения, реализован ли элемент ИБ и не имеет ли он явных ошибок.

7.5.3 Исчерпывающая выборка

При оценке мер обеспечения ИБ может использоваться достаточно большая выборка объектов оценки (по типу и количеству в пределах данного типа), а также и других считающихся особенно важными для достижения цели проверки конкретных объектов проверки. Объем выборки должен быть достаточен для обеспечения уровня покрытия, необходимого для определения, реализован ли элемент ИБ и не имеет ли он явных ошибок, и для обеспечения уверенности в том, что элемент ИБ реализован правильно и работает надлежащим образом на постоянной основе, а также что существует возможность непрерывного улучшения эффективности этого элемента ИБ.

8 Процесс оценки мер обеспечения информационной безопасности

8.1 Подготовка

Определение и хранение соответствующей совокупности ожидаемых результатов до, во время и после оценки имеет первостепенное значение для достижения приемлемого результата. Это означает предоставление информации, позволяющей руководству принимать верные, основанные на рисках решения о том, каким образом лучше всего реализовывать и эксплуатировать информационные системы. Тщательная подготовка организации и аудиторов, осуществляющих оценку мер обеспечения ИБ, является важным аспектом проведения эффективных оценок. В ходе подготовительной деятельности следует рассматривать вопросы, связанные с расходами, графиком, наличием необходимой компетентности и проведением оценки.

С точки зрения организации подготовка к оценке включает следующие основные мероприятия:

- обеспечение уверенности в том, что соответствующие политики, охватываемые оценкой, существуют и осознаны всеми структурными элементами организации;
- обеспечение уверенности в том, что все запланированные шаги по реализации мер обеспечения ИБ были успешно выполнены до оценки и соответствующим образом проанализированы руководством (это применимо только в том случае, если меры обеспечения ИБ отмечены как «полностью функционирующие», а не находятся на этапе подготовки/реализации);
- обеспечение уверенности в том, что выбранные меры обеспечения ИБ поручены соответствующим организационным единицам для разработки и реализации;
- установление цели и области оценки (т. е. предназначения оценки и того, что будет проверяться);
- уведомление основных должностных лиц организации о предстоящей оценке и выделение необходимых ресурсов для проведения оценки;
- установление соответствующих каналов связи между должностными лицами организации, заинтересованными в оценке;
- установление временных рамок для проведения оценки и основных контрольных точек принятия решений, необходимых организации для осуществления эффективного менеджмента оценки;
- выбор компетентного аудитора для проведения оценки мер обеспечения ИБ или аудиторской группы, которые будут ответственными за проведение оценки, учитывая вопросы независимости аудиторов, осуществляющих оценку мер обеспечения ИБ;
- сбор артефактов для предоставления аудиторам, проводящим оценку мер обеспечения ИБ (например, документации по мерам обеспечения ИБ, включая организационные схемы, политики, процедуры, планы, спецификации, проекты, записи, руководства администратора/оператора, документацию информационной системы, соглашения о межсистемной связи, результаты предыдущих проверок);
- установление правил взаимодействия между организацией и аудиторами, проводящими оценку мер обеспечения ИБ, позволяющих свести к минимуму неопределенности или неправильные представления о реализации мер обеспечения ИБ или слабых местах/недостатках мер обеспечения ИБ, установленных во время оценки;
- минимизация неопределенностей во взаимоотношениях организации с аудиторами ИБ с помощью механизма, который может иметь форму документа отслеживания.

В документе отслеживания могут отражаться предоставляемые (организацией) и запрашиваемые (аудиторами) документы, а также их достоверность. В документе могут содержаться запросы дополнительной информации и отслеживаться неоправданные задержки ее предоставления.

В дополнение к мероприятиям по планированию, осуществляемым организацией для подготовки к оценке, аудиторы, проводящие оценку мер обеспечения ИБ, должны начинать подготовку к оценке посредством следующих мер:

- достижения понимания общего функционирования организации (включая целевую задачу, функции и процессы бизнеса), а также того, каким образом информационные активы, попадающие в область оценки, поддерживают функционирование организации;
- достижения понимания общей структуры информационных активов (например, архитектуры системы);
- достижения глубокого понимания всех мер обеспечения ИБ, подлежащих оценке;
- изучения важных публикаций, на которые в мерах обеспечения ИБ есть ссылки;
- определения организационных единиц, ответственных за разработку и реализацию подлежащих оценке мер обеспечения ИБ;

- установления в организации соответствующих контактных лиц, необходимых для проведения оценки;

- получения артефактов, необходимых для проверки (например, документации по мерам обеспечения ИБ, включая организационные схемы, политики, процедуры, планы, спецификации, проекты, записи, руководства администратора/оператора, документацию информационной системы, соглашения о межсистемной связи, инвентарные списки активов);

- получения результатов предыдущих проверок, которые могут быть надлежащим образом повторно использованы для оценки (например, отчетов, обзоров, исследований уязвимостей, проверок физической безопасности, тестирования и оценки развития);

- встречи с соответствующими должностными лицами организации для обеспечения уверенности в общем понимании целей оценки, предлагаемой формы и области оценки;

- разработки плана оценки.

При подготовке к оценке мер обеспечения ИБ следует собрать необходимую исходную информацию, которая должна быть предоставлена аудиторам, осуществляющим оценку мер обеспечения ИБ. В рамках необходимой поддержки каждой конкретной оценки организация должна определить и подготовить доступ к организационным элементам (лицам или группам лиц), отвечающим за разработку, документирование, распространение, оценку, эксплуатацию, поддержку и обновление всех мер обеспечения ИБ, политик безопасности и взаимосвязанных процедур, для реализации соответствующих политикам мер обеспечения ИБ.

Доступность необходимой документации, а также ведущего персонала организации и проверяемых информационных систем крайне важна для успешной оценки мер обеспечения ИБ.

8.2 Планирование оценки

8.2.1 Обзор

При разработке планов оценки аудиторы ИБ должны определить вид оценки (например, полная или частичная оценка) и то, какие меры обеспечения ИБ и/или средства, расширяющие их возможности, должны быть включены в оценку на основе цели/области оценки. Аудиторы ИБ по возможности должны оценить и снизить риски и влияние оценки на обычное функционирование организации. Они должны выбрать соответствующие оценочные процедуры для проверки, основываясь на:

- элементах мер обеспечения ИБ и средствах, расширяющих их возможности, которые необходимо включить в оценку;

- атрибутах их глубины и покрытия.

Аудиторы ИБ должны приспособить выбранные процедуры оценки к уровню рисков информационной системы и к реальной рабочей среде организации. При необходимости они также должны разработать дополнительные процедуры оценки, не рассматриваемые в данном документе, в отношении мер обеспечения ИБ, а также средств, расширяющих их возможности, и обеспечить доверие к этим процедурам.

Результат планирования оценки должен быть документально оформлен в виде плана оценки. При планировании необходимо учитывать контекст, формирование базового уровня ожидаемого поведения в рамках определенного контекста, спецификации тестирования/оценивания и метод подтверждения достоверности выводов в контексте оценивания.

План должен включать разработку стратегии по применению расширенной процедуры оценки, если это необходимо, оптимизации процедур оценки для уменьшения дублирования работ и обеспечения относящихся к оценке экономически эффективных решений. После этого аудиторы ИБ должны оформить окончательный план оценки и получить необходимые санкции на его выполнение.

8.2.2 Определение охвата оценки

Охват определяет организационные и технические границы оценки. Охват оценки должен базироваться на выборе мер обеспечения ИБ в зависимости, например, от установленного графика непрерывного мониторинга, элементов плана действий и соответствующих этапов. Меры обеспечения ИБ с большей изменчивостью следует пересматривать чаще.

Охват оценки должен определяться аудитором ИБ совместно с руководством, используя документацию организации. Эта документация должна содержать перечень требований безопасности информационных активов и описывать элементы ИБ, установленные или планируемые для удовлетворения этих требований. Аудитор ИБ начинает с мер обеспечения ИБ, описанных в документации по ИБ, и определяет цель проверки. Оценка может охватывать все меры обеспечения ИБ организации либо

часть из них, так, например, в процессе постоянного мониторинга осуществляется непрерывная оценка части мер обеспечения ИБ информационных активов. Для проведения частичных оценок владелец информационных активов определяет проверяемые меры обеспечения ИБ вместе с заинтересованными в проверке официальными лицами организации.

8.2.3 Процедуры оценки

Процедура оценки состоит из совокупности целей оценки с соответствующим набором потенциальных методов оценки и объектов оценки. Формулировки определений целей оценки тесно связаны с сущностью мер обеспечения ИБ (т. е. с функциональными возможностями мер обеспечения ИБ). Это обеспечивает уверенность в прослеживаемости результатов оценки вплоть до фундаментальных требований к мерам обеспечения ИБ. По результатам применения процедуры оценки к мере обеспечения ИБ формируются выводы оценки. Эти выводы оценки впоследствии используются для определения общей эффективности мер обеспечения ИБ. Объекты оценки определяют конкретные элементы, подлежащие оценке, а также спецификации, механизмы, процессы и физических лиц.

В приложении А представлены примеры процедур оценки, предназначенных для оценки технического соответствия и совершенствований мер обеспечения ИБ. Практическое руководство в приложении А предназначено для сбора свидетельств с целью определения, правильно ли реализованы меры обеспечения ИБ, функционируют ли они, как задумывалось, и создают ли желаемый результат в отношении выполнения требований информационных активов к ИБ. Для каждых средств, включенных в оценку меры обеспечения ИБ, и каждого средства, расширяющего их возможности, аудиторы, проводящие оценку мер обеспечения ИБ, разрабатывают соответствующую процедуру оценки, обращаясь к приложению А. Совокупность выбранных процедур оценки различна для разных проверок и зависит от назначения текущей оценки (например, ежегодная оценка мер обеспечения ИБ, непрерывный мониторинг). В приложении А представлено практическое руководство по выбору соответствующих процедур оценки в зависимости от цели оценки.

Процедуры оценки могут быть специально приспособленными в отношении:

- выбранных методов и объектов оценки, необходимых для наиболее эффективного принятия соответствующих решений и выполнения целей оценки;
- выбранных значений атрибутов «глубины» и «охвата» метода оценки, необходимых для осуществления ожиданий оценки, на основе характеристик проверяемых мер обеспечения ИБ и конкретных, требующих принятия решений;
- исключения из процедур оценки тех мер обеспечения ИБ, которые были уже проверены при проведении другого адекватного процесса оценки;
- развития информационной системы или конкретной платформы и адаптированных процедур оценки конкретной организации для успешного выполнения оценки;
- использования результатов предыдущих проверок, если эти результаты сочтены применимыми;
- осуществления соответствующих корректировок процедур оценки, чтобы иметь возможность получения требуемых свидетельств оценки от внешних поставщиков (если они имеются);
- выбранных методов оценки, уделяя должное внимание их влиянию на организацию, наряду с обеспечением уверенности в выполнении целей оценки.

8.2.4 Особенности, относящиеся к объектам

Организации могут специфицировать, документировать и конфигурировать свои информационные активы различными способами, следовательно, содержание и применение существующих свидетельств оценки будут различаться. Это может приводить к необходимости применения различных методов оценки к разным объектам оценки, чтобы сформировать свидетельства оценки, необходимые для определения, являются ли меры обеспечения ИБ эффективными при их применении. Вследствие этого перечень методов и объектов оценки, представляемый вместе с каждой процедурой оценки, называется потенциальным, чтобы отразить необходимость в возможности выбора наиболее подходящих для конкретной оценки методов и объектов. К выбранным методам и объектам оценки относятся те, которые сочтены необходимыми для создания необходимых свидетельств оценки. Потенциальные методы и объекты в процедуре оценки предоставляются как ресурс, обеспечивающий выбор надлежащих методов и объектов. По существу, аудиторы ИБ должны действовать по собственному усмотрению, осуществляя выбор из потенциальных методов оценки и общего списка объектов оценки, связанных с каждым выбранным методом.

Аудиторы ИБ должны выбирать только те методы и объекты, которые наиболее эффективно способствуют принятию решений, связанных с целью оценки. Мера качества результатов оценки основана на правильности представленного логического обоснования, а не на конкретной совокупности при-

мененных методов и объектов. В большинстве случаев нет необходимости применять каждый метод оценки к каждому объекту оценки, чтобы получить желаемые результаты оценки. А для конкретных и всесторонних проверок, может быть, целесообразно использовать метод, не перечисленный в согласованном перечне потенциальных методов, или не использовать никакого из перечня известных методов.

8.2.5 Результаты предыдущих оценок

8.2.5.1 Обзор

Аудиторы ИБ должны использовать имеющуюся информацию о предыдущих оценках мер обеспечения ИБ, что будет способствовать большей эффективности оценок. Повторное использование результатов ранее признанных или утвержденных оценок информационных систем должно рассматриваться в рамках совокупности свидетельств для определения общей эффективности мер обеспечения ИБ.

При рассмотрении вопроса о повторном использовании результатов предыдущих проверок и ценности этих результатов для текущей оценки аудиторы ИБ должны определить:

- достоверность свидетельств;
- пригодность предыдущего анализа;
- применимость свидетельств при текущем состоянии информационных активов.

В определенных ситуациях бывает необходимо дополнить результаты предыдущей оценки, рассматриваемые на предмет их повторного использования, дополнительными мероприятиями оценки. Например, если при независимом проводимом третьей стороной оценивании продукта информационной технологии не проводилось тестирования применительно к конкретной настройке параметров конфигурации, которая применяется организацией в информационной системе, аудитору ИБ потребуется дополнить первоначальные результаты тестирования. Для этого необходимо дополнительное тестирование, которое охватит данную настройку параметров конфигурации для текущей среды информационной системы.

Информация, приведенная в 8.2.5.2—8.2.5.4, предназначена для оценки возможности использования результатов предыдущих проверок для текущей оценки.

8.2.5.2 Меняющиеся условия

Меры обеспечения ИБ, сочтенные эффективными во время предыдущих проверок, могут стать неэффективными в результате изменившихся условий, связанных с информационными активами или окружающей средой. Соответственно возможно, что результаты оценки, признанные ранее приемлемыми, могут больше не давать достоверных свидетельств для определения эффективности мер обеспечения ИБ и потребуется новая оценка. Применение результатов предыдущей оценки в ходе текущей оценки требует выявления всех изменений, произошедших со времени предыдущей оценки, и степени влияния этих изменений на результаты предыдущей оценки. Например, повторное использование результатов предыдущей оценки, включающей изучение политик и процедур обеспечения безопасности организации, может быть приемлемым, если определено, что никаких существенных изменений идентифицированных политик, процедур и среды риска не произошло.

8.2.5.3 Допустимость использования результатов предыдущих оценок

Допустимость использования результатов предыдущих проверок при оценке мер обеспечения ИБ должна координироваться и утверждаться лицами, использующими результаты оценки. Необходимо, чтобы владелец информационных активов сотрудничал с соответствующими должностными лицами организации (например, с директором по информационным технологиям, ответственным за информационную безопасность, ответственными за целевую задачу или владельцами информации) при определении допустимости использования результатов предыдущих проверок. Решение об использовании результатов предыдущих проверок должно документироваться в плане оценки и окончательном отчете.

В оценку безопасности допускается включать выводы предыдущих оценок безопасности, если:

- это специально разрешено в плане аудита;
- все ограничения и проблемы предыдущей оценки, связанные с проведением текущей оценки, отражены в документации, что включает в себя вопросы, частично решаемые в рамках текущих планов действий;
- у аудиторов ИБ есть все основания полагать, что на сегодняшний день результаты актуальны;
- любые текущие или процедурные изменения в мерах обеспечения ИБ или процессах, к которым они применяются, должным образом учитываются в текущей оценке;
- в отчете об оценке четко указаны возможные проблемы и риски, связанные с использованием результатов предыдущей оценки.

8.2.5.4 Временные аспекты

Как правило, с увеличением периода времени между текущей и предыдущими оценками достоверность/полезность результатов предыдущих оценок уменьшается. Это связано в основном с тем, что информационные активы или среда, в которой функционируют информационные активы, с большой вероятностью изменяются с течением времени, возможно, делая недействительными исходные условия или предположения, на которых была основана предыдущая оценка.

8.2.6 Рабочее задание

Независимость аудитора ИБ может быть критическим фактором при выполнении некоторых видов оценок, особенно для информационных активов со средним и высоким уровнями риска. Степень независимости аудитора, требуемая при оценке, должна быть постоянной. Например, неуместно повторно использовать результаты предыдущих оценок, в которых не требовалась независимость аудитора ИБ, в текущей оценке, требующей большей степени независимости.

8.2.7 Внешние системы

Представленные в приложении А методы и процедуры оценки должны быть соответствующим образом скорректированы для выполнения оценки внешних информационных систем. Поскольку организация не всегда имеет возможность проведения непосредственного контроля мер обеспечения ИБ, используемых во внешних информационных системах, или достаточного визуального контроля разработки, реализации и оценки этих мер обеспечения ИБ, то может потребоваться применение альтернативных подходов к оценке. Это может приводить к необходимости адаптации процедур оценки, описанных в приложении А. При необходимости согласованные меры обеспечения ИБ информационной системы документируются в договорах или соглашениях об уровне услуг. Аудитор ИБ должен проверять эти договоры или соглашения и в соответствующих случаях либо адаптировать процедуры для оценки мер обеспечения ИБ, представленных по этим соглашениям, либо результаты оценки мер обеспечения ИБ предоставлять через соглашения. Кроме того, аудиторы ИБ должны учитывать информацию, полученную при любых оценках, проведенных или находящихся в процессе проведения организациями, эксплуатирующими внешние информационные системы, которые имеют отношение к защищаемым информационным активам на основании проводимой оценки. Соответствующая информация, полученная в результате этих проверок, если она будет сочтена достоверной, должна быть включена в отчет.

8.2.8 Информационные активы и организация

Процедуры оценки могут быть приспособлены для анализа системы или конкретной платформы, или зависимостей конкретной организации. Такая ситуация часто возникает в процедурах проверок, связанных с мерами обеспечения ИБ из числа технических мер обеспечения ИБ (т. е. управление доступом, аудит и подотчетность, идентификация и аутентификация, защита систем и средств связи). Результаты последнего тестирования могут быть также применимы для текущей оценки, если его методы обеспечивают высокую степень прозрачности (например, что тестировалось, когда и каким образом). Протоколы тестирования на основе стандартов могут представлять примеры, как организации могут способствовать достижению подобного уровня прозрачности.

8.2.9 Расширенная процедура оценки

Организации обладают большой гибкостью при выполнении требований доверия к мерам обеспечения ИБ. Например, в отношении такого требования, как доверие своевременному рассмотрению недостатков. Организация может удовлетворять этому требованию по принципу «в зависимости от конкретной меры обеспечения ИБ», по принципу «в зависимости от вида меры обеспечения ИБ», по принципу «в зависимости от конкретной системы» или возможно даже по организационному уровню. Принимая во внимание такую гибкость, расширенная процедура оценки применяется по принципу «в зависимости от конкретной оценки» обычно в соответствии с тем, как организация решает достигать доверия к проверяемым информационным активам. Метод применения расширенной процедуры оценки должен документироваться в плане оценки. Далее организация выбирает соответствующие цели оценки из расширенной процедуры оценки на основе уровня рисков для информационных активов. Применение расширенной процедуры оценки предназначается для дополнения других процедур оценки с целью обеспечения уверенности в том, что меры обеспечения ИБ реализованы правильно, функционируют, как предназначалось, и дают желаемый результат в отношении выполнения применяемых требований ИБ.

8.2.10 Оптимизация

Аудиторы ИБ должны проявлять определенную степень гибкости в вопросе формирования плана оценки, отвечающего потребностям организации. Это дает возможность получения необходимых сви-

детельств при определении эффективности мер обеспечения ИБ при одновременном снижении общих расходов на оценку.

Комбинирование и объединение процедур оценки является одной из сфер, где может быть применена гибкость. Во время оценки методы оценки многократно применяются к различным объектам оценки в рамках конкретной области применения мер обеспечения ИБ.

Чтобы сэкономить время, уменьшить расходы на оценку и максимально увеличить полезность результатов оценки, аудиторы ИБ должны рассмотреть выбранные процедуры оценки для областей применения мер обеспечения ИБ и там, где это возможно и осуществимо, скомбинировать или объединить процедуры (или части процедур).

Например, аудиторы ИБ могут объединить опросы ключевых должностных лиц организации по различным темам, имеющим отношение к ИБ. Аудиторы ИБ могут воспользоваться другой возможностью существенного объединения процедур и экономии расходов путем одновременного изучения всех применяемых политик и процедур, касающихся обеспечения безопасности, или формирования групп взаимосвязанных политик и процедур, которые можно изучать как единый элемент. Получение и изучение параметров конфигурации сходных аппаратных и программных компонентов в соответствующих информационных системах является еще одним примером того, как можно обеспечить существенную эффективность оценки.

Дополнительной сферой, заслуживающей внимания при оптимизации процесса оценки, является последовательность, в которой осуществляется оценка мер обеспечения ИБ. Оценка некоторых мер обеспечения ИБ раньше других может предоставить информацию, облегчающую понимание и оценку других мер обеспечения ИБ. Например, сферы применения мер обеспечения ИБ могут создавать общие описания информационных активов. Оценка этих мер обеспечения ИБ в начале процесса оценки может обеспечить базовое понимание информационных активов, которое может помочь при оценке других мер обеспечения ИБ. Дополнительные рекомендации по многим мерам обеспечения ИБ также определяют взаимосвязанные меры обеспечения ИБ, которые могут предоставить полезную информацию для организации процедур оценки. Другими словами, последовательность осуществления оценки может способствовать многократному использованию информации оценки одной меры обеспечения ИБ при оценке других взаимосвязанных мер обеспечения ИБ.

8.2.11 Завершающий этап

После выбора процедур оценки (включая разработку необходимых процедур, не включенных в данный документ), их адаптации к конкретным информационным активам и к характерным условиям организации, оптимизации процедур для обеспечения эффективности, применения в необходимых случаях расширенной процедуры оценки и рассмотрения возможности влияния неожиданных событий на оценку плану оценки придается окончательная форма и устанавливаются сроки выполнения с включением основных контрольных точек процесса оценки.

По завершении разработки плана оценки он рассматривается и утверждается соответствующими должностными лицами организации. При этом данный план должен:

- практически быть законченным;
- соответствовать целям безопасности организации и анализу рисков организации;
- экономически быть эффективным в отношении ресурсов, выделенных для оценки.

Если в ходе оценки возможно прерывание обычного функционирования организации (например, в результате отвлечения ключевого персонала или возможных (временных) сбоев систем из-за тестирования на проникновение), в плане оценки должен быть указан масштаб такого прерывания и его временные рамки.

8.3 Выполнение оценки

После утверждения организацией плана оценки аудитор ИБ работает по нему в соответствии с согласованными контрольными точками и сроками.

Цели оценки достигаются путем применения выбранных методов оценки к выбранным объектам оценки и сбора/создания информации, необходимой для принятия решений, связанных с каждой целью оценки. Каждая формулировка решения относительно процедуры оценки, которую выполнил аудитор, проводящий оценку мер обеспечения ИБ, представляет собой один из следующих выводов:

- соответствует (С);
- частично соответствует (Ч);
- не соответствует (Н).

«Соответствует» означает, что для элемента меры обеспечения ИБ, который был определен в заявке на оценку, полученная в процессе оценки информация (т. е. собранные свидетельства) указывает на достижение цели проверки для него, что дает полностью приемлемый результат.

«Частично соответствует» означает, что элемент меры обеспечения ИБ не соответствует своей цели или что на момент оценки реализация меры обеспечения ИБ все еще находится в процессе внедрения, с разумной гарантией того, что элемент управления достигнет удовлетворительного результата «Соответствует».

«Не соответствует» означает, что для элемента меры обеспечения ИБ, который определен в заявке на оценку, полученная в процессе оценки информация указывает на потенциальные аномалии в функционировании или реализации элемента управления, которые должны быть устранены организацией. Кроме того, вывод «не соответствует» также может указывать на то, что по причинам, указанным в отчете о проверке, аудитор ИБ не смог получить информацию, достаточную для принятия конкретного решения, запрошенного в заявке на оценку.

Выводы аудитора ИБ (т. е. сделанные заключения) должны быть беспристрастными, содержать фактическую информацию о том, что было обнаружено в отношении проверяемой меры обеспечения ИБ. Для каждого вывода «не соответствует» аудиторы ИБ должны указать, какие элементы меры обеспечения ИБ затронуты (т. е. те аспекты меры обеспечения ИБ, которые были сочтены несоответствующими или которые не было возможности проверить), и насколько воздействие меры обеспечения ИБ отличается от планируемого или ожидаемого. Аудитор ИБ должен также отметить возможность нарушения конфиденциальности, целостности и доступности, обусловленную выводами «не соответствует». Если оценка показывает существенные несоответствия (т. е. выводы «не соответствует» указывают на существенное отклонение от запланированного состояния), аудитор, проводящий оценку мер обеспечения ИБ, должен немедленно информировать лицо, отвечающее за эту меру обеспечения ИБ, и руководство для незамедлительного запуска процедур смягчения последствий.

8.4 Анализ результатов и отчет

В плане оценки должны быть предоставлены цели оценки и детальный график действий по проведению оценки. Конечным результатом оценки является отчет о результатах оценки, в котором отражается уровень ИБ на основе реализованных мер обеспечения ИБ. Отчет включает информацию, поступающую от аудитора ИБ (в форме выводов оценки), необходимую для определения эффективности используемых мер обеспечения ИБ и общей эффективности деятельности организации в реализации соответствующих мер обеспечения ИБ. Отчет является важным фактором при определении рисков ИБ для операций (т. е. целевой задачи, функций), активов организации, кадров, других организаций и т. д.

Результаты оценки должны быть документально оформлены с установленным для оценки уровнем детальности в соответствии с форматом отчетности, предписываемым политикой организации. Формат отчетности должен также соответствовать виду проводимой оценки мер обеспечения ИБ (например, оценка, самостоятельно проводимая владельцами информационной системы, независимая оценка и подтверждение достоверности, независимые оценки мер обеспечения ИБ, проводимые аудиторами, и т. д.).

Владелец информационной системы полагается на квалификацию аудитора в сфере ИБ и его технические решения в вопросах проведения оценки мер обеспечения ИБ, а также предоставления конкретных рекомендаций по исправлению слабых мест или недостатков мер обеспечения ИБ и снижения или устранения выявленных уязвимостей.

Данные оценки, сформированные аудитором ИБ (т. е. результаты в форме определения о соответствии или несоответствии, список элементов мер обеспечения ИБ, не продемонстрировавших удовлетворительный результат, а также возможные нарушения безопасности информационных активов), предоставляются руководству в виде первичного (предварительного) отчета об оценке безопасности. Владельцы актива могут предпринять меры:

- либо по выполнению рекомендаций аудитора ИБ до завершения подготовки окончательной версии отчета при наличии определенных возможностей для устранения слабых мест или недостатков мер обеспечения ИБ;

- либо по устранению (прояснению) двусмысленностей или различий в интерпретации результатов оценки.

Аудитор ИБ должен снова проверить модифицированные, улучшенные или добавленные во время этого процесса меры обеспечения ИБ, прежде чем формировать окончательный отчет. Передача окончательного отчета руководству означает официальное завершение оценки мер обеспечения ИБ.

Поскольку результаты оценки в конечном счете влияют на состав мер обеспечения ИБ, а также на план действий и контрольные точки, владелец информационных активов рассматривает выводы аудитора ИБ и при содействии руководства организации определяет соответствующие шаги, которые необходимы для устранения слабых мест и недостатков, идентифицированных во время оценки. Форма отчетности по выводам оценки, в которой использованы выводы «соответствует», «частично соответствует» и «не соответствует», обеспечивает руководству организации наглядное представление конкретных слабых мест и недостатков обеспечения ИБ и способствует упорядоченному и структурированному подходу к уменьшению рисков в соответствии с процессом менеджмента рисков ИБ.

Например, владелец информационных активов после консультации с руководством организации может принять решение о том, что некоторые выводы оценки, отмеченные как «не соответствует», носят несущественный характер и не представляют особого риска для организации. Или, наоборот, владелец информационных активов и руководители могут решить, что определенные выводы, отмеченные как «не соответствует», являются существенными и требуют принятия незамедлительных корректирующих действий. Во всех случаях руководство организации проверяет каждый вывод «не соответствует» аудитора ИБ (т. е. потенциального неблагоприятного влияния на операции и активы организации, кадры, другие организации и т. д.) и решает, является ли вывод достаточно серьезным, чтобы заслуживать дальнейшего исследования или корректирующих действий. Может потребоваться привлечение высшего руководства к процессу смягчения последствий, чтобы обеспечить эффективное распределение ресурсов организации в соответствии с приоритетами, предоставляя в первую очередь ресурсы информационным активам, которые поддерживают наиболее критические бизнес-процессы организации, или исправляя недостатки, которые представляют наибольшую степень риска. В конечном счете выводы оценки и любые последующие действия по смягчению последствий, инициированные владельцем информационных активов в сотрудничестве с назначенным должностным лицом организации, приводят к модификации процессов менеджмента рисков ИБ, а также мер обеспечения ИБ. Соответственно базовые документы, используемые руководителями для определения состояния ИБ информационных активов, обновляются, чтобы отразить результаты оценки.

В заранее обозначенные сроки в плане устранения выявленных несоответствий или через определенный период времени после оценки, например, через три месяца после представления окончательного отчета, обычно производится контроль исполнения, сосредотачивающийся на нерешенных или «открытых» проблемах. Этот процесс включает в себя оценку правильности реализованных решений по предыдущим выводам. Организации могут также решить проводить мероприятия по контролю исполнения во время следующей оценки, особенно для тех проблем, которые не являются ни критичными, ни неотложными.

Приложение А
(справочное)

Начало сбора информации (не для информационных технологий)

Ведущий аудитор ИБ должен выделить отдельного аудитора с соответствующим уровнем компетенции и опытом для оценки каждой области ИБ.

Ниже приводятся примерные вопросы, которые могут быть заданы соответствующим сотрудникам организации (список не является исчерпывающим).

А.1 Общая информация

А.1.1 Безопасность, связанная с персоналом

a) Чувствует ли персонал себя ответственным и/или подотчетным за свои действия?

b) Доступны ли на рабочих местах специалисты, обладающие знаниями по безопасности и ИБ, для ответа на вопросы, мотивации персонала и предоставления необходимых инструкций?

c) Являются ли применяемые политики и процедуры четкими, конкретными, измеримыми, приемлемыми, реалистичными и привязанными ко времени?

d) Учитывается ли уровень функциональных знаний при приеме сотрудников на работу?

e) Надежен ли персонал, работающий с конфиденциальной информацией и системами, которые могут поставить под угрозу существование организации?

f) Можно ли полностью доверять персоналу?

g) Как определяется и каким образом измеряется степень доверия?

h) Производится ли оценка анкетно-биографических данных сотрудников?

А.1.2 Политики

a) Стратегическая согласованность

1) Заложены ли в основу политик безопасности коммерческие задачи и общая политика безопасности?

2) Каким образом взаимосвязаны политики в области информационных технологий, кадров и приобретений?

b) Полнота

1) Имеются ли политики информационной безопасности во всех секторах коммерческой деятельности (кадры, физические активы, информационные технологии, продажи, производство, НИОКР, контакты и т. п.)?

2) Являются ли политики достаточно полными и охватывающими вопросы стратегии, тактики и коммерческих операций?

c) Построение

1) Являются ли политики простыми выдержками из стандарта ИСО 27002 или меры обеспечения ИБ и их задачи адаптированы к конкретным условиям?

2) Содержат ли документы политики четкое определение ответственных лиц?

3) Политики или процедуры должны предопределять ожидаемые действия, отвечая на «основополагающие» вопросы: «кто», «когда», «зачем», «что», «где», «каким образом»:

- Если лицо, ответственное за выполнение действия, не определено, кто будет достигать поставленных целей?
- Если целевое время (когда) для выполнения действия не определено, будет ли оно начато или закончено в назначенное время?
- Если цель действия не определена (зачем), будет ли действие правильно понято и его важность адекватно рассмотрена?
- Если само действие (что) не определено, как можно будет его выполнить?
- Если действие не определяет объект, место, процесс, информационный актив или меру обеспечения ИБ, на которые оно должно воздействовать, как оно будет эффективно (где)?
- Если действие в процедуре не дает четкого определения того, как все должно быть сделано, как оно может быть правильно выполнено (каким образом)?
- Если для действия не определены индикаторы и меры обеспечения ИБ, направленные на проверку его правильного выполнения и достижения своих целей, то как организация может убедиться, что цели достигнуты или могут быть достигнуты (каким образом)?

4) Имеются ли меры обеспечения ИБ и среда для оценки реализации политик и достижения поставленных целей?

5) Цели политики должны быть конкретными, измеримыми, приемлемыми, реалистичными и привязанными ко времени. Если это не так, то:

- не имеющие четкого определения задачи сложно идентифицировать и лица, ответственные за их решения, как правило, не указываются;
- отсутствие возможности оценить степень достижения цели оставляет мало шансов на то, что организации удастся проверить, достигнута ли цель или нет;

- если задача не доведена до сведения персонала и не уяснена им (кто над чем должен работать), велик шанс того, что мера обеспечения ИБ будет понята неправильно, дезориентировано или отвлеченно;

- нереалистичная по меркам организации цель оставляет мало шансов на ее достижение;

- отсутствие временных рамок достижения цели (сроков, начала работы над ней и т. п.) повышает шансы на то, что действия так и не будут предприняты, а сама цель не будет достигнута.

А.1.3 Организация

a) Если роли сформулированы, а ответственность распределена, какие именно из них являются необходимыми и достаточными для решения бизнес-задач с учетом конкретной ситуации и существующих ограничений?

b) Определена ли связь с внешними инстанциями?

c) Переданы ли вопросы безопасности в ведение внешних подрядчиков при отсутствии у организации собственных возможностей для обеспечения безопасности?

d) Отражены ли вопросы безопасности в заключенных договорах?

А.2 Физическая безопасность и безопасность среды

А.2.1 Являются ли объекты безопасными для обработки информации?

a) Зоны

1) Достаточна ли степень изоляции общедоступных зон от внутренних помещений организации?

2) Выделены ли зоны для обработки особо важной информации сотрудниками или вычислительными системами?

3) Реализовано ли надлежащее разделение таких закрытых зон во избежание утечки информации?

b) Расположение

1) Имеется ли четкая идентификация таких зон, и правильно ли они расположены?

2) Имеются ли четкие границы таких зон (стены, потолок, полы и т. п.), и достаточно ли они надежны для защиты находящихся в их пределах активов?

3) Имеется ли соответствующая маркировка таких зон, и находятся ли критические зоны вне поля зрения «посторонних лиц»?

c) Входы-выходы

1) Обеспечивают ли двери, окна и прочие проходы в закрытом состоянии защиту, аналогичную обеспечиваемой границами зоны?

2) Имеются ли соответствующий контроль доступа для входа в зону и выхода из нее?

3) Имеется ли система предотвращения вторжений?

4) Предусмотрены ли аварийные выходы, обеспечивающие достаточную возможность эвакуации, для информации, людей и оборудования?

d) Коридоры и проходы

1) Обеспечена ли идентификация проходов к зонам и рабочим местам:

- пути для персонала;
- кабели (пути передачи информации).

2) Существуют ли альтернативные пути?

3) Обеспечена ли защита и мониторинг таких путей?

e) Мониторинг

1) Имеется ли возможность вести скрытое наблюдение?

2) Способны ли средства мониторинга обнаруживать вторжения на раннем этапе?

3) Когда ведется мониторинг?

4) Где и как хранятся и анализируются записанные данные?

f) Мебель

1) Подходит для хранения информации?

2) Правильно расположена?

3) Выполняет свои функции?

А.2.2 Являются ли объекты безопасными для информационных технологий? (Аспекты среды)

a) Обеспечение электроэнергией

1) Достаточное/надлежащее

2) Альтернативные источники?

b) Кондиционирование воздуха

1) Достаточное/надлежащее

2) Альтернативные источники?

c) Противопожарная безопасность

1) Достаточная/надлежащая

2) Альтернативные источники?

А.2.3 Являются ли объекты безопасными для людей?

a) Имеются ли аварийные входы (с соответствующими средствами управления)?

b) Представляют ли утечки (электроэнергии, воды, газа, жидкостей) потенциальную опасность для людей?

c) Представляют ли температура, влажность, материалы и вибрации потенциальную опасность для людей?
d) Размещено ли оборудование так, чтобы люди не могли получить травмы?
e) Управляются ли входы-выходы так, чтобы люди не могли получить травмы?
f) Обеспечивает ли установка и использование мебели безопасность людей?

A.3 Менеджмент инцидентов

a) Имеется ли определение инцидентов ИБ?
b) Предусмотрены ли средства реагирования на инциденты ИБ:
   1) Руководства?
   2) Роли и обязанности?

Приложение В
(справочное)

Практическое руководство по оценке технического соответствия информационной безопасности

В.1 Общая информация

В данном приложении представлена совокупность практических руководств по оценке технического соответствия ИБ с использованием технических мер обеспечения ИБ, описанных в ИСО/МЭК 27002. В данном приложении описана каждая мера обеспечения ИБ. ИСО/МЭК 27001 не требует от организаций использования мер обеспечения ИБ ИСО/МЭК 27002. Необходимыми могут быть другие меры обеспечения ИБ, такие как секторальные меры обеспечения ИБ из таких стандартов, как ИСО/МЭК 27010 и ИСО/МЭК 27017. Кроме того, организации могут разрабатывать собственные меры обеспечения ИБ. Однако в данном приложении рассмотрены меры обеспечения ИБ из ИСО/МЭК 27002. Они иллюстрируют различные методы по оценке технического соответствия, которые можно использовать.

В В.2.1—В.2.14 представлена таблица для каждого элемента ИБ из ИСО/МЭК 27002, содержание которой сгруппировано следующим образом:

«Техническая мера обеспечения ИБ» (с дополнительной технической информацией)

1. Стандарт реализации безопасности (с «Техническими примечаниями к стандарту реализации безопасности»)

1.1 Практическое руководство, Предполагаемые свидетельства, Метод

1.2 Практическое руководство, Предполагаемые свидетельства, Метод

2. Стандарт реализации безопасности (с «Техническими примечаниями к стандарту реализации безопасности»)

2.1 Практическое руководство, Предполагаемые свидетельства, Метод

2.2 Практическое руководство, Предполагаемые свидетельства, Метод

Для каждой технической меры обеспечения ИБ существует дополнительная техническая информация, помогающая аудиторам ИБ. Она в основном состоит из информации о серии «стандартов реализации безопасности», которые должны регулярно проверяться организацией для подтверждения, реализованы ли и эксплуатируются ли соответствующим образом применяемые стандарты или нет.

В каждом «Стандарте реализации безопасности» есть «Техническое примечание к стандарту реализации безопасности», предоставляющее дополнительную техническую информацию для процесса оценки. В нем также представлены: «Практическое руководство», «Предполагаемые свидетельства» и «Метод».

«Практическое руководство» предоставляет применяемую процедуру оценки соответствия для «стандарта реализации безопасности». В «Предполагаемых свидетельствах» приводятся некоторые примеры систем, файлов, документов или других элементов, которые могут быть приняты в качестве «свидетельств» в процедуре оценки соответствия. Следует обратить внимание на то, что названия свидетельств могут различаться в разных организациях. Однако использованные в данном приложении названия могут считаться общепризнанными в сфере оценки технического соответствия. «Метод» представляет соответствующий подход к технической оценке соответствия согласно приведенному выше «Практическому руководству».

В данном приложении не представлены исчерпывающие практические руководства по технической оценке, которые могут значительно помочь организациям в проведении оценки, внедрены ли соответствующим образом стандарты реализации безопасности и действуют ли они.

В.2 Оценка мер обеспечения информационной безопасности ИСО/МЭК 27002

В.2.1 ИСО/МЭК 27002, раздел 5 Политики информационной безопасности

ИСО/МЭК 27002, 5.1 Руководящие указания в части информационной безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 5.1.1 Политики информационной безопасности Набор политик ИБ должен быть разработан, утвержден высшим руководством, опубликован и доведен до сведения всех сотрудников и причастных внешних сторон
	Мера обеспечения ИБ	ИСО/МЭК 27002, 5.1.2 Пересмотр политик информационной безопасности Политики ИБ должны пересматриваться через заранее определенные промежутки времени или в случае значительных изменений для обеспечения их постоянной применимости, адекватности и эффективности

В.2.2 ИСО/МЭК 27002, раздел 6 Организация деятельности по информационной безопасности

ИСО/МЭК 27002, 6.1 Внутренняя организация деятельности по обеспечению информационной безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.1.1 Роли и обязанности по обеспечению информационной безопасности Все обязанности по обеспечению ИБ должны быть определены и распределены
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.1.2 Разделение обязанностей Пересекающиеся обязанности и зоны ответственности должны быть разделены для уменьшения возможности несанкционированного или непреднамеренного изменения или нецелевого использования активов организации
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.1.3 Взаимодействие с органами власти Следует поддерживать контакты с соответствующими органами власти
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.1.4 Взаимодействие с профессиональными сообществами Следует поддерживать соответствующие контакты
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.1.5 Информационная безопасность при управлении проектом При управлении проектами независимо от типа проекта должна приниматься во внимание информационная безопасность

ИСО/МЭК 27002, 6.2 Мобильные устройства и дистанционная работа		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.2.1 Политика использования мобильных устройств Должна быть принята политика и меры по управлению рисками, возникающими при использовании мобильных устройств
	Мера обеспечения ИБ	ИСО/МЭК 27002, 6.2.2 Дистанционная работа Должна быть реализована политика и поддерживающие ее меры для защиты информации, доступ к которой, а также обработка или хранение осуществляется на удаленных рабочих местах

В.2.3 ИСО/МЭК 27002, раздел 7 Безопасность, связанная с персоналом

ИСО/МЭК 27002, 7.1 При приеме на работу		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.1.1 Проверка Проверка кандидатов при приеме на работу должна проводиться в рамках применяемого законодательства, регламентов и этических норм, а также должна быть соразмерна требованиям бизнеса, категории информации, к которой будет предоставлен доступ, и предполагаемым рискам
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.1.2 Правила и условия работы В соглашениях между организацией и работниками, а также между организацией и подрядчиками должна быть прописана ответственность обеих сторон по обеспечению ИБ

ИСО/МЭК 27002, 7.2 Во время работы		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.2.1 Обязанности руководства организации Высшее руководство должно требовать от всех сотрудников и подрядчиков соблюдение мер ИБ в соответствии с установленными в организации политиками и процедурами
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.2.2 Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности Все сотрудники организации и при необходимости подрядчики должны быть соответствующим образом осведомлены и обучены, а также регулярно получать обновленные варианты политик и процедур организации, необходимых для выполнения своих должностных обязанностей

Окончание

ИСО/МЭК 27002, 7.2 Во время работы		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.2.3 Дисциплинарный процесс Должен существовать формализованный и доведенный до персонала дисциплинарный процесс по принятию мер в отношении сотрудников, совершивших нарушение ИБ

ИСО/МЭК 27002, 7.3 Увольнение и смена места работы		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 7.3.1 Прекращение или изменение трудовых обязанностей Ответственность и обязанности в области ИБ, которые остаются в силе после увольнения или смены места работы, должны быть определены, доведены до сведения работника или подрядчика и юридически закреплены

В.2.4 ИСО/МЭК 27002, раздел 8 Менеджмент активов

ИСО/МЭК 27002, 8.1 Ответственность за активы		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.1.1 Инвентаризация активов Информация, активы, связанные с информацией и средствами обработки информации, должны быть идентифицированы, а также должен быть составлен и поддерживаться в актуальном состоянии перечень этих активов
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.1.2 Владение активами У активов, включенных в перечень, должны быть определены владельцы
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.1.3 Допустимое использование активов Правила приемлемого использования информации и активов, связанных с информацией и средствами обработки информации, должны быть идентифицированы, документально оформлены и внедрены
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.1.4 Возврат активов Все сотрудники и внешние пользователи должны возвратить все организационные активы, находящиеся в их распоряжении, по окончании действия их трудовых договоров, контрактов или соглашений

ИСО/МЭК 27002, 8.2 Категорирование информации		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.2.1 Категорирование информации Информация должна быть категорирована с точки зрения требований законодательства, ценности, критичности и чувствительности к несанкционированному раскрытию или изменению
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.2.2 Маркировка информации Должен быть разработан и реализован соответствующий набор процедур маркировки информации в соответствии с принятой в организации системой категорирования информации
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.2.3 Обращение с активами Должны быть разработаны и реализованы процедуры обращения с активами в соответствии с принятой в организации системой категорирования информации

ИСО/МЭК 27002, 8.3 Обращение с носителями информации		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.3.1 Управление съемными носителями информации Должны быть реализованы процедуры по управлению сменными носителями информации в соответствии с принятой в организации системой категорирования информации

Окончание

ИСО/МЭК 27002, 8.3 Обращение с носителями информации			
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.3.2 Утилизация носителей информации Носители информации, в которых больше нет необходимости, должны быть надежным способом утилизированы в соответствии с формальными процедурами	
	Мера обеспечения ИБ	ИСО/МЭК 27002, 8.3.3 Перемещение физических носителей Во время транспортировки носители информации должны быть защищены от несанкционированного доступа, нецелевого использования или повреждения	

В.2.5 ИСО/МЭК 27002, раздел 9 Управление доступом

ИСО/МЭК 27002, 9.1 Требование бизнеса по управлению доступом			
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.1.1 Политика управления доступом Политика управления доступом должна быть разработана, задокументирована и периодически пересматриваться с точки зрения требований бизнеса и ИБ	
	Дополнительная техническая информация о мере обеспечения ИБ	Правила управления доступом должны быть дополнены официальными процедурами с распределением обязанностей. Управление доступом на основе ролей — это подход, успешно используемый многими организациями для связи прав доступа с бизнес-ролями	
1	Стандарт реализации безопасности	Управление доступом может быть реализовано разными способами, включая следующие: - PIM (управление привилегированными учетными записями); - системы электронной блокировки; - услуги охранника; - SIEM (управление информацией о безопасности и событиями безопасности). Примечание — У некоторых из этих способов имеются ограничения. Например, SIEM анализируют и хранят журналы только при использовании того или иного метода контроля доступа. Системы электронной блокировки могут использоваться для контроля физического доступа к ресурсу. PIM может использоваться для управления удостоверениями и соответствующими правами доступа	
	Техническое примечание к стандарту реализации безопасности	Сложность средств контроля доступа повышается с увеличением сложности защищаемого актива, угроз компьютерных атак и последствий успешных атак	
	1.1	Практическое руководство	Убедитесь в том, что к ресурсу имеют доступ только имеющие на это право люди
		Предполагаемые свидетельства	- Журналы доступа; - доступ к механизму контроля доступа
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь в том, что права доступа аннулируются, когда в них отпадает необходимость
		Предполагаемые свидетельства	- Отмененный аккаунт для тестирования; - журналы доступа; - доступ к администрированию пользователей
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Проверьте, можно ли обойти запрос на доступ без привилегированного аккаунта
		Предполагаемые свидетельства	- Журналы доступа; - идентификация без прав доступа; - идентификация с привилегиями для сравнения; - доступ к механизму контроля доступа
		Метод	Тестирование и подтверждение

Продолжение

ИСО/МЭК 27002, 9.1 Требование бизнеса по управлению доступом			
1	1.4	Практическое руководство	Убедитесь в том, что все события доступа отражаются в журналах и могут быть использованы для расследования
		Предполагаемые свидетельства	- Файлы журналов; - бизнес-требования к журналам
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Проверьте, возможно ли повысить привилегии доступа к ресурсам
		Предполагаемые свидетельства	- Журналы доступа; - идентификация без прав доступа; - доступ к механизму контроля доступа
		Метод	Тестирование и подтверждение
	1.6	Практическое руководство	Убедитесь, что невозможно обойти контроль доступа
		Предполагаемые свидетельства	- Журналы доступа; - идентификация без прав доступа; - доступ к механизму контроля доступа
		Метод	Тестирование и подтверждение
	1.7	Практическое руководство	Проверьте права доступа в черном и в белом списках и убедитесь, что ни один ресурс не пропущен
		Предполагаемые свидетельства	- Бизнес-требования; - бизнес-требования контроля доступа; - доступ к интерфейсу контроля доступа
		Метод	Тестирование и подтверждение
	1.8	Практическое руководство	Убедитесь, что невозможно клонировать или воспроизводить токены доступа или выдавать себя за другого
		Предполагаемые свидетельства	- Идентификация без прав доступа; - идентификация с чьими-либо правами доступа; - доступ к механизму контроля доступа
		Метод	Тестирование и подтверждение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.1.2 Доступ к сетям и сетевым службам Пользователям следует предоставлять доступ только к тем сетям и сетевым сервисам, на использование которых они получили конкретное разрешение	
	Дополнительная техническая информация о мере обеспечения ИБ	Несанкционированные и небезопасные подключения к сетевым услугам могут повлиять на всю организацию. Эта мера обеспечения ИБ имеет особое значение для сетевых подключений к конфиденциальным или критически важным бизнес-приложениям или для пользователей, находящихся в местах повышенного риска, например в общедоступных или внешних средах вне пределов зоны ИБ организации	
1	Стандарт реализации безопасности	В отношении использования сетей и сетевых сервисов должна быть сформирована соответствующая политика	

Продолжение

ИСО/МЭК 27002, 9.1 Требование бизнеса по управлению доступом			
	Техническое примечание к стандарту реализации безопасности	Эта политика должна определять: a) сети и сетевые услуги, доступ к которым разрешен; b) процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ; c) меры обеспечения ИБ и процедуры управления для защиты доступа к сетевым соединениям и сетевым услугам; d) средства, используемые для доступа к сетям и сетевым услугам (например, использование VPN или беспроводной сети); e) требования аутентификации пользователя для доступа к различным сетевым сервисам; f) мониторинг использования сетевых сервисов. Политика использования сетевых сервисов должна соответствовать политике управления доступом организации	
	1.1	Практическое руководство	Для определения используемых протоколов из ответов или запросов сетевых сервисов используйте анализ сетевого трафика, если это возможно. Это могут быть, например, протоколы Netbios, ARP, OSPF и т. д.
		Предполагаемые свидетельства	Доступ к сетевому трафику
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь, что широковещательные запросы и ответы ото всех узлов соответствуют сетевым диаграммам и другим документам
		Предполагаемые свидетельства	- Доступ к схемам сети; - доступ к сетевому трафику
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Выявите и идентифицируйте все открытые порты и сервисы в авторизованной сети с помощью сканирования портов. Запросите все сервисные баннеры (флаги) для обнаруженных портов TCP и UDP. Убедитесь, что обнаруженные сервисы обоснованы с учетом привилегий пользователя и системных функций
		Предполагаемые свидетельства	- Доступ к спецификациям системы; - разрешение на сканирование портов в сети
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Проверьте меры предотвращения доступа к услугам в сети или других сетях посредством подмены адресов
		Предполагаемые свидетельства	Имитацию адреса можно выполнить в тестовой или малозначимой среде
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Подсчитайте и идентифицируйте все системы с доступом к другим закрытым сетям посредством нескольких сетевых карт. Попытайтесь использовать такие точки входа, чтобы войти в закрытые сети
		Предполагаемые свидетельства	Полная схема сети

Окончание

ИСО/МЭК 27002, 9.1 Требование бизнеса по управлению доступом			
		Метод	Тестирование и подтверждение
	1.6	Практическое руководство	Подсчитайте и определите все сервисы удаленных рабочих столов, которые можно использовать для получения доступа к системам за пределами авторизованной сети. Попытайтесь получить несанкционированный доступ к закрытым сетям через удаленный рабочий стол
		Предполагаемые свидетельства	- Полная схема сети; - доступные сервисы удаленного рабочего стола, подключенные к системам вне авторизованной сети
		Метод	Тестирование и подтверждение
	1.7	Практическое руководство	Изучите и проверьте правила межсетевого экрана, чтобы убедиться, что сетям и сетевым сервисам предоставляется только предполагаемый доступ
		Предполагаемые свидетельства	- Доступ к правилам межсетевого экрана; - доступ к журналам межсетевого экрана
		Метод	Тестирование и подтверждение

ИСО/МЭК 27002, 9.2 Процесс управления доступом пользователей			
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.1 Регистрация и отмена регистрации пользователей Должен быть внедрен формализованный процесс регистрации и снятия с учета пользователей, обеспечивающий возможность назначения прав доступа	
	Дополнительная техническая информация о мере обеспечения ИБ	Для определения, ограничения и контроля привилегированного доступа пользователей к сетям, сервисам и ресурсам должны использоваться официальные процедуры	
1	Стандарт реализации безопасности	Должны быть документированы и реализованы следующие процессы: - регистрация и снятие с учета пользователей; - предоставление доступа пользователям; - управление привилегированными правами доступа; - управление секретной аутентификационной информацией пользователей; - пересмотр прав доступа пользователей; - аннулирование или изменение прав доступа	
	Техническое примечание к стандарту реализации безопасности	Предоставление привилегированных прав доступа должно контролироваться в рамках официального процесса в соответствии с положениями политики контроля доступа	
	1.1	Практическое руководство	Убедитесь в том, что идентификаторы всех пользователей уникальны и персонифицированы. Проведите выборочную оценку, чтобы убедиться в том, что учетные записи бывших сотрудников не активны. Убедитесь в отсутствии идентификаторов пользователей, не используемых в течение слишком длительного периода времени
		Предполагаемые свидетельства	- Доступ к администрированию пользователей; - доступ к списку бывших сотрудников или их идентификаторов
		Метод	Тестирование и подтверждение

Продолжение

ИСО/МЭК 27002, 9.2 Процесс управления доступом пользователей			
	1.2	Практическое руководство	Убедитесь в том, что сложность паролей достаточна, чтобы сделать их угадывание проблематичным, а также что имя пользователя не является общедоступной информацией (например, электронным адресом или номером социального страхования)
		Предполагаемые свидетельства	- Доступ к политике паролей; - авторизация по имени пользователя и паролю
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Убедитесь в том, что пользователю предлагается ответить на секретный вопрос или предоставить секретный ответ, или предоставить иную заранее определенную информацию для сброса паролей
		Предполагаемые свидетельства	- Доступ к политике паролей; - авторизация по имени пользователя и паролю; - доступ к функции сброса пароля; - авторизованная тестовая учетная запись
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Убедитесь в том, что в случае неправильного ввода пароля определенное количество раз учетная запись пользователя блокируется на определенный период времени
		Предполагаемые свидетельства	- Авторизованная тестовая учетная запись; - авторизация по имени пользователя и паролю
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Подсчитайте количество случаев использования учетных записей по умолчанию для целевых точек. Протестируйте возможность входа через точки аутентификации с использованием наиболее подходящих и известных методов взлома
		Предполагаемые свидетельства	Авторизация по имени пользователя и паролю
		Метод	Тестирование и подтверждение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.2 Предоставление пользователю права доступа Должен быть реализован формализованный процесс назначения или отмены прав доступа пользователей к системам и сервисам	
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.3 Управление привилегированными правами доступа Назначение и применение привилегированных прав доступа должно быть ограниченным и контролируемым	
	Дополнительная техническая информация	Управление привилегиями имеет большое значение, поскольку ненадлежащее их использование оказывает существенное воздействие на системы. Статус предоставляемых привилегий должен быть описан в документах, содержащих описание привилегий. Это необходимо, поскольку различны привилегии доступа, связанные с каждым системным продуктом (операционной системой, системой управления базами данных и каждым приложением). В качестве примеров типов привилегий можно перечислить: - root (UNIX, Linux); - администратор (Windows); - оператор архива (Windows);	

Продолжение

ИСО/МЭК 27002, 9.2 Процесс управления доступом пользователей			
		- суперпользователь (Windows); - системный администратор (СУБД); - администратор баз данных (СУБД). Привилегии должны предоставляться по минимальному принципу, исходя из насущных потребностей. Кроме того, привилегии не должны предоставляться на постоянной основе. В разных системах используются различные методы управления привилегиями. В качестве примеров управления привилегиями в системах можно привести: - в операционных системах привилегии определяются с помощью ACL (список прав доступа); - в СУБД задаются разнообразные стандартные привилегии; - в приложениях могут существовать разнообразные привилегии по умолчанию для функций управления приложениями, поэтому аудиторам ИБ следует определиться с уровнем оценки заранее; - в Secure OS имеется функция обязательного контроля доступа	
1	Стандарт реализации безопасности	Права доступа, связанные с каждым системным продуктом, например, операционная система, система управления базами данных и каждое приложение, а также пользователи, которым они должны быть предоставлены	
	Техническое примечание к стандарту реализации безопасности	Активность привилегированных пользователей должна контролироваться, поскольку неправильное использование привилегий оказывает значительное воздействие на системы. Методы обнаружения ненадлежащего использования привилегий различны для систем разных архитектур. Примечание — Типичными архитектурами системы являются: - мэйнфрейм; - Windows; - UNIX, Linux; - Secure OS	
	1.1	Практическое руководство	Убедитесь в том, что порядок предоставления привилегий изложен в документе их описания
		Предполагаемые свидетельства	Документ с описанием привилегий
		Метод	Анализ/Наблюдение
	1.2	Практическое руководство	Убедитесь в том, что настройки конфигурации систем соответствуют документу с описанием привилегий. Метод оценки использования привилегий зависит от системной архитектуры. Примеры методов оценки использования привилегий. 1) Мейнфрейм — оценка использования привилегий производится по отчету RACF. 2) UNIX, Linux или Windows — оценка использования привилегий производится путем изучения журналов. Примечания 1 RACF (средства управления доступом к ресурсам) представляет собой встроенное программное обеспечение мейнфрейма для управления безопасностью. 2 В операционных системах UNIX или Linux недостаточно ограничиваться только входом с помощью учетной записи root для оценки правомерности ее использования. Причина заключается в том, что обычный пользователь после входа в систему UNIX или Linux может получить привилегии root с помощью команды «su»

Окончание

ИСО/МЭК 27002, 9.2 Процесс управления доступом пользователей			
		Предполагаемые свидетельства	- Документ с описанием привилегий; - ACL (список прав доступа); - Отчет RACF
		Метод	Анализ/Наблюдение
2	Стандарт реализации безопасности	Привилегии должны предоставляться идентификаторам пользователей, отличных от тех, которые используются в повседневной работе	
	Техническое примечание к стандарту реализации безопасности	При привилегированном доступе существует возможность неправомерного использования. Поэтому использование привилегий на регулярной основе повышает вероятность несанкционированного доступа. При отсутствии необходимости в привилегиях пользователи должны использовать свои обычные идентификаторы. Если разрешен вход с правами root, то по журналу невозможно определить, кто именно входил в систему	
	2.1	Практическое руководство	Проверьте ACL-списки систем на наличие у пользователей обычного идентификатора наряду с привилегированным
		Предполагаемые свидетельства	Список прав доступа
		Метод	Анализ/Наблюдение
	2.2	Практическое руководство	Проверьте журнал и убедитесь в том, что для повседневной работы пользователь использует другой идентификатор пользователя. В системах UNIX или Linux следует убедиться в том, что конфигурация системы не дает возможности входа в систему с учетной записью root. Примечание — Если данные журналов показывают, что пользователь с привилегиями использует только свой привилегированный идентификатор, аудиторам ИБ необходимо провести интервью и выяснить возможность использования для повседневных задач непривилегированного идентификатора пользователя
		Предполагаемые свидетельства	- Файл журнала; - конфигурация системы для входа с учетной записью root
		Метод	Анализ/Наблюдение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.4 Процесс управления секретной аутентификационной информацией пользователей Предоставление секретной аутентификационной информации должно быть контролируемо посредством формального процесса управления	
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.5 Пересмотр прав доступа пользователей Владельцы активов должны регулярно пересматривать права доступа	
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.2.6 Аннулирование или корректировка прав доступа Права доступа к информации и средствам обработки информации всех сотрудников и внешних пользователей должны быть аннулированы по окончании действия их трудовых договоров, контрактов или соглашений или скорректированы при изменении	

ИСО/МЭК 27002, 9.3 Ответственность пользователей			
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.3.1 Использование секретной аутентификационной информации Пользователи должны соблюдать правила организации при использовании секретной аутентификационной информации	
	Дополнительная техническая информация о мере обеспечения ИБ	Секретными данными аутентификации могут быть полученные непосредственно биометрические данные пользователя, данные, полученные с помощью интеллектуальной карты[1)], и пароли. При использовании всех этих трех методов требуется техническая оценка управления паролями пользователей. Во избежание несанкционированного доступа к ресурсам компьютера, пароль должен быть создан и храниться в тайне ото всех, кому не разрешен доступ. Аутентификация по паролю используется многими ресурсами, такими как операционные системы, программы, базы данных, сети или веб-сайты. Качество паролей зависит от их длины и типа используемых символов, например буквенно-цифровых и специальных символов. В некоторых операционных системах, таких как Windows, пользователи могут настраивать параметры политики паролей. С другой стороны, разработчики приложений могут создать функцию аутентификации для конфигурирования политики паролей. Аудиторам следует проверить наличие и эффективность функций авторизации с помощью паролей, поддерживаемых компьютерными ресурсами	
	Стандарт реализации безопасности	Выбирайте качественные пароли с достаточным количеством символов, отвечающие следующим критериям: 1) легкость запоминания; 2) отсутствие в пароле каких-либо элементов, которые могут быть легко угаданы или получены посторонними, исходя из личной информации пользователя, например, имен, телефонных номеров, дат рождения и т. п.; 3) неподверженность словарным атакам (т. е. пароль не должен содержать слов, включенных в словари); 4) отсутствие последовательных идентичных символов, не должен состоять только из цифр или только из букв; 5) отличие от ранее использовавшихся паролей (с учетом n поколений)	
	Техническое примечание к стандарту реализации безопасности	Пароли, которые другой пользователь может легко запомнить, по сути, уязвимы	
1	1.1	Практическое руководство	Убедитесь в том, что правила выбора паролей отражены в политике паролей организации
		Предполагаемые свидетельства	Политика паролей организации
		Метод	Оценка
	1.2	Практическое руководство	Убедитесь в том, что настройки конфигурации системы (системная политика паролей) отражены в политике паролей организации
		Предполагаемые свидетельства	- Конфигурация системы (системная политика паролей); - политика паролей организации
		Метод	Анализ/Наблюдение
	1.3	Практическое руководство	Убедитесь в том, что в файле журнала отражены изменения паролей пользователями
		Предполагаемые свидетельства	Файл журнала
		Метод	Анализ/Наблюдение

[1)] Интеллектуальная или смарт-карта — это пластиковая карта со встроенной микросхемой. Назначение таких карт — одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

ИСО/МЭК 27002, 9.4 Управление доступом к системам и приложениям		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.4.1 Ограничение доступа к информации Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой управления доступом
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.4.2 Безопасные процедуры входа в систему Там, где это требует политика управления доступом, доступ к системам и приложениям должен осуществляться с помощью безопасной процедуры входа в систему
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.4.3 Система управления паролями Система управления паролями должна быть интерактивной и обеспечивать необходимое качество паролей
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.4.4 Использование привилегированных служебных программ Использование утилит, способных обойти меры обеспечения ИБ систем и прикладных программ, следует ограничить и строго контролировать
	Мера обеспечения ИБ	ИСО/МЭК 27002, 9.4.5 Управление доступом к исходному коду программы Доступ к файлам конфигураций программ должен быть ограничен, а сам файл конфигураций должен храниться в зашифрованном виде

В.2.6 ИСО/МЭК 27002, раздел 10 Криптография

ИСО/МЭК 27002, 10.1 Средства криптографической защиты информации		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 10.1.1 Политика использования средств криптографической защиты информации Должна быть разработана и внедрена политика использования средств криптографической защиты информации
	Дополнительная техническая информация о мере обеспечения ИБ	Криптография — это инструмент для защиты информации в вычислительных системах и коммуникациях. Криптографические системы являются неотъемлемой частью стандартных протоколов, прежде всего протокола безопасности транспортного уровня TLS, что позволяет легко включать надежное шифрование в широкий спектр приложений. Эти средства криптографической защиты могут использоваться для достижения различных целей ИБ, включая: 1) конфиденциальность: использование шифрования информации для защиты конфиденциальной или критической информации, хранящейся или передаваемой; 2) целостность: криптографические хеш-функции могут использоваться для проверки целостности информации; 3) аутентификация: криптографические протоколы могут использоваться для аутентификации пользователей и систем, запрашивающих доступ к ресурсу; 4) подлинность: неотказуемость сообщений или информации может быть достигнута с использованием криптографических методов, таких как алгоритмы подписи. Для защиты информации следует определить, какие угрозы ИБ следует предотвращать с помощью криптографии
1	Стандарт реализации безопасности	В алгоритмы шифрования заложен определенный уровень сложности, что затрудняет широкое использование средств криптографической защиты информации. При реализации средств криптографической защиты необходимо: 1) использовать ключи достаточной длины; 2) использовать протоколы, которые считаются сильными; 3) использовать криптографические алгоритмы, которые считаются надежными; 4) использовать реализации, которые проверены и известны как безопасные; 5) постоянно оценивать эффективность

Окончание

ИСО/МЭК 27002, 10.1 Средства криптографической защиты информации			
	Техническое примечание к стандарту реализации безопасности	Внедрение средств криптографической защиты информации должно осуществляться с использованием надежных и проверенных алгоритмов и реализаций. Не рекомендуется использовать собственные криптографические алгоритмы и реализации	
	1.1	Практическое руководство	Убедитесь, что сетевые сервисы с реализованными средствами криптографической защиты информации обеспечивают достаточную длину ключа и не используют слабые алгоритмы
		Предполагаемые свидетельства	- Стандартные криптографические методы; - доступ к зашифрованным сервисам
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь, что используемые средства криптографической защиты информации считаются надежными
		Предполагаемые свидетельства	- Реализация средств криптографической защиты информации; - механизм контроля используемых версий реализации
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Убедитесь, что мобильные устройства и устройства со съемными носителями защищены криптографическими средствами контроля с использованием надежных алгоритмов и достаточной длины ключа
		Предполагаемые свидетельства	- Стандартные криптографические методы; - доступ к мобильным устройствам со съемными носителями
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Убедитесь, что все криптографические ключи хранятся в надежном и безопасном месте и могут быть доступны только уполномоченным лицам
		Предполагаемые свидетельства	- Методы контроля доступа для криптографических ключей; - процесс хранения криптографических ключей
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Убедитесь в том, что ключи сервисов связи с реализованными средствами криптографической защиты имеют достаточную длину и что в их работе используются надежные алгоритмы
		Предполагаемые свидетельства	- Стандартные методы шифрования; - доступ к сервисам с шифрованием; - доступ к зашифрованным данным связи (например, сертификатам)
		Метод	Тестирование и подтверждение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 10.1.2 Управление ключами Необходимо разработать и внедрить политику по использованию, защите и управлению жизненным циклом криптографических ключей	

В.2.7 ИСО/МЭК 27002, раздел 11 Физическая безопасность и защита от воздействия окружающей среды

ИСО/МЭК 27002, 11.1 Зоны безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.1 Физический периметр безопасности Должны быть определены и использованы периметры безопасности для защиты зон, содержащих чувствительную или критически важную информацию и средства ее обработки
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.2 Меры и средства контроля и управления физическим доступом Безопасные зоны должны быть защищены соответствующими средствами контроля доступа, чтобы обеспечить доступ только авторизованному персоналу
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.3 Безопасность зданий, помещений и оборудования Должна быть разработана и реализована физическая защита зданий, помещений и оборудования
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.4 Защита от внешних угроз и угроз со стороны окружающей среды Должна быть разработана и реализована физическая защита зданий, помещений и оборудования от стихийных бедствий, злонамеренных атак или несчастных случаев
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.5 Работа в зонах безопасности Должны быть разработаны и применены процедуры для работы в безопасных зонах
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.1.6 Зоны погрузки и разгрузки Зоны погрузки и разгрузки и другие места, в которых могут находиться посторонние лица, должны контролироваться и по возможности изолироваться от средств обработки информации во избежание несанкционированного доступа

ИСО/МЭК 27002, 11.2 Оборудование		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.1 Размещение и защита оборудования Оборудование должно быть размещено и защищено таким образом, чтобы снизить риски ИБ от угроз и опасностей со стороны окружающей среды и возможности несанкционированного доступа
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.2 Вспомогательные услуги Оборудование должно быть защищено от сбоев электропитания и других сбоев, вызванных отказами в предоставлении вспомогательных услуг
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.3 Безопасность кабельной сети Силовые и телекоммуникационные кабели, используемые для передачи данных или для поддержки информационных услуг, должны быть защищены от перехвата информации, помех или повреждения
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.4 Техническое обслуживание оборудования Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.5 Перемещение активов Оборудование, информация или программное обеспечение не должны выноситься за пределы организации без предварительного разрешения
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.6 Безопасность оборудования и активов вне помещений организации При обеспечении безопасности активов, используемых вне помещений организации, следует принимать во внимание различные риски, связанные с работой вне помещений организации

Окончание

ИСО/МЭК 27002, 11.2 Оборудование		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.7 Безопасная утилизация или повторное использование оборудования Все элементы оборудования, содержащие устройства хранения данных, должны быть проверены, чтобы гарантировать, что любые чувствительные данные и лицензионное программное обеспечение были удалены или надежно перезаписаны перед утилизацией или повторным использованием
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.8 Оборудование, оставленное пользователем без присмотра Пользователи должны гарантировать, что оставленное без присмотра оборудование надлежащим образом защищено
	Мера обеспечения ИБ	ИСО/МЭК 27002, 11.2.9 Политика «чистого стола» и «чистого экрана» Должна быть установлена политика «чистого стола» для бумаг и съемных носителей и политика «чистого экрана» для средств обработки информации

В.2.8 ИСО/МЭК 27002, раздел 12 Безопасность при эксплуатации

ИСО/МЭК 27002, 12.1 Эксплуатационные процедуры и обязанности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.1.1 Документально оформленные эксплуатационные процедуры Эксплуатационные процедуры должны быть документированы и доступны всем нуждающимся в них пользователям
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.1.2 Процесс управления изменениями Изменения в организации, бизнес-процессах, средствах обработки информации и системах, которые влияют на информационную безопасность, должны быть управляемыми
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.1.3 Управление производительностью Необходимо осуществлять мониторинг, регулирование и прогнозирование (исходя из требований к производительности в будущем) использования ресурсов для обеспечения требуемой производительности системы
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.1.4 Разделение сред разработки, тестирования и эксплуатации Для снижения рисков несанкционированного доступа или изменений среды эксплуатации необходимо обеспечивать разделение сред разработки, тестирования и эксплуатации. В средах разработки и тестирования необходимо использовать обезличенные данные для снижения рисков, связанных со ссылками на реальные рабочие данные

ИСО/МЭК 27002, 12.2 Защита от вредоносных программ		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.2.1 Меры и средства информационной безопасности в отношении вредоносных программ Для защиты от вредоносных программ должны быть реализованы меры обеспечения ИБ по обнаружению, предотвращению и восстановлению, в сочетании с соответствующим информированием пользователей
	Дополнительная техническая информация	Вредоносное программное обеспечение — общий термин, используемый для обозначения кода (включая программное обеспечение, программы, скрипты), созданного для нанесения вреда компьютерной системе путем хищения информации, мошеннических или шпионских действий. При внедрении вредоносного программного обеспечения в компьютерную систему возникает угроза ее повреждения либо кражи хранящейся в ней информации. Одним из вариантов действия вредоносного ПО является повреждение других систем. В разряд вредоносного программного обеспечения входят вирусы, компьютерные черви, троянские кони, боты, шпионское ПО, недобросовестная реклама, а также прочие виды вредоносного и нежелательного программного обеспечения.

Продолжение

ИСО/МЭК 27002, 12.2 Защита от вредоносных программ			
		При условии подключения сети организации к интернету аудиторы ИБ должны проверить, что функции обнаружения / нейтрализации вредоносных программ размещены на границе интернета всесторонне и эффективно, и эти функции работают надлежащим образом. В частности, для оценки надлежащей работы функций по выявлению и/или нейтрализации вредоносного ПО аудиторам ИБ необходимо убедиться в своевременном обновлении файлов шаблонов или сигнатур, используемых для обнаружения вредоносных программ. Некоторые системы для обнаружения / нейтрализации вредоносного ПО используют файлы шаблонов или сигнатур, а другие выявляют аномальную работу компьютерной системы без помощи таковых. Поскольку существуют различные схемы подключения к интернету, такие как подключение сети организации к интернету через шлюз или прямое подключение каждого ПК к интернету, аудиторы ИБ должны убедиться, что система обнаружения/нейтрализации работает надлежащим образом в каждом случае. Примечание — Аудиторы ИБ должны иметь в виду, что возможности систем обнаружения/нейтрализации для неизвестных вредоносных программ, таких как атака «нулевого дня», ограничены
1	Стандарт реализации безопасности	Должны проводиться установка и регулярное обновление программного обеспечения обнаружения вредоносных программ и восстановления систем для эффективного сканирования компьютеров и носителей данных в качестве меры предосторожности или на регулярной основе. Сканирование должно включать: 1) проверку всех файлов на электронных или оптических носителях, а также всех получаемых по сети файлов перед их использованием; 2) проверку вложений в электронных письмах и загружаемых файлов перед их использованием. Проверка должна выполняться в разных точках, например, на серверах электронной почты, на настольных компьютерах и при попадании в сеть организации; 3) проверку веб-страниц	
	Техническое примечание к стандарту реализации безопасности	В шлюзе, который является входом в сеть организации, система выявления и нейтрализации вредоносного ПО должна выполнять свои функции для определенного набора сервисов и сетевых протоколов, таких как WWW, почта и FTP	
	1.1		К пунктам 1), 2) и 3) вышеуказанного стандарта реализации безопасности применимы следующие практические рекомендации: 1) Убедитесь путем анализа спецификации систем или схем сетей, что система обнаружения вредоносного кода и восстановления размещена эффективно и всеобъемлюще для любых файлов на электронных или оптических носителях, а также для файлов, полученных по сети. Аудиторы ИБ должны проверить, что система обнаружения/предотвращения размещена всеобъемлюще и эффективно, анализируя спецификацию системы или схемы сети. 2) Убедитесь путем анализа спецификации систем или схем сетей, что система обнаружения вредоносного кода и восстановления размещена эффективно и всеобъемлюще для любых вложений и загрузок электронной почты, включая серверы электронной почты, настольные компьютеры и шлюз. В спецификации системы система обнаружения вредоносного кода и восстановления может быть представлена как установленная на выделенном устройстве. Однако аудиторы ИБ отмечают, что она может также размещаться на серверах, которые предназначены для обеспечения некоторых других функций/сервисов (WWW, почта и FTP), и, таким образом, может быть представлена в спецификации системы без отдельного четкого описания.

Продолжение

ИСО/МЭК 27002, 12.2 Защита от вредоносных программ			
			Что касается настольных ПК, аудиторы ИБ отмечают, что система обнаружения вредоносного кода и восстановления зачастую представлена в спецификации системы без отдельного четкого описания. 3) Убедитесь путем анализа спецификации систем или схем сетей, которые включают веб-сервер, что система обнаружения вредоносного кода и восстановления размещена эффективно и всеобъемлюще для веб-страниц. Аудиторы по ИБ отмечают, что система обнаружения и восстановления зачастую представлена в спецификации системы без отдельного четкого описания. В таких случаях, как правило, средства обнаружения вредоносного ПО и восстановления системы бывают встроены в браузер. Для веб-сервера средства обнаружения вредоносного ПО и восстановления систем иногда четко описываются в спецификации системы отдельно, однако аудиторы ИБ отмечают, что часто они также размещаются на веб-серверах без четкого описания в спецификации системы
		Предполагаемые свидетельства	- Договорные документы; - проект архитектуры сетевых сервисов; - спецификация системы; - схема сети
		Метод	Анализ/Оценка
	1.2	Практическое руководство	1) Убедитесь путем наблюдения за средствами обработки информации, что система обнаружения вредоносных программ и восстановления работает надлежащим образом для проверки любых файлов на электронном или оптическом носителе, а также файлов, полученных по сети. Проверьте, правильно ли работает управляющее программное обеспечение в интегрированной системе в условиях, когда система обнаружения вредоносных программ и восстановления управляется в интегрированной среде. 2) Путем наблюдения за средствами обработки информации убедитесь, что система обнаружения вредоносных программ и восстановления установлена и работает надлежащим образом для обнаружения любых вложений и загрузок электронной почты на серверах электронной почты, на настольных компьютерах и в шлюзе. Для электронной почты убедитесь, что система обнаружения работает не только с вложенными файлами, но и с вредоносными вставками в тело писем в формате html. 3) Убедитесь путем наблюдения за средствами обработки информации, что система обнаружения вредоносных программ и восстановления работает надлежащим образом для веб-страниц. Для настольных ПК, которые используются для навигации или просмотра веб-страниц, убедитесь, что система обнаружения работает для несанкционированного управления Active X, сценариев и т. д. Для веб-сервера убедитесь, что система обнаружения работает не только для html-файлов, но и для вредоносных программ в веб-сервисах, таких как apache, IIS и т. д.

Продолжение

ИСО/МЭК 27002, 12.2 Защита от вредоносных программ			
		Предполагаемые свидетельства	Размещение средств обнаружения вредоносных программ и восстановления системы возможно на следующих системах (примеры): - файловый сервер; - сервер электронной почты; - отдельные настольные ПК; - переносные компьютеры; - отдельные средства обнаружения вредоносного ПО и восстановления систем в шлюзе (на границе между сетью организации и интернетом); - веб-сервер; - прокси-сервер; - веб-браузер; - прочее (устройства для блокирования физического подключения USB)
		Метод	Оценка/Наблюдение
	1.3	Практическое руководство	Соберите файлы журналов системы обнаружения и восстановления и убедитесь, что записи журналов показывают, что система работала и при обнаружении вредоносного ПО необходимые действия предпринимаются. Загрузив тестовый вирус EICAR, убедитесь, что для веб-страниц система обнаружения вредоносного ПО и восстановления работает полностью и эффективно. Примечание — Для настольных ПК журналы системы обнаружения и восстановления обычно хранятся на ПК. Для серверов и внешних устройств эти журналы иногда передаются посредством протокола передачи, такого как syslog, и хранятся в других системах. Для настольных ПК, которые используются для навигации или просмотра веб-страниц, функция обнаружения в веб-браузере может не создавать записи журналов, свидетельствующих, что эта функция была запущена. Но большая часть браузеров выдает сообщение при обнаружении неавторизованных скриптов
		Предполагаемые свидетельства	- Используемая система обнаружения; - файлы журналов системы обнаружения; - оповещения системы обнаружения; - сообщения системы обнаружения в веб-браузере; - веб-сервер с функцией загрузки файлов в веб-браузер
		Метод	- Анализ/Наблюдение; - тестирование и подтверждение
2	Стандарт реализации безопасности	Программное обеспечение для обнаружения вредоносного ПО и восстановления системы, используемое для сканирования компьютеров и носителей данных в качестве меры предосторожности, должно обновляться регулярно или в рамках определенной процедуры	
	Техническое примечание к стандарту реализации безопасности	В большинстве случаев имеются функции для автоматического обновления файлов шаблонов или сигнатур	
	2.1		Проверка настроек программного обеспечения для обнаружения и восстановления системы на наличие автоматического обновления файлов шаблонов или сигнатур или их регулярного обновления

Окончание

ИСО/МЭК 27002, 12.2 Защита от вредоносных программ			
		Предполагаемые свидетельства	Проект или спецификация системы обнаружения
		Метод	Проверка/Оценка
	2.2	Практическое руководство	Проверьте настройки программного обеспечения для обнаружения и восстановления системы на наличие автоматического обновления файлов шаблонов или сигнатур или их регулярного обновления
		Предполагаемые свидетельства	Настройки системы обнаружения
		Метод	Проверка/Наблюдение
	2.3	Практическое руководство	Убедитесь в том, что файлы шаблонов или сигнатур обновляются, сравнивая наименование продукта, версию и журнал обновлений файлов шаблонов или сигнатур. Примечание — Наименование и версию продукта для обнаружения вредоносного ПО и восстановления системы можно найти в файле справки продукта
		Предполагаемые свидетельства	Информация о системе обнаружения и нейтрализации вредоносного ПО, а именно: - наименование продукта; - версия продукта; - версия файла структуры или подписи
		Метод	Проверка/Наблюдение

ИСО/МЭК 27002, 12.3 Резервное копирование		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.3.1 Резервное копирование информации Следует регулярно создавать и проверять резервные копии информации, программного обеспечения и образов систем в соответствии с установленной политикой резервного копирования
	Дополнительная техническая информация о мере обеспечения ИБ	Чтобы выполнять резервное копирование надлежащим образом, необходимо определить стандарт организации в соответствии с политикой резервного копирования и отразить это в проектном документе по резервному копированию. Резервные копии используются для восстановления важной информации или программного обеспечения в случае события потери данных, такого как сбой или порча носителя информации. При разработке проекта резервного копирования в соответствии с политикой резервного копирования организация должна выбрать подходящее место хранения резервных копий, способ выполнения резервных копий и метод резервного копирования. С точки зрения места хранения резервных копий организация должна выбрать локальный или внешний вариант хранения резервных копий. Считается, что хранение копий на месте требует существенно меньших затрат времени на резервное копирование и восстановление. Хранение резервных копий вне площадки часто выбирается для того, чтобы предотвратить последствия локальных бедствий, таких как пожары, наводнения или землетрясения. Способ выполнения резервной копии может быть либо «онлайн», когда резервное копирование осуществляется через сеть или другой соответствующий канал связи, либо «офлайн». При резервном копировании «офлайн» резервные копии физически транспортируются на съемных носителях, таких как магнитные ленты, CD или DVD-диски. Кроме того, резервное копирование может выполняться различными методами резервного копирования: полное, инкрементное и дифференциальное.

Продолжение

ИСО/МЭК 27002, 12.3 Резервное копирование			
		При полном резервном копировании создается копия всех выбранных данных. Для этого требуется больше времени и места для данных по сравнению с другими методами, однако последующее восстановление данных будет самым простым и самым легким. Инкрементное резервное копирование означает создание резервных копий только тех данных, которые изменились с момента последнего резервного копирования. Это потребует меньше времени и емкости данных по сравнению с другими методами, но это наиболее сложный метод для восстановления. Дифференциальное резервное копирование подразумевает создание копии только тех данных, которые были изменены с момента последнего полного резервного копирования. Такой способ резервного копирования потребует меньше времени и информационной емкости, чем полное копирование, и последующее восстановление данных будет более простым по сравнению с инкрементным резервным копированием	
1	Стандарт реализации безопасности	Степень (т. е. полное или дифференциальное резервное копирование) и регулярность создания резервных копий должны отражать существующие в организации требования, требования к безопасности копируемых данных, а также степень важности копируемых данных для непрерывной работы организации	
	Техническое примечание к стандарту реализации безопасности	Организация в соответствии со своими требованиями должна выбрать надлежащую периодичность создания резервных копий и/или восстановления данных, а также определить объем копируемых данных. Аудиторам следует оценить уместность выбранного метода копирования с учетом существующих бизнес-требований. В качестве примера можно привести следующие варианты регулярного резервного копирования: - зеркальное отображение или репликация в режиме реального времени (наивысший уровень важности информации); - ежедневное копирование (при необходимости восстановления данных, как минимум, за день); - еженедельное копирование; - ежемесячное копирование	
	1.1	Практическое руководство	Убедитесь в том, что процедура резервного копирования запланирована в соответствии со стандартом реализации безопасности
		Предполагаемые свидетельства	- Спецификация резервного копирования; - документ, определяющий бизнес; - требования и требования безопасности; - план резервного копирования
		Метод	Проверка/Оценка
	1.2	Практическое руководство	Убедитесь в том, что настройки файлов конфигурации системы для резервного копирования соответствуют его описанию в плане
		Предполагаемые свидетельства	- План резервного копирования; - файлы конфигурации системы резервного копирования
		Метод	Проверка/Оценка
	1.3	Практическое руководство	Убедитесь в том, что резервное копирование осуществлено в соответствии с планом резервного копирования.
		Предполагаемые свидетельства	- План резервного копирования; - файлы журналов; - носители резервного копирования
		Метод	Проверка/наблюдение

Окончание

ИСО/МЭК 27002, 12.3 Резервное копирование			
	1.4	Практическое руководство	Убедитесь в том, что резервные копии хранятся в безопасном, изолированном помещении достаточных размеров
		Предполагаемые свидетельства	Спецификация места для хранения резервных копий
		Метод	Проверка/Оценка
2	Стандарт реализации безопасности	Процедуры восстановления следует регулярно проверять и тестировать, чтобы убедиться в их эффективности и в том, что они могут быть выполнены в течение времени, отведенного в оперативных процедурах для восстановления	
	Техническое примечание к стандарту реализации безопасности	Сложность и длительность восстановления данных зависит от применяемого метода, например, полное или дифференциальное копирование. Необходимо подготовить и отразить в документации план тестирования и проверки процедур восстановления данных	
	2.1	Практическое руководство	Убедитесь в том, что план тестирования и само тестирование проверяются регулярно
		Предполагаемые свидетельства	Записи о проверке плана и тестировании процедур восстановления данных
		Метод	Проверка/Оценка
	2.2	Практическое руководство	Проверьте, регулярно ли тестировался план тестирования и проверки, чтобы убедиться, что запланированные меры эффективны и могут быть выполнены в течение времени, отведенного в оперативных процедурах восстановления
		Предполагаемые свидетельства	- Записи о проведении тестирования процедуры восстановления; - план тестирования и проверки
		Метод	Проверка/Оценка

ИСО/МЭК 27002, 12.4 Регистрация и мониторинг		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.4.1 Регистрация событий Необходимо обеспечивать формирование, ведение и регулярный анализ журналов событий, фиксирующих действия пользователей, нештатные ситуации, ошибки и события ИБ
	Дополнительная техническая информация о мере обеспечения ИБ	Для выявления несанкционированной обработки данных важно вести журналы аудита, с помощью которых можно отследить действия пользователей, операторов системы, события безопасности и работу систем. Для обнаружения несанкционированных действий по обработке информации важно вести журналы аудита, которые используются для отслеживания действий пользователей, системных операторов, событий безопасности и систем. Чтобы обеспечить возможность анализа несанкционированных действий и событий безопасности, в журналах аудита должна содержаться следующая информация: - идентификаторы пользователя; - дата и время; - ключевые события, такие как вход и выход из системы; - идентификатор терминала; - сетевой адрес и протоколы. Для формирования необходимых записей, включающих вышеперечисленные данные, требуется, чтобы оборудование, которое записывает информацию в журналы, было соответствующим образом настроено. Технология ведения журнала зависит от структуры системы, архитектуры и используемых приложений.

Продолжение

ИСО/МЭК 27002, 12.4 Регистрация и мониторинг			
		Аудиторы ИБ должны учитывать различия в технологии ведения журналов для разных архитектур систем, таких как серверы и ПК. Примечание — Примерами возможных структур системы являются: - система клиент-сервер; - веб-система; - система тонких клиентов; - виртуализация; - использование ASP (поставщик сервисов приложений), SaaS (программное обеспечение как услуга) или облачных услуг. Примерами системных архитектур являются: - UNIX, Linux; - Windows; - Мэйнфрейм. Примерами типов журналов являются: - системный журнал; - журнал приложения	
1	Стандарт реализации безопасности	Необходимо обеспечить формирование журналов аудита, где фиксируются действия пользователей, исключения, а также события ИБ. По возможности журналы аудита должны содержать следующую информацию: a) идентификаторы пользователей; b) даты, время и детали ключевых событий, например входа в систему и выхода из нее; c) идентификаторы терминалов и по возможности их местонахождение; d) записи об успешных и неудачных попытках входа в систему; e) записи об успешных и неудачных попытках доступа к данным и другим ресурсам; f) изменения конфигурации системы; g) использование системных утилит и приложений; h) файлы, к которым осуществлялся доступ, и тип доступа; i) сетевые адреса и протоколы; j) аварийные оповещения системы контроля доступа; k) включение и выключение систем защиты, таких как антивирусные системы и системы обнаружения вторжений	
	Техническое примечание к стандарту реализации безопасности	Соответствующие меры защиты конфиденциальности должны быть приняты. По возможности системные администраторы не должны иметь разрешения на удаление или деактивацию журналов своих действий	
	1.1	Практическое руководство	Убедитесь в том, что процедура ведения журналов спроектирована в соответствии со стандартом реализации безопасности
		Предполагаемые свидетельства	- Спецификация; - документ с описанием требований; - проектная документация программного обеспечения
		Метод	Проверка/Оценка
	1.2	Практическое руководство	Убедитесь в том, что настройки файлов конфигурации системы для ведения журналов соответствуют описанию в проектной документации программного обеспечения
		Предполагаемые свидетельства	- Проектная документация программного обеспечения; - файл конфигурации системы
		Метод	Проверка/Оценка
	1.3	Практическое руководство	Убедитесь в том, что данные фактических файлов создаваемых журналов аудита соответствуют проектной документации системы.

Продолжение

ИСО/МЭК 27002, 12.4 Регистрация и мониторинг			
			Примечание — Некоторые записи в журналах аудита появляются постоянно, а некоторые — в зависимости от ситуации, например, данные об ошибках. Чтобы проверить, ведет ли система учет событий, появляющихся в зависимости от ситуации, от аудиторов ИБ могут потребоваться различные меры, такие как создание контрольного примера, проверка проектной документации системы
		Предполагаемые свидетельства	Файл журнала
		Метод	Проверка/Наблюдение
	1.4	Практическое руководство	В конкретных случаях длительность хранения журналов аудита определяется коммерческой целесообразностью, условиями договора или законодательными и/или нормативными требованиями. Например, журналы аудита с аварийными оповещениями, создаваемыми системой контроля доступа, должны храниться до завершения расследования событий, приведших к появлению инцидента. Примечание — В относительно новых и недолго работающих системах журналы аудита за согласованный период времени могут отсутствовать. В таких случаях для выполнения требования практического руководства 2.3 необходимо проверить выполнение требований 2.1 и 2.2
		Предполагаемые свидетельства	Файл журнала
		Метод	Проверка/Наблюдение
2	Стандарт реализации безопасности	Журналы аудита должны храниться в течение согласованного периода времени для проведения возможных расследований и мониторинга контроля доступа	
	Техническое примечание к стандарту реализации безопасности	В некоторых случаях длительность хранения журналов аудита определяется коммерческой целесообразностью, условиями договора или законодательными и/или нормативными требованиями. Например, журналы аудита с аварийными оповещениями, создаваемыми системой контроля доступа, должны храниться до завершения расследования событий, приведших к появлению инцидента. Примечание — В относительно новых и недолго работающих системах журналы аудита за согласованный период времени могут отсутствовать. В таких случаях для выполнения требований практического руководства 2.3 необходимо проверить пункты 2.1 и 2.2 практического руководства	
	2.1	Практическое руководство	Убедитесь в том, что срок хранения журналов аудита соответствует указанному в проектной документации системы
		Предполагаемые свидетельства	- Файл журнала; - проектная документация системы
		Метод	Проверка/Оценка
	2.2	Практическое руководство	Убедитесь в том, что настройки периода хранения журналов аудита в системе соответствуют проектной документации системы, или задан запрет на перезапись или удаление журналов аудита, если время хранения не определено
		Предполагаемые свидетельства	- Файл журнала; - проектная документация системы
		Метод	Проверка/Оценка

Продолжение

ИСО/МЭК 27002, 12.4 Регистрация и мониторинг			
	2.3	Практическое руководство	Убедитесь в том, что период хранения журналов аудита превышает согласованный период, исходя из временных меток файлов журнала или отметок времени в журнале
		Предполагаемые свидетельства	- Файл журнала; - проектная документация системы
		Метод	Проверка/Оценка
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.4.2 Защита информации регистрационных журналов Информация журналов и средств регистрации должна быть защищена от подделки и несанкционированного доступа	
	Дополнительная техническая информация о мере обеспечения ИБ	В системных журналах зачастую содержатся большие объемы информации, значительная часть которой не имеет отношения к мониторингу ИБ. Чтобы упростить поиск событий, имеющих значение для ИБ, можно рассмотреть возможность автоматического копирования нужных типов сообщений во второй журнал или использовать специальные системные утилиты или инструменты аудита для выполнения запросов и рационализации файлов	
1	Стандарт реализации безопасности	Меры обеспечения ИБ должны быть нацелены на защиту от несанкционированных изменений данных журналов и от проблем в работе средств ведения журналов	
	Техническое примечание к стандарту реализации безопасности	Необходимо обеспечивать защиту системных журналов, поскольку изменение или удаление в них данных может создать ложную уверенность в безопасности. Для защиты журналов их можно копировать в режиме реального времени в систему, находящуюся вне контроля системного администратора или оператора	
	1.1	Практическое руководство	Убедитесь, что только авторизованные и привилегированные пользователи могут получить доступ к файлам журналов. Доступ для чтения и записи должен быть ограничен привилегированными пользователями
		Предполагаемые свидетельства	- Доступ к серверу журналов; - доступ к журналам; - учетная запись привилегированного пользователя и обычная учетная запись
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь в том, что все файлы журналов передаются через безопасное соединение в систему управления (т. е. сервер журналов или СМИБ)
		Предполагаемые свидетельства	- Доступ к серверу журналов; - доступ к сетевым сервисам, используемым для передачи данных журналов
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Убедитесь в том, что все изменения файлов журналов могут отслеживаться системой менеджмента
		Предполагаемые свидетельства	- Доступ к системе управления журналами; - доступ к файлам журналов
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Убедитесь, что все непривилегированные или неожиданные изменения в файлах журнала могут быть идентифицированы
		Предполагаемые свидетельства	- Использование хешей/подписей; - доступ к системе управления журналами

Окончание

ИСО/МЭК 27002, 12.4 Регистрация и мониторинг			
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Убедитесь, что привилегированные и авторизованные пользователи не могут манипулировать своими собственными файлами журналов
		Предполагаемые свидетельства	- Учетная запись привилегированного пользователя; - доступ к системе управления журналами
		Метод	Тестирование и подтверждение
	1.6	Практическое руководство	Убедитесь в том, что у пользователей имеется доступ только к тем файлам журналов, которые соответствуют их правам
		Предполагаемые свидетельства	- Доступ к системе управления журналами; - доступ к журналам; - доступ к двум учетным записям пользователей с разными привилегиями
		Метод	Тестирование и подтверждение
	1.7	Практическое руководство	Убедитесь в том, что все изменения файлов журналов могут отслеживаться системой менеджмента
		Предполагаемые свидетельства	Убедитесь в надежности шифрования файлов журналов
		Метод	Тестирование и подтверждение
	1.8	Практическое руководство	Убедитесь в надежной защите системы управления журналами от несанкционированного доступа
		Предполагаемые свидетельства	Сетевой доступ к системе управления журналами
		Метод	Тестирование и подтверждение
	1.9	Практическое руководство	Проверьте возможность непривилегированного доступа к аварийным оповещениям, журналам, местам хранения уведомлений и активам
		Предполагаемые свидетельства	- Доступ к системе управления журналами; - доступ к файлам журналов
		Метод	Тестирование и подтверждение
2	Стандарт реализации безопасности	Журналы аудита должны храниться в течение согласованного периода времени, достаточного для проведения возможных расследований и мониторинга контроля доступа	
	Техническое примечание к стандарту реализации безопасности	В некоторых случаях длительность хранения журналов аудита определяется коммерческой целесообразностью, условиями договора или законодательными и/или нормативными требованиями. Например, журналы аудита с аварийными оповещениями, создаваемыми системой контроля доступа, должны храниться до завершения расследования событий, приведших к появлению инцидента. Примечание — В относительно новых и недолго работающих системах журналы аудита за согласованный период времени могут отсутствовать. В таких случаях для выполнения требований практического руководства 2.3 необходимо проверить пункты 2.1 и 2.2 практического руководства	
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.4.4 Синхронизация часов Часы всех систем обработки информации в рамках организации или домена безопасности должны быть синхронизированы с единым эталонным источником времени	

ИСО/МЭК 27002, 12.5 Контроль программного обеспечения, находящегося в эксплуатации		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.5.1 Установка программного обеспечения в эксплуатируемых системах Должны быть реализованы процедуры контроля установки программного обеспечения в системах, находящихся в эксплуатации

ИСО/МЭК 27002, 12.6 Менеджмент технических уязвимостей		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.6.1 Процесс управления техническими уязвимостями Должна быть своевременно получена информация о технических уязвимостях используемых информационных систем, оценена подверженность организации таким уязвимостям и приняты соответствующие меры в отношении связанного с этим риска ИБ
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.6.2 Ограничения на установку программного обеспечения Должны быть установлены и реализованы правила, регулирующие установку программного обеспечения пользователями

ИСО/МЭК 27002, 12.7 Особенности аудита информационных систем		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 12.7.1 Меры обеспечения информационной безопасности в отношении аудита информационных систем Требования к процессу регистрации событий [аудиту] и деятельности, связанной с контролем находящихся в эксплуатации систем, должны быть тщательно спланированы и согласованы для минимизации сбоев в бизнес-процессах

В.2.9 ИСО/МЭК 27002, раздел 13 Безопасность коммуникаций

ИСО/МЭК 27002, 13.1 Менеджмент информационной безопасности сетей		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.1.1 Меры и средства информационной безопасности сетей Сети должны управляться и контролироваться для обеспечения защиты информации систем и приложений
	Дополнительная техническая информация о мере обеспечения ИБ	Сетевой сервис — это услуга, которая предоставляется в сетевой компьютерной среде внутри организации или по методу аутсорсинга. Если организация пользуется сетевыми сервисами, ее конфиденциальная информация может передаваться с использованием аутсорсинговых сетевых сервисов. В связи с этим аудиторы должны учитывать, что необходимые функции безопасности, такие как шифрование и/или аутентификация, предоставляются сторонним поставщиком сетевых сервисов. Примеры систем, используемых для предоставления сетевых сервисов: - DNS; - DHCP; - брандмауэр/VPN; - антивирусный детектор; - система обнаружения/предотвращения вторжений
1	Стандарт реализации безопасности	Для конкретных сервисов должны быть определены необходимые меры безопасности, такие как функции безопасности, уровни обслуживания и требования к управлению. Организация должна иметь гарантии, что поставщики сетевых сервисов реализуют эти меры
	Техническое примечание к стандарту реализации безопасности	Важно обеспечить безопасность передачи информации, передаваемой с использованием сетевых сервисов. Требования к функциям безопасности обычно отражаются в бизнес-требованиях. В качестве примеров функций безопасности, связанных с сетевыми сервисами, можно указать следующие: - шифрование для предотвращения прослушивания; - контроль доступа к сети для предотвращения несанкционированного доступа;

Продолжение

ИСО/МЭК 27002, 13.1 Менеджмент информационной безопасности сетей			
		- система обнаружения/предотвращения вторжений для противодействия злонамеренным действиям; - фильтрация URL-адресов для предотвращения несанкционированного доступа через интернет; - реагирование на инциденты, связанные с неожиданными событиями системы безопасности	
	1.1		Убедитесь в том, что договорный документ с поставщиком услуг, в том числе и соглашение об уровне обслуживания (SLA), отвечает деловым и юридическим требованиям организации, а также требованиям безопасности
		Предполагаемые свидетельства	- Договорный документ; - документ с описанием требований
		Метод	Проверка/Оценка
	1.2		При проведении внутренней проверки убедитесь в том, что настройки системы, используемые для сетевых сервисов, соответствуют описанию в проекте сетевых сервисов
		Предполагаемые свидетельства	- Конфигурация системы; - проект сетевых сервисов
		Метод	Проверка/Оценка
	1.3		При проведении внутренней проверки убедитесь в том, что записи системы управления сетевыми сервисами в файлах журналов соответствуют проектной документации сетевых сервисов. Примеры записей сетевых сервисов: - аутентификация; - шифрование; - средства управления сетевым соединением; - скорость соединения; - отклик (если система работает в режиме реального времени); - длительность простоя
		Предполагаемые свидетельства	- Файлы журналов; - оповещения; - проектный документ сетевых сервисов
		Метод	Проверка/Наблюдение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.1.2 Безопасность сетевых сервисов Механизмы обеспечения безопасности, уровни обслуживания и требования к управлению для всех сетевых сервисов должны быть идентифицированы и включены в соглашения по сетевым сервисам независимо от того, будут ли они обеспечиваться силами организации или осуществляться с использованием аутсорсинга	
	Дополнительная техническая информация о мере обеспечения ИБ	Сетевой сервис — это услуга, которая предоставляется в сетевой компьютерной среде внутри организации или по методу аутсорсинга. Если организация пользуется сетевыми сервисами, ее конфиденциальная информация может передаваться с использованием аутсорсинговых сетевых сервисов. В связи с этим аудиторы должны учитывать, что необходимые функции безопасности, такие как шифрование и/или аутентификация, предоставляются сторонним поставщиком сетевых сервисов. Примеры систем, используемых для предоставления сетевых сервисов: - система имен доменов (DNS); - DHCP (протокол динамической настройки хостов); - межсетевой экран/VPN; - антивирусные системы; - системы обнаружения и предотвращения вторжений (IDS/IPS)	

Продолжение

ИСО/МЭК 27002, 13.1 Менеджмент информационной безопасности сетей			
1	Стандарт реализации безопасности	Необходимо определить и регулярно проверять способность поставщика сетевых сервисов обеспечивать безопасное управление согласованным набором услуг. Необходимо также согласовать возможность проведения аудита. Необходимо определить меры безопасности для конкретных услуг, такие как функции безопасности, уровни обслуживания и требования к управлению. Организация должна иметь гарантию того, что поставщики сетевых сервисов реализуют эти меры	
	Техническое примечание к стандарту реализации безопасности	Сетевые сервисы включают в себя предоставление соединений, сервисы частных сетей и сетей с дополнительными услугами, а также решения для обеспечения безопасности управляемых сетей, такие как использование межсетевых экранов и применение системы обнаружения вторжений. Сетевые сервисы могут варьироваться от простого сервиса с неуправляемой полосой пропускания до сложных предложений с дополнительными услугами	
	1.1	Практическое руководство	Убедитесь, что механизмы безопасности, включенные в соглашения о сетевых сервисах, регулярно тестируются и проверяются
		Предполагаемые свидетельства	- Доступ к соглашениям о сетевых сервисах; - доступ к отчетам о тестировании безопасности
		Метод	Изучение
	1.2	Практическое руководство	Убедитесь в том, что системы обнаружения и предотвращения вторжений распознают различные автоматизированные компьютерные атаки, а также злонамеренные действия, выполняемые вручную
		Предполагаемые свидетельства	- Наличие реализованных решений систем обнаружения и предотвращения вторжений; - доступ к журналам системы обнаружения и предотвращения вторжений
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	При проведении внутренней проверки убедитесь в том, что записи в полученных файлах журналов соответствуют проектной документации сетевых сервисов. Примеры записей сетевых сервисов: - аутентификация; - шифрование; - средства управления сетевым соединением; - скорость соединения; - отклик (если система работает в режиме реального времени); - длительность простоя
		Предполагаемые свидетельства	- Доступ к отдельной среде тестирования; - документально оформленная политика в отношении антивирусных средств и/или защиты от вредоносного ПО
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Убедитесь в том, что доступ к виртуальным частным сетям (VPN) и другим средствам удаленного доступа ограничен использованием надежных средств, таких как механизмы проверки подлинности и выхода за пределы среды
		Предполагаемые свидетельства	- VPN и прочие реализованные сервисы удаленного сетевого доступа; - список точек удаленного доступа

Продолжение

ИСО/МЭК 27002, 13.1 Менеджмент информационной безопасности сетей			
		Метод	Тестирование и подтверждение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.1.3 Разделение в сетях Группы информационных сервисов, пользователей и информационных систем в сети должны быть разделены	
	Дополнительная техническая информация о мере обеспечения ИБ	Одним из методов управления безопасностью больших сетей является разделение их на отдельные сетевые домены. Домены могут быть выбраны на основе уровней доверия (например, домен общего доступа, домен рабочего стола, домен сервера), на основе организационных единиц (например, кадры, финансы, маркетинг) или на основе некоторой комбинации, например, серверный домен, объединяющий несколько организационных единиц. Разделение может быть выполнено посредством использования или физически разных сетей, или разных логических сетей, например, виртуальных частных сетей	
1	Стандарт реализации безопасности	Необходимо четко определить периметр каждого домена. Доступ из одного домена в другой разрешается, но должен контролироваться по периметру посредством шлюза, например, межсетевого экрана или маршрутизатора с фильтрацией. Критерии разделения сетей на домены и возможности доступа через шлюзы должны быть основаны на оценке требований безопасности каждого домена. Оценка должна производиться в соответствии с политикой контроля доступа (см. 9.1.1), требованиями к доступу, ценностью и классификацией обрабатываемой информации. Необходимо также учитывать сравнительную стоимость требуемой технологии шлюза и ее воздействие на производительность сети. Беспроводные сети требуют особого внимания из-за присущих им нечетких периметров. В уязвимых средах необходимо рассматривать любой беспроводной доступ как внешнее соединение (см. 9.4.2) и обеспечивать изоляцию такого доступа от внутренних сетей до тех пор, пока доступ к внутренним системам не будет предоставлен шлюзом в соответствии с политикой безопасности сетей (см. 13.1.1)	
	Техническое примечание к стандарту реализации безопасности	Сети часто выходят за пределы границ организации вследствие формирующихся деловых партнерств, требующих объединения или совместного использования средств обработки информации и сетевых средств. Подобное расширение сети может повышать риск несанкционированного доступа к подключенным к сети информационным системам организаций, некоторые из которых требуют защиты от пользователей других сетей из-за их конфиденциальности или критичности	
	1.1	Практическое руководство	Убедитесь в том, что в виртуально разделенные сети нельзя проникнуть с помощью сканирования ping, переключения VLAN и/или внедрения новых виртуальных интерфейсов
		Предполагаемые свидетельства	Разделение сетей посредством виртуальных локальных сетей
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Проведите тестирование межсетевых экранов и убедитесь в том, что у злоумышленников нет возможности несанкционированного доступа к сети, а также в том, что контрольные точки не имеют известных уязвимостей
		Предполагаемые свидетельства	Сети разделены межсетевыми экранами
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Убедитесь в том, что системы с несколькими сетевыми интерфейсами в разных сетях регулярно получают обновления безопасности и не имеют известных уязвимостей. Уязвимые системы с интерфейсами в разных сетях могут использоваться для доступа к другим закрытым сетям

Окончание

ИСО/МЭК 27002, 13.1 Менеджмент информационной безопасности сетей			
		Предполагаемые свидетельства	Документация со списком всех беспроводных сетей
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Убедитесь, что в помещениях нет фальшивых точек доступа, которые не отражены в документации и могут предоставить доступ к отделенным сетям
		Предполагаемые свидетельства	Документация со списком всех беспроводных сетей
		Метод	Тестирование и подтверждение

ИСО/МЭК 27002, 13.2 Передача информации		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.2.1 Политики и процедуры передачи информации Должны существовать формализованные политики и процедуры передачи информации, а также соответствующие меры обеспечения ИБ, обеспечивающие защиту информации, передаваемой с использованием всех видов средств связи
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.2.2 Соглашения о передаче информации Безопасная передача деловой информации между организацией и внешними сторонами должна быть определена соглашениями
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.2.3 Электронный обмен сообщениями Следует обеспечивать соответствующую защиту информации при электронном обмене сообщениями
	Мера обеспечения ИБ	ИСО/МЭК 27002, 13.2.4 Соглашения о конфиденциальности или неразглашении Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности организации в обеспечении защиты информации, должны быть идентифицированы, документально оформлены и регулярно пересматриваться

В.2.10 ИСО/МЭК 27002, раздел 14 Приобретение, разработка и поддержка систем

ИСО/МЭК 27002, 14.1 Требования к безопасности информационных систем		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.1.1 Анализ и спецификация требований информационной безопасности Требования, относящиеся к ИБ, должны быть включены в перечень требований для новых информационных систем или для усовершенствования существующих информационных систем
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.1.2 Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования Информация, используемая в прикладных сервисах и передаваемая по сетям общего пользования, должна быть защищена от мошеннической деятельности, оспаривания договоров, а также несанкционированного раскрытия и модификации
	Дополнительная техническая информация о мере обеспечения ИБ	Необходимо обеспечить безопасную связь между клиентом и сервисами приложений. Для этого можно использовать: - аутентификацию; - реализацию отраженных в документации процессов подтверждения контента; - предоставление взаимодействующим партнерам всей информации о разрешениях на использования сервиса; - выполнение требований безопасности всеми взаимодействующими сторонами; - предоставление сторонами механизмов, обеспечивающих целостность, конфиденциальность и аутентичность передаваемых сообщений и содержащейся в них информации.

Продолжение

ИСО/МЭК 27002, 14.1 Требования к безопасности информационных систем			
		Большинство из этих требований может быть выполнено при использовании соответствующих мер и средств криптографической защиты информации (см. А.10). В договорах на обслуживание должны быть учтены все правовые аспекты	
1	Стандарт реализации безопасности	Безопасность сервисов приложений в общедоступных сетях тесно связана со средствами криптографической защиты информации. Эти средства могут быть использованы для достижения многих из описанных выше целей. Аутентификация и авторизация могут осуществляться с использованием хорошо известных и надежных протоколов аутентификации. Для обеспечения безопасной связи между клиентом и сервисом приложения через общедоступную сеть такой сервис может быть защищен с использованием известных криптографических методов с открытым ключом для обмена ключами и методов симметричной криптографии с блочным или потоковым шифрованием. Целостность данных, передаваемых через общедоступную сеть, можно обеспечить с помощью надежных алгоритмов криптографической подписи	
	Техническое примечание к стандарту реализации безопасности	Для защиты сервиса приложения в общедоступной сети от различных угроз ИБ и компьютерных атак необходимо, чтобы все протоколы и алгоритмы шифрования соответствовали мерам и средствам защиты информации, указанным в разделе А.10. Доступные через сети общего пользования приложения подвержены целому спектру связанных с сетями угроз. В их число входят мошеннические действия, споры по договорам или из-за разглашения информации. В связи с этим необходимо проведение детальной оценки рисков и выбор надлежащих мер и средств обеспечения безопасности. В разряд необходимых часто входят криптографические методы для аутентификации и защиты передаваемых данных	
	1.1	Практическое руководство	Убедитесь в том, что для данных и процессов аутентификации и авторизации используются надежные, хорошо известные и проверенные протоколы и алгоритмы
		Предполагаемые свидетельства	- Доступ к реализованному процессу аутентификации и авторизации; - доступ к алгоритмам и протоколам; - действительные данные аутентификации
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь в том, что приложение устойчиво к различным угрозам ИБ и компьютерным атакам уровня протоколов
		Предполагаемые свидетельства	- Доступ к протоколу связи; - доступ к каналу связи
		Метод	Тестирование и подтверждение
	1.3	Практическое руководство	Убедитесь в том, что обмен информацией устойчив к различным угрозам ИБ и компьютерным атакам уровня приложения, таким как внедрение кода, повышение привилегий, перехват сессий и небезопасные прямые ссылки на объекты
		Предполагаемые свидетельства	- Доступ к приложению без привилегий; - доступ к приложению с привилегиями
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Проведите идентификацию и тестирование использования и несоответствия данных от мониторов и датчиков с целью регистрации доступа к активам или взаимодействия с активами для конкретных свидетельств оспаривания отказа от своих действий. Отразите в документации степень фиксируемого взаимодействия

Продолжение

ИСО/МЭК 27002, 14.1 Требования к безопасности информационных систем			
		Предполагаемые свидетельства	Доступ к журналам и системе мониторинга
		Метод	Изучение
	1.5	Практическое руководство	Убедитесь в том, что все методы взаимодействия надлежащим образом регистрируются с надлежащей идентификацией
		Предполагаемые свидетельства	Доступ к журналам и системе мониторинга
		Метод	Изучение
	1.6	Практическое руководство	Убедитесь в том, что у пользователей приложений нет возможности удалить журналы приложений
		Предполагаемые свидетельства	Доступ к приложению
		Метод	Тестирование и подтверждение
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.1.3 Защита транзакций прикладных сервисов Информацию, используемую в транзакциях прикладных сервисов, следует защищать для предотвращения неполной передачи, ложной маршрутизации, несанкционированного изменения, раскрытия, дублирования или воспроизведения сообщений	
	Дополнительная техническая информация о мере обеспечения ИБ	Защита транзакций сервисов приложений является важным фактором при реализации и поддержании соответствующих служб системы безопасности. Сервисы приложений используют определенную информацию для аутентификации, управления системой или общего обмена информацией. В такую информацию могут входить реквизиты доступа, системные команды, личная информация и многие другие данные, требующие защиты. Необходимые сервисам приложений данные должны быть защищены от различных компьютерных атак и угроз ИБ	
1	Стандарт реализации безопасности	Для защиты информации, передаваемой в службу приложений, рекомендуется: 1) использовать цифровые подписи для каждой вовлеченной стороны; 2) использовать шифрование каналов связи между всеми вовлеченными сторонами; 3) использовать проверенные и надежные безопасные протоколы; 4) использовать протоколы, гарантирующие, что транзакция является действительной, конфиденциальной и закрытой; 5) для хранения деталей транзакций не использовать общедоступную систему	
	Техническое примечание к стандарту реализации безопасности	Объем принятых мер и средств должен соответствовать уровню риска, связанного с каждой формой транзакции сервиса приложений	
	1.1	Практическое руководство	Убедитесь, что все сертификаты SSL организации действительны и выданы надежным центром сертификации
		Предполагаемые свидетельства	- Используемый сертификат SSL; - доступ к сервису приложения
		Метод	Тестирование и подтверждение
	1.2	Практическое руководство	Убедитесь в том, что обмен данными между всеми сторонами шифруется с использованием надежных криптографических алгоритмов с достаточной длиной ключа
		Предполагаемые свидетельства	- Стандартные методы шифрования и длина ключей; - доступ к обмену данными с шифрованием
		Метод	Тестирование и подтверждение

Окончание

ИСО/МЭК 27002, 14.1 Требования к безопасности информационных систем			
	1.3	Практическое руководство	Убедитесь в том, что обмен данными устойчив к различным угрозам ИБ и компьютерным атакам на уровне приложений, таким как межсайтовый скриптинг, подделка межсайтовых запросов и недействительные перенаправления и пересылки
		Предполагаемые свидетельства	- Доступ к приложению без привилегий; - доступ к приложению с привилегиями
		Метод	Тестирование и подтверждение
	1.4	Практическое руководство	Проверьте устойчивость приложения или протокола к известным компьютерным атакам, таким как атака через посредника или атака повторением
		Предполагаемые свидетельства	- Доступ к обмену данными; - стандартные протоколы связи
		Метод	Тестирование и подтверждение
	1.5	Практическое руководство	Убедитесь в надежном хранении приложения всех конфиденциальных данных
		Предполагаемые свидетельства	Доступ к базе данных приложения
		Метод	Тестирование и подтверждение
	1.6	Практическое руководство	Убедитесь в том, что внешний доступ к базе данных закрыт, а также что для ограничения доступа используются надежные механизмы аутентификации
		Предполагаемые свидетельства	Доступ к базе данных приложения
		Метод	Тестирование и подтверждение
	1.7	Практическое руководство	Убедитесь в том, что транзакция остается действительной даже при потере соединения из-за неправильного перенаправления или неполной передачи данных
		Предполагаемые свидетельства	- Доступ к обмену данными; - доступ к журналам приложения
		Метод	Тестирование и подтверждение
	1.8	Практическое руководство	Убедитесь в том, что приложение пользуется минимальным набором прав. Убедитесь в том, что прав не больше, чем это необходимо
		Предполагаемые свидетельства	Доступ к данным о пользователях в базе данных приложения
		Метод	Тестирование и подтверждение

ИСО/МЭК 27002, 14.2 Безопасность в процессах разработки и поддержки		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.1 Политика безопасной разработки Правила разработки программного обеспечения и систем должны быть установлены и применены к разработкам в рамках организации
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.2 Процедуры управления изменениями системы Необходимо управлять изменениями в системах в течение жизненного цикла разработки посредством применения формализованных процедур управления изменениями

Окончание

ИСО/МЭК 27002, 14.2 Безопасность в процессах разработки и поддержки		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.3 Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы При внесении изменений в операционные платформы критически важные для бизнеса приложения должны быть проверены и протестированы, чтобы обеспечить уверенность в отсутствии неблагоприятного воздействия на деятельность или безопасность организации
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.4 Ограничения на изменения пакетов программ Следует избегать модификаций пакетов программ, ограничиваясь необходимыми изменениями, и строго контролировать все изменения
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.5 Принципы безопасного проектирования систем Принципы безопасного проектирования систем должны быть установлены, документированы, поддерживаться и применяться к любым работам по реализации информационной системы
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.6 Безопасная среда разработки Организация должна установить и надлежащим образом защищать безопасные среды разработки, используемые для разработки и интеграции систем на всех стадиях жизненного цикла разработки системы
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.7 Разработка с использованием аутсорсинга Организация должна осуществлять надзор и мониторинг разработки систем, выполняемой подрядчиками
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.8 Тестирование безопасности систем Тестирование функциональных возможностей безопасности должно осуществляться в процессе разработки
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.2.9 Приемо-сдаточные испытания системы Для новых информационных систем, обновлений и новых версий должны быть разработаны программы приемо-сдаточных испытаний и установлены связанные с ними критерии

ИСО/МЭК 27002, 14.3 Тестовые данные		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 14.3.1 Защита тестовых данных Тестовые данные следует тщательно выбирать, защищать и контролировать

В.2.11 ИСО/МЭК 27002, раздел 15 Взаимоотношения с поставщиками

ИСО/МЭК 27002, 15.1 Информационная безопасность во взаимоотношениях с поставщиками		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 15.1.1 Политика информационной безопасности во взаимоотношениях с поставщиками Требования ИБ, направленные на снижение рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиком и документированы
	Мера обеспечения ИБ	ИСО/МЭК 27002, 15.1.2 Рассмотрение вопросов безопасности во взаимоотношениях с поставщиками Все соответствующие требования ИБ должны быть установлены и согласованы с каждым поставщиком, который может получить доступ к информации организации, обрабатывать, хранить, передавать информацию или предоставлять соответствующие компоненты ИТ-инфраструктуры
	Мера обеспечения ИБ	ИСО/МЭК 27002, 15.1.3 Цепочка поставок информационно-коммуникационных технологий Соглашения с поставщиками должны содержать требования по рассмотрению рисков ИБ, связанных с цепочкой поставок продуктов и услуг информационно-коммуникационных технологий

ИСО/МЭК 27002, 15.2 Управление услугами, предоставляемыми поставщиком		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 15.2.1 Мониторинг и анализ услуг поставщика Организация должна регулярно проводить мониторинг, проверку и аудит деятельности поставщика по предоставлению услуг
	Мера обеспечения ИБ	ИСО/МЭК 27002, 15.2.2 Управление изменениями услуг поставщика Требуется управлять изменениями в предоставляемых поставщиками услугах, включая поддержку и улучшение существующих политик, процедур, а также мер обеспечения ИБ, с учетом категории информации бизнеса, задействованных систем и процессов, а также результатов переоценки рисков ИБ

В.2.12 ИСО/МЭК 27002, раздел 16 Менеджмент инцидентов информационной безопасности

ИСО/МЭК 27002, 16.1 Менеджмент инцидентов информационной безопасности и улучшений		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.1 Обязанности и процедуры Должны быть установлены обязанности и процедуры менеджмента для обеспечения уверенности в быстром, эффективном и надлежащем реагировании на инциденты ИБ
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.2 Сообщения о событиях информационной безопасности Требуется как можно скорее сообщать о событиях ИБ по соответствующим каналам управления
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.3 Сообщения о недостатках информационной безопасности Работники и подрядчики, использующие информационные системы и услуги организации, должны обращать внимание на любые замеченные или предполагаемые недостатки ИБ в системах или сервисах и сообщать о них
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.4 Оценка и принятие решений в отношении событий информационной безопасности Должна быть проведена оценка событий ИБ и принято решение, следует ли их классифицировать как инциденты ИБ
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.5 Реагирование на инциденты информационной безопасности Реагирование на инциденты ИБ должно осуществляться в соответствии с документально оформленными процедурами
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.6 Анализ инцидентов информационной безопасности Знания, приобретенные в результате анализа и урегулирования инцидентов ИБ, должны использоваться для уменьшения вероятности или влияния будущих инцидентов
	Мера обеспечения ИБ	ИСО/МЭК 27002, 16.1.7 Сбор свидетельств В организации должны быть определены и применяться процедуры для идентификации, сбора, получения и сохранения информации, которая может использоваться в качестве свидетельств

В.2.13 ИСО/МЭК 27002, раздел 17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации

ИСО/МЭК 27002, 17.1 Непрерывность информационной безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 17.1.1 Планирование непрерывности информационной безопасности Организация должна определить свои требования к ИБ и менеджменту непрерывности ИБ при неблагоприятных ситуациях, например, во время кризиса или бедствия
	Мера обеспечения ИБ	ИСО/МЭК 27002, 17.1.2 Реализация непрерывности информационной безопасности Организация должна устанавливать, документировать, реализовывать и поддерживать процессы, процедуры, а также меры и средства для обеспечения требуемого уровня непрерывности ИБ при неблагоприятных ситуациях

Окончание

ИСО/МЭК 27002, 17.1 Непрерывность информационной безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 17.1.3 Проверка, анализ и оценивание непрерывности информационной безопасности Организация должна регулярно проверять установленные и реализованные меры и средства по обеспечению непрерывности ИБ, чтобы обеспечить уверенность в их актуальности и эффективности при возникновении неблагоприятных ситуаций

ИСО/МЭК 27002, 17.2 Резервирование оборудования		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 17.2.1 Доступность средств обработки информации Средства обработки информации должны быть внедрены с учетом резервирования, достаточного для выполнения требований доступности

В.2.14 ИСО/МЭК 27002, раздел 18 Соответствие

ИСО/МЭК 27002, 18.1 Соответствие правовым и договорным требованиям		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.1.1 Идентификация применимых законодательных и договорных требований Все значимые для организации и каждой информационной системы правовые, регулятивные и договорные требования, а также подходы организации к выполнению этих требований должны быть четко определены, документированы и поддерживаться в актуальном состоянии
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.1.2 Права на интеллектуальную собственность Должны быть реализованы соответствующие процедуры для обеспечения уверенности в соблюдении правовых, регулятивных и договорных требований, связанных с правами на интеллектуальную собственность и правами использования проприетарных программных продуктов
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.1.3 Защита записей Записи должны быть защищены от потери, уничтожения, фальсификации, несанкционированного доступа и разглашения в соответствии с правовыми, регулятивными, договорными и бизнес-требованиями
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.1.4 Конфиденциальность и защита персональных данных Конфиденциальность и защита персональных данных должны обеспечиваться в соответствии с требованиями соответствующего законодательства и правилами там, где это применимо
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.1.5 Регулирование криптографических мер обеспечения информационной безопасности Криптографические меры обеспечения информационной безопасности должны использоваться с соблюдением требований всех соответствующих соглашений, правовых и регулятивных актов

ИСО/МЭК 27002, 18.2 Проверки информационной безопасности		
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.2.1 Независимая проверка информационной безопасности Подход организации к менеджменту информационной безопасностью и ее реализация (т. е. цели, меры и средства, политики, процессы и процедуры ИБ) должны проверяться независимо друг от друга через запланированные интервалы времени или в случае значительных изменений
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.2.2 Соответствие политикам и стандартам безопасности Руководители в пределах своей зоны ответственности должны регулярно проверять соответствие процессов и процедур обработки информации соответствующим политикам безопасности, стандартам и любым другим требованиям безопасности
	Мера обеспечения ИБ	ИСО/МЭК 27002, 18.2.3 Анализ технического соответствия Информационные системы должны регулярно проверяться на предмет соответствия стандартам и политикам ИБ организации

Приложение С
(справочное)

Рекомендации по технической оценке облачных услуг (инфраструктура как услуга)

С.1 Область применения и цель приложения

В данном приложении содержатся рекомендации по оценке внедрения и использования мер обеспечения ИБ, а также по реализации правил ИСО/МЭК 27017. Данное приложение дополняет приложение В настоящего стандарта, в котором рассматриваются меры обеспечения ИБ, а также практическое руководство ИСО/МЭК 27002.

Цель данного приложения — обозначить для аудиторов аспекты оценки облачных услуг, предоставляемых по принципу «инфраструктура как услуга». Область применения настоящего приложения показана на рисунке С.1. Системы предоставления облачных услуг разнообразны и подвержены непрерывным изменениям благодаря быстрому развитию инновационных технологий. В настоящем приложении не рассматривается какая-то конкретная система, его целью являются практические методы оценки, примечания и объекты оценки.

Кроме того, в данном приложении содержится информация для инженеров—поставщиков облачных услуг, которая будет включать принятые меры безопасности, чтобы узнать, как следует проверять услугу, и указывать маршрут технической оценки. Следование рекомендациям позволяет не только аудиторам выполнять оценку надлежащим образом, но и поставщикам облачных услуг разрабатывать конкретные меры обеспечения ИБ для того, чтобы их собственная служба соответствовала ИСО/МЭК 27017.

Обработчик ПДн публичного облака должен своевременно предоставить потребителю сервиса облачных вычислений всю необходимую информацию, что позволит потребителю сервиса облачных вычислений гарантировать соответствие обработчика ПДн публичного облака определенным целям и принципам ограничений. При этом также будет гарантироваться, что никакие ПДн не обрабатываются обработчиком ПДн публичного облака или любым из его субподрядчиков для иных целей, не предусмотренных предписаниями потребителя сервиса облачных вычислений.

Рисунок С.1 — Область применения настоящего приложения

С.2 Связь с другими международными стандартами

Настоящее приложение и ИСО/МЭК 27017 связаны со следующими стандартами:

а) ИСО/МЭК 27018, который описывает меры и средства контроля и управления защитой ПДн в облачных услугах.

Настоящее приложение относится к инфраструктуре как услуге. В такой инфраструктуре клиенты облачных услуг сами несут ответственность за защиту своей собственной информации, хранящейся на используемой клиентом облачных услуг виртуальной машине. Это означает, что поставщик облачных услуг не может контролировать персональные данные на виртуальной машине и, следовательно, этот вопрос не рассматривается в настоящем стандарте.

Персональные данные, которые должен поддерживать поставщик облачных услуг, включают в себя и информацию о клиентах облачных услуг. Эти данные управляются и хранятся под управлением служб модели реализации, описанной ниже. Кроме того, при управлении услугами персональные данные должны обрабатываться в соответствии с ИСО/МЭК 27018;

b) ИСО/МЭК 17788, в котором дается обзор и терминология облачных вычислений;

c) ИСО/МЭК 17789, содержащий основные концепции по компонентам конфигурации облачных услуг.

ИСО/МЭК 17789 определяет архитектуру облачных услуг с точки зрения их роли и деятельности. При оценке необходимо использовать подходы, учитывающие реализацию облачной системы, включая подтверждение пригодности конфигурации механизма виртуализации.

В настоящем приложении представлена модель реализации облачной системы, которая отображает функциональные компоненты, определенные в ИСО/МЭК 17789.

С.3 Структура настоящего приложения

В начале данного приложения предлагается модель среды облачных услуг с использованием инфраструктуры в качестве предлагаемой услуги. Эта модель описывает взаимосвязь между типами ресурсов и виртуализацией, а также концепцию клиентов и арендаторов облачных услуг. Сервер, сеть и хранилище рассматриваются как типы ресурсов.

Требования к технической оценке описаны в том же формате, что и в приложении В, в порядке тем, относящихся к модели, отдельным типам ресурсов и управлению услугами:

a) Разъяснение типичных технологий

Разъяснение технологических элементов и руководств, связанных с внедрением виртуализации. В случаях, когда существует несколько методов реализации, разъясняются типичные методы.

b) Меры обеспечения ИБ, определенные в ИСО/МЭК 27017

Ссылка на меры обеспечения ИБ в ИСО/МЭК 27017, которые связаны с виртуализацией.

c) Методика технической оценки мер обеспечения ИБ ИСО/МЭК 27017

Описание руководства по методике оценки мер обеспечения ИБ ИСО/МЭК 27017.

В случаях, когда существует несколько методов реализации, разъясняется один из них.

С.4 Модель среды облачных услуг (инфраструктура как услуга)

С.4.1 Суть модели

Широкое разнообразие технологий облачных услуг не дает возможности рассмотреть их все по отдельности. Кроме того, технологии облачных услуг являются новыми и все еще находятся в процессе технического развития. С учетом этого проводить стандартизацию методов технической оценки на базе отдельных и специализированных технологий нецелесообразно. Аудитор ИБ может с учетом данной методологической модели определить, были ли фактически реализованные технологии мер обеспечения ИБ разработаны на основе проекта мер обеспечения ИБ и собирать свидетельства для фактической оценки.

С.4.2 Модель и ее компоненты

В данной инфраструктуре среда является обязательным условием, посредством которого предоставляются облачные услуги:

a) виртуальные ресурсы, непосредственно используемые клиентами облачных услуг;

b) механизмы виртуализации, которые устанавливают эти ресурсы;

c) управление услугами для контроля и обеспечения механизмов виртуализации.

На рисунке С.2 представлена модель реализации системы, обеспечивающей предоставление облачных услуг.

Примечание — Эта мера и средства контроля и управления являются дополнением к более общей мере и средству контроля и управлению в соответствии с А.3.1 и не заменяет или отменяет ее.

Важной концепцией этой модели является виртуализация и разделение ресурсов.

В механизмах виртуализации физические ресурсы предоставляются в виде виртуальных ресурсов с компонентами абстрагирования и управления ресурсами с правами доступа, разделенными арендатором.

Область аренды — это область, в которой концентрируются виртуальные ресурсы, выделенные каждому контролируемому доступу. Заказчику облачных услуг по запросу может быть предоставлено несколько областей аренды. Как правило, к области аренды имеют доступ несколько пользователей, которые используют ее для обработки информации.

Модель имеет четыре компонента. Три из них, физические ресурсы, механизмы виртуализации и виртуальные ресурсы, образуют такие типы ресурсов, как сервер, сеть и хранилище.

a) **Физические ресурсы** — это физическое оборудование, необходимое для предоставления облачных услуг. В качестве компонентов в их число входят серверное оборудование, сетевое оборудование и оборудования для хранения данных.

Физическое сетевое оборудование включает в себя физическую сетевую интерфейсную карту (NIC), которая соединяет сервер с сетью. Физическое оборудование для хранения включает адаптер шины (HBA) и FC-коммутаторы, которые соединяют сервер с хранилищем.

b) **Механизмы виртуализации** используются для создания виртуальных ресурсов, предоставляемых облачными сервисами. Для виртуализации серверов используется гипервизор. Для виртуализации сетей применяются виртуальные локальные сети (VLAN) и программно-определяемые сети (SDN). Подобные механизмы используются в большинстве устройств хранения.

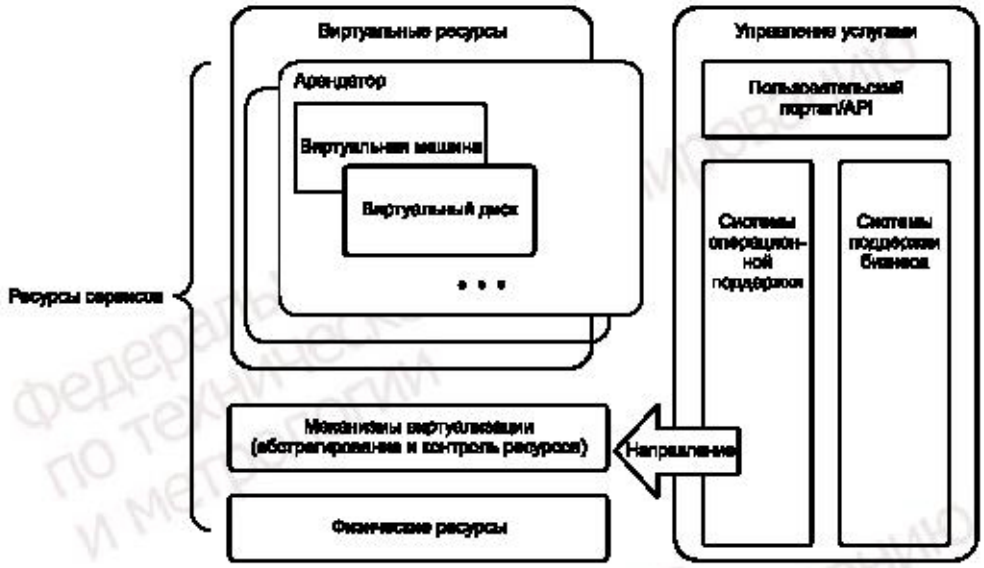

Рисунок С.2 — Модель реализации системы, обеспечивающей предоставление облачных услуг

c) **Виртуальные ресурсы** создаются функцией виртуализации и предоставляются клиентам облачных услуг. Это такие ресурсы, как облачные сервисы, виртуальные машины, виртуальные сети и виртуальные хранилища. Виртуальные ресурсы обычно обозначают комплекс виртуально сформированных ресурсов.

Примечание — Сеть и хранилище могут виртуализироваться серверами. Например, виртуализированные коммутаторы, конфигурирующие виртуальную сеть, могут быть созданы гипервизором, который виртуализирует сервер.

d) **Управление услугами** — это компонент модели, представляющий собой систему, которая дает возможность поставщику предоставлять облачные услуги клиенту и интерфейс для облачной системы.

С помощью вышеупомянутой функции виртуализации производится выделение виртуальных ресурсов, необходимых для облачных услуг. Эта функция также осуществляет мониторинг и управление физическими ресурсами, а также контролирует надлежащую работу всей облачной среды.

Управление услугами также включает в себя функции портала, утилиты и прикладные программные интерфейсы (API), что дает возможность клиенту облачных услуг работать в заданных пределах, например, открывать и активировать/деактивировать виртуальные машины.

С.4.3 Соответствие ИСО/МЭК 17789

Функциональные компоненты, определенные в ИСО/МЭК 17789, фактически реализуются в данном приложении посредством элементов реализации, используемых для каждого компонента в зависимости от типа или уровня целевого ресурса.

Примеры контроля доступа:

- Контроль доступа к физическим дискам Диск;
- Контроль доступа для каждой области аренды Механизмы виртуализации;
- Контроль доступа к виртуальным дискам Механизмы виртуализации;
- Контроль доступа в каждой виртуальной машине ОС виртуальной машины.

В модель реализации, описываемую в данном приложении, включены многоуровневые функции и компоненты ИСО/МЭК 17789, обслуживающие облачные функции, а в состав управления услугами модели реализации входят системы бизнес-поддержки (BSS) или операционной поддержки (OSS) ИСО/МЭК 17789.

Многоуровневые функции, относящиеся к интеграции и безопасности, реализованы в целевых механизмах с соответствующими правами доступа.

С.5 Общая практика в модели реализации

С.5.1 Общая информация

Далее в данном разделе рассматривается практика оценки, общая для виртуализации серверов, виртуализации сети и виртуализации хранилища.

С.5.2 Применение технологий виртуализации в облачных услугах

Как упоминалось выше, виртуализация состоит из функций виртуализации и виртуальных ресурсов. В инфраструктуре как услуге пользователи облачных услуг получают доступ к этим виртуальным ресурсам.

При проведении технической оценки облачной системы требуются следующие оценки механизмов виртуализации:

a) Безопасность операций

Поскольку работа механизмов виртуализации напрямую влияет на виртуальные ресурсы, убедитесь, что операции выполняются надлежащим образом.

b) Определение среды

Убедитесь в том, что определены журналы и события, о которых должны информироваться облачные клиенты (уведомления об ошибках, предупреждения, информация о превышении пороговых значений), в параметрах механизмов виртуализации для обеспечения сбора и регистрации информации.

Убедитесь в том, что избыточность виртуальных механизмов и виртуальных ресурсов также задана в параметрах механизмов виртуализации и может быть оценена.

c) Управление производительностью

В каждой виртуализации проверяется, управляется ли связь виртуальных ресурсов, предоставляемых клиентам облачных услуг, с физическими ресурсами.

Облачные вычисления предоставляют логические ресурсы, доступные статистически одновременно. Таким образом, общие предоставляемые виртуальные ресурсы больше, чем общие физические ресурсы (превышение аренды, превышение объема).

С.5.3 Проведение технической оценки общих аспектов механизма виртуализации

С.5.3.1 Безопасность при эксплуатации

Мера обеспечения ИБ	ИСО/МЭК 27017, 12.1.2 Процесс управления изменениями
Рекомендации по реализации для поставщика облачных услуг	Поставщик должен обеспечивать клиента информацией об изменениях в предоставляемых облачных услугах и используемых системах, которые могут негативно сказаться на ИБ клиента облачных услуг. Следующая информация поможет потребителю облачных услуг определить воздействие изменений на информационную безопасность: - категории изменений; - планируемая дата и время внесения изменений; - техническое описание изменений в облачных сервисах и базовых системах; - уведомление о начале и завершении реализации изменений. Если поставщик облачных услуг предоставляет облачный сервис, зависящий от другого однорангового поставщика облачных услуг, то поставщик таких услуг должен уведомлять потребителя таких облачных услуг об изменениях облачных услуг со стороны другого поставщика
Дополнительная техническая информация	Потенциально значимые изменения для клиента облачных услуг приведены ниже: Сервер: - обновление или модернизация гипервизора; - изменения параметров гипервизора и в определениях среды. Сеть: - изменения в определениях виртуальных локальных сетей; - изменения в конфигурации, определениях среды и параметрах сетевых устройств, включая коммутатор, маршрутизатор, брандмауэр и балансировщик нагрузки. Хранилище: - изменения в определениях устройств; - изменения зонирования сети хранения данных и т. д. Оборудование: - обновление прошивки. Программное обеспечение: - обновление программного обеспечения; - применение программных исправлений (патчей); - применение исправлений безопасности. Данные изменения могут оказывать различное воздействие на клиентов облачных услуг. Клиент и поставщик облачных услуг должны согласовать, уведомление о каких изменениях должны доводиться до сведения клиента с учетом уровня их возможного воздействия

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 12.1.2 Процесс управления изменениями	
1	Стандарт реализации безопасности	В системе управления изменениями необходимо определить и обеспечить соответствующее оповещение клиентов облачных услуг, которые подвергаются прямому или косвенному воздействию	
	Техническое примечание к стандарту реализации безопасности	Поскольку между информационными ресурсами существует взаимная связь, воздействию могут подвергаться клиенты облачных услуг, использующие другие ресурсы, зависящие от изменяемых. Как правило, конфигурации аппаратного и программного обеспечения находятся и обновляются в базе данных управления конфигурациями (CMDB). Аппаратные и программные ресурсы, выделяемые каждому клиенту облачных услуг, также управляются со стороны базы данных управления конфигурациями, OSS (системы поддержки операций) или BSS (системы поддержки бизнеса). Эти системы управляют взаимоотношениями аппаратного и программного обеспечения с клиентами облачных услуг, на которых воздействуют изменения этого аппаратного и программного обеспечения	
	1.1	Практическое руководство	Проверьте, определен ли круг клиентов облачных услуг, использующих подлежащие изменениям информационные ресурсы
		Предполагаемые свидетельства	Результаты поиска в базе данных управления конфигурациями и т. д. (Результаты поиска клиентов облачных услуг, использующих определенные информационные ресурсы)
		Метод	Проверка/Наблюдение
	1.2	Практическое руководство	Убедитесь в понимании соответствующих отношений при наличии зависимостей или воздействий между информационными ресурсами
		Предполагаемые свидетельства	Результаты поиска в базе данных управления конфигурациями и т. д. (Результаты поиска информационных ресурсов, которые подвергаются воздействию определенных информационных ресурсов при наличии зависимостей между ними)
		Метод	Проверка/Наблюдение
	1.3	Практическое руководство	Проверьте, правильно ли предоставляется информация об управлении изменениями, которая должна направляться клиентам облачных услуг. Удостоверьтесь, что: - предоставляется информация об изменениях, затрагивающих клиентов облачных услуг (также и о косвенных воздействиях); - имеются соглашения с клиентами или определен соответствующий уровень воздействия
		Предполагаемые свидетельства	Почтовые сообщения клиентам облачных услуг Портал для клиентов облачных услуг
		Метод	Проверка/Наблюдение

Мера обеспечения ИБ	ИСО/МЭК 27017, 12.1.3 Управление производительностью
Рекомендации по реализации для поставщика облачных услуг	Поставщик облачных услуг должен контролировать общую емкость вычислительных ресурсов, чтобы предотвратить инциденты ИБ, вызванные нехваткой ресурсов
Дополнительная техническая информация	Поставщик облачных услуг предоставляет следующие облачные ресурсы: - вычислительные мощности ЦП, оперативная память; - полоса пропускания сети; - объем памяти для хранения данных.

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 12.1.3 Управление производительностью	
		В облачной системе управление производительностью является обязательным для предотвращения ситуаций нехватки вычислительных ресурсов в периоды пиковой нагрузки. Управление производительностью должно быть реализовано не только в облачной системе в целом, но и в каждом отдельном блоке, поскольку вычислительные ресурсы могут не предоставляться вне блока облачной системы	
1	Стандарт реализации безопасности	Определите уровень, после которого должны быть добавлены вычислительные ресурсы, и выполните необходимые действия при его достижении	
	Техническое примечание к стандарту реализации безопасности	Укажите определенный порог для вычислительных ресурсов и проведите мониторинг, чтобы выдать сигнал тревоги, когда использование может превысить этот порог. Проведите мониторинг использования вычислительных ресурсов с помощью облачной системы, оборудования, программного обеспечения и т. д.	
	1.1	Практическое руководство	Проверьте, как контролируются вычислительные ресурсы, для которых в соответствии с требованиями необходимо управление производительностью
		Предполагаемые свидетельства	Определение мониторинга облачной системы Отчет о производительности
		Метод	Проверка/Наблюдение
	1.2	Практическое руководство	Проверьте, подается ли сигнал тревоги, когда использование ресурсов превышает пороговое значение
		Предполагаемые свидетельства	Настройки оповещений для системы мониторинга облачных услуг (убедитесь в том, что определен сигнал тревоги для срабатывания по порогу) Журнал событий системы мониторинга облачных услуг (проверьте, был ли выдан сигнал тревоги в прошлом)
		Метод	Проверка/Наблюдение

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.12.1.5 Безопасность операций администратора	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставить документацию о критических операциях и процедурах тем клиентам облачных услуг, которым это необходимо	
Дополнительная техническая информация		Неудачные изменения облачной вычислительной среды, как правило, отражаются на ее клиентах, которые не могут пользоваться облачными услугами. Наиболее серьезные последствия для клиентов — удаление и уничтожение данных клиентов в хранилище. Предполагается, что временный выход из строя или отключение облачной вычислительной среды не может привести к уничтожению активов, даже в случае отмены выполняемых транзакций	
1	Стандарт реализации безопасности	Только предварительно авторизованные операторы могут удалять данные	
	Техническое примечание к стандарту реализации безопасности	Для работы с административными привилегиями, которые позволяют удалять данные клиентов облачных услуг в хранилище, должен требоваться уровень аутентификации, отличный от уровня аутентификации для обычной работы	
	1.1	Практическое руководство	Убедитесь в ограниченном количестве идентификаторов с административными привилегиями и наличии отдельной процедуры работы с административными привилегиями
		Предполагаемые свидетельства	Список идентификаторов пользователей с возможностью работы с хранилищем данных и т. п. Работа с административными привилегиями
		Метод	Проверка/Наблюдение

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 12.4.1 Регистрация событий	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить возможности ведения журналов для потребителя облачных услуг	
Дополнительная техническая информация		Как описано в разделе «Дополнительная информация для облачных служб» ИСО/МЭК 27017, поставщик облачных услуг отвечает за ведение журнала и мониторинг компонентов инфраструктуры облачных услуг в среде «инфраструктура как сервис», рассматриваемой в этом документе. Они включают: - Журналы и события гипервизора; - Журналы и события брандмауэра и балансировки нагрузки; - Журналы и события хранилища и оборудования сети хранения данных. Поскольку эти компоненты инфраструктуры совместно используются клиентами облачных услуг, в журналах регистрируются события для всех клиентов облачных сервисов в целом. Возникает необходимость извлечь и предоставить информацию, относящуюся только к соответствующему клиенту облачных услуг	
1	Стандарт реализации безопасности	Ведутся журналы с записью событий, которые должны быть предоставлены клиентам облачных услуг	
	Техническое примечание к стандарту реализации безопасности	Для ведения журнала и сбора событий используется функция компонентов инфраструктуры облачных услуг. Форма представления выходных документов журнала определяется параметрами компонентов инфраструктуры облачных услуг	
	1.1	Практическое руководство	Убедитесь в том, что для компонентов инфраструктуры облачных услуг заданы параметры ведения журналов или событий
		Предполагаемые свидетельства	Определение параметров инфраструктуры облачных услуг
		Метод	Проверка/Наблюдение
Мера обеспечения ИБ		ИСО/МЭК 27017, 12.4.4 Синхронизация времени	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставить клиенту облачных услуг информацию о времени, используемом провайдерами облачных услуг в процессе мониторинга и регистрации событий компонентами инфраструктуры, и о том, как можно синхронизировать локальное время со временем в облаке	
Дополнительная техническая информация		Для клиентов облачных сервисов в среде «инфраструктура как сервис» необходима синхронизация времени виртуальной машины со средой облачных услуг. Как правило, используются следующие методы синхронизации: - NTP (сетевой протокол сервиса времени); - метод гипервизора	
1	Стандарт реализации безопасности	Для синхронизации времени виртуальной машины поставщик облачных услуг использует метод NTP или гипервизор	
	Техническое примечание к стандарту реализации безопасности	Клиенты облачных услуг должны настроить синхронизацию времени своих собственных виртуальных машин на основе соответствующего метода	
	1.1	Практическое руководство	Убедитесь, предоставляет ли поставщик облачных услуг метод синхронизации времени
		Предполагаемые свидетельства	Результат проверки наличия NTP-сервера и доступности этого сервера для клиентов облачных услуг по протоколу NTP Результат проверки синхронизации с помощью гипервизора и возможности использования клиентами облачных услуг такой функции синхронизации времени
		Метод	Тестирование

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.12.4.5 Мониторинг облачных служб	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить потребителю возможность мониторинга определенных аспектов работы облачных услуг, относящихся к потребителю. Например, возможность отслеживания использования облачных услуг в качестве платформы для злонамеренных компьютерных атак или утечки конфиденциальных данных из облачных сервисов. Использование функций мониторинга должно быть защищено средствами контроля доступа. Эти функции должны иметь доступ только к той информации, которая относится к собственному экземпляру облачных услуг потребителя. Поставщик облачных услуг должен предоставить их потребителю документацию о возможностях средств мониторинга. Необходимо обеспечить соответствие результатов мониторинга данным журналов событий (см. 12.4.1) и выполнение условий соглашения об уровне обслуживания	
Дополнительная техническая информация		В общем случае, поскольку определить злонамеренное использование облачных сервисов сложно, то следует отмечать превышение определенных лимитов сетевого трафика и доступа к хранилищу как таковых	
1	Стандарт реализации безопасности	Используйте функции ведения журнала или мониторинга для обнаружения ситуаций, определяемых как недобросовестное использование облачных услуг	
	Техническое примечание к стандарту реализации безопасности	См. 12.4.1	
	1.1	Практическое руководство	Проверьте, что система мониторинга определена таким образом, чтобы обнаруживать события, определяемые как злонамеренное использование облачных услуг
		Предполагаемые свидетельства	Определение параметров системы мониторинга
		Метод	Проверка/Наблюдение

Мера обеспечения ИБ		ИСО/МЭК 27017, 12.6.1 Процесс управления техническими уязвимостями	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставлять потребителям облачной службы информацию об управлении техническими уязвимостями, относящимися к облачным службам и используемым им информационным системам	
Дополнительная техническая информация		Технические уязвимости зависят от версий программного обеспечения. В целом, поскольку компоненты инфраструктуры облачных услуг используют более одной версии из одного и того же программного обеспечения, необходимо определить, существуют ли уязвимости в используемых вычислительных ресурсах	
1	Стандарт реализации безопасности	При обнаружении технических уязвимостей в компонентах инфраструктуры облачных услуг необходимо определить потребителей облачных услуг, которые используют вычислительные ресурсы с уязвимостями, и предоставить им информацию об этих уязвимостях. Для определения взаимосвязей вычислительных ресурсов с клиентами облачных услуг см. 12.1.2 «Управление изменениями»	
	Техническое примечание к стандарту реализации безопасности	Для определения взаимосвязей вычислительных ресурсов с клиентами облачных услуг см. 12.1.2 «Управление изменениями»	
	1.1	Практическое руководство	Проверьте, выявлены ли клиенты службы, использующие вычислительные ресурсы с найденными уязвимостями, и получили ли они информацию о технических уязвимостях
		Предполагаемые свидетельства	Уведомления по электронной почте о технических уязвимостях; информация портала и т. д.
		Метод	Проверка/Наблюдение

С.6 Виртуализация серверов

С.6.1 Общие сведения о виртуализации серверов

Виртуализация сервера создает образ физического сервера (состоящего из центрального процессора, памяти, устройств ввода-вывода и т. д.) на логическом ресурсе. В общем виде структура виртуализации серверов представлена на рисунке С.3.

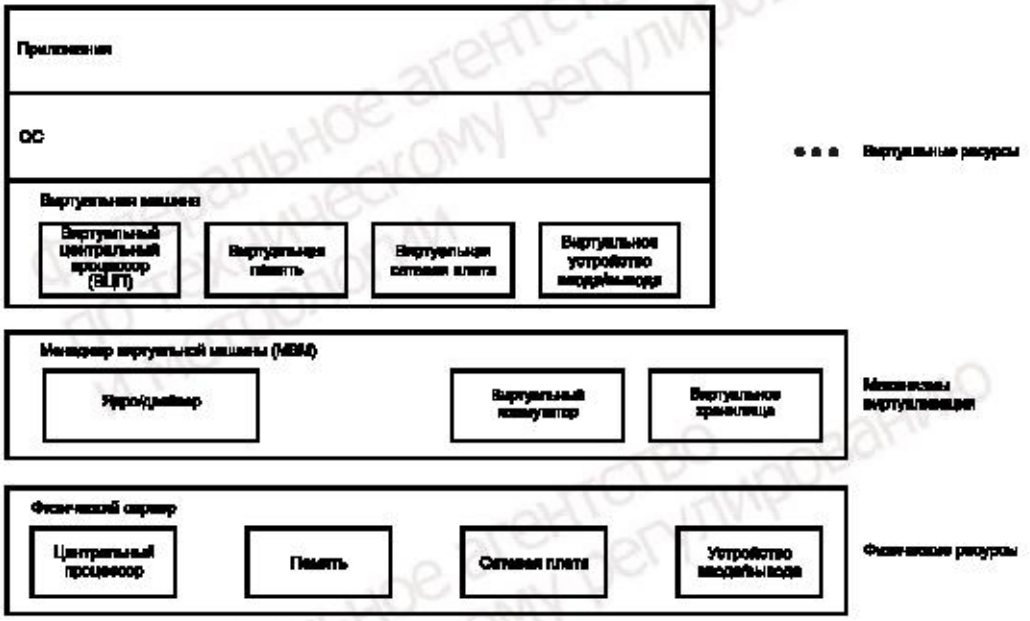

Рисунок С.3 — Обобщенная схема виртуализации серверов

a) **Виртуализация центрального процессора (ЦП)** под управлением монитора виртуальных машин (МВМ) выделяет виртуальным машинам клиентов физический процессор (ядро) на физическом сервере в качестве ресурса виртуализации на основе виртуального «ядра».

Виртуализация ЦП обеспечивает возможность избыточной аренды или выделения виртуальных ЦП в количестве, превышающем общее количество физических ядер ЦП всего сервера.

При избыточной аренде VMM выполняет планирование ЦП и переключение виртуальных ЦП, распределенных на физические ядра ЦП. В связи с этим следует обратить внимание на то, что одновременная интенсивная работа более чем одной ВМ увеличивает частоту конфликтов физических ЦП, потребляет ресурсы ЦП для планирования ЦП, а кроме того, вызывает задержку при выделении ресурсов ЦП, что может повлиять на производительность обработки.

b) **Виртуализация памяти** распределяет память виртуальной машины по памяти физического сервера. Как и в случае виртуализации ЦП, виртуализация памяти допускает избыточную аренду, что означает, что общий объем памяти, видимый виртуальными машинами, больше, чем фактический объем памяти на физическом сервере. Превышение аренды на память разрешается либо путем динамического выделения памяти для виртуальной машины (раздувание), либо посредством совместного использования идентичной памяти несколькими виртуальными машинами. В обоих случаях сумма минимальных объемов памяти, выделенной каждой виртуальной машине, должна быть меньше, чем объем доступной памяти физического сервера.

c) **Виртуализация хранилища**: хранилище виртуальной машины рассматривается как набор файлов в хранилище физического сервера. Однако существуют проблемы передачи больших объемов данных при переносе виртуального сервера между физическими серверами, связанные с загрузкой каналов передачи, быстродействием устройств хранения данных и т. д. Поэтому, как правило, в проекте системы, предоставляющей облачные услуги, предусматривается использование общего сервера хранения данных с доступом к данным через сеть хранения данных (SAN).

d) **Виртуализация ввода/вывода** виртуализирует совокупность периферийных устройств: сетевые интерфейсные карты, адаптеры шины и адаптеры последовательного порта. Виртуальный порт адаптера используется при подключении к виртуальной машине, которая настроена для работы под МВМ с настройками МВМ, или при

подключении к порту физического адаптера на физическом сервере. Следует обратить внимание на то, что функции ввода-вывода адаптера шины и сетевой интерфейсной карты используются совместно в большей степени по сравнению с памятью и процессорами и часто становятся узким местом в функции виртуализации.

С.6.2 Применение виртуализации серверов в облачных услугах

a) Разделение клиентов при виртуализации серверов

В общем проекте виртуализированной среды виртуализированные серверы представляют собой полностью независимые ресурсы, соединенные с виртуальными машинами посредством виртуальной сети.

Поэтому для разделения ресурсов виртуальных машин требуются минимальные меры безопасности сети. Особое внимание в среде виртуализации следует уделить исправлениям уязвимостей самой среды виртуализации, предоставленным легитимными источниками.

Кроме того, специальная среда виртуализации должна обеспечивать быстрый обмен данными как между виртуальными машинами для непосредственного взаимного обмена, так и для обмена данными между виртуальными машинами через физический порт физического сервера. Поэтому следует обратить внимание на другие отличные от сетевых карт устройства ввода/вывода.

Для защиты виртуальных ресурсов существует технология, с помощью которой осуществляется доступ к памяти и операциям ввода-вывода из МВМ или из привилегированной виртуальной машины. Используя эту технологию, можно отслеживать поведение виртуальной машины и для защиты ресурсов обнаруживать недопустимые программные операции.

Однако несмотря на то, что доступ из МВМ или привилегированной ВМ повышает защищенность виртуальных ресурсов, внедрять такую технологию следует с осторожностью, поскольку недобросовестные пользователи могут получить возможность для совершения компьютерной атаки.

b) Обеспечение доступности при виртуализации серверов

Динамическая миграция — это функция, которая переносит рабочую среду виртуальной машины на другой физический сервер без деактивации виртуальной машины. Динамическая миграция реализуется путем запуска на виртуальной машине памяти целевого физического сервера образа виртуальной машины, записанного в общем хранилище, передачи через локальную сеть данных кэш-памяти, а также завершения виртуального ввода-вывода. Такой механизм позволяет передавать содержимое памяти по локальной сети в режиме динамической миграции, при это решающее значение имеет безопасность данных в памяти и безопасность локальной сети. Динамический перенос виртуальной машины между физическими серверами либо осуществляется администратором, либо обеспечивается технологией высокой доступности, посредством которой виртуальная машина может автоматически мигрировать между физическими серверами в случае возникновения сбоя в среде.

Если мониторинг с помощью такого рода технологии высокой доступности обнаруживает сбой, то предоставление услуг приостанавливается на время, необходимое для активации образа виртуальной машины, работающей на неисправном физическом сервере, на другом нормально работающем физическом сервере. Отказоустойчивая среда виртуализации является технологией, которая позволяет сократить время приостановки предоставления услуг, предусмотренное технологией высокой доступности. Отказоустойчивая среда виртуализации обеспечивает управление первичной и вторичной виртуальными машинами на нескольких физических серверах и постоянно синхронизирует обе виртуальные машины. При нормальной работе первичная виртуальная машина предоставляет услугу, а для обеспечения устойчивости к сбоям вторичная виртуальная машина может заменить ее в тот момент, когда произошел сбой. Следует обратить внимание, что обе технологии требуют наличия ресурсов на другом физическом сервере, а не на одном и том же физическом сервере.

c) Администрирование производительности виртуализации сервера

Виртуальная память или ресурсы ЦП могут динамически распределяться во время работы с использованием соответствующей ОС. Поскольку ресурсов на физическом сервере может быть выделено не более чем есть физически, необходимо гарантировать наличие свободного места для переноса виртуальной машины с помощью описанной выше технологии динамической миграции на другой физический сервер с учетом ресурсов, используемых другими виртуальными машинами. Ресурсы физического сервера определяются следующими показателями:

- количество ядер процессора;
- размер памяти;
- производительность дискового ввода/вывода;
- размер диска;
- производительность сетевого ввода/вывода.

Общий объем требуемых ресурсов можно рассчитать путем умножения суммы этих показателей, предоставленных в качестве сервисов для простой виртуализированной среды, на издержки, требуемые для виртуализации. Для обеспечения доступности сервиса необходимо предусмотреть запас для каждого физического сервера, а также ресурсов.

Приоритет показателей и способ предоставления услуг зависят от бизнес-модели или соглашения об уровне обслуживания поставщика облачных услуг. В любом случае очень важно, чтобы предоставляемые в текущий момент ресурсы и доступные ресурсы подвергались мониторингу для обеспечения непрерывного предоставления аппаратных ресурсов. Такой мониторинг выполняется главным образом средствами управления услугами для обеспечения целостности всей среды облачных сервисов. Однако следует обратить внимание на то, что инструмент

мониторинга использования ресурсов может быть установлен как на МВМ, так и на привилегированной виртуальной машине на сервере виртуализации.

С.6.3 Проведение технической оценки виртуализации сервера

С.6.3.1 Управление доступом

Информация о разделении при виртуализации серверов приведена в С.6.2.

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.1 Разделение в виртуальных вычислительных средах	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить надлежащее логическое разделение данных клиентов облачных услуг, виртуализированных приложений, операционных систем, хранилищ и сетей, в том числе: - разделение ресурсов, используемых клиентами облачных сервисов в средах с несколькими арендаторами; - отделение внутреннего администрирования поставщика облачных услуг от ресурсов, используемых клиентами облачных услуг. В тех случаях, когда облачная служба обеспечивает среду с несколькими арендаторами, поставщик облачных услуг должен внедрить меры и средства обеспечения ИБ для надлежащей изоляции ресурсов, используемых различными арендаторами. Поставщик облачных услуг должен учитывать риски, связанные с использованием программного обеспечения, применяемого заказчиком облачных услуг, в условиях, обеспечиваемых поставщиком услуг	
Дополнительная техническая информация		Реализация логического разделения зависит от технологий, применяемых для виртуализации	
1	Стандарт реализации безопасности	Разделение потребителей облачных услуг в средах с несколькими арендаторами	
	Техническое примечание к стандарту реализации безопасности	Между виртуальными машинами, использующими память и виртуальные порты, существует связь, которая потенциально может стать связью между виртуальными ресурсами	
	1.1	Практическое руководство	Необходимо деактивировать функции непосредственного доступа между виртуальными машинами
		Предполагаемые свидетельства	Необходимо убедиться, что в мониторе виртуальных машин отключены функции непосредственного доступа между виртуальными машинами
		Метод	Проверка/Наблюдение, Проверка/Оценка
2	Стандарт реализации безопасности	Отделение внутреннего администрирования поставщика облачных услуг от виртуальных сред потребителей облачных услуг	
	Техническое примечание к стандарту реализации безопасности	В рамках разделения ВМ и МВМ управление ВМ-МВМ может быть активным, как было отмечено выше. Кроме того, поскольку связь ВМ-МВМ может быть создана с помощью инструментов, реализуемых из соображений безопасности и доступности безопасности или доступности этой связи, то уязвимости в этих инструментах могут оказаться лазейкой в конфигурации ВМ-МВМ	
	2.1	Практическое руководство	В программном обеспечении для виртуализации должны использоваться функции разделения. Включите функцию секционирования в среде виртуализации
		Предполагаемые свидетельства	Подтверждение политики управления доступом в МВМ. Убедитесь, что в МВМ выключен механизм «Transparent Page Sharing»
		Метод	Проверка/Наблюдение, Проверка/Оценка
	2.2	Практическое руководство	Физическое разделение кластера виртуальных систем
		Предполагаемые свидетельства	Необходимо подтвердить, что функция поддержки виртуализации на физическом сервере активна

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.1 Разделение в виртуальных вычислительных средах	
		Метод	Проверка/Наблюдение, Проверка/Оценка
3	Стандарт реализации безопасности	Необходимо принять меры по управлению уязвимостями	
	Техническое примечание к стандарту реализации безопасности	В платформах виртуализации (ОС хостов, гипервизор и т. д.) должны использоваться продукты, созданные с учетом мер безопасности (с учетом общих критериев и т. д.)	
	3.1	Практическое руководство	Убедитесь, что продукты, используемые в платформах виртуализации, созданы с учетом мер безопасности
		Предполагаемые свидетельства	Базовая проектная документация для платформы виртуализации
		Метод	Проверка/Оценка
	3.2	Практическое руководство	Обмен информацией об уязвимостях в операциях
		Предполагаемые свидетельства	Подтверждение статуса обмена информацией об уязвимостях (проверка информации, размещенной на странице портала и т. д.)
		Метод	Проверка/Наблюдение

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.2 Защита виртуальных машин	
Рекомендации по реализации для поставщика облачных услуг		При настройке виртуальных машин клиенты и поставщики облачных услуг должны обеспечивать соответствующую защиту (например, должны быть включены только те порты, протоколы и службы, которые необходимы для работы облачных служб) и для каждой используемой виртуальной машины принимать соответствующие технические меры безопасности (например, противодействие вредоносному ПО, ведение журнала)	
Дополнительная техническая информация		ВМ/МВМ и физический сервер обеспечивают не только работу операционной системы ВМ, но и защиту виртуальных машин. Поскольку все они тесно связаны, то для повышения уровня защиты виртуальных машин требуется сотрудничество клиента облачных услуг и поставщика облачных услуг	
1	Стандарт реализации безопасности	При настройке виртуальных машин должны быть включены только необходимые устройства и/или услуги	
	Техническое примечание к стандарту реализации безопасности	Что касается усиления виртуальной машины, то подобная мера обеспечения ИБ не является каким-то новым улучшением виртуального сервера, поскольку к нему могут быть применены общие технологии усиления сервера. Однако существует технология для МВМ, обеспечивающая безопасность сервера. Если используется эта технология, то метод ее оценки также должен соответствовать методу, определенному в ИСО/МЭК 27002	
	1.1	Практическое руководство	Убедитесь, что МВМ настроен для обеспечения минимального функционала ВМ
		Предполагаемые свидетельства	Результат подтверждения
		Метод	Проверка/Наблюдение, Проверка/Оценка
	1.2	Практическое руководство	Опишите, какой тип услуги будет добавлен в образ ОС виртуальной машины, предоставленный по умолчанию в МВМ или в системе управления услугами, и подтвердите, что информация о дополнительной услуге выводится на экран конфигурации новой виртуальной машины, созданной системой управления облачными услугами

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.2 Защита виртуальных машин	
		Предполагаемые свидетельства	Результат подтверждения
		Метод	Проверка/Наблюдение, Проверка/Оценка
2	Стандарт реализации безопасности	При создании виртуальной среды следует снижать риски атак вредоносных программ и уязвимостей на сервер, который предоставляет виртуальную среду	
	Техническое примечание к стандарту реализации безопасности	В зависимости от технологии виртуализации можно добавлять различные приложения с использованием общей ОС, но следует избегать избыточных ролей, функций и приложений. МВМ должен обеспечивать работу основных элементов инфраструктуры, таких как антивирусное программное обеспечение, агент резервного копирования и т. д. В идеале следует использовать МВМ со всеми функциями, которые могут устранить уязвимости	
	2.1	Практическое руководство	Необходимо убедиться, что услуги на хостах ограничены до минимума. Рекомендуется использовать ОС в минимальной конфигурации
		Предполагаемые свидетельства	Необходимо проверить услуги на виртуальной машине, убедиться в том, что они соответствуют минимальной конфигурации и отметить это в проектной документации
		Метод	Проверка/Наблюдение, Проверка/Оценка
	2.2	Практическое руководство	Убедитесь, что обновления безопасности выполняются соответствующим образом для МВМ и приложений, включая и сам МВМ
		Предполагаемые свидетельства	Убедитесь, что нет необходимости выполнять обновления благодаря внедрению инструмента обновления
		Метод	Проверка/Наблюдение, Тестирование
	2.3	Практическое руководство	Убедитесь, что загрузчик или МВМ никоим образом не изменены
		Предполагаемые свидетельства	Подтвердите, что SecureBoot активен, проверив экран UEFI
		Метод	Проверка/Наблюдение
3	Стандарт реализации безопасности	При настройке виртуальных машин убедитесь, что для каждой используемой виртуальной машины реализованы соответствующие меры и средства обеспечения безопасности (например, защита от вредоносных программ, ведение журнала)	
	Техническое примечание к стандарту реализации безопасности	В дополнение к общепринятой практике управления уязвимостями на серверах существуют программное обеспечение, такое как драйверы для более эффективного использования квази-виртуальных сред, и программное обеспечение для управления гостевыми машинами с сервера и т. д., которое должно быть установлено в связи с тем, что среда является виртуальной	
	3.1	Практическое руководство	Соберите информацию об уязвимостях в инструментах и драйверах, используемых в виртуальных средах, и подготовьте модель для объявления об обновлениях для клиентов облачных услуг
		Предполагаемые свидетельства	Убедитесь, что журналы уведомлений и клиенты облачных услуг могут подтвердить соответствующие данные
		Метод	Проверка/Наблюдение

С.7 Виртуализация сети

С.7.1 Общие сведения о виртуализации сетей

Классическая сетевая виртуализация представляет собой средство обеспечения нескольких независимых коммуникаций в одной физической сети. Сетевая виртуализация на сервере представляет собой средство подключения нескольких виртуальных машин, находящихся на одном физическом сервере. Виртуальные машины могут быть перемещены на другой физический сервер в случае сбоя физического сервера, на котором была размещена соответствующая виртуальная машина, или в случае высокой интенсивности использования физического ресурса. Характерно, что виртуальные машины при этом сохраняют свои VLAN-идентификаторы и IP-адреса. На рисунке 4 показана конфигурация виртуальных машин и сети, к которой они подключены.

a) Виртуальный коммутатор

Функция логического L2-коммутатора обеспечивается монитором виртуальной машины.

Он находится между физической сетевой платой и виртуальной машиной и получает/отправляет пакеты. Поскольку физическая сетевая карта прозрачно передает пакеты, виртуальный коммутатор подключается через физическую сетевую карту к физическому коммутатору.

b) Виртуальная сетевая плата

Функция логической сетевой платы, обеспечиваемая монитором виртуальной машины, для подключения виртуальной машины к виртуальному коммутатору.

c) Виртуальный маршрутизатор

Функция логического маршрутизатора обеспечивается программным обеспечением, установленным на виртуальной машине, или самой виртуальной машиной, выполняющей роль маршрутизатора. Виртуальный коммутатор также может выполнять функции маршрутизатора.

d) Виртуальный межсетевой экран

Функция логического межсетевого экрана, обеспечиваемая программным обеспечением, установленным на виртуальной машине, или фактическая виртуальная машина, функционирующая в качестве межсетевого экрана.

С.7.2 Применение виртуализации сетей в облачных услугах

a) Разделение клиентов при виртуализации сетей

Виртуальная машина, используемая клиентами, имеет уникальные виртуальные MAC-адрес и IP-адрес. Поскольку логическая сеть, соединяющая одну или несколько виртуальных машин, настраивается отдельно для каждого клиента, клиенты разделены как в физической сети, так и на физическом сервере.

b) Обеспечение доступности при виртуализации сетей

В случае сбоя физического сервера доступность виртуальных машин и виртуальной сети на сервере может быть обеспечена путем их перемещения на другую физическую машину. Когда происходит сбой физического сетевого адаптера, установленного на физическом сервере, то если физический сетевой адаптер настроен с резервированием, виртуальная сеть переключается на другой физический сетевой адаптер без изменения фактической виртуальной машины, что позволяет сохранить ее доступность.

c) Управление полосами пропускания и адресным пространством при виртуализации сети

Поскольку при облачных услугах, как правило, создается множество виртуальных сетей в ограниченной физической сети, суммарная ширина логических полос пропускания для виртуальных сетей может значительно превышать ширину физической полосы пропускания физической сети. Кроме того, поскольку виртуальные машины могут перемещаться с одного физического сервера на другой, сохраняя при этом свои идентификаторы VLAN и/или IP-адреса, количество идентификаторов VLAN, которые должны быть установлены в физическом коммутаторе, и/или новое количество MAC-адресов имеют тенденцию к увеличению.

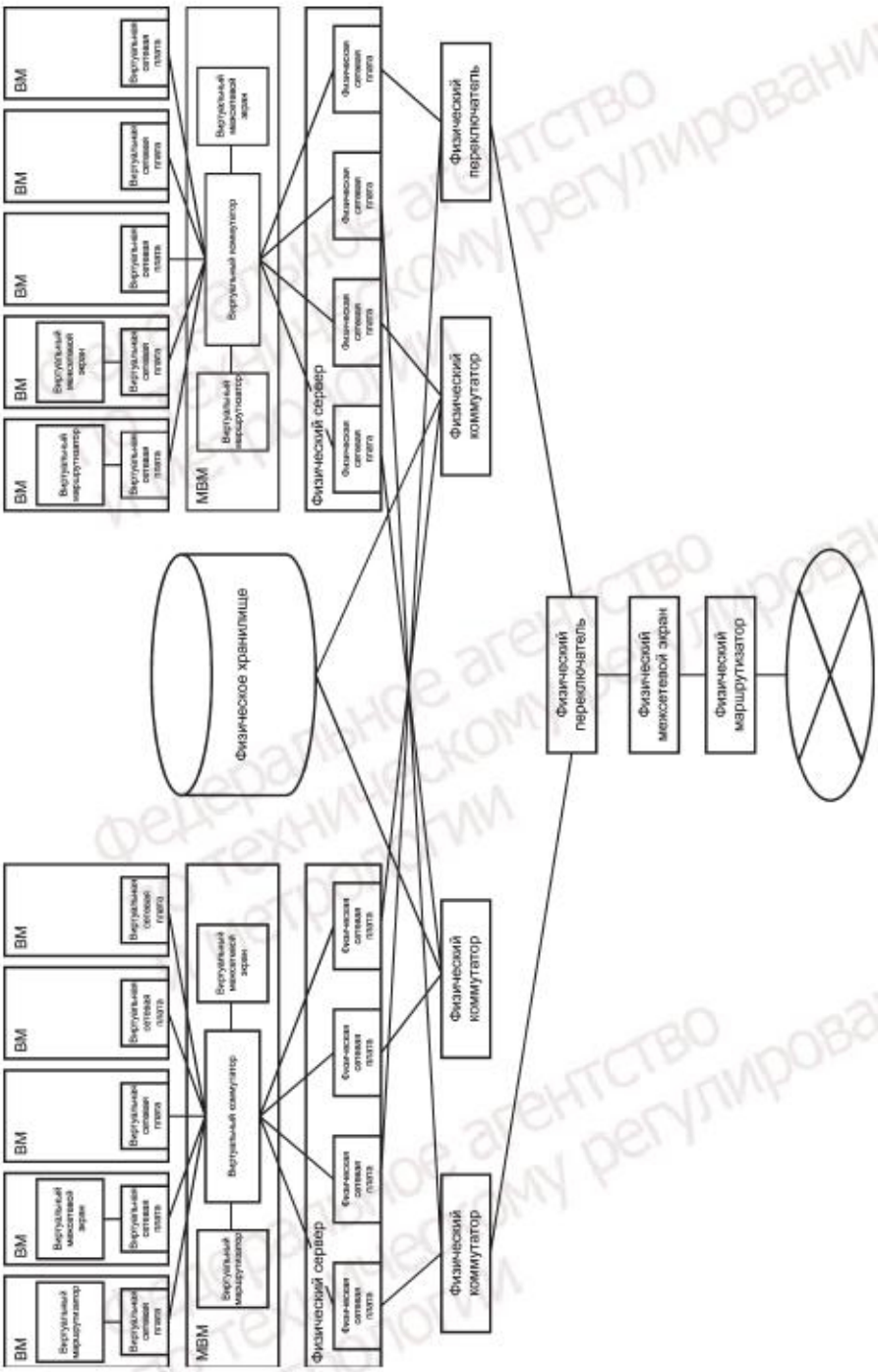

Рисунок С.4 — Обобщенная схема виртуализации сетей

С.7.3 Проведение технической оценки виртуализации сети

С.7.3.1 Управление доступом

С.7.3.2 Криптография

Мера обеспечения ИБ		ИСО/МЭК 27017, 10.1.1 Политика использования средств криптографической защиты информации	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставлять информацию клиенту облачных услуг о специфике использования средств криптографической защиты обрабатываемой им информации. Поставщик облачных услуг также должен предоставлять клиенту облачных услуг информацию о любых предоставляемых возможностях, которые могут помочь клиенту облачных услуг в применении собственных средств криптографической защиты информации	
Дополнительная техническая информация		Информация потребителей облачных услуг при доступе к облачным услугам шифруется	
1	Стандарт реализации безопасности	Пользовательские данные шифруются с помощью сетевых устройств или функций шифрования сервера	
	Техническое примечание к стандарту реализации безопасности	При шифровании используются протоколы шифрования, такие как SSL/TLS, SSH, IPSec и т. д.	
	1.1	Практическое руководство	Убедитесь, что сетевые устройства или серверы настроены для шифрования связи
		Предполагаемые свидетельства	Настройки конфигурации для шифрования на устройстве связи или сервере
		Метод	Проверка/Наблюдение, Проверка/Оценка
	1.2	Практическое руководство	Используйте анализатор пакетов для мониторинга трафика по каналу связи и подтверждения того, что полезный сетевой трафик зашифрован
		Предполагаемые свидетельства	Данные мониторинга трафика, полученные из анализатора пакетов
		Метод	Проверка/Наблюдение, Проверка/Оценка

С.7.3.3 Безопасность системы связи

Мера обеспечения ИБ		ИСО/МЭК 27017, 13.1.3 Разделение в сетях
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить следующее разделение доступа в сети: - каждого арендатора от других в предоставляемой среде; - среды внутреннего администрирования поставщика облачных услуг от среды облачных услуг клиентов. При необходимости поставщик облачных услуг должен помочь клиенту облачного сервиса проверить разделение, реализованное поставщиком облачных услуг
Дополнительная техническая информация		Для разделения сетей в облачных услугах возможно как физическое разделение с использованием физических сетей, в которых физические ресурсы не зависят друг от друга, так и логическое разделение на логические сети, совместно использующие физические ресурсы. Логические сети могут быть определены не только в физических сетях, но и на физических серверах
1	Стандарт реализации безопасности	Если потребитель облачных услуг использует отдельный индивидуальный физический ресурс (например, физический сервер, физическое хранилище), то в качестве конкретной сети для каждого потребителя облачных услуг он, соответственно, использует физическую сеть, состоящую из отдельного независимого устройства связи и линии связи.

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 13.1.3 Разделение в сетях	
		Если несколько потребителей облачных услуг в качестве арендаторов используют один и тот же физический ресурс (например, физический сервер, физическое хранилище), то они используют логически независимую сеть VLAN для каждого арендатора или виртуальной машины. Администратор облачных услуг, осуществляющий управление физическими ресурсами (например, физическим сервером, физическим хранилищем), которые используются потребителями облачных услуг, подключен к физическому порту, отличному от порта для потребителей облачных услуг, и в качестве административной сети использует физическую сеть, состоящую из физически независимого устройства связи и линии связи. Администратор облачных услуг, осуществляющий управление физическими ресурсами (например, физическим сервером, физическим хранилищем), которые используются потребителями облачных услуг, подключен к логическому порту, отличному от порта для потребителей облачных услуг, и в качестве административной сети использует логически независимую сеть VLAN	
	Техническое примечание к стандарту реализации безопасности	В случае физического разделения сетей разные физические порты на одном и том же физическом активе будут иметь разные идентификаторы. В случае логического разделения сетей разные логические сети в одной физической сети будут иметь разные идентификаторы сети VLAN, сети VSAN или разные маски подсети	
	1.1	Практическое руководство	Убедитесь, что для каждого арендатора настроена независимая сеть, не имеющая каких-либо лазеек
		Предполагаемые свидетельства	Информация о маршрутизации для сетей и идентификаторы сетей, выделенные арендаторам (таблица коммутации, таблица маршрутизации и т. д.)
		Метод	Проверка/Наблюдение, Проверка/Оценка
	1.2	Практическое руководство	Убедитесь в том, что только авторизованные лица могут получить доступ к сети, настроенной для арендаторов
		Предполагаемые свидетельства	Привилегии доступа для сетей, выделенные арендаторам (сервер контроля доступа, таблица управления правами доступа к сетевым устройствам и т. д.)
		Метод	Проверка/Наблюдение, Проверка/Оценка
	1.3	Практическое руководство	Убедитесь, что административная сеть, используемая поставщиком облачных услуг, настроена независимо от других сетей, а также убедитесь, что только лица, авторизованные поставщиком облачных услуг, могут получить доступ к настроенной административной сети
		Предполагаемые свидетельства	Настройки прав доступа и информация о маршрутизации для сети управления, используемой поставщиком облачных услуг
		Метод	Проверка/Наблюдение, Проверка/Оценка

Мера обеспечения ИБ	ИСО/МЭК 27017, CLD.13.1.4 Согласованность методов обеспечения безопасности виртуальных и физических сетей
Рекомендации по реализации для поставщика облачных услуг	Поставщик облачных услуг должен определить и документировать политику ИБ для конфигурации виртуальной сети в соответствии с политикой ИБ для физической сети. Поставщик облачных услуг должен убедиться, что конфигурация виртуальной сети соответствует политике ИБ, независимо от того, какие средства используются для ее реализации

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.13.1.4 Согласованность методов обеспечения безопасности виртуальных и физических сетей	
Дополнительная техническая информация		Если средства для настройки физических ресурсов (например, физического коммутатора, физического маршрутизатора, физической линии связи, физического сервера, физического хранилища) не зависят от средств для настройки виртуальной сети, для которой физические ресурсы являются ее частью, то для согласования параметров вручную требуются определенные навыки и полное внимание специалиста, который осуществляет конфигурацию параметров. Существуют различные примеры технических средств, которые основаны не только на навыках выполняющего настройку специалиста, а сами согласовывают настройки виртуальной сети с параметрами физической сети автоматически	
1	Стандарт реализации безопасности	Каждый отдельный элемент мер обеспечения ИБ должен быть отделен от виртуальной и физической сети, а принятая архитектура сети должна объединять все эти элементы мер обеспечения ИБ. Для управления виртуальными и физическими сетями на уровне коммутатора должен использоваться не виртуальный коммутатор, а физический коммутатор, реализующий функцию виртуального коммутатора. Следует использовать механизм синхронизации изменения параметров виртуального и физического коммутатора с динамической миграцией виртуальных машин. Кроме того, следует использовать идентификаторы сети VLAN, которые полностью адаптированы для использования тех же параметров сети даже после перемещения виртуальной машины при динамической миграции. Система администрирования виртуальных и физических сетей должна быть унифицирована, и эту унифицированную систему используют для настройки параметров	
	Техническое примечание к стандарту реализации безопасности	В случае изменения маршрутизации из-за сбоя или миграции виртуальной машины, маршрутизация виртуальных сетей по физическим сетям изменится. Кроме того, если на одном физическом сервере работает несколько арендаторов или определено несколько виртуальных машин, то на физическом сервере для виртуальных сетевых устройств (виртуальный коммутатор, виртуальный маршрутизатор и т. д.) будет настроено несколько виртуальных сетей	
	1.1	Практическое руководство	Убедитесь, что существует физический маршрут для виртуальной сети
		Предполагаемые свидетельства	Идентификатор виртуальной сети, настроенной на физическом сетевом устройстве, идентификатор виртуальной сети, настроенной на виртуальном сетевом устройстве на физическом сервере
		Метод	Проверка/Наблюдение, Проверка/Оценка
	1.2	Практическое руководство	Убедитесь, что виртуальная сеть совместима с конфигурацией физической сети, которую она использует для своих маршрутов (такие, например, параметры конфигурации, как маршрутизация, коммутация, фильтрация, управление полосой, управление приоритетами, управление доступом)
		Предполагаемые свидетельства	Конфигурация выбора маршрута (таблица коммутации, таблица маршрутизации и т. д.), фильтрация, управление полосой пропускания, расстановка приоритетов и настройка контроля доступа на физических и виртуальных сетевых устройствах
		Метод	Проверка/Наблюдение, Проверка/Оценка

С.8 Виртуализация хранилища

С.8.1 Общие сведения о виртуализации хранилища

Виртуализация хранилища представляет собой создание логического (виртуального) образа физического хранилища (диска).

Обобщенная структура виртуализации хранилища представлена на рисунке С.5.

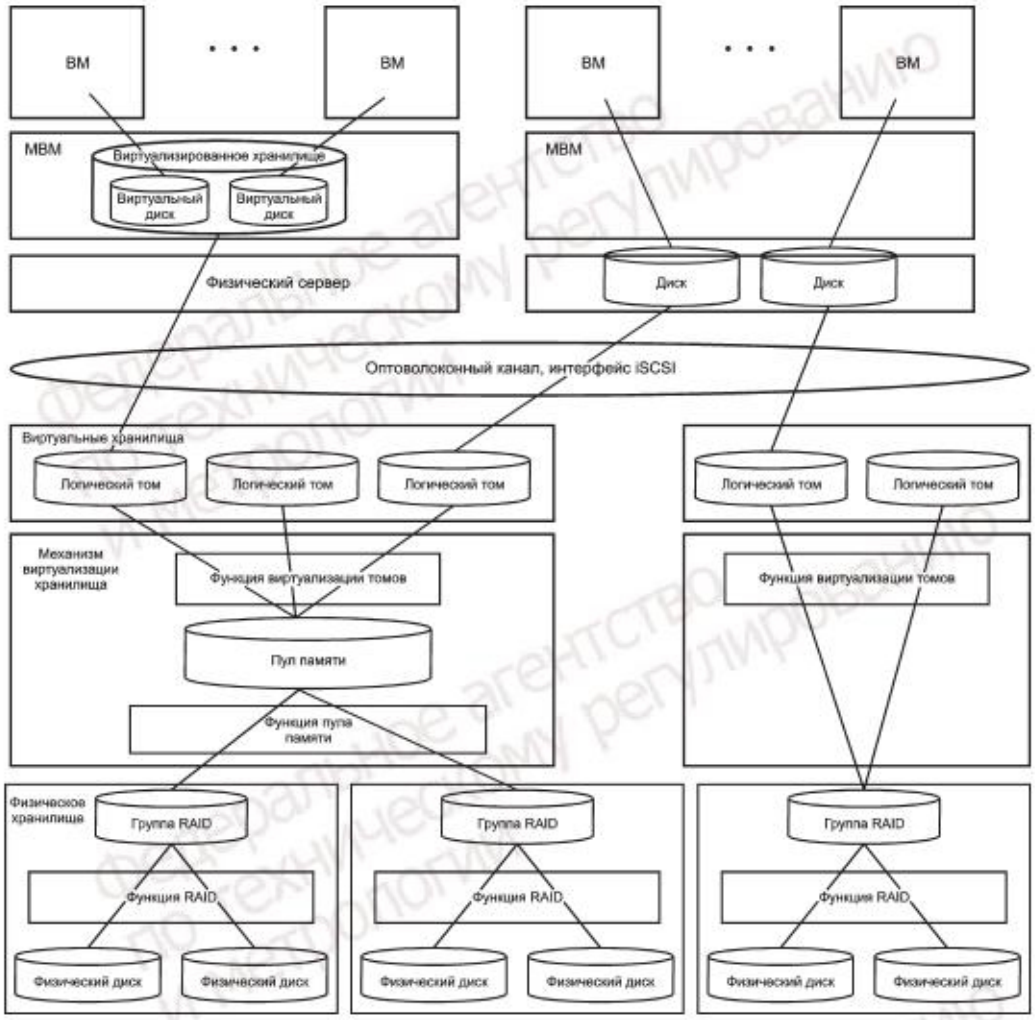

Рисунок С.5 — Структура виртуализации хранилища

a) Логический том

Важнейшим элементом виртуализации хранилища является логический том. Логический том — это единица хранения, которая может распознаваться гипервизором или ОС на виртуальной машине как отдельный виртуальный ресурс хранилища. Физические диски виртуализируются с помощью функции виртуализации хранилища.

b) Массив RAID

В последнее время все чаще в качестве устройств хранения данных используется такой логический том, как массив RAID (массив независимых дисков с избыточностью), в котором для повышения отказоустойчивости объединены более одного физического диска и используется механизм, позволяющий оптимизировать избыточность распределенных данных. Распределение данных по нескольким физическим дискам обеспечивает возможность обработки данных при повреждении физического диска.

RAID-массив позволяет виртуализировать несколько физических дисков, объединенных в один логический том.

c) Пул памяти

Функция, которая обрабатывает физические диски или логические тома как один большой логический том (пул памяти). Это функция обеспечивает гибкость работы хранилища, включая и объем дискового пространства, в

комбинации с возможностью увеличения емкости за счет добавления новых дополнительных физических дисков в существующий пул памяти.

Иногда такую функцию называют «логическая единица» или «логическое устройство» (LDev).

d) Виртуализация емкости хранилища

Функция, которая при запросе логического тома выделяет любую емкость, практически независимо от физической емкости хранилища.

При хранении данных на логическом томе это реализуется путем динамического выделения по необходимости области хранения из пула памяти. Эта функция предназначена для повышения эффективности использования ресурса хранилища.

e) Зонирование сети хранения данных

Сеть хранения данных (SAN), использующая оптоволоконный канал (FC), может разделять соединения на зоны по портам оптоволоконного коммутатора. При разделении на зоны с помощью этой функции зонирования функции хранилища для виртуализации запросов на хранилище в другой зоне блокируются.

С.8.2 Применение виртуализации хранилища в облачных услугах

a) Разделение клиентов при виртуализации хранилища

Разделение клиентов при виртуализации хранилищ осуществляется либо путем зонирования логического тома, либо зонирования сети хранения данных для каждого клиента. Следует обратить внимание, что логический том, созданный гипервизором, не обязательно назначается одному арендатору.

К виртуализации хранилища с помощью функции виртуализации сервера следует относиться с осторожностью в связи с тем, что если виртуализация хранилища или разделение клиентов происходит при виртуализации сервера, то разделение хранилища для клиентов не может быть достигнуто путем использования логических томов.

b) Расширение функций доступности при виртуализации хранилища

Доступность облачных услуг может быть расширена с помощью технологий RAID, избыточных маршрутов в оптоволоконном коммутаторе, маршрутов HBA и SAN, изменяющих конфигурацию сети хранения данных, а также функций резервного копирования, поддерживаемых физическим оборудованием хранилища.

c) Управление емкостью в виртуализации хранилища

Пул памяти и виртуализация емкости применяются при виртуализации хранения, чтобы упростить управление емкостью хранения во всех облачных сервисах и упростить управление емкостью логических томов для каждого клиента. В этом случае требуется управление как физической емкостью хранилища, предоставляемой облачным службам, так и емкостью логической памяти, предоставленной арендатору.

С.8.3 Проведение технической оценки виртуализации хранилища

С.8.3.1 Управление доступом

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.1 Разделение в виртуальных вычислительных средах
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить надлежащее логическое разделение данных для клиентов облачных услуг, виртуализированных приложений, операционных систем, хранилищ и сетей, чтобы: - разделить ресурсы, используемые клиентами облачных сервисов в средах, используемых нескольким клиентами; - отделить внутреннее администрирование поставщика облачных услуг от ресурсов, используемых клиентами облачных услуг. В тех случаях, когда облачные услуги используются одновременно несколькими клиентами, поставщик облачных услуг должен внедрить меры обеспечения ИБ, обеспечивающие надлежащую изоляцию используемых различными арендаторами ресурсов. Поставщик облачных услуг должен учитывать риски, связанные с эксплуатацией заказчиком облачных услуг стороннего программного обеспечения в рамках услуг, предлагаемых поставщиком
Дополнительная техническая информация		Типичные методы разделения хранилища: - создание логических томов для каждого арендатора и реализация управления доступом на основе логических томов; - разделение клиентов с использованием зонирования сети хранения данных
1	Стандарт реализации безопасности	Функции сегментации, обеспечиваемые виртуализированной структурой хранилища, позволяют выполнять разделение потребителей облачных услуг
	Техническое примечание к стандарту реализации безопасности	Сегментация хранилища может быть реализована гипервизором. В этом случае, ввиду структуры виртуализации хранилища, нет необходимости отделения каждого потребителя облачных услуг

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, CLD.9.5.1 Разделение в виртуальных вычислительных средах	
	1.1	Практическое руководство	В случае если клиенту предоставляется логический том, следует убедиться в том, что в настройках параметров функции виртуализации хранилища право доступа ограничено только этим клиентом
		Предполагаемые свидетельства	Параметры устройства хранения. Параметры программы управления хранилищем
		Метод	Проверка/Наблюдение
	1.2	Практическое руководство	При разделении клиентов посредством зонирования сети хранения данных, используя настройки параметров оборудования сети хранения данных, следует убедиться, что зоны выделены для каждого арендатора и что зоны хранилища недоступны другим арендаторам
		Предполагаемые свидетельства	Определение зонирования для устройства управления оптоволоконного канала, входящего в состав сети хранения данных
		Метод	Проверка/Наблюдение

С.8.3.2 Криптография

Мера обеспечения ИБ		ИСО/МЭК 27017, 10.1.1 Политика использования средств криптографической защиты информации	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставлять информацию клиенту облачных услуг о специфике использования средств криптографической защиты обрабатываемой им информации. Поставщик облачных услуг также должен предоставлять клиенту облачных услуг информацию о любых предоставляемых возможностях, которые могут помочь клиенту облачных услуг в применении собственных средств криптографической защиты	
Дополнительная техническая информация		Одним из способов шифрования хранилища является шифрование логического тома	
1	Стандарт реализации безопасности	Шифрование данных клиентов осуществляется с использованием функции шифрования для логических томов	
	Техническое примечание к стандарту реализации безопасности	Метод хранения ключей шифрования, стойкость шифрования и т.д. зависят от используемого устройства хранения	
	1.1	Практическое руководство	В случае применения функции шифрования для логических томов в виртуализации хранилища следует убедиться, что соответствующий логический том зашифрован с использованием дисплея состояния или утилит, предоставляемых функцией виртуализации хранилища
		Предполагаемые свидетельства	Параметры устройства хранения. Параметры программы управления хранилищем
		Метод	Проверка/Наблюдение

С.8.3.3 Безопасность при эксплуатации

Мера обеспечения ИБ		ИСО/МЭК 27017, 12.3.1 Резервное копирование информации	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставить спецификации своих возможностей резервного копирования клиенту облачного сервиса. В общем случае спецификации должны включать следующую информацию: - объем и график резервного копирования; - методы резервного копирования и форматы данных, включая шифрование (по необходимости); - сроки хранения резервных данных; - процедуры проверки целостности данных резервного копирования; - процедуры и сроки восстановления данных из резервной копии; - процедуры тестирования функций резервного копирования; - место хранения резервных копий. Поставщик облачных услуг должен обеспечивать безопасный и отдельный доступ к резервным копиям, таким как виртуальные моментальные снимки, если такая услуга предлагается клиентам облачных услуг	
Дополнительная техническая информация		Если оборудование хранения или программное обеспечение, которое реализует функцию виртуализации при виртуализации хранения, по какой-то причине дает сбой, то сохраняется информация, необходимая для восстановления до прежнего состояния, обеспечивающего предоставление услуг. Такая информация включает в себя параметры функции виртуализации хранилища и информацию о настройке логических томов	
1	Стандарт реализации безопасности	Резервное копирование информации о параметрах и определениях должно осуществляться с помощью утилиты функции виртуализации хранилища или другой системной утилиты	
	Техническое примечание к стандарту реализации безопасности	Если изменение виртуального ресурса хранилища влияет на информацию об определении, резервные копии данных обновляются в момент инициирования изменений или в течение надлежащего периода времени	
	1.1	Практическое руководство	Убедитесь, что информация о параметрах и определениях скопирована. Убедитесь, что изменения виртуальных ресурсов, а также время запуска и периоды резервного копирования соответствуют действительности. Проверьте, можно ли восстановить предыдущие виртуальные ресурсы из резервной копии
		Предполагаемые свидетельства	Параметры устройства хранения. Параметры программы управления хранилищем
		Метод	Проверка/Наблюдение

С.9 Управление услугами

С.9.1 Общие сведения об управлении услугами

Управление услугами представляет собой набор функций, обеспечиваемых инфраструктурой как услугой, которая позволяет потребителям облачных услуг настраивать виртуальные сети, серверы и хранилища. Управление услугами предоставляет потребителям облачных услуг через портал или другие средства интерфейс управления виртуализированными конфигурациями и поддерживает сгенерированные настройки в базе данных управления конфигурациями.

За настройку безопасности виртуальных ресурсов, предоставляемых поставщиком облачных услуг, отвечает непосредственно клиент облачных услуг, который самостоятельно выполняет настройку, например, конфигурации безопасности виртуальной машины.

Однако пользователю облачных услуг не разрешен непосредственный доступ к настройке функций механизмов виртуализации и извлечения журналов. Кроме этих действий, функции управления услугами заключаются в обеспечении взаимосвязей между физическими ресурсами и виртуальными структурами или ресурсами, а также между виртуальными ресурсами и клиентами облачных услуг. Как правило, для установления этих взаимосвязей и используется база данных управления конфигурацией (CMDB).

Пользовательский портал обеспечивает доступ к виртуальным ресурсам клиентов облачной службы и функциям виртуализации с учетом упомянутых ограничений. Кроме того, пользователям облачных услуг доступна функция отображения различных уведомлений, в том числе и об инцидентах, происходящих в облачной системе.

На рисунке С.6 показана система управления услугами в модели облачных услуг.

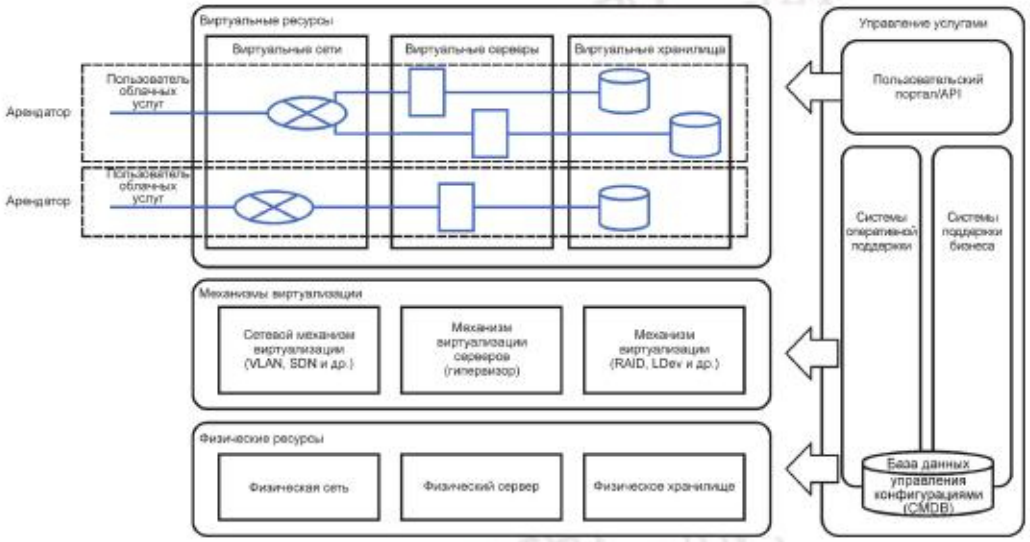

Рисунок С.6 — Система управления услугами в модели облачных услуг

С.9.2 Управление облачными услугами

a) Управление доступом

Каждая функция виртуализации наделена механизмами как контроля доступа к самой функции виртуализации, так и контроля доступа к виртуальным ресурсам. Метод аутентификации (пароль), объект применяемых прав доступа (идентификатор пользователя и т. д.) и область контроля различны для разных категорий: сети, сервера и хранилища. Управление услугами обеспечивает унифицированное управление доступом клиентов облачных услуг в качестве арендаторов путем использования соответствующих средств управления доступом для разных категорий.

b) Аутентификация пользователей

Исходной предпосылкой контроля доступа должна быть надлежащая аутентификация клиентов облачных услуг. В рамках управления услугами основными интерфейсами для клиентов облачных услуг являются пользовательские порталы и API-интерфейсы, однако аутентификация пользователей должна выполняться в первой точке доступа.

Отдельные аспекты разрешений пользователя определяются максимальным объемом доступных ему ресурсов, балансом расходов, условиями договоров и выставленными счетами. Эти аспекты управляются системой поддержки бизнеса (BSS).

В свою очередь, настройка параметров конфигурации функции виртуализации потребителями облачных услуг и управление доступом посредством вышеупомянутой функции виртуализации управляется системой поддержки операций (OSS).

c) Управление конфигурацией

Взаимосвязь между физическими серверами и виртуальными серверами, работающими на этих физических серверах; взаимосвязь между виртуальными серверами и потребителями облачных услуг; взаимосвязь между потребителями облачных услуг и условиями договоров, платежами и т. д. является важной информацией для управления и эксплуатации облачных услуг. Такая информация вместе с определениями взаимосвязей используется применяемыми средствами контроля доступа.

В системе управления услугами информация о таких конфигурациях хранится и управляется в базе данных управления конфигурациями. BSS и OSS ссылаются на эту базу данных управления конфигурацией и работают во время обновления.

В системе управления услугами информация об этих конфигурациях хранится и управляется в базе данных управления конфигурациями (CMDB). Система поддержки бизнеса и система поддержки операций используют данную базу данных управления конфигурацией и обновляют ее.

d) Менеджмент инцидентов

Менеджмент инцидентов для событий, происходящих на физических ресурсах, настроенных для предоставления облачных услуг, функций виртуализации, виртуальных ресурсов и т. д.; поиск и устранение неисправностей, а также обмен уведомлениями между поставщиком и потребителями облачных услуг обычно осуществляются системой управления услугами. Функциональные возможности менеджмента инцидентов обычно предоставляются клиентам облачных услуг на портале пользователя.

С.9.3 Проведение технической оценки управления услугами

С.9.3.1 Управление доступом пользователей

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.2.1 Регистрация и отмена регистрации пользователей	
Рекомендации по реализации для поставщика облачных услуг		Для управления доступом клиентов к облачным услугам пользователей облачных услуг поставщик облачных услуг должен предоставить клиенту облачного сервиса функции регистрации и отмены регистрации пользователей и спецификации использования этих функций	
Дополнительная техническая информация		В ИСО/МЭК 27017 (см. 9.2.1) рассматривается добавление и удаление пользователей облачных услуг в системе управления услугами. Для регистрации и удаления пользователей на виртуальных ресурсах потребитель облачных услуг, как правило, использует функциональные возможности активного ресурса (например, ОС ВМ). Поставщик облачных услуг также может предоставить потребителю облачных услуг возможность восстановления собственных данных. Способ восстановления собственных данных потребителем облачных услуг не должен зависеть от поставщика облачных услуг или от состояния системы. Кроме того, поставщик облачных услуг должен предоставлять потребителям облачных услуг возможность беспрепятственно заменять поставщика облачных услуг для снижения риска блокировки	
1	Стандарт реализации безопасности	Управление пользователями облачных услуг осуществляется в системе управления услугами. Средства управления доступом к функциям виртуализации контролируются системой управления услугами и явно не предоставляются потребителям облачных услуг	
	Техническое примечание к стандарту реализации безопасности	В случаях, если управление пользователями облачной службы возможно через портал управления услугами, на портале должна быть представлена возможность регистрации и удаления. Поскольку управление клиентом облачного сервиса является важным элементом безопасности, поставщики облачных услуг могут осуществлять регистрацию и удаление пользователей облачного сервиса при контакте с указанными пользователями	
	1.1	Практическое руководство	Подтвердите, что клиенты облачных услуг имеют возможность зарегистрировать или удалить пользователей облачных услуг через портал клиентов облачных услуг, API и т. д.
		Предполагаемые свидетельства	Экран портала и результаты действия. API, прочие интерфейсы и результаты работы API
		Метод	Проверка/Наблюдение, Тестирование

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.2.2 Предоставление пользователю права доступа
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставить функции управления правами доступа пользователей облачных услуг со стороны потребителя облачных услуг, а также спецификации для использования этих функций
Дополнительная техническая информация		В ИСО/МЭК 27017 (см. 9.2.2) рассматривается предоставление доступа для пользователей облачных услуг в системе управления услугами. Обеспечение доступа к виртуальным ресурсам (например, ОС ВМ) не входит в рамки подраздела 9.2.2
1	Стандарт реализации безопасности	Управление пользователями облачных услуг реализовано в системе управления услугами

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.2.2 Предоставление пользователю права доступа	
	Техническое примечание к стандарту реализации безопасности	Управление правами доступа для пользователей облачных услуг, обеспечиваемое управлением услугами, необязательно должно быть идентичным управлению правами доступа в функциях виртуализации. Однако в управлении услугами должно быть реализовано управление привилегиями доступа в соответствии со спецификацией управления услуг, предоставляемой потребителям облачных услуг. Предоставление доступа к управлению услугами обеспечено в виде управления услугами на портале для пользователей облачных услуг. Единая регистрация, упомянутая в разделе «Дополнительная информация для облачных служб» в этом средстве управления, реализуется на портале управления службами, а в качестве репрезентативного типа реализации может быть предоставлен язык разметки утверждений безопасности (SAML)	
	1.1	Практическое руководство	Убедитесь, что функции управления правами доступа пользователей облачных услуг предоставлены как элемент управления на пользовательском портале
		Предполагаемые свидетельства	Экран портала и результаты действия
		Метод	Проверка/Наблюдение, Тестирование
	1.2	Практическое руководство	При наличии функции единого входа необходимо убедиться, что она может использоваться с применяемыми протоколами
		Предполагаемые свидетельства	Внешнее приложение с функцией единого входа. Результат доступа к управлению услугами через внешнее приложение
		Метод	Проверка/Наблюдение, Тестирование

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.2.3 Управление привилегированными правами доступа	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставить надлежащие методы аутентификации для администраторов облачных услуг, клиента облачных услуг в соответствии с административными возможностями облачных услуг, в соответствии с выявленными рисками. Например, поставщик облачных услуг может предоставить возможность многофакторной аутентификации или разрешить использование сторонних средств многофакторной аутентификации	
Дополнительная техническая информация		ИСО/МЭК 27017 (см. 9.2.3) рассматривает рекомендации предоставления доступа для пользователей облачных услуг в системе управления услугами. Обеспечение доступа к виртуальным ресурсам (например, ОС ВМ) не подпадает под действие подраздела 9.2.3	
1	Стандарт реализации безопасности	«Достаточно строгая аутентификация», как определено в этом средстве обеспечения безопасности, реализована в качестве аутентификации на портале и в управлении услугами	
	Техническое примечание к стандарту реализации безопасности	Многофакторная аутентификация, приведенная в качестве примера «достаточно строгой аутентификации» в данном средстве обеспечения безопасности, может использовать следующие компоненты: - биометрическая аутентификация; - аутентификация с использованием токена в дополнение к паролям; - аутентификация по сертификату клиента	
	1.1	Практическое руководство	Убедитесь, что достаточно надежная аутентификация используется для аутентификации на портале управления услугами
		Предполагаемые свидетельства	Метод аутентификации и результаты тестирования достаточно строгой аутентификации, предоставляемой поставщиком облачных услуг
		Метод	Проверка/Наблюдение, Тестирование

Продолжение

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.4.1 Ограничение доступа к информации	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставлять клиенту средства управления доступом, которые позволяют ему ограничивать доступ к своим облачным услугам, своим функциям облачных услуг и своим данным, поддерживаемым услугами	
Дополнительная техническая информация		В ИСО/МЭК 27017 (см. 9.4.1) рассматривается предоставление доступа для пользователей облачных услуг в системе управления услугами. Обеспечение доступа к виртуальным ресурсам (например, ОС ВМ) не подпадает под действие подраздела 9.4.1	
1	Стандарт реализации безопасности	Информация и права доступа к ней, предоставляемые потребителю облачных услуг посредством управления услугами, предоставляются исключительно клиенту конкретного заказчика облачных услуг, и никакая информация или права доступа к ней не могут предоставляться другим клиентам. Благодаря функциям управления клиентами на портале, в тех случаях, когда можно определить информацию и привилегии доступа, обрабатываемые на основе клиента, такие операции становятся возможными	
	Техническое примечание к стандарту реализации безопасности	Несколько клиентов облачных сервисов совместно используют функцию виртуализации в облачных сервисах. Разделение клиентов осуществляется с помощью функции управления доступом к виртуализации, поэтому каждый клиент облачной службы не может получить доступ к информации других клиентов облачной службы. Контроль доступа на основе клиента может быть реализован в рамках управления услугами, а не с использованием контроля доступа для функции виртуализации	
	1.1	Практическое руководство	Используя функции управления для предоставления информации и привилегий доступа, убедитесь, что информация о других клиентах на портале недоступна
		Предполагаемые свидетельства	Экран работы портала и результаты действия
		Метод	Проверка/Наблюдение, Тестирование
	1.2	Практическое руководство	Убедитесь, что в тех случаях, когда предоставляется функциональность для обеспечения контроля доступа на основе клиента, доступ к облачным сервисам возможен в рамках диапазона привилегий доступа, настроенных для клиента
		Предполагаемые свидетельства	Экран управления потребителями и операции на портале и т. д. Результаты доступа при применении ограничений прав доступа для клиента
		Метод	Проверка/Наблюдение, Тестирование

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.4.4 Использование привилегированных служебных программ
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен определить требования для всех служебных программ, используемых в облачных услугах. Поставщик облачных услуг должен обеспечить, чтобы любое использование служебных программ, способных обходить обычные рабочие процедуры или процедуры безопасности, строго ограничивалось уполномоченным персоналом, и чтобы использование таких программ регулярно оценивалось и проверялось
Дополнительная техническая информация		Служебные программы, подключенные к функции виртуализации, могут влиять на ресурсы, не относящиеся к клиенту облачных услуг. Если клиенту облачных услуг требуются результаты служебной программы, показывающие состояние функции виртуализации и т. д., то результаты должны быть предоставлены клиенту облачного сервиса так, чтобы это не повлияло на других клиентов
1	Стандарт реализации безопасности	Потребителю облачных услуг запрещено напрямую использовать виртуализированные служебные программы, предоставляющие необходимую информацию, во избежание негативного влияния на других клиентов. Получение подобной информации должно осуществляться через управление услугами

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, 9.4.4 Использование привилегированных служебных программ	
	Техническое примечание к стандарту реализации безопасности	Служебные программы, описанные в 9.4.4 ИСО/МЭК 27017, включают: - извлечение спецификаций виртуального сервера, журналов, информации о производительности, связанной с виртуализацией сервера; - получение информации о трафике и прочих данных, связанных с виртуализацией сети; - получение копий томов, информации о доступе и прочих данных, связанных с виртуализацией сервера	
	1.1	Практическое руководство	Убедитесь, что информация из служебной программы, предоставленной клиентом облачной службы, не включает информацию, относящуюся к другим клиентам
		Предполагаемые свидетельства	Результаты использования служебной программы
		Метод	Проверка/Наблюдение, Тестирование
2	Стандарт реализации безопасности	Когда клиент облачных услуг использует служебную программу для функции виртуализации в среде клиента, то параметры виртуализации должны быть настроены таким образом, чтобы не затронуть никого, кроме этого клиента	
	Техническое примечание к стандарту реализации безопасности	Как правило, сложно использовать служебную программу, которая связана с функцией виртуализации внутри виртуального ресурса. Для проведения технической оценки в соответствии с ИСО/МЭК 27017 (см. 9.4.4) необходимо определить, существует ли какая-либо утилита, которая может превышать необходимые ресурсы виртуального ресурса, повлиять на другие ресурсы и выполнить следующие проверки, если такие ресурсы были затронуты	
	2.1	Практическое руководство	Убедитесь, что для утилит, которые могут влиять на другие ресурсы, в функции виртуализации определены параметры блокировки таких действий. Примечание — При выполнении подобных тестов следует учитывать, что это может привести к сбою в среде облачных услуг
		Предполагаемые свидетельства	Определения параметров функции виртуализации и т. д.
		Метод	Проверка/Наблюдение

С.9.3.2 Криптография

Мера обеспечения ИБ		ИСО/МЭК 27017, 10.1.1 Политика использования средств криптографической защиты информации
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен предоставлять информацию клиенту облачных услуг о специфике использования средств криптографической защиты обрабатываемой им информации. Поставщик облачных услуг также должен предоставлять клиенту облачных услуг информацию о любых предоставляемых возможностях, которые могут помочь клиенту облачных услуг в применении собственных средств криптографической защиты информации
Дополнительная техническая информация		В управлении услугами эти меры обеспечения ИБ необходимы для шифрования доступа к порталу и т. д.
1	Стандарт реализации безопасности	Примером внедрения шифрования доступа к порталу является HTTP через SSL/TLS
	Техническое примечание к стандарту реализации безопасности	Для обмена данными с порталом управления услугами используется протокол https

Окончание

Мера обеспечения ИБ		ИСО/МЭК 27017, 10.1.1 Политика использования средств криптографической защиты информации	
	1.1	Практическое руководство	Необходимо подтвердить, что в качестве протокола для портала управления услугами используется https
		Предполагаемые свидетельства	Протокол, используемый для доступа к порталу. Сертификат, используемый для доступа к порталу, и т. д.
		Метод	Проверка/Наблюдение
2	Стандарт реализации безопасности	Отдельные виды информации, относящейся к средству безопасности типа «Примечание», будут храниться для управления информацией о потребителях и пользователях облачных услуг при управлении услугами. Шифрование, определенное для этого средства безопасности, должно применяться к этой информации при необходимости в соответствии с политикой облачного провайдера	
	Техническое примечание к стандарту реализации безопасности	Шифрование данных, управление которыми осуществляется в облачной среде, представляет собой меру обеспечения ИБ самого поставщика облачных услуг и отлично от функционала, предоставляемого потребителю облачных услуг, как определено в этом средстве безопасности	
	2.1	Практическое руководство	н/д
		Предполагаемые свидетельства	н/д
		Метод	—

С.9.3.3 Менеджмент инцидентов информационной безопасности

Мера обеспечения ИБ		ИСО/МЭК 27017, 16.1.2 Сообщения о событиях информационной безопасности	
Рекомендации по реализации для поставщика облачных услуг		Поставщик облачных услуг должен обеспечить следующие механизмы: - передачи сообщений о событиях ИБ от потребителя облачных услуг к поставщику облачных услуг; - передачи сообщений о событиях ИБ от поставщика облачных услуг к потребителю облачных услуг; - отслеживания потребителем облачных услуг статуса сообщения о событии ИБ	
Дополнительная техническая информация		Как отмечается в разделе ИСО/МЭК 27017 «Дополнительная информация для облачных услуг», данные механизмы реализуются посредством телефона, электронной почты и т. д.	
1	Стандарт реализации безопасности	Функционал портала может предоставить в рамках управления услугами потребителю облачных услуг интерфейс для управления инцидентами ИБ, как определено в этом средстве обеспечения безопасности	
	Техническое примечание к стандарту реализации безопасности	При реализации этой функции в управлении услугами будут обрабатываться как сообщения, полученные от клиента облачных услуг, так и информация, предоставляемая поставщиком облака, а клиенты облачных услуг будут иметь возможность понимать текущую ситуацию, связанную с рассматриваемым инцидентом	
	1.1	Практическое руководство	Убедитесь, что портал предоставляет отчеты об инциденте ИБ и обеспечивает функциональность для оценки ситуации
		Предполагаемые свидетельства	Экраны, связанные с инцидентами ИБ, и операции на портале и т. д.
		Метод	Проверка/Наблюдение

С.10 Таблица соответствия ИСО/МЭК 27017 и настоящего приложения

Таблица С.1 — Соответствие ИСО/МЭК 27017 и настоящего приложения

Раздел	Название	Общее значение	Виртуализация серверов	Виртуализация сети	Виртуализация хранилища	Управление услугами
5	Политики информационной безопасности	Не применимо, поскольку не относится к «техническим» аспектам				
5.1	Руководящие указания в части информационной безопасности					
6	Организация деятельности по информационной безопасности	Не применимо, поскольку не относится к «техническим» аспектам				
6.1	Внутренняя организация деятельности по обеспечению информационной безопасности					
6.2	Мобильные устройства и дистанционная работа					
CLD.6.3	Взаимоотношения потребителей и поставщиков облачных услуг					
7	Безопасность, связанная с персоналом	Не применимо, поскольку не относится к «техническим» аспектам				
7.1	При приеме на работу					
7.2	Во время работы					
7.3	Увольнение и смена места работы					
8	Менеджмент активов	Не применимо, поскольку понятие «физические ресурсы» выходит за рамки указанного стандарта				
8.1	Ответственность за активы					
CLD.8.1	Ответственность за активы					
8.2	Категорирование информации					
8.3	Обращение с носителями информации					
9	Управление доступом	Общее описание управления доступом для клиентов облачных услуг приводится в разделе «Управлении услугами». Настоящий раздел не охватывает вопросы контроля доступа для операторов поставщика облачных услуг, эти вопросы рассматриваются в разделе 12. В этом разделе рассматриваются возможные настройки контроля доступа для каждого пользователя в функции виртуализации/виртуальных ресурсов, если они используются				
9.1	Требования бизнеса по управлению доступом	—	—	—	—	—
9.2	Процесс управления доступом пользователей	R	R	R	R	9.2.1 9.2.2 9.2.3
9.3	Ответственность пользователей	—	—	—	—	—
9.4	Управление доступом к системам и приложениям	R	R	R	R	9.4.1 9.4.4

Продолжение таблицы С.1

Раздел	Название	Общее значение	Виртуализация серверов	Виртуализация сети	Виртуализация хранилища	Управление услугами
CLD.9.5	Управление доступом к данным потребителя облачных услуг в виртуальной среде совместного использования	R	CLD.9.5.1 CLD.9.5.2	13.1.3	CLD.9.5.1	L
10	Криптография	Рассматриваются случаи шифрования функцией виртуализации по необходимости				
10.1	Криптографическая защита информации		10.1.1	10.1.1	10.1.1	10.1.1
11	Физическая безопасность и защита от воздействия окружающей среды	Не применимо, поскольку понятие «физические ресурсы» выходит за рамки указанного стандарта				
11.1	Зоны безопасности	—	—	—	—	—
11.2	Оборудование	—	—	—	—	—
12	Безопасность при эксплуатации	Основное внимание уделяется действиям оператора поставщика услуг для функции виртуализации/виртуальных ресурсов				
12.1	Эксплуатационные процедуры и обязанности	12.1.2 12.1.3	L	L	L	L
CLD.12.1	Эксплуатационные процедуры и обязанности	CLD12.1.5	L	L	L	L
12.2	Защита от вредоносных программ	—	—	—	—	—
12.3	Резервное копирование	R	R	R	12.3.1	L
12.4	Регистрация и мониторинг	12.4.1 12.4.4	L	L	L	L
CLD.12.4	Регистрация и мониторинг	CLD12.4.5	L	L	L	L
12.5	Контроль программного обеспечения, находящегося в эксплуатации	—	—	—	—	—
12.6	Менеджмент технических уязвимостей	12.6.1	L	L	L	L
12.7	Особенности аудита информационных систем	—	—	—	—	—
13	Безопасность системы коммуникаций	Безопасность сети				
13.1	Менеджмент безопасности сетей	R	R	13.1.3	L	—
CLD.13.1	Менеджмент безопасности сетей	R	R	CLD.13.1.4	L	L
13.2	Передача информации	—	—	—	—	—
14	Приобретение, разработка и поддержка систем	Не применимо, поскольку не имеет прямого отношения к технической модели				
14.1	Требования к безопасности информационных систем					

Окончание таблицы С.1

Раздел	Название	Общее значение	Виртуализация серверов	Виртуализация сети	Виртуализация хранилища	Управление услугами
14.2	Безопасность в процессах разработки и поддержки					
14.3	Тестовые данные	—	—	—	—	—
15	Взаимоотношения с поставщиками	Не применимо, поскольку не относится к «техническим» аспектам				
15.1	Информационная безопасность во взаимоотношениях с поставщиками					
15.2	Управление услугами, предоставляемыми поставщиком	—	—	—	—	—
16	Менеджмент инцидентов информационной безопасности					
16.1	Менеджмент инцидентов информационной безопасности и улучшений	R	R	R	R	16.1.2
17	Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации					
17.1	Непрерывность информационной безопасности					
17.2	Резервирование оборудования					
18	Соответствие					
18.1	Соответствие правовым и договорным требованиям					
18.2	Проверка информационной безопасности					

Примечание — В настоящей таблице использованы следующие условные обозначения:
знак «—» — в ИСО/МЭК 27017 не определены меры обеспечения ИБ поставщика облачных услуг;
«L» — ссылка на соответствующий раздел находится слева от этой графы;
«R» — ссылка на соответствующий раздел находится справа от этой графы;
пустая ячейка — никаких технических действий не требуется.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
ISO/IEC 27017:2015	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] ISO Guide 73, Risk management — Vocabulary

[2] ISO 19011:2018, Guidelines for auditing management systems

[3] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[4] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[5] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[6] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[7] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing

[8] ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[9] NIST Special publication (SP) 800-53A, Guide for reviewing the controls in federal information systems, July 2008. Available from: https://csrc.nist.gov/publications/PubsSPs.html

[10] Institute For Security And Open Methodologies. Open-Source Security Testing Methodology Manual. Available from: http://www.isecom.org/research/osstmm.html

[11] Federal Office for Information Security (BSI). Germany, Standard 100-1, Information Security Management Systems (ISMS); 100-2, IT-Grundschutz Methodology; 100-3, Risk Analysis based on IT-Grundschutz and IT-Grundschutz Catalogues, 100-4, Business Continuity Management (available in German and English). Available from: https://www.bsi.bund .de/EN/Topics/ITGrundschutz/itgrundschutz.html

[12] Information Security Forum, The Standard of Good Practice for Information Security, 2007. Available from: https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030 IDT

Ключевые слова: информационная безопасность, мера обеспечения информационной безопасности, оценка информационной безопасности, оценка технического соответствия, метод оценки, план оценки, процедура оценки, аудитор

Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 24.05.2021. Подписано в печать 22.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 10,70. Уч.-изд. л. 9,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru