ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью

ISO/IEC TR 27008:2011
Information technology -- Security techniques -- Guidelines for auditors on information security controls
(IDT)

Издание официальное

Москва
Стандартинформ
2015

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ФГУП «ВНИИНМАШ»), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от «11» июня 2014 г. № 569-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TR 27008:2011 «Информационная технология. Методы обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью» (ISO/IEC TR 27008:2011 «Information technology – Security techniques – Guidelines for auditors on information security controls»)

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 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 (gost.ru)

Содержание

Введение

ИСО/МЭК ТО 27008 был подготовлен совместным техническим комитетом ИСО/МЭК СТК 1 «*Информационная технология*», подкомитетом ПК 27 «*Методы и средства обеспечения безопасности ИТ*».

Настоящий стандарт поддерживает определенный в ИСО/МЭК 27001 и ИСО/МЭК 27005 процесс менеджмента риска системы менеджмента информационной безопасности (СМИБ), а также меры и средства контроля и управления, включенные в ИСО/МЭК 27002.

Настоящий стандарт предоставляет руководство по проверке мер и средств контроля и управления информационной безопасностью организации, например, в организации, процессах бизнеса и системном окружении, включая проверку технического соответствия.

За рекомендациями по аудиту элементов систем менеджмента следует обращаться к ИСО/МЭК 27007, а по проверке соответствия СМИБ требованиям для целей сертификации – к ИСО/МЭК 27006.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью

Information technology – Security techniques – Guidelines for auditors on information security controls

Дата введения — 2015—06—01

1 Область применения

Настоящий стандарт предоставляет руководство по проверке реализации и функционирования мер и средств контроля и управления, включая проверку технического соответствия мер и средств контроля и управления информационных систем, согласно установленным в организации стандартам по информационной безопасности.

Настоящий стандарт применим для организаций всех видов и любой величины, включая акционерные общества открытого и закрытого типа, государственные учреждения и некоммерческие организации, проводящие проверки информационной безопасности и технического соответствия. Настоящий стандарт не предназначен для аудитов систем менеджмента.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок следует использовать только указанное издание, для недатированных ссылок – последнее издание указанного документа (включая все его изменения).

ИСО/МЭК 27000:2009[1)] *Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология (*ISO/IEC 27000:2009, *Information technology – Security techniques –Information security management systems – Overview and vocabulary*).

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями:

3.1 **объект проверки** (review object): Конкретный проверяемый элемент.

3.2 **цель проверки** (review objective): Формулировка, описывающая, что должно быть достигнуто в результате проверки.

3.3 **стандарт реализации безопасности** (security implementation standard): Документ, предписывающий санкционированные способы реализации безопасности.

4 Структура настоящего стандарта

Настоящий стандарт содержит описание процесса проверки мер и средств контроля и управления информационной безопасностью, включая проверку технического соответствия.

В разделе 5 представлена вводная информация.

В разделе 6 представлен общий обзор проверок мер и средств контроля и управления информационной безопасностью.

В разделе 7 представлены методы проверок , а в разделе 8 – деятельность по проверке–.

В приложении А приведено практическое руководство по проверке технического соответствия, а в приложении В дается описание начала сбора информации –.

[1)] Отменен. Действует ИСО/МЭК 27000:2014. Для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только указанный ссылочный стандарт.

5 Предпосылки

Меры и средства контроля и управления информационной безопасностью организации должны выбираться организацией на основе результата оценки риска в рамках процесса менеджмента риска информационной безопасности, чтобы снижать свои риски до допустимого уровня. Однако организации, решившие не реализовывать СМИБ, могут отдать предпочтение другим способам выбора, реализации и поддержки мер и средств контроля и управления информационной безопасностью.

Часть мер и средств контроля и управления информационной безопасностью организации обычно осуществляется путем реализации технических мер и средств контроля и управления информационной безопасностью, например, когда информационные активы включают информационные системы.

Технические меры и средства контроля и управления информационной безопасностью необходимо определять, документально оформлять, реализовать и поддерживать в соответствии со стандартами, относящимися к информационной безопасности. С течением времени на эффективность мер и средств контроля и управления информационной безопасностью и в конечном счете на применение в организации стандартов информационной безопасности могут оказывать негативное влияние внутренние факторы, такие как корректировки информационных систем, конфигурации функций безопасности и изменения окружающей среды информационных систем, а также внешние факторы, такие как совершенствование навыков атаки. У организаций должна быть строгая программа контроля изменений, касающихся информационной безопасности. Организации должны регулярно проверять, осуществляется ли соответствующее применение стандартов, касающихся реализации безопасности, и их действие. Проверка технического соответствия включена в ИСО/МЭК 27002:2005 в качестве одной из мер и средств контроля и управления, осуществляемой вручную и/или посредством специальных проверок с помощью автоматизированных инструментальных средств. Она может осуществляться лицами, выполняющими роль, не задействованную в осуществлении меры и средства контроля и управления (например, владельцем системы или персоналом, отвечающим за конкретные меры и средства контроля и управления), или внутренними или внешними специалистами по обеспечению информационной безопасности, включая аудиторов информационной технологии (ИТ).

Результат проверки технического соответствия объясняет фактический уровень технического соответствия реализации информационной безопасности в организации требованиям стандартов. Это обеспечивает уверенность в том, что состояние технических мер и средств контроля и управления соответствует стандартам информационной безопасности или, в противном случае, служит основой для совершенствования. В начале проверки должна быть четко установлена последовательность отчетности по аудиту и должна обеспечиваться целостность процесса отчетности. Должны предприниматься шаги, чтобы обеспечить:

- получение соответствующими ответственными сторонами неизмененной копии отчета непосредственно от аудиторов, проводящих проверку мер и средств контроля и управления информационной безопасностью;
- невозможность получения несоответствующими или неуполномоченными сторонами копии отчета от аудиторов, проводящих проверку мер и средств контроля и управления информационной безопасностью;
- возможность беспрепятственного выполнения работы аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью.

Проверки мер и средств контроля и управления информационной безопасностью, в особенности проверки технического соответствия могут помочь организации:

- установить и понять степень серьезности потенциальных проблем или недостатков реализации и действия мер и средств контроля и управления информационной безопасностью, стандартов информационной безопасности и, в результате, технических мер и средств контроля и управления информационной безопасностью организации;
- установить и понять потенциальное влияние на организацию воздействия недостаточно ослабленных угроз и уязвимостей информационной безопасности;
- установить приоритеты в действиях по уменьшению риска информационной безопасности;
- подтвердить, что вопрос, касающийся ранее установленных или возникающих слабых мест или недостатков информационной безопасности, был адекватным образом решен;
- поддерживать бюджетные решения в рамках инвестиционного процесса и другие решения руководства, связанные с совершенствованием менеджмента информационной безопасности организации.

Настоящий стандарт предназначен для проверки мер и средств контроля и управления информационной безопасностью, включая проверку технического соответствия относительно реализации организацией установленного стандарта по информационной безопасности. Настоящий стандарт не

предназначен для предоставления какого-либо конкретного руководства по проверке соответствия в отношении измерений, оценки риска или аудита СМИБ, как определено в ИСО/МЭК 27004, ИСО/МЭК 27005 или ИСО/МЭК 27007 соответственно.

Использование настоящего стандарта в качестве отправной точки процесса определения процедур для проверки мер и средств контроля и управления информационной безопасностью способствует более стабильному уровню информационной безопасности в рамках организации. Он предлагает необходимую гибкость в уточнении параметров процесса проверки на основе целевой задачи и целей бизнеса, политик и требований организации, известной информации об угрозах и уязвимостях, представлений об операционной деятельности, зависимостей информационных систем и платформ и готовности рисковать.

Примечание – ИСО Руководство 73 определяет готовность рисковать как величину и вид риска, который организация готова рассматривать, сохранять или принимать.

6 Обзор проверок мер и средств контроля и управления информационной безопасностью

6.1 Процесс проверки

Приступая к конкретной проверке, относящейся к информационной безопасности, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, обычно начинают со сбора предварительной информации, рассмотрения планируемого объема и содержания работ, установления связи с руководителями и другими контактными лицами в соответствующих частях организации и расширенной оценки риска, связанного с проверкой, чтобы разработать документацию по проверке, представляющую собой руководство по осуществляемой проверочной деятельности. Для эффективного осуществления проверок назначенные аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны быть хорошо подготовлены как в области мер и средств контроля и управления, так и в области тестирования (например, эксплуатация применимых инструментальных средств, техническая цель тестирования). На этом уровне могут быть установлены приоритетные этапы работы по проверке в соответствии с осознаваемыми рисками, также этапы работы могут быть спланированы согласно определенному процессу бизнеса или системы или могут быть разработаны просто для последовательного охвата всех сфер, входящих в область проверки.

Предварительная информация может поступать из различных источников:

- книги, Интернет, технические руководства, стандарты и другие общие сведения, содержащиеся в исследовательских работах по распространенным рискам и мерам и средствам контроля и управления в данной сфере, материалах конференций, симпозиумов, семинаров или форумов;
- результаты предыдущих проверок, тестирований и оценок, частично или полностью относящихся к текущей области проверки и так или иначе выполненных аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью (например, предварительные тесты безопасности, проведенные специалистами по обеспечению информационной безопасности, могут дать обширные знания по безопасности основных прикладных систем);
- сведения о соответствующих инцидентах информационной безопасности, ситуациях, близких к инцидентам, вопросах поддержки и изменениях, полученные от службы технической поддержки ИТ, из процессов менеджмента изменений ИТ, процессов менеджмента инцидентов ИТ и из аналогичных источников;
- общие перечни контрольных проверок и договоров, касающихся проверки мер и средств контроля и управления информационной безопасностью и проводимых аудиторами или специалистами по информационной безопасности с опытом работы в данной сфере.

Может быть уместным проведение пересмотра планируемой области проверки в свете предварительной информации, особенно если план проверки, первоначально определивший область проверки, подготавливался за много месяцев до этого. Например, дополнительные проверки могут раскрыть проблемы, заслуживающие более глубокого исследования, или, наоборот, могут обеспечить бóльшую уверенность в некоторых областях, позволяя сосредоточить назначенную работу на чем-то другом.

На начальном этапе важно установить связи с руководителями и контактными лицами, связанными с проверкой. По завершении процесса проверки от этих людей требуется понимание выводов проверки, чтобы адекватно реагировать на отчет о результатах проверки. Взаимопонимание, взаимное уважение и способность объяснить процесс проверки существенно повышают качество и эффективность результата.

Поскольку способ документального оформления своей работы разными лицами различается, то для многих функций проверки используют стандартизированные процессы проверки, поддерживаемые документами-шаблонами для рабочих материалов, такими как контрольные перечни для проверки, опросные листы по внутреннему контролю, графики тестирования, таблицы управления риском и т. д.

Контрольный перечень для проверки (или аналогичный документ) является основным документом по нескольким причинам:

- в нем изложены планируемые сферы проверочной деятельности, возможно, и уровни детального описания отдельных тестов по проверке и ожидаемые/идеальные выводы;
- он предоставляет состав работ, способствуя обеспечению уверенности в полном охвате планируемой области;
- необходимый для создания контрольного перечня анализ в первую очередь подготавливает аудиторов, проводящих проверку мер и средств контроля и управления информационной безопасностью, к последующей практической проверочной деятельности, в то время как заполнение контрольного перечня в ходе проверки способствует развитию аналитического процесса, из которого будут выводиться данные для отчета о результатах проверки;
- он предоставляет рамки для фиксирования результатов предварительной обработки информации и практической проверочной деятельности, а также, например, место для ссылок и комментариев к собранным свидетельствам проверки;
- он может быть проверен руководителями аудита или другими аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью, как часть процесса по обеспечению качества проверки;
- будучи полностью заполненным, он (наряду со свидетельствами проверки) представляет собой достаточно подробную запись о проведенной проверочной деятельности и полученных выводах, которая может потребоваться для обоснования или подтверждения отчета о результатах проверки, информирования руководства и/или помощи при планировании будущих проверок.

Аудиторы информационной безопасности должны проявлять осторожность, чтобы просто использовать общие контрольные перечни для проверки, составленные другими, так как за исключением возможной экономии времени это, вероятно, сведет на нет некоторые из вышеперечисленных выгод. [Это, по-видимому, менее проблематично в случае прямых проверок соответствия или сертификационных проверок, потому что требования, которые должны выполняться обычно являются достаточно определенными.]

Основной объем практической проверочной деятельности состоит из серии тестов, проводимых самими аудиторами или по их запросу, для сбора свидетельств проверки и их рассмотрения часто путем сравнения с ожидаемыми результатами, которые выводятся из соответствующих обязательств по обеспечению соответствия, стандартов или из более общей оценки хороших практических приемов. Например, один из тестов в рамках проверки информационной безопасности, изучающий меры и средства контроля и управления для защиты от вредоносного программного средства, может проверять, существуют ли на всех применяемых компьютерных платформах соответствующие антивирусные программы. При применении для проверки тестов, подобных указанному, часто используют метод выборки, поскольку для всеохватывающей проверки обычно бывает недостаточно ресурсов. Практические приемы выборки различаются в зависимости от аудиторов, ситуаций и могут включать случайную выборку, стратифицированную выборку и другие более сложные статистические методы выборки (например, использование дополнительной выборки, если первоначальные результаты неудовлетворительны, чтобы подтвердить степень слабости мер и средств контроля и управления). Как правило, полное тестирование возможно в тех случаях, когда свидетельства могут быть собраны и протестированы электронным способом, например, используя запросы SQL[1)] в базе данных свидетельств проверки, подобранных из систем или баз данных менеджмента активов. Подход к выборочному аудиторскому обследованию должен, по крайней мере, частично определяться рисками, связанными с подвергающейся аудиту сферой деятельности.

Собранные в ходе проверки свидетельства должны отмечаться, упоминаться или вноситься в список рабочих документов проверки. Свидетельства проверки, наряду с анализом, выводами, рекомендациями по проверке и отчетами о результатах проверки, должны быть надлежащим образом защищены аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью, особенно в связи с тем, что некоторые свидетельства являются крайне чувствительными и/или ценными. Защита данных, извлеченных, например, из используемых в организации баз данных с целью проверки, должна обеспечиваться в той же степени, что и защита самих баз данных, путем использования мер и средств контроля и управления доступом, шифрования и т. д. Автоматизированные инструментальные средства проверки, запросы, утилиты/программы извлечения данных

[1)] SQL (Structured Query Language) – Язык структурированных запросов.

и т. д. должны строго контролироваться. Защита распечаток, сделанных или полученных аудиторами, проводящими проверку мер и средств контроля и управления информационной безопасностью, должна обеспечиваться путем содержания их «под замком» для предотвращения несанкционированного раскрытия или модификации. В случае особенно чувствительных проверок риски, а, следовательно, необходимые меры и средства контроля и управления информационной безопасностью должны быть идентифицированы и подготовлены на раннем этапе проверки.

Заполнив контрольный перечень для проверки, проведя серию тестов и собрав достаточно свидетельств проверки, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, смогут изучить свидетельства, определить степень обработки рисков информационной безопасности и проверить потенциальное влияние любых остаточных рисков. На этом этапе обычно составляется проект отчета о результатах проверки в произвольной форме, его качество рассматривается в рамках функции проверки и обсуждается с руководством, особенно с руководством филиалов организации, отделов, функциональных подразделений или групп, непосредственно подпадающих под проверку, и, возможно, также других затрагиваемых подразделений организации.

Руководители аудита должны беспристрастно рассматривать свидетельства аудита с целью проверки что:

- существует достаточное количество свидетельств проверки для обеспечения фактической основы, подтверждающей все выводы проверки;
- все выводы и рекомендации являются важными в отношении области проверки, а все несущественные вопросы исключаются.

Если, исходя из выводов, планируется дальнейшая работа по проверке, это должно быть отмечено в отчете.

Процесс анализа, как и планирование проверки, по существу, основан на риске, хотя и располагает бóльшей информацией благодаря свидетельствам, собранным во время проверочной деятельности. В то время как прямые проверки соответствия обычно могут давать ряд относительно простых результатов «пройдено/не пройдено» с достаточно очевидными рекомендациями, проверки информационной безопасности часто формируют вопросы, требующие размышлений и обсуждений руководства до принятия решения о том, какие действия (если таковые необходимы) будут соответствующими. В некоторых случаях руководство может вынести решение о принятии некоторых рисков, идентифицированных в результате проверки информационной безопасности, в других – не принимать рекомендации проверки в точности так, как они изложены – это право руководства, но оно также несет ответственность за свои решения. В этом отношении аудиторская проверка мер и средств контроля и управления информационной безопасностью имеет рекомендательное, а не практическое значение, хотя и обладает существенным влиянием и опирается на надежные практические приемы проверки и фактические свидетельства.

Аудиторская проверка мер и средств контроля и управления информационной безопасностью должна предоставить организации, с учетом оценки, обоснованную уверенность в том, что деятельность по обеспечению информационной безопасности (не все будут реализовывать систему менеджмента) достигает установленных целей. В результате проверки должно предоставляться изложение отличий между реальностью и эталоном. Если эталоном является внутренняя политика, то она должна быть очень четкой. Для уверенности в этом во внимание могут приниматься критерии, приведенные в приложении В. При аудиторской проверке мер и средств контроля и управления информационной безопасностью должны учитываться внутренние политики и процедуры в рамках области проверки. Недостающие важные критерии неформально все же могут быть применены в организации. Отсутствие критериев, идентифицированных как критические, может быть причиной потенциальных несоответствий.

6.2 Подбор персонала

Проверка мер и средств контроля и управления информационной безопасностью требует от персонала объективного анализа и профессиональных навыков в сфере отчетности. В случаях, когда речь идет о проверке 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 проверку мер и средств контроля и управления информационной безопасностью, должны обладать:

- способностью различать риски информационных систем и архитектур безопасности, основанной на понимании концептуальных структур, поддерживающих информационные системы;
- знанием хороших практических приемов обеспечения информационной безопасности, таких как методы и средства контроля и управления информационной безопасностью, представленные в ИСО/МЭК 27002 и других стандартах по безопасности;
- способностью к изучению сложной технической информации для идентификации любых существенных рисков и возможностей модернизации;

- прагматизмом в отношении практических ограничений проверок, как информационной безопасности, так и информационной технологии.

Настоятельно рекомендуется, чтобы лица, перед которыми ставится задача проведения проверки мер и средств контроля и управления информационной безопасностью, но которые не имеют аудиторского опыта, были официально ознакомлены с основами профессии аудитора: 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.

Для достижения цели проверки может быть создана группа проверки, состоящая из аудиторов, осуществляющих проверку мер и средств контроля и управления информационной безопасностью, 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 выгоды от привлечения специалистов к данной предметной области, выбираемых либо из собственных, либо из внешних ресурсов, для выполнения проверки в необходимом объеме.

Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны также подтвердить, что служба и персонал, отвечающие за обеспечение информационной безопасности, присутствуют, являются достаточно квалифицированными в области информационной безопасности и своих конкретных целевых задач и имеют в своем распоряжении необходимые ресурсы.

В рамках программы организации по противодействию мошенничеству аудиторам, проводящим проверку мер и средств контроля и управления информационной безопасностью, необходимо работать в тесном сотрудничестве с финансовыми аудиторами на каждом из этапов: планирование аудита, проведение аудита и анализ результатов аудита.

7 Методы проверок

7.1 Обзор

Основу концепции проверки мер и средств контроля и управления обычно составляют процедуры проверки, отчетность по проверке и контроль исполнения. Структура и содержание процедур проверки учитывают цели и методы проверки.

Аудиторы, проводя проверку мер и средств контроля и управления информационной безопасностью, могут использовать три метода проверки:

- изучение;
- опрос;
- тестирование.

В соответствующих разделах содержится набор атрибутов и значения атрибута для каждого метода проверки. Для атрибута «глубина» значение целевого атрибута основывается на строгости и уровне детальности проверки, определенных для значения общего атрибута. Значение детального атрибута основывается на строгости и уровне детальности проверки, определенных для значения целевого атрибута. Для атрибута «охват» значение специального атрибута основывается на числе и виде объектов проверки, определенных для значения репрезентативного атрибута. Значение всестороннего атрибута основывается на числе и виде объектов проверки, определенных для значения специального атрибута.

Методы «Изучение» и «Тестирование» могут поддерживаться при помощи применения широко признанных автоматизированных инструментальных средств. Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны рассматривать влияние действия этих инструментальных средств на обычное функционирование объекта проверки. Если часть проверки основана на таком инструментальном средстве, то аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны продемонстрировать или предоставить свидетельства того, что это инструментальное средство обеспечивает надежные результаты.

7.2 Метод проверки: изучение

7.2.1 Общая информация

Изучение – процесс сверки, обследования, проверки, наблюдения, исследования или анализа одного или нескольких объектов проверки с целью облегчения понимания и достижения ясности или получения свидетельств, результаты которых используются для поддержки решения о существовании, функциональных возможностях, правильности и полноте мер и средств контроля и управления, а также возможности их совершенствования с течением времени.

Объекты проверки обычно включают в себя:

- спецификации[1)] (например, политики, планы, процедуры, требования к системам, проекты);
- механизмы (например, функциональные возможности, реализуемые аппаратным, программным, программно-аппаратным способом);
- процессы (например, операции, администрирование, менеджмент, испытания систем).

К типичным действиям аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, можно отнести:

- проверку политик, планов и процедур обеспечения информационной безопасности;
- анализ проектной документации систем и спецификаций интерфейсов;
- наблюдение за операциями резервного копирования систем и проверка результатов учений, проводимых в соответствии с планом действий в чрезвычайных ситуациях;
- наблюдение за процессом реагирования на инциденты;
- изучение технических инструкций и руководств пользователя/администратора;
- проверка, изучение или наблюдение за функционированием механизма ИТ в аппаратных средствах/программном обеспечении информационной системы;
- проверка, изучение или наблюдение за деятельностью по менеджменту изменений и регистрации, связанной с информационной системой;
- проверка, изучение или наблюдение за мерами физической защиты, связанными с функционированием информационной системы.

7.2.2 Атрибуты

7.2.2.1 Общее изучение

Общее изучение обычно состоит из высокоуровневых проверок, рассмотрений, наблюдений или обследований объекта проверки. Этот вид изучения проводится с использованием ограниченной совокупности свидетельств или документации (например, описания функционального уровня механизмов; описания высокоуровневого процесса для процессов; фактическая документация для спецификаций). Общее изучение обеспечивает уровень понимания мер и средств контроля и управления, необходимый для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок.

7.2.2.2 Целевое изучение

Целевое изучение обычно состоит из высокоуровневых проверок, рассмотрений, наблюдений или обследований и более углубленного изучения/анализа объекта проверки. Этот вид изучения проводится с использованием значительной совокупности свидетельств или документации (например, описания функционального уровня и, где это необходимо и доступно, высокоуровневая проектная информация для механизмов; высокоуровневое описание процессов и процедуры реализации для процессов; фактическая документация и взаимосвязанные документы для спецификаций). Целевое изучение обеспечивает уровень понимания меры и средства контроля и управления безопасностью, необходимый для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок. Оно также дает бóльшее основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось.

7.2.2.3 Детальное изучение

Детальное изучение обычно состоит из высокоуровневых проверок, рассмотрений, наблюдений или обследований и более углубленного, всестороннего и тщательного изучения/анализа объекта проверки. Этот вид изучения проводится с использованием обширной совокупности свидетельств или документации (например, описания функционального уровня и, где это необходимо и доступно, высокоуровневая проектная информация, низкоуровневая проектная информация и информация по реализации для механизмов; высокоуровневые описания процессов и детальные процедуры реализации для процессов; а также фактическая документация и взаимосвязанные документы для спецификаций). Детальное изучение обеспечивает уровень понимания меры и средства контроля и управления, необходимый для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок, существует ли возросшее основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось, на постоянной и непротиворечивой основе, и что обеспечивается поддержка постоянного совершенствования эффективности меры и средства контроля и управления.

7.2.2.4 Репрезентативное изучение

Репрезентативное (выборочное) изучение использует характерную выборку объектов проверки (по виду и числу в пределах вида) для обеспечения уровня охвата, необходимого для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок.

[1)] Спецификация – документ, устанавливающий требования (см. ГОСТ ИСО 9000–2011, пункт 3.7.3)

7.2.2.5 Специальное изучение

Специальное изучение использует характерную выборку объектов проверки (по виду и числу в пределах вида) и другие конкретные исследования объектов проверки, сочтенные особенно важными для достижения цели проверки. Оно также обеспечивает уровень охвата, необходимый для определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок, и возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось.

7.2.2.6 Всестороннее изучение

Всестороннее изучение, использует достаточно большую выборку объектов проверки (по виду и числу в пределах вида) и другие конкретные исследования объектов проверки, сочтенные особенно важными для достижения цели проверки, чтобы обеспечить уровень охвата, необходимый для определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок, возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось, на постоянной и непротиворечивой основе, а также что обеспечивается поддержка постоянного совершенствования эффективности меры и средства контроля и управления.

7.3 Метод проверки: опрос

7.3.1 Общая информация

Опрос – процесс проведения бесед с лицами или группами лиц в рамках организации с целью содействия пониманию, достижению ясности или указанию местонахождения свидетельств. Результаты его должны использоваться для поддержки решения о существовании меры и средства контроля и управления безопасностью, функциональных возможностях, правильности, полноте мер и средств контроля и управления и возможности их совершенствования с течением времени.

К объектам проверки обычно относятся отдельные лица или группы лиц.

Типичная деятельность аудитора, проводящего проверку меры и средства контроля и управления информационной безопасностью, может включать опрос:

- руководителей;
- владельцев информационных активов и лиц, ответственных за целевую задачу;
- служащих, отвечающих за информационную безопасность;
- руководителей в сфере информационной безопасности;
- сотрудников отдела кадров;
- руководителей отдела кадров;
- руководителей, отвечающих за оборудование;
- служащих, отвечающих за обучение;
- операторов информационных систем;
- сетевых и системных администраторов;
- руководителей площадок;
- служащих, обеспечивающих физическую защиту;
- пользователей.

7.3.2 Атрибуты

7.3.2.1 Общий опрос

Общий опрос состоит из хорошо организованных бесед общего назначения с отдельными лицами или группами лиц. Этот вид опроса проводится с использованием совокупности обобщенных вопросов высокого уровня. Общие опросы обеспечивают уровень понимания меры и средства контроля и управления безопасностью, необходимый для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок.

7.3.2.2 Целевой опрос

В дополнение к необходимым элементам общего опроса, целевой опрос включает углубленное обсуждение конкретных сфер с лицами или группами лиц. При этом виде опроса дополнительно используются конкретные вопросы, касающиеся конкретных сфер, ответы на которые указывают на необходимость более глубокого исследования. Целевые опросы обеспечивают уровень понимания меры и средства контроля и управления, необходимый для определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок и возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось.

7.3.2.3 Детальный опрос

В дополнение к необходимым целевым опросам, детальный опрос включает более глубокие «зондирующие» вопросы в конкретных сферах, ответы на которые указывают на потребность в более глубоком исследовании или, где это требуется, процедурах проверки. Детальные опросы обеспечивают уровень понимания меры и средства контроля и управления безопасностью, необходимый для

определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок, возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и на постоянной и непротиворечивой основе функционируют, как предназначалось, а также что обеспечивается поддержка постоянного совершенствования эффективности меры и средства контроля и управления.

7.3.3 Атрибут «охвата»

Атрибут «охвата» рассматривает объем или широту процесса опроса и затрагивает типы лиц, подлежащих опросу (по их роли и соответствующим обязанностям в организации), число лиц, подлежащих опросу (по типу), и конкретных лиц, подлежащих опросу.

7.3.3.1 Репрезентативный опрос

Репрезентативный (выборочный) опрос – опрос выбранной группы лиц с ключевыми ролями в организации для обеспечения уровня охвата, необходимого для определения, реализованы ли мера и средство контроля и управления и нет ли в них очевидных ошибок.

7.3.3.2 Специальный опрос

Специальный опрос – опрос выбранной группы лиц с ключевыми ролями в организации и других конкретных лиц, сочтенных особенно важными для достижения цели проверки, чтобы обеспечить уровень охвата, необходимый для определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок и возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и функционируют, как предназначалось.

7.3.3.3 Всесторонний опрос

Всесторонний опрос – опрос достаточно большой выбранной группы лиц с ключевыми ролями в организации и других конкретных лиц, сочтенных особенно важными для достижения цели проверки, чтобы обеспечить уровень охвата, необходимый для определения, реализованы ли мера и средство контроля и управления, нет ли в них очевидных ошибок, возросло ли основание для уверенности в том, что мера и средство контроля и управления реализованы правильно и на постоянной и непротиворечивой основе функционируют, как предназначалось, а также что обеспечивается поддержка постоянного совершенствования эффективности меры и средства контроля и управления.

7.4 Метод проверки: тестирование

7.4.1 Общая информация

Тестирование – процесс испытания одного или нескольких объектов проверки при определенных условиях, который проводится для сравнения реального поведения с ожидаемым. Результаты используются для поддержки решения о наличии, эффективности, функциональных возможностях, правильности, полноте мер и средств контроля и управления и возможности их совершенствования с течением времени. Тестирование должно выполняться с особой тщательностью компетентными специалистами, и до начала тестирования руководством должно быть рассмотрено и утверждено возможное влияние тестирования на функционирование организации. При этом должны учитываться также варианты проведения тестирования в нерабочие периоды времени, в условиях низкой загруженности или даже в хорошо воспроизведенной тестовой среде. Сбои или недоступность систем из-за тестирования могут оказывать существенное влияние на обычные операции бизнеса организации. Это может приводить к нежелательным финансовым последствиям и к влиянию на репутацию организации, поэтому при планировании тестирования и его надлежащем договорном оформлении (включая рассмотрение правовых аспектов) следует соблюдать особую тщательность.

Ошибочные результаты тестирования, как положительные, так и отрицательные, должны тщательно изучаться аудитором, проводящим проверку мер и средств контроля и управления информационной безопасностью, прежде чем делать какие-либо умозаключения.

К типичным объектам проверки относятся механизмы (например, аппаратные, программные, программно-аппаратные средства) и процессы (например, операции, администрирование, управление системами; испытания).

Типичные действия аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью:

- тестирование механизмов управления доступом, идентификации, аутентификации и анализа этих механизмов;
- тестирование конфигурационных установочных параметров безопасности;
- тестирование устройства физического управления доступом;
- тестирование на проникновение для ключевых компонентов информационных систем;
- тестирование операций резервного копирования информационных систем;
- тестирование способности реагирования на инциденты;
- практическая проверка способности планирования действий в чрезвычайных ситуациях;
- тестирование реагирования систем безопасности, способных обнаруживать вторжения, подавать сигналы тревоги и осуществлять реагирование;

- тестирование криптографических алгоритмов и механизмов хэширования;
- тестирование механизмов менеджмента идентификаторов пользователей и привилегий;
- тестирование механизмов авторизации;
- проверка каскадной устойчивости мер безопасности.

Примечание – К тестированию атрибуты не применяются.

7.4.2 Виды тестирования

7.4.2.1 Тестирование слепым методом

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, тестирует объект проверки без каких-либо предварительных знаний его дополнительных характеристик, помимо общедоступных. Объект проверки подготавливается к проверке лицом, заблаговременно знающим все детали проверки. Слепая проверка в основном осуществляется на основе навыков аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Объем и глубина слепой проверки могут быть настолько обширными, насколько позволяют знания и работоспособность аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Таким образом, это тестирование имеет ограниченное применение при проверках безопасности и его следует избегать. Его обычно называют «этичным хакерством».

7.4.2.2 Тестирование двойным слепым методом

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, тестирует объект проверки без каких-либо предварительных знаний его дополнительных характеристик, помимо общедоступных. Аудитор заранее не сообщает об области проверки или используемых тестах. При двойной слепой проверке тестируется подготовленность объекта проверки к неизвестным параметрам рассмотрения.

7.4.2.3 Тестирование методом серого ящика

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, тестирует объект проверки, располагая ограниченным знанием о его защите и активах, но полным знанием о доступных тестах. Объект проверки подготавливается к проверке лицом, заблаговременно знающим все детали проверки. Проверка методом серого ящика осуществляется на основе навыков аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Основным свойством этого тестирования является результативность. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему проверку мер и средств контроля и управления информационной безопасностью, перед тестированием, а также от надлежащих знаний аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Таким образом, это тестирование имеет ограниченное применение при проверках безопасности и его следует избегать. Этот вид тестирования часто называется «тестированием уязвимостей», и оно чаще всего инициируется объектом в качестве действия по самооценке.

7.4.2.4 Тестирование методом двойного серого ящика

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, тестирует объект проверки, располагая ограниченным знанием о его защите и активах, но полным знанием о доступных тестах. Аудитор заранее сообщает об области и сроках проверки, но не о тестах. Проверка методом двойного серого ящика тестирует подготовленность объекта к неизвестным параметрам рассмотрения. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему проверку мер и средств контроля и управления информационной безопасностью, и объекту проверки перед тестированием, а также от применяемых знаний аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью.

7.4.2.5 Тестирование тандемным методом

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, и объект проверки подготавливаются к проверке, для обоих заранее известны все детали проверки. При тандемном методе тестируется защита и меры и средства контроля и управления объекта. Однако при его использовании не может осуществляться тестирование подготовленности объекта к неизвестным параметрам рассмотрения. Основным свойством данного тестирования является доскональность, поскольку аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, имеет полное представление обо всех тестах и ответных действиях. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему проверку мер и средств контроля и управления информационной безопасностью, перед тестированием, а также от надлежащих знаний аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Это тестирование часто называют «внутренней проверкой», и ауди-

тор, проводящий проверку мер и средств контроля и управления информационной безопасностью, часто играет активную роль в общем процессе обеспечения безопасности.

7.4.2.6 Инверсионный метод

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, тестирует объект проверки, располагая полным знанием о его процессах и операционной безопасности, однако объекту проверки ничего не сообщается о том, что, как или когда будет тестировать аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью. Основным свойством этого тестирования является проверка подготовленности объекта к неизвестным параметрам и направлениям рассмотрения. Объем и глубина зависят от качества информации, предоставленной аудитору, проводящему проверку мер и средств контроля и управления информационной безопасностью, а также от надлежащих знаний и творческого подхода аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью. Это тестирование часто называют «ходом красных».

Рисунок 1 – Виды тестирования

7.4.3 Расширенные процедуры проверки

Дополнительно с процедурами проверки, применяемыми к отдельным мерам и средствам контроля и управления, может применяться расширенная процедура проверки . Расширенная процедура проверки предназначена для совместного использования с другими процедурами проверки. Она дополняет их, что способствует обеспечению уверенности в эффективности мер и средств контроля и управления.

Расширенная процедура проверки и соответствующие объекты проверки также тесно связаны с уровнем риска информационной системы.

8 Деятельность

8.1 Подготовка

Установление и сохранение соответствующей совокупности ожидаемых результатов до, во время и после проверки имеет первостепенное значение для достижения приемлемого результата. Это означает предоставление информации, позволяющей руководству принимать верные основанные на риске решения о том, каким образом лучше всего реализовывать и эксплуатировать информационные системы. Тщательная подготовка организации и аудиторов, осуществляющих проверку мер и средств контроля и управления информационной безопасностью, является важным аспектом проведения эффективных проверок. В ходе подготовительной деятельности следует рассматривать вопросы, связанные с расходами, графиком, наличием необходимой компетентности и проведением проверки.

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

- обеспечение уверенности в том, что соответствующие политики, охватывающие проверки, существуют и осознаны всеми структурными элементами организации;
- обеспечение уверенности в том, что все запланированные шаги по реализации мер и средств контроля и управления успешно выполнены до проверки и были соответствующим образом проанализированы руководством (это применимо только в том случае, если мера и средства контро-

ля и управления отмечена как «полностью функционирующая», а не находится на этапе подготовки/реализации);

- обеспечение уверенности в том, что выбранные меры и средства контроля и управления поручены соответствующим организационным единицам для разработки и реализации;
- установление цели и области проверки (т. е. предназначения проверки и того, что будет проверяться);
- уведомление основных должностных лиц организации о предстоящей проверке и выделение необходимых ресурсов для проведения проверки;
- установление соответствующих каналов связи между должностными лицами организации, заинтересованными в проверке;
- установление временных рамок для проведения проверки и основных контрольных точек принятия решений, необходимых организации для осуществления эффективного менеджмента проверки;
- определение и выбор компетентного аудитора для проведения проверки мер и средств контроля и управления информационной безопасностью или аудиторской группы, которые будут ответственными за проведение проверки, учитывая вопросы независимости аудитора, осуществляющего проверку мер и средств контроля и управления информационной безопасностью;
- сбор артефактов для предоставления аудиторам, проводящим проверку мер и средств контроля и управления информационной безопасностью (например, документации по мерам и средствам контроля и управления информационной безопасностью, 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 проверку мер и средств контроля и управления информационной безопасностью, позволяющих свести к минимуму неопределенности или неправильные представления о реализации мер и средств контроля и управления или слабых местах/недостатках мер и средств контроля и управления, установленных во время проверки.

В дополнение к мероприятиям по планированию, осуществляемым организацией для подготовки к проверке, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны начинать подготовку к проверке посредством:

- достижения общего понимания функционирования организации (включая целевую задачу, функции и процессы бизнеса), а также того, каким образом информационные активы, попадающие в область проверки, поддерживают функционирование организации;
- достижения понимания структуры информационных активов (например, архитектуры системы);
- достижения полного понимания всех мер и средств контроля и управления, подлежащих проверке;
- изучения важных публикаций, на которые ссылаются в мерах и средствах контроля и управления;
- определения организационных единиц, ответственных за разработку и реализацию подлежащих проверке мер и средств контроля и управления, которые поддерживают информационную безопасность;
- установления соответствующих контактных лиц в организации, необходимых для проведения проверки;
- получения артефактов, необходимых для проверки (например, политик, процедур, планов, спецификаций, проектов, записей, руководств администратора/оператора, документации информационной системы, соглашений о межсистемной связи);
- получения результатов предыдущих проверок, которые могут быть надлежащим образом повторно использованы для проверки (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 проверки, предлагаемой строгости и области проверки;
- разработки плана проверки.

При подготовке к проверке мер и средств контроля и управления информационной безопасностью должна быть собрана необходимая исходная информация, которая должна быть предоставлена аудиторам, осуществляющим проверку мер и средств контроля и управления информационной безопасностью. В рамках необходимой поддержки конкретной проверки организация должна определить и подготовить доступ к элементам организации (лицам или группам лиц), отвечающим за разработку, документирование, распространение, проверку, эксплуатацию, поддержку и обновление всех мер и средств контроля и управления безопасностью, политик безопасности и взаимосвязанных процедур

для реализации соответствующих политикам мер и средств контроля и управления. Аудитору, проводящему проверку мер и средств контроля и управления информационной безопасностью, также необходим доступ к политикам безопасности информационной системы и любым взаимосвязанным процедурам реализации, к любым материалам, связанным с реализацией и функционированием мер и средств контроля и управления (например, планам обеспечения безопасности, записям, графикам, отчетам о результатах проверки, отчетам о последующих действиях, соглашениям, комплекту аккредитационных и лицензионных документов) и подлежащим проверке объектам.

Доступность необходимой документации, а также ведущего персонала организации и проверяемых информационных систем крайне важна для успешной проверки мер и средств контроля и управления информационной безопасностью.

8.2 Разработка плана

8.2.1 Обзор

При разработке планов проверки аудиторы, осуществляющие проверку мер и средств контроля и управления информационной безопасностью, должны определить вид проверки (например, полная или частичная проверка) и то, какие меры и средства контроля и управления и/или средства, расширяющие их возможности, должны быть включены в проверку на основе цели/области проверки. Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны оценить и снизить риск и влияние (где это возможно) проверки на обычное функционирование организации и выбрать на основе мер и средств контроля и управления и средств, расширяющих их возможности, необходимые процедуры проверки, которые необходимо включить в проверку и в соответствующие атрибуты «глубины» и «охвата».

Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны приспособить выбранные процедуры проверки к уровню риска информационной системы и к реальной рабочей среде организации. При необходимости они также должны разработать дополнительные процедуры проверки, не рассматриваемые в данном документе, в отношении мер и средств контроля и управления безопасностью, а также средств, расширяющих их возможности, и обеспечить доверие к этим процедурам.

Должен быть разработан план, включающий этапы определения контекста, формирования 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 проверки, если это необходимо, оптимизации процедур проверки для уменьшения дублирования работ и обеспечения экономически эффективных решений, относящихся к проверке. После этого аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны окончательно оформить план проверки и получить необходимые санкции на его выполнение.

8.2.2 Область

Документация должна содержать обзор требований безопасности информационных активов и описывать имеющиеся или планируемые меры и средства контроля и управления для выполнения этих требований. Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, вначале изучает меры и средства контроля и управления, описанные в документации по обеспечению информационной безопасности, а затем – цель проверки. Проводиться может полная проверка всех мер и средств контроля и управления информационной безопасностью в организации или частичная проверка только тех мер и средств контроля и управления, которые обеспечивают защиту информационных активов (например, во время непрерывного мониторинга, где подмножества мер и средств контроля и управления в информационных активах проверяются на постоянной основе). Для проведения частичных проверок владелец информационных активов работает совместно с заинтересованными в проверке должностными лицами организации над определением того, какие меры и средства контроля и управления должны проверяться. Выбор мер и средств контроля и управления зависит от установленного графика непрерывного мониторинга, пунктов плана действий и соответствующих контрольных точек. Меры и средства контроля и управления, отличающиеся большей изменчивостью, должны проверяться чаще.

8.2.3 Процедуры проверки

Процедура проверки состоит из совокупности целей проверки, каждая с соответствующим набором потенциальных методов проверки и объектов проверки. Формулировки определений в целях проверки тесно связаны с сущностью меры и средства контроля и управления (т. е. с функциональными возможностями меры и средства контроля и управления). Это обеспечивает уверенность в прослеживаемости результатов проверки вплоть до фундаментальных требований меры и средства контроля и управления. По результатам применения процедуры проверки к мере и средству контроля и управления формируются выводы проверки. Эти выводы проверки впоследствии используются для определения общей эффективности меры и средства контроля и управления. Объекты проверки оп-

ределяют конкретные элементы, подлежащие проверке, а также спецификации, механизмы, процессы и физических лиц.

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

Процедуры проверки могут быть специально приспособленными в отношении:

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

8.2.4 Особенности, относящиеся к объектам

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

Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны выбирать только те методы и объекты, которые наиболее эффективно способствуют принятию решений, связанных с целью проверки. Мера качества результатов проверки основана на правильности представленного логического обоснования, а не на конкретной совокупности примененных методов и объектов. В большинстве случаев нет необходимости применять каждый метод проверки к каждому объекту проверки, чтобы получить желаемые результаты проверки. А для конкретных и всесторонних проверок может быть целесообразно использовать метод, не перечисленный в согласованном перечне потенциальных методов, или не использовать никакой из перечня известных методов.

8.2.5 Предыдущие заключения

8.2.5.1 Обзор

Аудиторы, проводящие проверку меры и средства контроля и управления информационной безопасностью, должны использовать имеющуюся информацию о предыдущих проверках меры и средства контроля и управления, что будет способствовать большей эффективности проверок. По-

вторное использование результатов ранее признанных или утвержденных проверок информационных систем должно рассматриваться в рамках совокупности свидетельств для определения общей эффективности мер и средств контроля и управления.

При рассмотрении вопроса о повторном использовании результатов предыдущих проверок и ценности этих результатов для текущей проверки аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны определить:

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

В определенных ситуациях бывает необходимо дополнить результаты предыдущей проверки, рассматриваемые на предмет их повторного использования, дополнительными мероприятиями проверки, для полного удовлетворения целей проверки. 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, проводящему проверку мер и средств контроля и управления информационной безопасностью, может потребоваться дополнить первоначальные результаты тестирования. Для этого необходимо дополнительное тестирование, которое охватит данную настройку параметров конфигурации для текущей среды информационной системы.

Информация последующих подразделов должна приниматься во внимание при рассмотрении результатов предыдущих проверок на предмет их повторного использования при текущей проверке.

8.2.5.2 Меняющиеся условия

Меры и средства контроля и управления, сочтенные эффективными во время предыдущих проверок, могут стать неэффективными в результате изменившихся условий, связанных с информационными активами или окружающей средой. Соответственно результаты проверки, признанные ранее приемлемыми, могут больше не давать достоверных свидетельств для определения эффективности мер и средств контроля и управления, и потребуется новая проверка. Применение результатов предыдущей проверки в ходе текущей проверки требует определения любых изменений, произошедших со времени предыдущей проверки, и влияния этих изменений на результаты предыдущей проверки. Например, повторное использование результатов предыдущей проверки, 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 проверок

Допустимость использования результатов предыдущих проверок при проверке мер и средств контроля и управления должна координироваться и утверждаться лицами, использующими результаты проверки. Важно, 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 проверки и окончательном отчете.

Проверки безопасности могут включать выводы предыдущих проверок безопасности, пока:

- это специально разрешено в плане аудита;
- у аудиторов, проводящих проверку мер и средств контроля и управления информационной безопасности, существуют достаточные основания считать, что выводы остаются адекватными;
- любые технологические или процедурные изменения в мерах и средствах контроля и управления или процессах, к которым они применяются, адекватным образом учитываются при текущей проверке с точки зрения безопасности;
- использование и любые потенциальные последствия менеджмента риска вследствие принятия предыдущих выводов аудита четко излагаются в отчете о результатах аудита.

8.2.5.4 Временные аспекты

С увеличением периода времени между текущей и предыдущими проверками достоверность/полезность результатов предыдущих проверок 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 проверка.

8.2.6 Рабочее задание

Независимость аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, может быть критическим фактором при некоторых видах проверок, особенно для информационных активов со средним и высоким уровнями риска. Степень независимости

аудитора, требуемая при проверке, должна быть постоянной. Например, неуместно повторно использовать результаты предыдущих самооценок, в которых не требовалась независимость аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, при текущей проверке, требующей большей степени независимости.

8.2.7 Внешние системы

Представленные в приложении А методы и процедуры проверки должны быть соответствующим образом скорректированы для выполнения проверки внешних информационных систем. Поскольку организация не всегда имеет возможность проведения непосредственного контроля мер и средств контроля и управления безопасностью, используемых во внешних информационных системах, или достаточного визуального контроля разработки, реализации и проверки этих мер и средств контроля и управления, то может потребоваться применение альтернативных подходов к проверке. Это может приводить к необходимости адаптации процедур проверки, описанных в приложении А. При необходимости согласованные меры и средства контроля и управления информационной системы документируются в договорах или соглашениях об уровне услуг. Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, должен проверять эти договоры или соглашения и в соответствующих случаях либо адаптировать процедуры для проверки мер и средств контроля и управления, представленных по этим соглашениям, либо результаты проверки мер и средств контроля и управления предоставлять через соглашения. Кроме того, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны учитывать информацию, полученную при любых проверках, проведенных или находящихся в процессе проведения организациями, эксплуатирующими внешние информационные системы, которые имеют отношение к защищаемым информационным активам на основании проводимой проверки. 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 проверки могут быть приспособлены для рассмотрения системы или конкретной платформы, или зависимостей конкретной организации. Такая ситуация часто возникает в процедурах проверок, связанных с мерами и средствами контроля и управления безопасностью из числа технических мер и средств контроля и управления информационной безопасностью (т. е. управление доступом, аудит и подотчетность, идентификация и аутентификация, защита систем и средств связи). Результаты последнего тестирования могут быть также применимы для текущей проверки, 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 проверки

Организации обладают большой гибкостью при выполнении требований доверия к мерам и средствам контроля и управления информационной безопасностью. Например, в отношении такого требования, как доверие своевременному рассмотрению недостатков. Организация может удовлетворять этому требованию по принципу «в зависимости от конкретной меры и средства контроля и управления», по принципу «в зависимости от вида меры и средства контроля и управления», по принципу «в зависимости от конкретной системы» или возможно даже по организационному уровню. Принимая во внимание эту гибкость, расширенная процедура проверки из 7.4.3 применяется по принципу «в зависимости от конкретной проверки» обычно в соответствии с тем, как организация решает достигать доверия к проверяемым информационным активам. Метод применения расширенной процедуры проверки должен документироваться в плане проверки. Далее организация выбирает соответствующие цели проверки из расширенной процедуры проверки на основе уровня риска для информационных активов. Применение расширенной процедуры проверки предназначается для дополнения других процедур проверки, чтобы увеличивать основание для уверенности в том, что меры и средства контроля и управления реализованы правильно, функционируют, как предназначалось, и дают желаемый результат в отношении выполнения применяемых требований информационной безопасности.

8.2.10 Оптимизация

Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны проявлять определенную степень гибкости в вопросе формирования плана проверки, отвечающего потребностям организации. Это дает возможность получения необходимых свидетельств при определении эффективности мер и средств контроля и управления безопасностью при одновременном снижении общих расходов на проверку.

Комбинирование и объединение процедур проверки является одной из сфер, где может быть применена гибкость. Во время проверки методы проверки многократно применяются к различным

объектам проверки в рамках конкретной области применения мер и средств контроля и управления информационной безопасностью.

Чтобы сэкономить время, уменьшить расходы на проверку и максимально увеличить полезность результатов проверки, аудиторы, проводящие проверку меры и средства контроля и управления информационной безопасностью, должны рассмотреть выбранные процедуры проверки для областей применения меры и средства контроля и управления и там, где это возможно и осуществимо, скомбинировать или объединить процедуры (или части процедур).

Например, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, могут захотеть объединить опросы ключевых должностных лиц организации по различным темам, имеющим отношение к информационной безопасности. Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, 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, что можно обеспечить существенную эффективность проверки.

Дополнительной сферой, заслуживающей внимания при оптимизации процесса проверки, является последовательность, в которой осуществляется проверка мер и средств контроля и управления. Проверка некоторых мер и средств контроля и управления раньше других может предоставить информацию, облегчающую понимание и проверку других мер и средств контроля и управления. Например, сферы применения мер и средств контроля и управления могут создавать общие описания информационных активов. Проверка этих мер и средств контроля и управления безопасностью в начале процесса проверки может обеспечить базовое понимание информационных активов, которое может помочь при проверке других мер и средств контроля и управления безопасностью. Дополнительные рекомендации по многим мерам и средствам контроля и управления также определяют взаимосвязанные меры и средства контроля и управления, которые могут предоставить полезную информацию для организации процедур проверки. Другими словами, последовательность осуществления проверки может способствовать многократному использованию информации проверки одной меры и средства контроля и управления при проверке других взаимосвязанных мер и средств контроля и управления.

8.2.11 Итоговое оформление

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

После того как план проверки сформирован, он рассматривается и утверждается соответствующими должностными лицами организации для обеспечения уверенности в полноте плана, согласовании с целями безопасности организации и проверке риска организации, а также экономической эффективности в отношении выделенных для проверки ресурсов. Если в течение проверки возможно прерывание обычного функционирования организации (например, в результате отвлечения ключевого персонала или возможных (вре́менных) сбоев систем из-за тестирования на проникновение), в плане проверки должен подчеркиваться масштаб такого прерывания и его временны́е рамки.

8.3 Проведение проверок

После утверждения организацией плана проверки аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, работает по нему в соответствии с согласованными контрольными точками и сроками.

Цели проверки достигаются путем применения назначенных методов проверки к выбранным объектам проверки и сбора/создания информации, необходимой для принятия решений, связанных с каждой целью проверки. Каждая формулировка решения относительно процедуры проверки, которую выполнил аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, представляет собой один из следующих выводов:

- выполняется (В);
- частично выполняется (Ч);
- не выполняется (Н).

Вывод «выполняется» означает, что для части меры и средства контроля и управления, к которой относится формулировка решения, полученная информация проверки (т. е. собранные свидетельства) указывает на то, что цель проверки для меры и средства контроля и управления выполнена

с вполне приемлемым результатом. Вывод «частично выполняется» означает, что часть меры и средства контроля и управления не направлена на свою цель или что во время проверки реализация меры и средства контроля и управления все еще продолжается, обоснованно обеспечивая уверенность в том, что мера и средство контроля и управления достигнет результата «выполняется» (В). Вывод «не выполняется» означает, что для части меры и средства контроля и управления, к которой относится формулировка решения, полученная информация проверки указывает на потенциальную аномалию функционирования или реализации меры и средства контроля и управления, которая возможно должна быть рассмотрена организацией. Вывод «не выполняется» также может означать, что по детально изложенным в отчете о результатах проверки причинам аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, был не в состоянии получить достаточно информации, чтобы принять конкретное решение, требуемое в формулировке решения.

Выводы аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью (т. е. вынесенные решения), должны быть беспристрастными, содержать фактическую информацию о том, что было обнаружено в отношении проверяемой меры и средства контроля и управления. Для каждого вывода «не выполняется» аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны указать, какие части меры и средства контроля и управления затронуты (т. е. те аспекты меры и средства контроля и управления, которые были сочтены несоответствующими или которые не было возможности проверить), и должны описать, насколько мера и средство контроля и управления отличается от планируемого или ожидаемого состояния. Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, должен также отметить возможность компрометации конфиденциальности, целостности и доступности, соответствующую выводам «не выполняется». Если проверка показывает существенные несоответствия (т. е. делаются выводы «не выполняется», которые указывают на существенное отклонение от запланированного состояния), аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, должен немедленно информировать лицо, отвечающее за эту меру и средство контроля и управления, и руководство, чтобы незамедлительно могли быть инициированы процедуры для уменьшения последствий.

8.4 Анализ результатов и отчет о результатах

План проверки предоставляет цели проверки и детальный график действий по проведению такой проверки. Конечным результатом проверки является отчет о результатах проверки, в котором отражается уровень информационной безопасности на основе реализованных мер и средств контроля и управления информационной безопасностью. Отчет включает информацию, поступающую от аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью (в форме выводов проверки), необходимую для определения эффективности используемых мер и средств контроля и управления и общей эффективности деятельности организации в реализации выбранных и соответствующих мер и средств контроля и управления, на основе выводов аудитора. Отчет является важным фактором при определении рисков информационной безопасности для операций (т. е. целевой задачи, функций), активов организации, кадров, других организаций и т. д.

Результаты проверки должны быть документально оформлены с предназначенным для проверки уровнем детальности в соответствии с форматом отчетности, предписываемым политикой организации. Формат отчетности должен также соответствовать виду проводимой проверки мер и средств контроля и управления (например, самооценка, проводимая владельцами информационной системы, независимая проверка и подтверждение достоверности, независимые проверки мер и средств контроля и управления, проводимые аудиторами, и т. д.).

Владелец информационной системы полагается на квалификацию в сфере информационной безопасности и технические решения аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, в вопросах проведения проверки мер и средств контроля и управления безопасностью, а также предоставляющего конкретные рекомендации по исправлению слабых мест или недостатков мер и средств контроля и управления и снижению или устранению выявленных уязвимостей.

Информация по проверке, формируемая аудитором, проводящим проверку мер и средств контроля и управления информационной безопасностью (т. е. выводы «выполняется» или «не выполняется», идентификация тех частей мер и средств контроля и управления безопасностью, которые не дают удовлетворительного результата, и описание проистекающей отсюда возможности компрометации информационных активов), предоставляется руководителям в форме первоначального отчета (проекта) о проверке безопасности. Владельцы активов могут решить действовать в соответствии с выбранными рекомендациями аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, до придания отчету окончательной формы, если существуют конкретные возможности исправления слабых мест или недостатков мер и средств контроля и управления или исправления/прояснения неправильного понимания или толкования результатов проверки.

Аудитор, проводящий проверку мер и средств контроля и управления информационной безопасностью, должен снова проверить модифицированные, улучшенные или добавленные во время этого процесса меры и средства контроля и управления, прежде чем формировать окончательный отчет. Передача окончательного отчета руководству означает официальное завершение проверки мер и средств контроля и управления информационной безопасностью.

Поскольку результаты проверки в конечном счете влияют на содержание мер и средств контроля и управления информационной безопасностью, а также на план действий и контрольные точки, владелец информационных активов рассматривает выводы аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, и при содействии руководства организации определяет соответствующие шаги, которые необходимы для устранения слабых мест и недостатков, идентифицированных во время проверки. Форма отчетности по выводам проверки, в которой использованы выводы «выполняется» и «не выполняется», делает наглядными для руководства организации конкретные слабые места и недостатки обеспечения информационной безопасности и способствует упорядоченному и структурированному подходу к уменьшению рисков в соответствии с процессом менеджмента риска информационной безопасности. Например, владелец информационных активов после консультации с руководством организации может принять решение о том, что некоторые выводы проверки, отмеченные как «не выполняется», 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 выполняется», являются существенными и требуют принятия незамедлительных корректирующих мер. Во всех случаях руководство организации проверяет каждый вывод «не выполняется» аудитора, проводящего проверку мер и средств контроля и управления информационной безопасностью, и составляет собственное мнение относительно серьезности вывода (т. е. потенциального неблагоприятного влияния на операции и активы организации, кадры, другие организации и т. д.), и является ли вывод достаточно серьезным, чтобы заслуживать дальнейшего исследования или корректирующих мер. Может потребоваться привлечение высшего руководства к процессу смягчения последствий, чтобы обеспечить эффективное распределение ресурсов организации в соответствии с приоритетами организации, предоставляя в первую очередь ресурсы информационным активам, которые поддерживают наиболее критические процессы бизнеса организации, или исправляя недостатки, которые представляют наибольшую степень риска. В конечном счете выводы проверки и любые последующие действия по смягчению последствий, инициированные владельцем информационных активов в сотрудничестве с назначенным должностным лицом организации, приводят в действие модификации процесса менеджмента риска информационной безопасности, а также мер и средств контроля и управления информационной безопасностью. Соответственно базовые документы, используемые руководителями для определения состояния информационной безопасности информационных активов, обновляются, чтобы отразить результаты проверки.

В заранее определенные контрольные точки или фиксированные периоды времени после проверки, например, через три месяца после представления окончательного отчета, обычно проводится проверка контроля исполнения, сосредотачивающаяся на нерешенных или «открытых» проблемах. Она включает проверку правильности реализованных решений по предыдущим выводам. Организации могут также решить проводить мероприятия по контролю исполнения во время следующей проверки, особенно для тех вопросов, которые не являются критичными или неотложными.

Приложение А
(справочное)

Практическое руководство по проверке технического соответствия

В данном приложении представлена совокупность практических руководств по проверке технического соответствия с использованием технических мер и средств контроля и управления, описанных в ИСО/МЭК 27002. Каждая мера и средство контроля и управления в данном приложении описана согласно нижеуказанной структуре, формулировкам и руководствам.

«Техническая мера и средство контроля и управления» (с «дополнительной технической информацией»)

1 Стандарт реализации безопасности (с «Техническим примечанием к стандарту реализации безопасности»)

1.1 Практическое руководство, Предполагаемые свидетельства, Метод

1.2 Практическое руководство, Предполагаемые свидетельства, Метод

2 Стандарт реализации безопасности (с «Техническим примечанием к стандарту реализации безопасности»)

2.1 Практическое руководство, Предполагаемые свидетельства, Метод

2.2 Практическое руководство, Предполагаемые свидетельства, Метод

2.3 Для каждой технической меры и средства контроля и управления существует дополнительная техническая информация, помогающая аудиторам, проводящим проверку мер и средств контроля и управления информационной безопасностью. 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 проверки. В нем также представлены: «Практическое руководство», «Предполагаемые свидетельства» и «Метод».

«Практическое руководство» предоставляет применяемую процедуру проверки 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 проверки 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 проверки технического соответствия. «Метод» представляет соответствующий подход к технической проверке соответствия согласно приведенному выше «Практическому руководству».

В данном приложении не представлены исчерпывающие практические руководства по проверке технического соответствия, которые могут значительно помочь организациям в проведении проверки, введены ли соответствующим образом стандарты реализации безопасности и действуют ли они.

Таблица А.1

А.1 Техническая проверка мер и средств контроля и управления, применяемых против вредоносной программы		
Мера и средство контроля и управления		**ИСО/МЭК 27002 10.4.1 Меры и средства контроля и управления против вредоносной программы** Необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей.
Дополнительная техническая информация		Вредоносная программа (вредоносное программное средство) – это общий термин, используемый для обозначения кода, программного средства, программы, сценария, предназначенных для нанесения ущерба компьютерной системе путем хищения информации, мошенничества, шпионажа, саботажа и вандализма. При внесении вредоносного программного средства в компьютерную систему может быть причинен ущерб системе или может быть похищена информация из системы. Также возможно, что оно причинит ущерб другим системам. Вредоносное программное средство включает вирусы, червей, троянских коней, боты, шпионское программное средство, программы, запускающие рекламу, и другие нежелательные программные средства. В условиях соединения сети организации с Интернетом аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны проверить, что функции обнаружения/предупреждения вредоносного программного средства комплексно и эффективно размещены на границе с Интернетом и эти функции действуют соответствующим образом. Чтобы проверить, действуют ли функции обнаружения/предупреждения соответственно, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны получить подтверждение, обновляются ли файлы-шаблоны или сигнатуры, используемые для обнаружения вредоносного программного средства. Некоторые системы обнаружения/предупреждения разрабатываются для обнаружения вредоносного программного средства посредством использования файлов-шаблонов или сигнатур, а некоторые создаются для обнаружения аномального поведения компьютерной системы без использования файлов-шаблонов или сигнатур. Поскольку существует несколько моделей соединения с Интернетом, таких как соединение сети организации с Интернетом через шлюз или подключение каждого персонального компьютера (ПК) к Интернету напрямую, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны убедиться, что система обнаружения/предупреждения соответствующим образом работает при любой модели соединения. Примечание – Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны сознавать, что возможности системы обнаружения/предупреждения в отношении неизвестного вредоносного программного средства (такого как «Zero day») ограничены
1	Стандарт реализации безопасности	Установка и регулярное обновление программных средств по обнаружению вредоносных программ и исправлению ситуации для осуществления сканирования компьютеров и носителей данных в качестве предупредительной меры и средства контроля и управления или на стандартной основе. Проводимые проверки должны включать: 1) проверку любых файлов перед их использованием на электронных или оптических носителях данных или файлов, полученных по сети, на предмет наличия вредоносной программы; 2) проверку вложений электронной почты и загрузок на предмет наличия вредоносной программы перед их использованием; эта проверка должна осуществляться в разных точках, например, на почтовых серверах, в настольных компьютерах, при вхождении в сеть организации; 3) проверку веб-страниц на предмет наличия вредоносной программы

Продолжение таблицы А.1

1	Техническое примечание к стандарту реализации безопасности	Система обнаружения/предупреждения вредоносного программного средства на межсетевом шлюзе, на входе в сеть организации должна соответствующим образом взаимодействовать с различными сетевыми сервисами или протоколами, такими как WWW, электронная почта и FTP[1)]	
	1.1	Практическое руководство	Практические руководства 1), 2) и 3) применяются для «стандарта реализации безопасности»: 1) проверить комплексное и эффективное размещение системы/устройства обнаружения вредоносной программы и исправления ситуации для любых файлов на электронных или оптических носителях данных или файлов, полученных по сети, путем проверки спецификации системы или сетевых диаграмм. Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, проверяют комплексное и эффективное размещение системы обнаружения/предупреждения путем проверки спецификации системы или сетевых диаграмм; 2) проверить комплексное и эффективное размещение системы/устройства обнаружения вредоносной программы и исправления ситуации для любых вложений электронной почты и загрузок путем проверки спецификации системы или сетевых диаграмм, которые включают почтовые серверы, настольные компьютеры и межсетевой шлюз. Система/устройство обнаружения вредоносной программы и исправления ситуации иногда четко описывается в спецификации системы как особое устройство, однако аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, отмечают, что она также размещается на серверах, предназначенных для предоставления некоторых других функций/сервисов (WWW, электронная почта и FTP), и таким образом в действительности она размещается в спецификации системы без четкого описания. Для настольных ПК аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, отмечают, что система/устройство обнаружения вредоносной программы и исправления ситуации размещается наследственно в спецификации системы без четкого описания; 3) проверить комплексное и эффективное размещение системы/устройства обнаружения вредоносной программы и исправления ситуации для веб-страниц путем проверки спецификации системы или сетевых диаграмм, которые включают веб-сервер. Для настольных ПК, использующихся для просматривания веб-страниц, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, отмечают, что система/устройство обнаружения вредоносной программы и исправления ситуации располагается наследственно в спецификации системы без четкого описания. В этом случае система/устройство обнаружения вредоносной программы и исправления ситуации может располагаться наследственно в браузере. Для веб-сервера система/устройство обнаружения вредоносной программы и исправления ситуации иногда четко описывается в спецификации системы как особое устройство, однако аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, отмечают, что она также располагается наследственно в спецификации системы без четкого описания.
		Предполагаемые свидетельства	Спецификация системы, сетевые диаграммы
		Метод	Изучение/Проверка

[1)] FTP (File Transfer Protocol) – протокол передачи файлов

Продолжение таблицы А.1

	1.2	Практическое руководство	Практические руководства 1), 2) и 3) применяются для «Стандарта реализации безопасности»: 1) проверить размещение и соответствующее функционирование системы/устройства обнаружения вредоносной программы и исправления ситуации в отношении любых файлов на электронных или оптических носителях данных или файлов, полученных по сети, путем наблюдения за средствами обработки информации. Проверить, работают ли соответствующим образом программные средства менеджмента в интегрированной системе в условиях, когда система/устройство обнаружения вредоносной программы и исправления ситуации регулируется в интегрированной системе; 2) проверить размещение и соответствующее функционирование системы/устройства обнаружения вредоносной программы и исправления ситуации для любых вложений электронной почты и загрузок на почтовых серверах, в выборочных настольных компьютерах и шлюзе путем наблюдения за средствами обработки информации. Для электронной почты проверить, работает ли система/устройство обнаружения не только в отношении вложенных файлов, но и в отношении вредоносной программы на html-странице электронной почты; 3) проверить размещение и соответствующее функционирование системы/устройства обнаружения вредоносной программы и исправления ситуации в отношении любых веб-страниц путем наблюдения за средствами обработки информации. Для настольных ПК, использующихся для просматривания веб-страниц, проверить, работает ли система/устройство обнаружения в отношении несанкционированных «Active X control», скриптов[1)] и т. д. Для веб-сервера проверить, работает ли система/устройство обнаружения не только в отношении html-файлов, но и в отношении вредоносной программы в веб-сервисах, таких как и Apache, IIS[2)] и т. д.
		Предполагаемые свидетельства	Средства системы/устройства обнаружения вредоносной программы и исправления ситуации размещаются, например, на/в: - файловом сервере; - почтовом сервере; - выборочных настольных ПК; - мобильных компьютерах; - единой системе обнаружения вредоносной программы и исправления ситуации, размещенной на межсетевом шлюзе (границе между сетью организации и Интернетом); - веб-сервере; - прокси-сервере; - веб-браузере; - иных устройствах (например, на устройстве для блокирования USB, вставляемом физически).
		Метод	Изучение/Наблюдение

[1)] Скрипт –небольшая программа или макрос, исполняемые приложением или операционной системой при конкретных обстоятельствах, например, при регистрации пользователя в системе. Скрипты часто хранятся в виде текстовых файлов, которые интерпретируются во время исполнения.

[2)] IIS (Internet Information Server) – Информационный сервер Internet.

Окончание таблицы А.1

	1.3	Практическое руководство	Собрать журналы регистрации системы обнаружения и исправления ситуации и проверить, показывают ли записи журналов регистрации, что система работает и что при обнаружении вредоносного программного средства принимаются необходимые меры. Примечания 1 Для настольных ПК стандартные журналы регистрации системы обнаружения и исправления ситуации хранятся в ПК. Для серверов и внешних устройств эти журналы регистрации иногда передаются в другие системы через протокол передачи, такой как syslog, и хранятся в них. 2 Для настольных ПК, использующихся для просмотра веб-страниц, функция обнаружения в веб-браузере может не создавать записи в журнале регистрации, показывающие, что функция работает. Чаще большинство браузеров показывает сообщение, когда обнаруживаются несанкционированные скрипты.
		Предполагаемые свидетельства	- Система обнаружения в процессе эксплуатации - Журналы регистрации системы обнаружения - Записи сигналов тревоги системы обнаружения - Сообщения системы обнаружения в веб-браузере
		Метод	Изучение/Наблюдение
2	Стандарт реализации безопасности	Программные средства по обнаружению вредоносной программы и исправлению ситуации для осуществления сканирования компьютеров и носителей данных в качестве предупредительной меры должны обновляться регулярно или на стандартной основе	
	Техническое примечание к стандарту реализации безопасности	Для большинства случаев существуют функции автоматического обновления файлов-шаблонов или сигнатур	
	2.1	Практическое руководство	Проверить проектирование программных средств по обнаружению вредоносной программы и исправлению ситуации на предмет обновления файлов-шаблонов или сигнатур автоматически или на стандартной основе
		Предполагаемые свидетельства	Проект или спецификация системы обнаружения
		Метод	Изучение/Проверка
	2.2	Практическое руководство	Проверить установки программных средств по обнаружению вредоносной программы и исправлению ситуации на предмет обновления файлов-шаблонов или сигнатур автоматически или на стандартной основе
		Предполагаемые свидетельства	Установки системы обнаружения
		Метод	Изучение/Наблюдение
	2.3	Практическое руководство	Проверить осуществление обновления файлов-шаблонов или сигнатур, проведя наблюдение за наименованием продукта, версией и журналом регистрации обновлений файлов-шаблонов или сигнатур. Примечание – Информацию о наименовании продукта и версии системы обнаружения и исправления ситуации можно найти в справочном файле продукта
		Предполагаемые свидетельства	Информация о системе обнаружения/предупреждения, т. е: - наименование продукта; - версия продукта; - версия файлов-шаблонов или сигнатур
		Метод	Изучение/Наблюдение

Таблица А.2

А.2 Техническая проверка мер и средств контроля и управления для контрольной регистрации	
Мера и средство контроля и управления	**ИСО/МЭК 27002 10.10.1. Контрольная регистрация** Необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом
Дополнительная техническая информация	Для обнаружения несанкционированных действий по обработке информации важно создание записей в контрольных журналах, которые используются для отслеживания действий пользователей, операторов систем, связанных с безопасностью событий и систем. Чтобы можно было проанализировать, происходит ли несанкционированная деятельность и связанные с безопасностью события, контрольные журналы должны содержать следующую информацию: - идентификатор пользователя; - дату и время; - основные события, такие как вход в систему и выход из системы; - идентификатор терминала; - сетевой адрес и протоколы. Для создания необходимых записей, включая вышеприведенную информацию, оборудование, создающее контрольные журналы, должно быть соответствующим образом настроено или к нему должны применяться некоторые правила. Метод протоколирования зависит от структуры и архитектуры системы и реализованных приложений. Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны учитывать различие методов протоколирования для различной архитектуры систем, например, серверов и ПК. Примечание – Примеры структур системы, которые затрагиваются: - система клиент-сервер; - система на базе Интернет-технологий; - система «тонкий клиент»; - виртуализация; - использование ASP (поставщиков услуг по аренде приложений), SaaS (программного обеспечения как услуги) или облачных вычислений. Примеры архитектур систем, которые затрагиваются: - UNIX, Linux; - Windows; - мэйнфрейм. Примеры видов контрольных журналов, которые затрагиваются: - системный журнал; - контрольный журнал прикладных программ.
1 Стандарт реализации безопасности	Должны создаваться контрольные журналы, фиксирующие действия пользователей, отклонения от нормы и события, связанные с информационной безопасностью. Контрольные журналы должны включать, где это необходимо: a) идентификаторы пользователей; b) дату, время и подробности основных событий, например, входа в систему и выхода из системы; c) идентификатор терминала или местонахождение, если это возможно; d) записи успешных и неудачных попыток доступа к системе; e) записи успешных и неудачных попыток доступа к данным и другим ресурсам; f) описания изменений в конфигурации системы; h) описание использования утилит и приложений; i) файлы, к которым получен доступ, и вид доступа; j) сетевые адреса и протоколы; k) сигналы тревоги, производимые системой управления доступом; l) описание активации и деактивации систем защиты, таких как антивирусные системы и системы обнаружения вторжений

Продолжение таблицы А.2

	Техническое примечание к стандарту реализации безопасности	Чтобы обнаружить связанные с безопасностью события и выяснить их причины, аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, проверяют и анализируют состояние функционирования, использования и изменения систем по записям контрольного журнала. Чтобы расследовать события и причинную связь инцидентов нужно сочетать контрольные журналы многих систем. По этой причине важно понимание местонахождения и вида контрольных журналов с точки зрения структуры/архитектуры/конфигурации систем	
	1.1	Практическое руководство	Проверить, основано ли проектирование протоколирования данных аудита системы на стандарте реализации безопасности
		Предполагаемые свидетельства	- Документация спецификации - Документация определения требований - Документация проектирования программного обеспечения
		Метод	Изучение/Проверка
	1.2	Практическое руководство	Проверить, таковы ли установки конфигурационных файлов протоколирования данных аудита системы, как описано в документации по проектированию системы
		Предполагаемые свидетельства	- Документация проектирования программного обеспечения - Конфигурационный файл системы
		Метод	Изучение/Наблюдение
	1.3	Практическое руководство	Проверить, таковы ли записи существующих контрольных журналов, как описано в документации по проектированию системы. Примечание – В контрольных журналах есть записи, появляющиеся постоянно, и записи, такие как записи об ошибках, появляющиеся в определенных случаях. Чтобы проверить, фиксирует ли система записи, появляющиеся только в определенных случаях, аудиторам, проводящим проверку мер и средств контроля и управления информационной безопасностью, может потребоваться применение различных мер, включая создание совокупности тестовых данных, проверку документации по проектированию системы
		Предполагаемые свидетельства	- Контрольный журнал
		Метод	Изучение/Наблюдение
	1.4	Практическое руководство	Проверить целостность записей в контрольных журналах, чтобы определить, является ли протоколирование данных аудита соответствующим. Примечание – Некоторые записи, которые должны фиксироваться в контрольных журналах, могут отсутствовать из-за недостатков в функционировании, возможностях системы или по каким-то другим причинам, даже если установка протоколирования данных аудита является соответствующей
		Предполагаемые свидетельства	- Контрольный журнал
		Метод	Изучение/Наблюдение

Окончание таблицы А.2

2	Стандарт реализации безопасности	Контрольные журналы должны храниться в течение согласованного периода времени для содействия будущим расследованиям и мониторингу управления доступом	
	Техническое примечание к стандарту реализации безопасности	В некоторых случаях периоды хранения контрольных журналов определяются целями бизнеса, договором и законами/предписаниями. Например, контрольные журналы, которые содержат сигналы тревоги, поднятые системой управления доступом, должны храниться до завершения расследования событий и причинной связи инцидентов. Примечание – Хранение контрольных журналов относительно «молодой» системы, деятельность которой только что началась, не осуществляется в течение согласованного периода времени. В этом случае для выполнения практического руководства 2.3 нужно провести проверку по практическим руководствам 2.1 и 2.2	
	2.1	Практическое руководство	Проверить, таков ли период хранения контрольных журналов, как описано в документации по проектированию системы
		Предполагаемые свидетельства	- Контрольный журнал - Документация по проектированию системы
		Метод	Изучение/Наблюдение
	2.2	Практическое руководство	Проверить, установлен ли период хранения контрольных журналов системы, как описано в документации по проектированию системы, или, не применяются ли установки перезаписи или стирания контрольных журналов до завершения периода хранения
		Предполагаемые свидетельства	- Контрольный журнал - Документация по проектированию системы
		Метод	Изучение/Наблюдение
	2.3	Практическое руководство	Проверить, превышает ли период хранения контрольных журналов период, установленный путем наблюдения отметок времени в контрольных журналах, или фиксирование времени в контрольном журнале
		Предполагаемые свидетельства	- Контрольный журнал - Документация по проектированию системы
		Метод	Изучение/Наблюдение

Таблица А.3

А.3 Техническая проверка мер и средств контроля и управления для управления привилегиями			
Мера и средство контроля и управления	**ИСО/МЭК 27002 11.2.2. Управление привилегиями** Предоставление и использование привилегий необходимо ограничивать и контролировать		
Дополнительная техническая информация	Управление привилегиями является важной задачей, потому что несоответствующее использование привилегий оказывает существенное влияние на системы. Состояние распределения привилегий должно быть описано в документах, определяющих привилегии (документация определения привилегий). Поскольку привилегии доступа связаны с каждым системным продуктом (операционная система, система управления базой данных и каждое приложение), то они отличаются. Примерыи видов привилегий: - суперпользователь (UNIX, Linux); - администратор (Windows); - оператор резервного копирования (Windows); - опытный пользователь (Windows); - администратор системы (DBMS[1]); - администратор базы данных (DBMS). Распределение привилегий должно быть минимальным, на основе принципа необходимого использования. К тому же они не обязательно должны распределяться постоянно. Метод управления привилегиями различается в системах. Примеры управления привилегиями на основе систем: - в операционной системе (ОС) привилегии определяет ACL[2]; - в DBMS различные привилегии определяются по умолчанию; - в приложении могут определяться различные привилегии по умолчанию для функции менеджмента приложения, поэтому аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны заранее определить уровень проверки; - в защищенных ОС есть функция обязательного управления доступом		
1 Стандарт реализации безопасности	Должны быть определены привилегии доступа, связанные с каждым системным продуктом, например, ОС, системой управления базой данных и каждым приложением, а также пользователи, среди которых нужно распределить привилегии		
Техническое примечание к стандарту реализации безопасности	Деятельность наделенных привилегиями пользователей должна подвергаться мониторингу, поскольку несоответствующее использование привилегий оказывает существенное влияние на системы. Методы обнаружения несоответствующего использования привилегий различаются, если архитектура систем различна. Примечание – Типичными архитектурами систем являются: - мэйнфрейм; - Windows; - UNIX, Linux; - защищенные операционные системы		
1.1	Практическое руководство	Проверить, описано ли распределение привилегий в документации определения привилегий	
	Предполагаемые свидетельства	Документация определения привилегий	
	Метод	Изучение/Наблюдение	

[1] DBMS (Database Management System) – Система управления базами данных, СУБД.
[2] ACL (Access Control List) – Список управления доступом.

Продолжение таблицы А.3

	1.2	Практическое руководство	Проверить, таковы ли установки конфигурации системы, как описано в документах, определяющих привилегии. Метод проверки действия привилегий различается в зависимости от архитектуры систем. Примеры метода проверки действия привилегий: 1) (в случае мэйнфрейма) проверить, является ли состояние использования привилегий соответствующим, посредством проверки отчета RACF[1)]; 2) (в случае UNIX, Linux или Windows) проверить, является ли состояние использования привилегий соответствующим, путем изучения журналов регистрации, показывающих использование привилегий. Примечания 1 RACF – это связующее программное обеспечение менеджмента безопасности в мэйнфрейме. 2 В UNIX или Linux рискованно проверять только вход в систему с полномочиями суперпользователя для исследования несоответствующего использования привилегий суперпользователя. Причина этого заключается в том, что обычный пользователь может стать суперпользователем, использовав команду «su» после входа в систему UNIX или Linux.
		Предполагаемые свидетельства	- Документация определения привилегий - Список управления доступом - Отчет RACF
		Метод	Изучение/Наблюдение
2	Стандарт реализации безопасности	Привилегии должны быть назначены другому идентификатору пользователя, отличному от того, который применяется для обычного использования в бизнесе	
	Техническое примечание к стандарту реализации безопасности	В случае доступа по привилегиям существует возможность несанкционированной деятельности по случайности, и ситуация использования привилегий регулярно становится очагом несанкционированного доступа. Если деятельность не требует привилегий, пользователи должны использовать стандартный идентификатор. Если разрешен вход в систему по привилегии «суперпользователь», то из журнала регистрации невозможно идентифицировать, кто входит в систему	
	2.1	Практическое руководство	Проверить, имеют ли привилегированные пользователи обычный идентификатор пользователя помимо привилегированного идентификатора, путем наблюдения за ACLs систем
		Предполагаемые свидетельства	- Список управления доступом
		Метод	Изучение/Наблюдение

[1)] RACF (Resource access control facility) – средство управления доступом к ресурсу.

Окончание таблицы А.3

	2.2	Практическое руководство	Проверить, используют ли для привилегии иной идентификатор пользователя, отличный от того, который применяется для обычного бизнеса, посредством наблюдения за системным журналом регистрации. В случае UNIX или Linux проверить, что системная конфигурация способствует тому, что система не допускает вход с полномочиями «суперпользователя». Примечание – Аудиторы, проводящие проверку мер и средств контроля и управления информационной безопасностью, должны прибегнуть к опросам для проверки, применяется ли в случае привилегии иной идентификатор пользователя, отличный от того, который применяется для обычного использования в бизнесе, когда журнал регистрации показывает, что в случае привилегии используется только привилегированный идентификатор
		Предполагаемые свидетельства	- Системный журнал регистрации - Системная конфигурация входа с полномочиями «суперпользователя»
		Метод	Изучение/Наблюдение

Таблица А.4

А.4 Техническая проверка мер и средств контроля и управления для резервирования информации		
Мера и средство контроля и управления		**ИСО/МЭК 27002 10.5.1. Резервирование информации** Резервное копирование информации и программного средства должно выполняться и тестироваться на регулярной основе в соответствии с установленной политикой резервирования
Дополнительная техническая информация		Чтобы соответствующим образом проводить резервное копирование, должен быть определен стандарт организации в соответствии с политикой резервного копирования, и он должен отражаться в проектной документации по резервному копированию. Резервные копии используются для восстановления важной информации или программ в случаях, сопровождающихся потерей данных, таких как бедствие или сбой носителя данных. При проектировании резервного копирования организации следует выбрать адекватную площадку для резервного копирования, канал резервного копирования и метод резервного копирования в соответствии с политикой резервного копирования. Организация должна выбрать, какой будет площадка для резервного копирования – внутренней или внешней. Создание резервной копии и восстановление при резервном копировании на месте считаются значительно более быстрыми по сравнению с их осуществлением при внешнем резервном копировании. Внешнее резервное копирование часто выбирается с целью предотвращения влияния локальных бедствий, таких как пожар, затопление или землетрясение. Организация должна определить, каким будет канал резервного копирования – онлайновый или офлайновый. Онлайновое резервное копирование означает, что данные копируются через сеть или линию связи. Офлайновое резервное копирование означает, что резервные копии данных физически транспортируются на переносных носителях, таких как цифровая лента с линейной записью или компакт-диск/цифровой многофункциональный диск. Метод резервного копирования подразделяется на полное резервное копирование, инкрементное резервное копирование и дифференциальное резервное копирование. Полное резервное копирование означает, что делается резервная копия всех данных, выбранных для резервного копирования. Оно требует больше времени и информационной емкости по сравнению с другими методами, но является наиболее простым и легким методом с точки зрения восстановления. Инкрементное резервное копирование означает, что делается резервная копия данных, изменившихся со времени последнего резервного копирования. Оно требует меньше времени и информационной емкости по сравнению с другими методами, но является наиболее сложным методом с точки зрения восстановления. Дифференциальное резервное копирование означает, что делается резервная копия данных, изменившихся со времени последнего полного резервного копирования. Оно требует меньше времени и информационной емкости, чем полное резервное копирование, и является более простым и легким методом с точки зрения восстановления, по сравнению с инкрементным резервным копированием
1	Стандарт реализации безопасности	Степень (например, полное или дифференциальное резервное копирование) и частота резервного копирования должны определяться требованиями бизнеса организации, требованиями безопасности задействованной информации и критичностью информации для непрерывной деятельности организации

Продолжение таблицы А.4

	Техническое примечание к стандарту реализации безопасности	В соответствии с требованиями своего бизнеса организация должна выбрать адекватное время резервного копирования/восстановления и информационную емкость для резервного копирования. Специалисты по оценке должны оценить, адекватный ли метод резервного копирования выбран для выполнения требований бизнеса. Примерами повторяемости, которая используется, являются: - зеркальное копирование или тиражирование в режиме реального времени (когда критичность информации максимальна); - ежедневное копирование (когда требуется восстановление данных с резервной копии с давностью, по крайней мере, в пределах дня); - еженедельное копирование; - ежемесячное копирование.	
	1.1	Практическое руководство	Проверить, основано ли проектирование резервного копирования на стандарте реализации безопасности
		Предполагаемые свидетельства	- Документально оформленная спецификация резервного копирования - Документально оформленные определения требований бизнеса и требований безопасности - Проектная документация по резервному копированию
		Метод	Изучение/Проверка
	1.2	Практическое руководство	Проверить, таковы ли установки конфигурационных файлов системы для резервного копирования, как описано в проектной документации по резервному копированию
		Предполагаемые свидетельства	- Проектная документация по резервному копированию - Конфигурационные файлы системы для резервного копирования
		Метод	Изучение/Проверка
	1.3	Практическое руководство	Проверить, осуществляется ли резервное копирование, как описано в проектной документации по резервному копированию
		Предполагаемые свидетельства	- Проектная документация по резервному копированию - Журналы регистрации - Резервные носители данных
		Метод	Изучение/Наблюдение
2	Стандарт реализации безопасности	Процедуры восстановления должны регулярно проверяться и тестироваться, чтобы обеспечить уверенность в их эффективности и возможности их выполнения в течение времени, выделенного в операционных процедурах для восстановления	
	Техническое примечание к стандарту реализации безопасности	Сложность и требуемое время восстановления различаются в зависимости от используемого метода, такого как полное или дифференциальное резервное копирование. Должен подготавливаться и документироваться план тестирования и проверки процедур восстановления	
	2.1	Практическое руководство	Проверить, регулярно ли проверяется план тестирования и проверки
		Предполагаемые свидетельства	- Записи о проверке плана тестирования и проверки
		Метод	Изучение/Проверка

Окончание таблицы А.4

	2.2	Практическое руководство	Проверить, регулярно ли тестируется план тестирования и проверки, чтобы обеспечить уверенность в эффективности процедур восстановления и возможности их выполнения в течение времени, выделенного в операционных процедурах для восстановления
		Предполагаемые свидетельства	- Записи тестирования восстановления - План тестирования и проверки
		Метод	Изучение/Проверка

Таблица А.5

А.5 Техническая проверка мер и средств контроля и управления для обеспечения безопасности сетевых услуг		
Мера и средство контроля и управления		**ИСО/МЭК 27002 10.6.2. Безопасность сетевых услуг** Средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента всех сетевых услуг должны быть определены и включены в любой договор по сетевым услугам, вне зависимости от того, будут ли они обеспечиваться силами организации или в рамках договоров аутсорсинга
Дополнительная техническая информация		Сетевая услуга – это услуга, предоставляемая в сетевой вычислительной среде либо внутри организации, либо с использованием аутсорсинга. Когда организация использует сетевые услуги, конфиденциальная информация организации может передаваться способом, присущем аутсорсинговой сетевой услуге. Таким образом, специалисты по оценке должны учитывать, что необходимые функции безопасности, такие как шифрование и/или аутентификация, обеспечиваются привлеченным поставщиком сетевых услуг. Примерами систем, используемых для сетевых услуг, являются: - DNS[1]; - DHCP[2]; - межсетевой экран/виртуальная частная сеть; - антивирусный детектор; - IDS[3] / IPS[4]
1	Стандарт реализации безопасности	Должны быть идентифицированы необходимые для конкретных услуг меры безопасности, такие как функции безопасности, уровни услуг и требования менеджмента. Организация должна обеспечить уверенность в том, что поставщики сетевых услуг реализуют эти меры
	Техническое примечание к стандарту реализации безопасности	При использовании сетевых услуг важны меры безопасности, обеспечивающие защиту передаваемой посредством их информации. Требования функций безопасности обычно включаются в требования бизнеса. Примеры функций безопасности, связанных с сетевыми услугами: - шифрование для защиты от подслушивания; - управление сетевым доступом для защиты от несанкционированного доступа; - IDS/IPS для защиты от злонамеренных действий; - фильтрация URL[5] для защиты от несанкционированного веб-доступа; - реагирование на инциденты, т. е. на неожиданные события, связанные с безопасностью

[1] DNS (Domain Name System) – Система доменных имён.
[2] DHCP (Dynamic Host Configuration Protocol) – Протокол динамического конфигурирования узла [хост-машины].
[3] IDS (Intrusion Detection System) – Система обнаружения вторжений.
[4] IPS (Intrusion Prevention System) – Система предотвращения вторжений.
[5] URL (Uniform Resource Locator) – Унифицированный указатель ресурса, URL – адрес.

Окончание таблицы А.5

	1.1	Практическое руководство	Проверить, удовлетворяет ли требованиям бизнеса, правовым требованиям и требованиям безопасности организации договорная документация, включая предоставляемое поставщиком услуг SLA
		Предполагаемые свидетельства	- Договорная документация - Документация, определяющая требования
		Метод	Изучение/Проверка
	1.2	Практическое руководство	В случае внутренних сетевых услуг проверить, таковы ли, как описано в проектной документации на сетевые услуги, установки системы, используемой для сетевых услуг
		Предполагаемые свидетельства	- Конфигурация системы - Проектная документация на сетевые услуги
		Метод	Изучение/Проверка
	1.3	Практическое руководство	В случае внутренних сетевых услуг проверить, таковы ли, как описано в проектной документации на сетевые услуги, записи существующих системных журналов регистрации, используемых для сетевых услуг. Примеры записей, относящихся к сетевым услугам: - аутентификация; - шифрование; - меры и средства контроля и управления сетевыми соединениями; - скорость коммутации; - реакция (в случае онлайновых систем); - продолжительность простоя
		Предполагаемые свидетельства	- Системные журналы регистрации - Предупредительные сигналы тревоги - Проектная документация на сетевые услуги
		Метод	Изучение/Наблюдение

Таблицы А.6

А.6 Техническая проверка мер и средств контроля и управления для обязанностей пользователей			
Мера и средство контроля и управления		**ИСО/МЭК 27002 11.3.1. Использование паролей** Пользователи должны придерживаться общепринятой практики в области безопасности при выборе и использовании паролей	
Дополнительная техническая информация		Для предотвращения несанкционированного доступа к компьютерным ресурсам следует создавать пароли и хранить их в секрете от тех, кому не разрешен доступ. Паролевая аутентификация – это метод аутентификации пользователя, используемый несколькими ресурсами, такими как операционные системы, программы, базы данных, сети или веб-сайты. Качество пароля зависит от его длины и вида символов, таких как буквенно-цифровые символы и знаки. В некоторых операционных системах, таких как Windows, у пользователей может быть возможность конфигурирования параметров политики паролей. С другой стороны, разработчики приложений могут разработать функцию аутентификации для конфигурирования политики паролей. Специалисты по оценке должны оценить эффективность функций авторизации с паролями, размещенных на вычислительных средствах, и соответствующую работу этих функций	
1	Стандарт реализации безопасности	Выбор качественных паролей достаточной минимальной длины, которые: 1) легко запоминаются; 2) не основаны на том, что кто-то другой может легко отгадать или получить, используя связанную с данным лицом информацию, например, фамилии, номера телефонов, даты рождения и т. д.; 3) невосприимчивы к атакам методом подбора по словарю (т. е. не состоят из слов, включенных в словари); 4) не состоят из последовательных, идентичных, полностью цифровых или полностью буквенных символов	
	Техническое примечание к стандарту реализации безопасности	Пароли, которые легко запомнить другому пользователю, уязвимы в целом	
	1.1	Практическое руководство	Проверить, прописаны ли в политике паролей организации правила выбора паролей
		Предполагаемые свидетельства	- Политика паролей организации
		Метод	Изучение/Проверка
	1.2	Практическое руководство	Проверить, таковы ли, как описано в политике паролей организации, установки конфигурации системы (политика паролей системы)
		Предполагаемые свидетельства	- Конфигурация системы (политика паролей системы) - Политика паролей организации
		Метод	Изучение/Наблюдение
	1.3	Практическое руководство	Проверить, отражено ли изменение пользователями паролей в журналах регистрации
		Предполагаемые свидетельства	- Системный журнал регистрации
		Метод	Изучение/Наблюдение

Приложение В
(справочное)

Начало сбора информации (отличной от ИТ)

Ведущий аудитор в группе, проводящей проверку мер и средств контроля и управления информационной безопасностью, должен назначать аудитора, проводящего проверку мер и средств контроля и управления, с соответствующей компетентностью и опытом для каждой области информационной безопасности.

По каждой указанной ниже сфере для соответствующего персонала приведен не исчерпывающий перечень примерных вопросов.

В.1 Кадровые ресурсы и безопасность

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

b) Существуют ли «на месте» специалисты, обладающие знаниями по обеспечению безопасности и информационной безопасности, для ответа на вопросы, мотивации персонала и предоставления необходимого руководства?

c) Являются ли применяемые политики и процедуры четкими и SMART[1)] (конкретными, измеримыми, приемлемыми, реалистичными, привязанными ко времени)?

d) Осуществляется ли наем персонала в соответствии с ожидаемыми «операционными» знаниями?

e) Является ли персонал заслуживающим доверия, чтобы обращаться с чувствительной информацией и системами, которые могут подвергать опасности продолжительность существования организации?

f) Является ли персонал таким, которому можно полностью доверять?

g) Как определяется и измеряется доверие?

В.2 Политики

a) Иерархия:

i) выводятся ли политики информационной безопасности из целей бизнеса и общей политики безопасности?

ii) как осуществляется связь между политиками ИТ, кадровыми политиками, политиками приобретения и т. д.?

b) Полнота:

i) рассматриваются ли в политиках вопросы обеспечения информационной безопасности во всех секторах деятельности бизнеса (кадровом, физическом, ИТ, продаж, производства, научно-исследовательском, договоров и т. д.)?

ii) являются ли политики полными в плане охвата стратегии, тактики и операций?

c) Формулировка:

i) сформированы ли политики по принципу «копия–вставка», изложенному в ИСО/МЭК 27002, или же цели контроля и меры и средства контроля и управления приспособлены к конкретному контексту?

ii) написаны ли политики с четкой идентификацией ответственного лица (лиц)?

iii) ожидаемое в рамках политики или процедуры действие должно рассматривать «основополагающие» вопросы: кто, когда, зачем, что, где, каким образом:

- если лицо (кто), ответственное за выполнение деятельности, не определено, то кто будет достигать установленных целей?
- если плановое время (когда) для выполнения деятельности не определено, то будет ли она начата и завершена в должное время?
- если задача или цель деятельности не определена (зачем), то будет ли деятельность правильно понята, а ее значимость адекватно учтена?
- если сама деятельность (что) не определена, то как будет возможно ее выполнить?

[1)] SMART (Self-Monitoring Analysis and Reporting Technology) – Технология самоконтроля, анализа и составления диагностических отчётов.

- если деятельность не определяет объект, место, процесс, информационный актив или «меру и средство контроля и управления», на которые она должна оказывать влияние (где), то какова будет ее эффективность?
- если деятельность в процедуре четко не определяет, каким образом все должно выполняться, то как она может быть выполнена правильно (каким образом?)
- если деятельность также не определяет показатели и меры и средства контроля и управления, направленные на проверку ее развития и достижения целей, то как организация может быть уверена, что цели достигаются или могут быть достигнуты?

iv) существуют ли меры и средства контроля и управления и среда проверки, чтобы определить, приводятся ли в действие и реализуются ли положения политики и достигаются ли цели?

v) цели в формулировке политики должны учитывать критерии SMART (конкретные, измеримые, приемлемые, реалистичные, привязанные ко времени). Если же этого не происходит, то:

- не отличающиеся конкретностью цели нелегко ясно осознать, а лицо(а), отвечающее(ие) за их достижение, обычно не определено(ы);
- если цель не является измеримой, то мало шансов, что организация сможет проверить, достигается она или нет;
- если цель не сообщается персоналу и неприемлема для персонала, которому придется следовать ей, то велика вероятность того, что мера и средство контроля и управления будет неправильно понята, обойдена или «отключена»;
- если цель нереалистична по отношению к реальным возможностям организации, то мало шансов, что когда-нибудь она будет достигнута;
- если цель не определена по отношению ко времени (когда она должна быть достигнута, когда предполагается начать деятельность и т. д.), то существует большая вероятность того, что никакие действия не будут предприняты и цель никогда не будет достигнута.

B.3 Организация

a) Определена ли и распределена ли совокупность ролей и обязанностей, необходимых и достаточных для выполнения целей бизнеса с учетом конкретного контекста и ограничений?

b) Определена ли связь с внешними органами?

c) Возлагается ли ответственность за обеспечение безопасности на внешние ресурсы, если у организации нет внутренних возможностей?

d) Рассматриваются ли вопросы информационной безопасности в договорах?

B.4 Физическая безопасность и безопасность внешней среды

B.4.1 Безопасны ли площадки для информации?

a) «Зоны»

i) являются ли площадки, доступные для публики, достаточно изолированными от площадок для бизнеса?

ii) определены ли зоны, где обрабатывается наиболее критичная информация (персоналом или системами информационных и коммуникационных технологий (ИКТ)?

iii) достаточно ли изолированы эти «безопасные зоны», чтобы избежать обмена информацией?

b) Месторасположения

i) являются ли различные зоны четко определенными и соответствующим образом расположенными?

ii) являются ли «границы» (стены, потолок, пол и т. д.) четко определенными, а их прочность соответствующей для защиты содержащихся активов?

iii) присутствует ли соответствующая маркировка местоположений, и находятся ли критические зоны вне поля зрения «посторонних лиц»?

c) «Входы/выходы» – точки доступа

i) обеспечивают ли окна и двери и «проходы» через границы такую же защиту, как «границы», когда они закрыты?

ii) существует ли соответствующее управление доступом для входа в и выхода из «месторасположения»?

iii) существует ли система предупреждения вторжений?

iv) существуют ли «запасные выходы», предусматривающие достаточную мобильность информации, людей и оборудования?

d) Коридоры и «пути»

i) определены ли «пути» к зонам и площадкам:
- пути для людей;
- кабели (пути для информации);

i) существуют ли альтернативные пути?
ii) обеспечиваются ли защита и мониторинг этих «путей»?

e) Мониторинг
i) могут ли ресурсы мониторинга обеспечивать видение, не будучи увиденными?
ii) могут ли ресурсы мониторинга увидеть вторжение, появляющееся издалека?
iii) когда мониторинг активен?
iv) где и как хранятся и анализируются записи?

f) Окружающая обстановка
i) является ли она соответствующей для хранения информации?
ii) является ли она надлежащим образом размещенной?
iii) функционирует ли, как ожидалось?

B.4.2 Безопасны ли площадки для ИКТ? (Аспекты внешней среды)

a) Энергоснабжение
i) достаточное/соответствующее?
ii) альтернативное?

b) Кондиционирование воздуха
i) достаточное/соответствующее?
ii) альтернативное?

c) Средства пожаротушения
i) достаточные/соответствующие?
ii) альтернативные?

B.4.3 Безопасны ли площадки для людей?

a) Существуют ли запасные выходы (с соответствующими мерами и средствами контроля и управления)?

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

c) Представляют ли температура, влажность, вещества и вибрации потенциальную опасность для людей?

d) Размещается ли оборудование таким образом, чтобы люди не имели возможности получить травму?

e) Определены ли «входы/выходы» и управляются ли они так, чтобы люди не имели возможности получить травму?

f) Установлена ли и поддерживается ли окружающая обстановка таким образом, чтобы люди не имели возможности получить травму?

B.4.4 Менеджмент инцидентов

a) Определены ли инциденты информационной безопасности?

b) Существуют ли возможности реагирования на инциденты информационной безопасности:
i) руководства?
ii) ролей и обязанностей?
iii) средств и ресурсов?

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000–2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ИСО/МЭК 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
Примечание – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: – IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements* (ИСО/МЭК 27001:2005, *Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования*) *
[2] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*
[3] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk manage-ment*
[4] ISO/IEC 27006:2007, *Information technology – Security techniques – Requirements for bodies providing audits and certification of information security management systems* (ИСО/МЭК 27006:2007, *Информационные технологии. Методы и средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности*) *
[5] ISO/IEC 27007:2011, *Information technology – Security techniques – Guidelines for information security management systems auditing*
[6] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing* (ИСО 19011:2002, *Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента*) *
[7] ISO Guide 73:2009, *Risk management – Vocabulary*
[8] NIST Special publication (SP) 800-53A, *Guide for reviewing the controls in federal information systems*, July 2008. Доступен на: http://csrc.nist.gov/publications/PubsSPs.html
[9] Institute For Security AndOpen Methodologies, *Open-Source Security Testing Methodology Manual*. Доступен на: http://www.isecom.org/osstmm/
[10] 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* (доступен на немецком и английском). Доступен на: https://www.bsi.bund.de/cln_174/EN/Publications/publications_node.html
[11] Information Security Forum, *The Standard of Good Practice for Information Security*, 2007. Доступен на: https://www.securityforum.org/services/publicresearch/

* Официальный перевод этого стандарта находится в Федеральном информационном фонде.

УДК 006.034:004.056:004.057.2 ОКС 35.040

Ключевые слова: информационная безопасность, мера и средство контроля и управления, проверка информационной безопасности, проверка технического соответствия, метод проверки, план проверки, процедура проверки, аудитор

Подписано в печать 12.01.2015. Формат 60x84 1/8.
Усл. печ. л. 5,12. Тираж 40 экз. Зак. 147.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»
123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru