2. ПРОЦЕССЫ ПРОВЕРКИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

В данной главе рассматриваются основные процессы анализа СУИБ: мониторинг ИБ, самооценка ИБ, внутренний и внешний аудит ИБ и анализ СУИБ со стороны руководства организации. Для всех процессов выделяются основные цели и задачи, принципы и этапы осуществления, виды проверок, формы отчетности. Анализируется деятельность в организации подразделения внутреннего аудита, контролирующего вопросы ИБ. Исследуется процесс управления программой внешнего аудита ИБ. Затрагиваются вопросы компетентности аудиторов ИБ и взаимоотношения внешних аудиторов ИБ с проверяемой организацией. Перечисляются инструментальные средства, используемые при проведении различных проверок в области ИБ.

2.1. Виды проверок СУИБ

Процессы проверки и оценки СУИБ традиционно включают в себя следующие элементы:

- контекст, который определяет входные данные: цели и назначение процесса, вид (независимая оценка, самооценка), объект, область действия, ограничения, ресурсы и роли;
- критерии;
- модель;
- методы;
- мероприятия процесса: сбор свидетельств и проверка их достоверности, измерение и оценивание атрибутов объекта;
- выходные данные.

В ходе различных проверок исследуется соответствие областей деятельности организации в рамках СУИБ заранее установленным стандартам, политикам и правилам по обычно наиболее ощутимым характеристикам, которые можно измерить или оценить с достаточной объективностью. Поскольку любые оценки опираются на модели и методики оценки, главная трудность при глобальной оценке СУИБ организации состоит в выборе наиболее подходящей модели с учетом специфики деятельности организации. Оценка значима только тогда, когда значима выбранная модель. Основным принципом здесь является гибкость. Модель должна соответствовать реальной ситуации и модифицироваться при изменении действующих факторов и условий ее применения. Должна постоянно проверяться совместимость модели с полученными результатами.

Проверка и оценка ИБ и СУИБ как части системы обеспечения ИБ (СОИБ) организации и, как результат, выявление признаков деградации

используемых защитных мер могут проводиться путем выполнения следующих процессов на уровне как всей организации, так и ее отдельных активов – систем, сетей, сервисов, самой информации:

1) мониторинга и контроля используемых защитных мер (как непрерывные во времени, постоянно проводимые процессы);

2) самооценки ИБ (проводимые в рамках заданного интервала времени с установленными программой и планом проведения);

3) внешнего и внутреннего аудита ИБ (проводимые с установленными программой и планом проведения);

4) анализа (в том числе со стороны руководства) функционирования СУИБ (проводимые с установленной периодичностью).

Мировой опыт в области ОИБ определяет вышеуказанные процессы проверки СУИБ как важнейшие в непрерывном цикле процессов управления ИБ организации. Все они являются частью группы процессов «проверка» СУИБ (п. 4.6.3 первой части серии учебных пособий), действенным механизмом отслеживания состояния СУИБ и определения, насколько эффективно и результативно работают все ее элементы. В случае если что-то работает не как запланировано, в рамках СУИБ существуют весьма гибкие механизмы по устранению несоответствий и их причин и непрерывному тактическому и стратегическому улучшению СУИБ и СОИБ.

Проверке и оценке подлежат все направления деятельности СУИБ:

- управление защитными мерами и СЗИ;
- управление всеми активами – информацией, процессами, продуктами и услугами, средствами вычислительной техники (СВТ), работниками – пользователями СВТ и т. д.;
- управление рисками ИБ;
- управление инцидентами ИБ;
- управление персоналом, включая службу ИБ;
- управление изменениями и обновлениями;
- управление документами и записями, относящимися к деятельности СУИБ;
- управление непрерывностью бизнеса (УНБ);
- управление контрольными мероприятиями в области проверки уровня ИБ (мониторинг, внутренние и внешние аудиты ИБ);
- управление информированием и обучением вопросам ОИБ;
- управление эффективностью деятельности в области ОИБ.

Различным проверкам при этом подвергают следующие объекты:

- документация (например, политики, планы, процедуры, системные требования, проекты);
- механизмы (например, функциональность, реализованная в АО, ПО и т. д.);
- процессы (например, функционирование, администрирование и управление системами).

Требования и действия различных проверок СУИБ тщательно планируются и согласовываются, чтобы свести к минимуму риск для бизнес-процессов. Защитные меры при проведении проверок обычно учитывают следующее [11, 12]:

- требования проверок необходимо согласовать с соответствующим руководством;
- объем работ по проверкам следует согласовывать и контролировать;
- при проведении проверок необходимо использовать доступ только для чтения к ПО и данным;
- другие виды доступа могут быть разрешены только в отношении изолированных копий файлов системы, которые необходимо удалять по завершении проверок;
- необходимо четко идентифицировать и обеспечивать доступность необходимых ресурсов информационных систем (ИС) для выполнения проверок;
- требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать;
- весь доступ должен подвергаться мониторингу и регистрироваться с целью обеспечения протоколирования для последующих ссылок;
- все процедуры, требования и обязанности проверок следует документировать.

Сделаем важное замечание. Проверка ИБ и проверка СУИБ очень тесно взаимосвязаны и часто предполагают выполнение схожих действий, на которые в данной главе и делается основной акцент, и поэтому в большей степени рассматриваются вопросы проверки и оценки ИБ. Подтверждение оправданности такого подхода можно найти, например, в трех направления оценки, принятых для банковских организаций РФ в стандарте СТО БР ИББС 1.0–2010 [13]:

1) управление ИБ (основное направление для оценки деятельности СУИБ);

2) текущий уровень ИБ;

3) уровень осознания ИБ как внутреннего побудительного мотива организации поддерживать деятельность по управлению ИБ на всех стадиях модели PDCA для СУИБ.

Так, осознание проблем ИБ и необходимости ОИБ для достижения основных бизнес-целей организации находит свое выражение, например, в заинтересованной поддержке со стороны руководства всей деятельности СУИБ, ее анализе, утверждении политик и т. п. Поскольку основным результатом деятельности СУИБ является ОИБ (с той или иной успешностью, к сожалению, не всегда соответствующей необходимому для конкретной организации уровню), то результат проверки ИБ непосредственно указывает и на эффективность и результативность функционирования СУИБ.

Проверка и оценка СУИБ, адекватности выбора защитных мер, их эффективности и контролируемости осуществляется на основе следующих документов:

- стандартов, стратегий, концепций и политик, определяющих цели и задачи ОИБ организации;
- документов, содержащих свидетельства выполнения уточнения/пересмотра целей и задач ОИБ организации;
- документов, обосновывающих выбор защитных мер;
- документов, содержащих план реализации защитных мер;
- документов, содержащих свидетельства контроля правильности реализации и эксплуатации защитных мер;
- документов, определяющих порядок тестирования используемых защитных мер;
- документов, содержащих свидетельства выполнения деятельности по тестированию используемых защитных мер;
- документов, содержащих доказательства выполнение деятельности по контролю за реализацией действующих положений и требований по ОИБ и т. д.

Выявленный в результате проверок уровень ИБ организации соответствует высокому, если процессы СУИБ проводятся осознанно на основе прогноза, мониторинга и анализа внутренней и внешней среды, развития и изменения целей бизнеса организации.

Рассмотрим подробнее перечисленные подпроцессы проверки ИБ и СУИБ.

2.2. Мониторинг ИБ

Мониторинг ИБ – это ключевой элемент управления рисками ИБ в изменяющейся информационной среде организации. Под ***мониторингом ИБ и контролем защитных мер*** (далее – мониторинг ИБ) будем понимать ***постоянное наблюдение за объектами и субъектами, влияющими на ОИБ организации, а также сбор, анализ и обобщение результатов наблюдений***.

Основными *целями мониторинга ИБ* являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных для каждого из направлений деятельности СУИБ в соответствии с заданными целями, а также обеспечение полной, своевременной, достоверной информацией для принятия обоснованных решений в области ИБ. Такими целями анализа могут быть следующие [1, 2, 11–15]:

1) контроль за реализацией положений внутренних и внешних документов по ОИБ в организации для обнаружения отклонений от принятых требований бизнеса и требований по ОИБ (например, зафиксированных в политике в отношении логического доступа (ПЛД) к информационным активам);

2) контроль качества (результативности и эффективности) используемых защитных мер;

3) выявление нештатных, в том числе злоумышленных, действий с информационными активами и бизнес-процессами организации;

4) выявление событий ИБ, часть из которых в дальнейшем классифицируется как инциденты ИБ;

5) выявление уязвимостей активов, которыми могут воспользоваться злоумышленники для реализации атак на системы, сети и сервисы как самой организации, так и ее бизнес-партнеров или пользователей общедоступных сетей типа Интернета;

6) обеспечение доказательной базы на случай расследования компьютерных преступлений.

Процессы мониторинга ИБ в рамках процесса управления ИБ включают следующее:

1) поиск, отслеживание, наблюдение, накопление, систематизация, оценивание сведений, относящихся к области ИБ;

2) прогнозирование состояния и качества всех объектов и процессов в информационной среде организации.

Мониторинг ИБ обеспечивает прозрачность автоматизированных бизнес-процессов (основных, вспомогательных и управленческих) и гарантирует их наблюдаемость в течение всего времени их функционирования, что, как следствие, повышает уровень доверия бизнеса к ним. Также мониторинг ИБ способствует повышению чувства ответственности работников организации за свои действия, влияющие на ИБ, помогает в обнаружении неправильного использования ресурсов и действует в качестве сдерживающего фактора для лиц, способных попытаться нанести ущерб организации. И, наконец, во время мониторинга выявляются ошибки в самой обработке информации и ее результатах, связанные как со сбоями в функционировании СВТ, так и с человеческим фактором, позволяющие в дальнейшем оптимизировать процесс эксплуатации (с точки зрения соблюдения установленных регламентов) и функционирования систем, сетей и сервисов [16].

Мониторинг ИБ реализуется на основе непрерывного наблюдения за регистрируемыми событиями, влияющими на ИБ, в конкретной среде (системе, сети, сервисе) и контроля за соблюдением базовых требований по ОИБ и предписанных регламентов (контроль штатности режима функционирования этой среды). В процессе мониторинга события ИБ подвергаются тщательному и регулярному анализу, на основе которого делается вывод о наличии или отсутствии, а также возможности наступления инцидента ИБ. На основе полученных во время мониторинга ИБ результатов составляются соответствующие отчеты и далее выполняются заранее запрограммированные действия, направленные на устранение выявленных уязвимостей, прерывание недопустимых видов событий и т. п.

Следовательно, можно сделать вывод, что мониторинг ИБ и управление инцидентами ИБ очень тесто взаимосвязаны (рис. 2.1) [16].

Рис. 2.1. Взаимосвязь мониторинга ИБ и управления инцидентами ИБ: ⇢ *– потоки управления;* ⇨ *– потоки данных*

В процессе реагирования на инцидент ИБ предусматриваются процедуры пересмотра и улучшения процессов управления инцидентами ИБ как на регулярной основе (периодически), так и по результатам обработки любого существенного инцидента ИБ. Завершающий отчет по каждому инциденту ИБ сохраняется в базе данных (БД) инцидентов ИБ и включает данные, которые могут быть использованы в будущем при обработке подобных инцидентов, включая их предвестники и явные признаки. Предложения по улучшению процессов управления инцидентами ИБ касаются вопросов использования дополнительного инструментария или ресурсов, обучения персонала и т. п., то есть всего, что необходимо для принятия решений, направленных на выбор и реализацию мер по совершенствованию управления инцидентами ИБ, оценки рисков ИБ и инициирования улучшений ОИБ, обновления и/или реализации новых защитных мер ИБ и, в итоге, совершенствования СУИБ. Изменение защитных мер, регламентов и ролей персонала также неизбежно отражается на управлении инцидентами ИБ. Если, например, в процессе пересмотра управления инцидентами ИБ появилась рекомендация о включении дополнительного параметра мониторинга на сервере системы, то этот вопрос, скорее всего, нельзя решить в только рамках управления инцидентами ИБ. Потребуется еще внесение изменений в конфигурации СЗИ с соответствующими регламентами и многое другое.

Понятие мониторинга ИБ также тесно связано и с понятием аудита ИБ (рис. 2.2) [16]. Процесс мониторинга ИБ является необходимым

предшествующим этапом обработки рисков ИБ, предоставляя для нее исходные данные за счет выявления отклонений от штатного режима функционирования всей среды и отдельных систем (от заданных требований и предписанных регламентов) и передавая информацию по уже свершившимся инцидентам ИБ и потенциально возможным нарушениям ИБ. Мониторинг ИБ дает руководству организации возможность определить, адекватны ли используемые защитные меры и должным ли образом решаются задачи по ОИБ, возложенные на отдельных работников или эксплуатируемые ИТ, и спланировать соответствующие корректирующие действия.

Рис. 2.2. Взаимосвязь аудита и мониторинга ИБ

Мониторинг ИБ осуществляется на основе следующих документов:

1) отчетность по оперативной оценке ИБ;

2) документы, определяющие процедуры мониторинга ИБ.

Подчеркивая контролирующие функции мониторинга ИБ, следует отметить, что техническим аспектам мониторинга ИБ свойственна иерархичность, предполагающая необходимость наличия контролирующих механизмов на всех уровнях контроля – физическом, сетевом, операционных систем (ОС), прикладном.

Во многом результаты мониторинга ИБ зависят от качества и полноты базовых настроек и механизмов регистрации событий ИБ и на этой основе собранной информации, которая, в свою очередь, влияет на дальнейшую обработку рисков ИБ. Основной объем такой информации поступает из системных журналов регистрации (англ. *log files*), записывающих события ИБ и регистрирующих различные отказы. Эти журналы хранятся в течение согласованного с руководством организации периода времени и обычно включают следующую важную с точки зрения ОИБ информацию:

- идентификатор (ID) пользователя;
- даты, времена входа и выхода субъектов доступа и подробности ключевых событий;

- имя хоста, инициировавшего событие, подлежащее регистрации, и/или его местоположение;
- записи успешных и отклоненных попыток доступа к объектам доступа;
- изменения в системной конфигурации;
- изменения списков субъектов и объектов доступа;
- изменения полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов);
- все привилегированные действия (использование учетной записи супервизора, запуск и останов системы, подсоединение/отсоединение устройств ввода/вывода);
- запуск программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам;
- использование системных утилит и приложений;
- все установленные сессии;
- файлы, к которым осуществлялся доступ, и тип доступа;
- сетевые адреса и протоколы;
- изменения в интенсивности и объемах входящего/исходящего трафика (включая интернет-трафик);
- печать материалов, содержащих сведения конфиденциального характера;
- обращения к критичным системам и сервисам (например, веб-серверу, серверам БД, почтовому серверу, службам синхронизации и т. п.);
- системные предупреждения и сбои;
- тревоги, поднятые системой управления доступом и системой обнаружения вторжений (СОВ);
- изменения или попытки изменения настроек и средств управления защитой систем;
- активация и дезактивация систем защиты, таких как антивирусные системы и СОВ;
- появление новых устройств с неконтролируемым доступом (точки беспроводного доступа, подключенные USB-устройства и пр.) и т. п.

Факторы риска в данном контексте таковы:

- критичность процессов приложения;
- ценность, уязвимость и критичность вовлеченной информации;
- прошлый опыт проникновения в систему и неправильного использования системы, а также частота использования уязвимостей систем и их защиты;
- степень межсистемной связи (особенно с сетями общего доступа);
- несанкционированная дезактивация средства ведения журналов;
- нарушение целостности и полноты записи данных в журнал;
- проблема переполнения дискового пространства и невозможность последующей записи событий в журнал;
- потеря информации из журнала при перезапуске системы.

Более эффективным является применение централизованного журналирования и формирования политики сохранности журналов, в противном случае злоумышленник может получать доступ к журналам в различных точках среды. При таком подходе проще осуществлять централизованную обработку за счет корреляции событий и архивирование, гибко варьируя периоды хранения архива и объемы хранимых данных. Чем меньше период отчуждения журналов, тем меньше вероятность несанкционированных манипуляций с ними. В идеале данные немедленно по факту регистрации должны поступать в центральный архив, что накладывает определенные ограничения на применение защищенных коммуникаций от источника до архива.

Средства ведения системного журнала и информация, содержащаяся в нем, должны быть защищены соответствующими средствами управления от НСД и эксплуатационных проблем, включая следующие:

- отключение средств регистрации;
- изменение типов зарегистрированных сообщений;
- редактирование или удаление файла системного журнала;
- регистрацию случаев полного заполнения носителей журналов, а также случаев невозможности записи событий вследствие сбоев либо случаев перезаписи новых данных поверх старых.

Для некоторых журналов требуется архивирование в рамках выполнения политики хранения документации или сбора и сохранения доказательств для расследования инцидентов ИБ.

Поскольку объем информации в этих журналах очень велик, целесообразно автоматически копировать соответствующие типы сообщений в отдельный журнал и/или использовать подходящие системные утилиты или средства ведения журнала, а также инструментальные средства для анализа данных. При распределении ответственности за анализ журнала необходимо учитывать разделение ролей между проводящим анализ и теми, чьи действия подвергаются мониторингу.

Сами СЗИ и СОВ должны уметь сначала распознавать события ИБ, а затем генерировать, записывать, хранить и анализировать собранную ими в процессе функционирования информацию о событиях ИБ, оповещать (посылать уведомления) об этом администратора/оператора и, возможно, осуществлять заданные ответные действия (разрыв соединений и т. п.) [17–19].

СОВ – динамические средства мониторинга ИБ, заслуживающие отдельного изучения, но в рамках более специализированных учебных курсов [15]. Их структуру (рис. 2.3) можно представить совокупностью элементов:

1. Модули слежения, состоящие из управляемых из единого центра агентов (детекторов, датчиков, сенсоров, а в вырожденном случае – одного детектора), осуществляющие первичную регистрацию и сбор информации, поступающей из контролируемой среды для анализа.

В зависимости от класса СОВ агенты могут размещаться на рабочих станциях, серверах, защищать какой-либо сегмент сети или всю сеть целиком. На этом уровне может выполняться первичная фильтрация данных с целью уменьшения их объема для проведения дальнейшего, более тщательного анализа.

Рис. 2.3. Структура СОВ

2. Модуль сбора информации для анализа, который приводит ее к единому формату, возможно, осуществляет дальнейшую фильтрацию, сохраняет в БД и направляет для анализа соответствующему модулю.

3. Анализатор – модуль анализа собранной информации, предназначенный для выявления атак и подозрительных событий/действий.

4. Модуль управления/администрирования, позволяющий конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты и реагировать на атаки.

5. Модуль управления обновлениями.

6. БД результатов анализа, включая хранилище собранной информации.

7. База знаний об используемых СОВ методов обнаружения вторжений (ОВ) (интеллектуальный или поведенческий, на хосте или в сети).

8. БД атак, то есть описаний их признаков на соответствующем формализованном языке.

9. Модуль генерации отчетов с различной детализацией, предназначенный для разных потребителей этой информации – руководства, специалистов по ИБ и т. д.

10. Интерфейс пользователя со средствами визуализации.

11. Другие дополнительные компоненты, включая те, которые позволяют провести мониторинг работы самой СОВ.

Мониторинг ИБ должен осуществляться для различных элементов среды организации – ИС, целостности ПО, устройств, конфигураций, электронной почты, связи с Интернетом, парольной защиты и т. п. Так, например, в рамках процедур мониторинга ИБ с различной степенью периодичности соответствующими ответственными лицами (например, системным/сетевым администратором и оператором) обязательно выполняются следующие действия:

- анализ отчетов/журналов регистрации СЗИ и служебных программ (ежедневно);
- анализ возможностей доступа пользователей к сетевым ресурсам (ежедневно);
- выявление попыток несанкционированной установки приложений пользователем (ежедневно);
- проверка сетевого взаимодействия (один раз в неделю);
- проверка работы сервисов и служб (один раз в неделю);
- профилактика БД (один раз в неделю);
- антивирусная профилактика серверов (1 раз в неделю);
- проверка времени последнего обновления антивирусных баз (один раз в неделю);
- проверка наличия обновлений ОС и серверных приложений (один раз в неделю);
- проверка целостности ОС (один раз в 2 недели);
- принудительная проверка отказоустойчивости систем (один раз в 2 недели);
- профилактика дисковой и файловой подсистем на серверах (один раз в 2 недели);
- профилактическая остановка серверов (один раз в 2 недели);
- составление отчета доступа к интернет-ресурсам (один раз в месяц);
- проверка обновления клиентских приложений (по необходимости);
- удаление временных и устаревших копий файлов (по необходимости) и т. п.

Анализ всех журналов подразумевает понимание угроз ИБ, которым подвержена система, и причин их возникновения.

Деятельность администратора/оператора может контролироваться СОВ, управляемой за пределами области их полномочий, и должна заноситься в отдельный журнал, в котором отражается следующее:

- время, когда произошло событие (благоприятный исход или сбой);
- информация о событии (например, файлы, с которыми работали) или сбое (например, случившаяся ошибка и предпринятое корректирующее действие);
- какая учетная запись и какой администратор/оператор были вовлечены;
- какие процессы были затронуты.

Системные журналы и журналы администратора/оператора обязательно защищаются, поскольку если данные в них могут быть модифицированы или стерты, то сам факт существования этих журналов может создать обманчивое чувство безопасности.

Любые сбои и отказы фиксируются журналах, после чего обязательно анализируются и по каждому из них предпринимается соответствующее действие. Отказы, о которых сообщили пользователи или системные программы и которые относятся к проблемам с системами обработки или обмена информацией, регистрируются. В организации устанавливаются четкие правила обработки отказов, включая анализ журналов их регистрации и корректирующих мер, что гарантирует удовлетворительное разрешение проблем с отказами и то, что средства управления не были подвергнуты риску, а предпринятое действие полностью реализовано.

В различных ИС компетентным персоналом включается режим регистрации ошибок и отказов, если эта системная функция имеется и доступна. При этом уровень регистрации, необходимый для отдельных систем, определяется оценкой рисков ИБ, с учетом возможного ухудшения функционирования во время отказов.

Для обеспечения точности заполнения журналов важна правильная установка компьютерных часов (таймера), например, по Универсальному глобальному (по Гринвичу), местному декретному или «летнему» времени. Должна существовать процедура, которая проверяет и исправляет любое отклонение или его значимое изменение. Неточные журналы могут затруднять расследования и искажать доказательства инцидентов ИБ. Часы, связанные с передачей времени по радио от государственных атомных часов, могут использоваться как главные часы для регистрирующих систем. Для поддержки синхронизации всех серверов с главными часами может использоваться сетевой протокол службы времени.

В организации заранее разрабатываются и документально фиксируются все процедуры мониторинга ИБ, включая контроль параметров конфигурации и настроек средств и механизмов защиты, а также процедуры анализа данных регистрации, действий и операций. Они основываются на документально определенных критериях выявления неправомерных или подозрительных действий и транзакций. Указанные процедуры проводятся на регулярной основе персоналом организации, ответственным за ОИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СОИБ. Также документально определяются, а затем выполняются процедуры сбора и хранения информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию самих защитных мер.

Для проведения процедур мониторинга и анализа собранной информации часто используются специализированные программные и (или) технические средства.

Результаты выполнения процедур мониторинга ИБ постоянно анализируются и документально фиксируются. Информация обо всех инцидентах ИБ, выявленных в процессе мониторинга ИБ, в обязательном порядке включается в БД инцидентов ИБ.

Хорошей практикой является регулярный и зафиксированный документально пересмотр процедур мониторинга ИБ в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз ИБ и уязвимостей, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра определяется соответствующими утвержденными документами.

Также документально определяются роли, связанные с выполнением и пересмотром процедур мониторинга ИБ, и назначаются ответственные за выполнение указанных ролей.

2.3. Самооценка ИБ

Часто используемой практикой проверки уровня ИБ, выявления недостатков СУИБ и подготовки к внутреннему и внешнему аудитам ИБ (за счет оценки соответствия ИБ критериям аудита ИБ) является самооценка ИБ, проводимая организацией своими силами по инициативе руководства на основе принятых в организации документов (политик, регламентов, процедур и т. п.) и методик [13, 20, 21].

Под ***самооценкой ИБ организации*** будем понимать ***систематический и документируемый процесс получения ее сотрудниками свидетельств деятельности организации по ОИБ и установления степени выполнения установленных критериев самооценки ИБ***. Свидетельства деятельности по ОИБ в организации в рамках процесса самооценки ИБ называются *свидетельствами самооценки ИБ*. *Критерии самооценки ИБ* – совокупность политики, процедур или требований, используемых для сопоставления с ними свидетельств самооценки ИБ.

Цель самооценки ИБ – предоставление организации рекомендаций, основанных на фактах, касающихся областей применения ресурсов для улучшения ее деятельности в области ОИБ. Самооценка ИБ может быть полезной при измерении достижений в сравнении с целями, а также для повторной оценки постоянного соответствия этим целям.

Результаты самооценки ИБ оформляются в виде отчетов, анализируются руководством для понимания и устранения существующих в организации проблем ИБ и выявленных недостатков СОИБ, но до проведения независимого внешнего аудита ИБ не могут служить декларацией о соответствии критериям аудита ИБ, пока этого не подтвердит независимый внешний аудит ИБ.

Международный опыт показывает, что проведение самооценки ИБ дает организации следующие преимущества [22, 23]:

- использование при оценке своей деятельности в области ИБ и ее результатов единого комплекса критериев, который нашел широкое применение во многих странах;
- систематический подход к совершенствованию деятельности по ОИБ;
- получение объективных оценок уровня ИБ организации, основанных на фактах, а не на личном восприятии отдельных работников или руководителей;
- обучение персонала применению принципов ОИБ;
- внедрение различных инициатив и передовых методов ОИБ в повседневную деятельность организации;
- выявление и анализ процессов ОИБ, в которые можно ввести улучшения;
- определение глубины изменений, происшедших с момента проведения предыдущей самооценки ИБ;
- возможность распространения передового опыта лучших подразделений организации или других организаций;
- возможность признания и стимулирования посредством премирования достижений подразделений и работников;
- возможность сравнения с лучшими результатами, достигнутыми как в данной организации, так и в других.

Руководство организации определяет и обеспечивает ресурсы для поддержки процесса самооценки ИБ, включая определение лиц, ответственных за все аспекты самооценки ИБ, и соответствующее финансовое и инфраструктурное обеспечение необходимых функций самооценки ИБ, таких как сбор, анализ, хранение, передачу и распространение данных.

В процессе самооценки ИБ проводятся оценка степени выполнения требований стандартов, политики и т. п. и на ее основе вычисление итогового уровня ИБ для всей организации в целом или ее отдельных подразделений.

Для проведения самооценки ИБ в организации документально определяется следующее:

- порядок формирования, сбора и хранения качественных и количественных свидетельств самооценки ИБ;
- периодичность проведения самооценки ИБ;
- порядок хранения и использования результатов самооценки ИБ.

Работы по проведению самооценки ИБ проводятся сотрудниками организации, принимающими непосредственное участие в деятельности по ОИБ (как правило, это сотрудники службы ИБ), и включают следующие этапы:

1) подготовка к проведению самооценки ИБ – формирование группы по организации самооценки ИБ из числа сотрудников организации или

ее отдельного подразделения, сбору и анализу данных самооценки ИБ; определение руководителя проверяющей группы; формирование плана проведения самооценки ИБ; установление ролей и обязанностей для выполнения и использования результатов самооценки ИБ; определение формы отчета с результатами самооценки ИБ;

2) проведение самооценки ИБ в соответствии с программой и планом проведения – анализ документов и собственно самооценка ИБ на месте;

3) формирование результатов проведенной самооценки ИБ (подготовка и рассылка отчета с результатами самооценки ИБ) и информирование руководства организации о ее результатах.

Составляется, утверждается и далее реализуется программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки. Самооценка ИБ может проводиться в рамках программы внутреннего и внешнего аудитов ИБ, разработанной в организации.

Для каждой проводимой в организации самооценки ИБ документально оформляется, согласуется со всеми заинтересованными сторонами, а также утверждается ответственный за процесс самооценки ИБ (из числа представителей высшего руководства организации) и план проведения самооценки, определяющий:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- порядок, даты и сроки выполнения мероприятий самооценки ИБ, а именно порядки и сроки выполнения мероприятий по анализу документов, проведению самооценки ИБ на месте, подготовке и рассылке отчета с результатами самооценки ИБ;
- распределение ролей среди членов проверяющей группы – работников организации, связанных с проведением самооценки ИБ (анализом документов, проведением самооценки на месте, подготовкой и рассылкой отчета с результатами самооценки ИБ) и выполнением программы самооценок ИБ, а также назначение ответственных за выполнение указанных ролей.

Обычно ответственный за процесс самооценки ИБ имеет следующие обязанности:

- взаимодействовать с руководителями проверяемых подразделений для содействия самооценке ИБ;
- создавать возможности сбора данных для самооценки ИБ;
- назначать квалифицированный персонал для разработки и реализации плана самооценки ИБ;
- обеспечивать использование единого процесса по всей организации для процедур самооценки ИБ.

При проведении самооценки ИБ организации необходимо:

- ознакомиться с принятой методикой, в частности с набором показателей ИБ (частных и групповых), направлениями оценки, способом вычисления групповых показателей ИБ и оценок в рамках направлений и итогового уровня соответствия ИБ организации установленным требованиям;
- провести определение набора частных показателей ИБ, попадающих в область самооценки ИБ;
- провести оценивание необходимых частных показателей ИБ;
- провести вычисление значений оценок групповых показателей ИБ, значений оценок в рамках направлений и итогового уровня ИБ.

При определении размера и состава группы для проведения самооценки ИБ (проверяющей группы) учитывается компетентность, в основе которой лежит уровень квалификации ее участников. Если участники проверяющей группы не обладают необходимыми знаниями и опытом по специальным вопросам, то в группу включают технических экспертов, работающих под руководством участников проверяющей группы. Если при рассмотрении результатов работы эксперта проверяющей группой выявляются существенные несоответствия между его заключением и информацией (документами, тестовыми данными) проверяемой организации либо проверяющая группа считает, что выводы эксперта необоснованны, то проверяющей группе рекомендуется провести дополнительные процедуры, обеспечивающие проверку обоснованности заключения эксперта, или назначить другого эксперта. Заключение технического эксперта обычно включается в рабочие документы проверяющей группы. Если в исключительном случае эксперт дает устные разъяснения, то такие разъяснения отражаются проверяющей группой в ее рабочих документах. Использование работы технического эксперта при проведении самооценок ИБ не снимает ответственности за заключение с членов проверяющей группы.

Члены проверяющей группы готовят рабочие документы, необходимые для регистрации результатов самооценки ИБ и хранимые, по крайней мере, до окончания самооценки ИБ. Документы, содержащие конфиденциальную или частную информацию, всегда хранятся с соблюдением соответствующих требований по ОИБ.

Самооценку ИБ на месте в подразделении обычно предваряют вступительным совещанием с участием членов проверяющей группы и лиц, ответственных за проверяемые подразделения организации, подлежащие проверке. На совещании, где председательствует руководитель проверяющей группы, происходит следующее:

- представляются участники проверяющей группы, включая изложение их ролей;
- согласовывается график проведения самооценки ИБ;

- излагаются действия по проведению самооценки ИБ и осуществляется ознакомление с методами и процедурами, используемыми при проведении самооценки ИБ;
- согласовываются источники, способы получения и обмена информацией между проверяющей группой и представителями проверяемых подразделений, включая достоверность свидетельств самооценки ИБ, необходимых для оценивания частных показателей;
- согласовывается доступность ресурсов и оборудования, необходимых проверяющей группе;
- согласовываются принципы обеспечения конфиденциальности;
- осуществляется ознакомление с формой составления отчета с результатами проведения самооценки ИБ;
- дается информация о порядке рассмотрения замечаний проверяемых подразделений организации по проведению или заключению по результатам самооценки ИБ.

Анализ документов, выполняемый в процессе самооценки ИБ, производится с целью сбора первичных и дополнительных (когда самооценка ИБ проводится непосредственно на месте в проверяемом подразделении организации) свидетельств самооценки. Они позволяют оценить значения частных показателей ИБ выбранной организацией методики.

Документы, содержащие свидетельства выполнения деятельности по ОИБ, могут быть следующими: реестры и описи; регистрационные журналы; протоколы; приказы и распоряжения; акты; договоры; отчеты, а также устные высказывания сотрудников проверяемых подразделений и результаты наблюдений членов проверяющей группы за деятельностью по реализации требований нормативных документов по ОИБ.

Полученные свидетельства самооценки ИБ и источники их получения фиксируются путем составления листов сбора свидетельств. На основании собранных свидетельств самооценки ИБ проверяющие формируют оценки частных показателей.

По окончании этапа проведения самооценки ИБ на месте, как правило, проводится заключительное совещание с участием представителей проверяющей группы и проверяемой организации или ее отдельных подразделений под председательством руководителя проверяющей группы. На совещании представляются результаты оценивания по каждому из частных показателей таким образом, чтобы они были понятны и признаны всеми заинтересованными лицами в организации. Любые разногласия по оцениванию частных показателей обсуждаются и по возможности разрешаются. Если единое мнение не найдено, то это фиксируется документально. На совещании могут быть представлены рекомендации по повышению уровня ИБ.

По результатам проведения всех этапов самооценки ИБ готовится отчет, утверждаемый ответственным за процесс самооценки ИБ и содержащий следующее:

- сведения об организации, проводившей самооценку ИБ;
- сведения о руководителе и членах проверяющей группы;
- сроки проведения самооценки ИБ;
- краткое изложение процесса самооценки;
- любые неразрешенные разногласия;
- заявление о конфиденциальном характере содержания отчета с результатами самооценки ИБ;
- заполненные анкеты оценивания групповых показателей ИБ;
- документы, обосновывающие исключение частных показателей из области самооценки;
- заполненные листы сбора свидетельств самооценки, подтверждающие выставленные оценки частных показателей ИБ;
- документы, содержащие результаты самооценки ИБ по направлениям оценки и итоговый уровень соответствия ИБ организации установленным требованиям, возможно с наглядным представлением (например, в виде круговой диаграммы оценивания групповых показателей ИБ, определенной и описанной в методике);
- лист рассылки отчета с результатами самооценки ИБ.

Проверенный и приобретший окончательную форму отчет с результатами самооценки ИБ распространяется между всеми заинтересованными сторонами, включая главу организации, руководителей и сотрудников подразделения ИБ.

Члены организации получают доступ к отчету с результатами самооценки ИБ в соответствии с принципом необходимого знания и имеющимися у них правами.

Иногда может потребоваться распространить результаты самооценки ИБ среди внешних заинтересованных сторон, включая органы регулирования, акционеров, клиентов и поставщиков.

2.4. Внутренний аудит ИБ

Через запланированные интервалы времени организация должна проводить внутренние аудиты ИБ, рассматривая их как важнейшую форму контроля руководством функционирования СУИБ.

Первоначально аудит возник в финансовой области, после чего его применение постепенно распространилось и на другие категории, такие как качество и окружающая среда. По мере развития концепции обеспечения качества аудиты стали проводится для продукции, процессов и систем качества. После появления в 1987 г. стандартов ISO серии 9000 широкое распространение получили аудиты систем менеджмента качества и в организациях стали вводиться внутренний аудит и анализ со

стороны руководства, из которых выросла и получила широкое распространение самооценка ИБ, охватывающая всю деятельность организации. При этом аудит ИБ (как внутренний, так и внешний) по содержанию стал разделяться на два вида [24–26]:

Аудит ИБ организации – проверка состояния защищенности интересов/целей организации в процессе их реализации в условиях внутренних и внешних угроз ИБ, а также предотвращение утечки защищаемой информации и возможных несанкционированных и непреднамеренных воздействий на нее. Аудитом ИБ также считается системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ организации в соответствии с определенными критериями и показателями ИБ и адекватности ИБ поставленным целям и задачам бизнеса для увеличения эффективности и рентабельности экономической деятельности организации.

Аудит ИБ систем информационных технологий (ИТ), эксплуатирующихся в организации (как самостоятельный аудит или как часть аудита ИБ организации) – проверка состояния защищенности конфиденциальной информации в организации от внутренних и внешних угроз ИБ, а также ПО и АО, от которого зависит бесперебойное функционирование систем ИТ. Данный вид подразумевает как *документальный*, так и *технический* аудит состояния защищенности информации при ее сборе, обработке, хранении с использованием различных систем ИТ. Технический аудит осуществляется семейством программных и технических средств контроля, обеспечивающих деятельность по регистрации событий ИБ, а также (возможно) по исследованию нарушений ИБ на основе данных регистрации. Во время его проведения дается общая оценка архитектуры и информационных потоков (Интернет, электронная почта, веб-приложения, файлы и т. д.), проверяется наличие и текущее состояние СОИБ, актуальность применяемых политик, технических регламентов и инструкций. При этом исследуется, насколько адекватно корпоративная и частные ПолИБ настроены в ПО, АО, каналах связи и процессах (например, оценивается текущее состояние конфигураций и правил фильтрации сетевого оборудования с точки зрения ОИБ сетевой инфраструктуры, правильность существующей архитектуры обработки данных). Дополнительно анализируется полнота и актуальность организационно-распорядительной и методической документации, уровень сопровождения СЗИ.

Определим ***внутренний аудит ИБ как регламентированную внутренними документами организации деятельность по контролю функционирования ее СУИБ и различных аспектов ОИБ, осуществляемую представителями специального контрольного органа – подразделения организации в рамках помощи органам управления организации***. В стандартах ISO/IEC и ГОСТ Р ИСО/МЭК 19011 внутренний

аудит называется *аудитом первой стороной*, который проводится самой организацией или от ее имени [9, 10].

Основными преимуществами внутренних аудитов ИБ перед внешними являются:

- знание внутренними аудиторами особенностей своей организации;
- отсутствие предубежденного отношения сотрудников проверяемых подразделений к внутренним аудиторам, которые не воспринимаются как посторонние для организации лица;
- отсутствие дефицита времени при аудите, ограничивающем возможности более детального изучения проверяемого подразделения;
- меньшие затраты на проведение внутреннего аудита по сравнению с внешним.

Исходными документами для проведения внутреннего аудита ИБ могут быть:

- документы, определяющие порядок проведения внутреннего аудита ИБ;
- программа внутреннего аудита ИБ;
- документы по результатам ранее проведенных внутренних аудитов ИБ с предложениями по развитию в области управления ИБ.

Программа внутренних аудитов ИБ планируется с учетом статуса и важности процессов и областей обеспечения и управления ИБ, которые нужно проверять, а также результатов предыдущих аудитов. Обязательно определяются критерии, область действия, частота и методы внутреннего аудита ИБ. Ответственность за планирование и проведение аудитов и требования для их планирования и проведения, а также для сообщения результатов и поддержания записей в рабочем состоянии, определяются в документированной процедуре внутреннего аудита ИБ. Руководство, ответственное за проверяемую область, должно гарантировать, что действия по устранению обнаруженных несоответствий и их причин предпринимаются без неоправданной задержки. Последующая деятельность включает в себя проверку предпринятых действий и составление отчета по результатам этой проверки.

2.4.1. Цели и задачи внутренних аудитов ИБ

Целями внутренних аудитов ИБ является определение следующего [1, 2, 11, 12]:

1) соответствуют и адекватны ли документы, деятельность и результаты в области управления ИБ требованиям применяемых международных, национальных и иных стандартов в области ИБ и относящихся к ним законов или норм;

2) соответствуют и адекватны ли деятельность и результаты в области управления ИБ выявленным требованиям по ОИБ, разработанным в самой организации;

3) эффективно ли реализуются и поддерживаются в рабочем состоянии запланированные мероприятия по управлению и обеспечению ИБ;

4) выполняются ли, как ожидается, цели, средства, процессы и процедуры СУИБ организации.

Для достижения этих целей решаются следующие задачи:

- подтверждение соответствия документов, деятельности и ее результатов для СУИБ установленным требованиям;
- подтверждение достижения целей в области ОИБ;
- подтверждение выполнения регламентирующих и законодательных требований и договорных обязательств;
- анализ и устранение причин выявленных несоответствий;
- предотвращение появления проблем ИБ;
- подтверждение устранения несоответствий и выполнения корректирующих действий;
- оценка эффективности функционирующей СУИБ;
- установление степени понимания персоналом целей, задач и требований, установленных документами СУИБ;
- обеспечение уверенности руководства и потребителя в результативности СУИБ;
- обеспечение отслеживания ОИБ для бизнес-процессов;
- выявление возможности улучшений СУИБ.

Внутренний аудит ИБ обеспечивает руководство организации информацией об эффективности и продуктивности СУИБ, являются ли их ПолИБ и политика СУИБ удовлетворительными или нет и какие требуются изменения, чтобы они стали таковыми.

Результаты внутренних аудитов ИБ служат основой входных данных для анализа СУИБ со стороны руководства и дают полезную информацию независимым экспертам при проведении внешних аудитов ИБ.

2.4.2. Организационные принципы внутреннего аудита ИБ

Выделяют следующие *организационные принципы внутреннего аудита, применимые к области ИБ* [23]:

Независимость – проводящие проверки лица не несут прямой ответственности за проверяемую деятельность и не зависят от руководителя проверяемого подразделения с тем, чтобы исключить возможность необъективных и пристрастных выводов аудиторских проверок.

Единообразие – каждая аудиторская проверка осуществляется по единой официально установленной процедуре, что обеспечивает ее упорядоченность, однозначность и сопоставимость.

Системность – планирование и проведение проверки по различным видам деятельности и процессам осуществляется с учетом установленной их структурной взаимосвязи в СУИБ.

Документированность – проведение каждой проверки определенным образом документируется с тем, чтобы обеспечить сохранность и сравнимость информации о фактическом состоянии объекта.

Предупредительность – каждая проверка планируется, и персонал проверяемого подразделения заранее уведомляется о цели, объекте, критериях, времени и методах ее проведения с тем, чтобы обеспечить необходимый уровень доверия к аудиторам и исключить возможность уклонения персонала от предоставления и демонстрации всех требуемых данных.

Регулярность – проверки проводятся с определенной периодичностью с тем, чтобы все процессы системы и все подразделения организации были объектом постоянного анализа и оценивания со стороны руководства организации.

Доказательность – процедуры и методы, используемые при проверках, обеспечивают надежность заключений по их результатам.

Открытость – результаты каждой проверки носят открытый характер, то есть являются доступными для ознакомления любым сотрудником проверенного подразделения, если не оговорено обратное.

2.4.3. Принципы обеспечения эффективности внутреннего аудита ИБ

Основной фактор успеха проведения внутреннего аудита ИБ в организации – это соблюдение взаимосвязанных *принципов обеспечения его эффективности* [23]:

Ответственность – каждый работающий в организации внутренний аудитор как субъект внутреннего контроля несет ответственность (экономическую, административную, дисциплинарную) за ненадлежащее выполнение каждой из контрольных функций, ясно определенной и формально закрепленной за конкретным субъектом.

Сбалансированность – аудитору не предписываются контрольные функции, не обеспеченные средствами для их выполнения. Не должно быть средств, несвязанных с той или иной функцией. При определении обязанностей субъекта контроля должен быть предписан соответствующий объем прав и возможностей, и наоборот.

Своевременное сообщение об отклонениях от нормы – информация об отклонениях предоставляется лицам, уполномоченным принимать решения по соответствующим отклонениям, в максимально короткие сроки. Если сообщение запаздывает, нежелательные последствия отклонений усугубляются; объект переходит уже в другое состояние (действие), что лишает смысла сам проведенный контроль. При предварительном контроле несвоевременное сообщение о возможности возникновения отклонений также лишает смысла проведенный контроль.

Соответствие контролирующей и контролируемой систем – степень сложности системы внутреннего аудита ИБ должна соответствовать степени сложности подконтрольной системы.

Комплексность – объекты всех типов должны быть охвачены адекватным внутренним аудитом ИБ.

Разделение обязанностей – функции между участвующими в проведении внутреннего аудита ИБ распределяются таким образом, чтобы за одним человеком не были закреплены одновременно, например, следующие функции: санкционирование операций, регистрация операций, обеспечение сохранности данных, осуществление инвентаризации.

Разрешение и одобрение – должно быть обеспечено формальное разрешение и одобрение всех операций внутренних аудиторов ответственными официальными лицами в пределах их полномочий.

2.4.4. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации

Внутренний аудит ИБ в организации проводит соответствующее подразделение, занимающееся всеми аспектами внутреннего аудита ее деятельности и среди прочих вопросов контролирующее ИБ. Практическая польза наличия такого подразделения для каждой отдельно взятой организации различна, но в общем случае она заключается в следующем [27–29]:

1) это позволит высшему руководству наладить эффективный контроль за ОИБ в отдельных подразделениях организации;

2) проводимые внутренними аудиторами целевые контрольные проверки и анализ выявляют резервы и наиболее перспективные направления совершенствования управления ИБ, позволяют непрерывно совершенствовать все процессы ОИБ;

3) внутренние аудиторы наряду с контролем часто выполняют и консультативные функции в отношении должностных лиц различных служб в головной организации, ее филиалах и дочерних компаниях.

Для контроля за ОИБ подразделению внутреннего аудита необходимо осуществить следующее: выявить и четко определить область его действия в отношении проверок ИБ, основные функции, полномочия и статус, необходимые для достижения поставленных целей в области внутреннего аудита ИБ; разработать схемы взаимоотношений, определить обязанности, права и ответственность всех работников подразделения, документально закрепить это в должностных инструкциях и Положении о подразделении; интегрировать подразделение в структуру управления организацией; разработать внутрикорпоративные стандарты внутреннего аудита ИБ и Кодекса этики.

Основные *требования к организации системы внутреннего аудита ИБ* также обусловливают эффективное функционирование его системы [27–29]:

1. Ущемление интересов – необходимо создавать специальные условия, при которых любые отклонения ставят заинтересованного в них работника или подразделение организации в невыгодное положение и побуждают их к регулированию «узких мест».

2. Недопущение концентрации прав первичного контроля в руках одного лица.

3. Заинтересованность и должное участие руководства организации.

4. Приемлемость/пригодность методологии внутреннего аудита ИБ. Ставящиеся цели и задачи внутреннего аудита ИБ должны быть рациональными. Программы внутреннего аудита, применяемые методы и распределение контрольных функций должны быть целесообразными.

5. Непрерывность развития и совершенствования. Система внутреннего аудита ИБ должна быть построена таким образом, чтобы ее можно было гибко настраивать на решение новых задач, возникающих в результате изменения внутренних и внешних условий функционирования организации, и обеспечить возможность ее расширения и модернизации.

6. Приоритетность – абсолютный контроль над обычными незначительными операциями не имеет смысла и только отвлекает силы от более важных задач.

7. Исключение ненужных этапов, шагов или процедур в проведении внутреннего аудита ИБ – его необходимо организовывать рационально, так как это часто связано с дополнительными затратами труда и средств.

8. Персональная ответственность – каждая отдельная контрольная функция должна быть закреплена за одним ответственным. Закрепление нескольких контрольных функций за одним ответственным вполне допустимо.

9. Аудитор оценивает законность всех операций, но ответственность он несет за необнаружение операций с негативными последствиями. Данное требование не распространяется на ситуации, когда во избежание ошибок и/или злоупотреблений отдельных должностных лиц (ответственных) принимается коллегиальное решение.

10. Потенциальное замещение функций – временное выбытие отдельных субъектов внутреннего аудита ИБ – не должно прерывать контрольные процедуры. Для этого каждый внутренний аудитор должен уметь выполнять контрольную работу вышестоящего, нижестоящего и одного-двух работников своего уровня во избежание потери адекватной связи с объектом контроля за время их выбытия.

11. Регламентация – подчиненность аудиторской деятельности в организации установленным регламентам и формальным правилам, регулирующим порядок этой деятельности.

2.5. Внешний аудит ИБ

Подход организации к управлению ИБ и реализации ОИБ (цели и средства управления, политика, процессы и процедуры ОИБ) должны независимо и объективно анализироваться через запланированные промежутки времени или по мере значительных изменений в реализации защиты. Независимый анализ инициируется руководством организации. Он необходим для того, чтобы обеспечить долгосрочность, адекватность и результативность подхода организации к управлению ИБ, а также оценить возможности улучшения за счет внедрения корректирующих действий и потребность в изменениях в подходе к защите, включая политику и цели в области управления ИБ. Таким анализом является внешний аудит ИБ.

***Внешний аудит ИБ** – **систематический, независимый и документируемый процесс получения свидетельств деятельности организации по ОИБ и установления степени выполнения в ней критериев аудита ИБ, проводимый внешней по отношению к проверяемой независимой проверяющей организацией и допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации**.*

При этом *критерии аудита ИБ* – совокупность требований по ОИБ, характеризующая некоторый уровень ИБ и используемая для сопоставления с ними свидетельств аудита ИБ, а *свидетельства аудита ИБ* – записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита ИБ и могут быть проверены (свидетельства могут быть качественными или количественными).

Критерии аудита ИБ выступают в качестве эталона, с которым сравниваются свидетельства аудита ИБ, и могут присутствовать в стандартах, политиках, условиях контракта, документации, программах и планах [9, 10, 14, 20]. Примеры критериев аудита СУИБ: методология и результаты оценки рисков ИБ и их соответствие установленным требованиям; показатели эффективности реализованных средств управления и их применение в соответствии с установленными правилами измерения; внутренние аудиты СУИБ и анализ со стороны руководства с принятием решений о корректирующих действиях и т. д.

Согласно стандартам ISO/IEC и ГОСТ Р ИСО/МЭК 19011 внешние аудиты включают обычно так называемые аудиты второй и третьей сторонами [9, 10]. *Аудиты второй стороной* проводятся сторонами, заинтересованными в деятельности организации, например потребителями или другими лицами от их имени. *Аудиты третьей стороной* проводятся внешними независимыми аудиторскими организациями, например такими, которые обеспечивают сертификацию/регистрацию соответствия стандартам ISO 9001, 14001 или 27001. Таким образом заказчиком аудита ИБ может являться сама проверяемая организация или

любая другая организация/лицо, имеющие законное право потребовать аудит ИБ и заказавшие его.

В стандартах ISO/IEC и ГОСТ Р ИСО/МЭК 27006 [5, 6], следуя основным положениям ISO/IEC и ГОСТ Р ИСО/МЭК 17021 [28, 29], внешний аудит ИБ рассматривается как часть деятельности по сертификации систем менеджмента, обеспечивающей независимое свидетельство того, что эта система соответствует установленным требованиям, способствует последовательной реализации принятой политики и целей и внедрена результативно. Такой *аудит* называется *первичным сертификационным*, и он обязательно предшествует сертификации системы. Кроме этого бывают *надзорные аудиты* в течение первого и второго года после сертификации (инспекционный контроль для подтверждения продолжения реализации утвержденной и сертифицированной СУИБ, рассмотрения предпосылок для изменений в СУИБ, связаны с изменениями в работе проверяемой организации, и подтверждения постоянного соответствия требованиям сертификации), *аудиты повторной сертификации* в течение третьего года до истечения срока действия сертификата и *специальные аудиты* (с расширением области или внеплановые).

В стандартах ISO/IEC и ГОСТ Р ИСО/МЭК 27006 [5, 6] также отмечается, что аудит СУИБ может объединяться с аудитами других систем управления организации. Это возможно, если аудиты удовлетворяют всем требованиям по сертификации СУИБ. Все элементы, значимые для СУИБ, должны быть четко выражены и легко идентифицируемы в отчетах о результатах аудитов. Объединение аудитов не должно отрицательно влиять на качество аудита СУИБ. Также важно обеспечить защиту от утечки информации, получаемой на всех стадиях аудита ИБ, соглашение о чем должно быть достигнуто перед его началом.

Цели внешнего аудита ИБ определяет заказчик аудита – организация или лицо, его заказавшее. Обычно требуется подтверждение одного или сразу двух положений:

1) проверяемая организация придерживается собственных политики, целей и процедур в области ОИБ;

2) соответствие СУИБ проверяемой организации всем требованиям стандартов ISO/IEC и ГОСТ Р ИСО/МЭК 27001 и целям политики организации.

В основе внешнего аудита ИБ лежит стремление руководства организации с помощью проведения независимой и компетентной оценки определить истинный уровень организации работ в области ОИБ и степень соответствия ИБ организации установленным критериям аудита ИБ – совокупности требований по ОИБ, определенных в признанных организацией документах и характеризующих некоторый уровень ИБ. Оценка соответствия ИБ организации критериям аудита ИБ проводится на основе документов по ОИБ и фактов, свидетельствующих о выполнении, частичном выполнении или невыполнении установленных тре-

бований по ОИБ. Следовательно, внешний аудит ИБ должен сосредоточиться в первую очередь на следующем [5, 6]:

- соблюдении требований к документации, сформулированных в ISO/IEC и ГОСТ Р ИСО/МЭК 27001;
- ответственности руководства за ПолИБ;
- проведенной организацией оценке рисков ИБ и на том, дают ли эти оценки сопоставимые и воспроизводимые результаты;
- получении свидетельств, что анализ угроз ИБ является значимым и соответствующим работе организации;
- установлении, согласуются ли процедуры по идентификации, изучению и оценке угроз ИБ, активов, уязвимости и воздействий, а также результаты их применения с политикой, целями и планами организации;
- процессе обработки рисков ИБ в организации;
- оценке выбора целей и средств управления ИБ в рамках СУИБ, основанных на процессах обработки рисков ИБ;
- анализе и измерениях эффективности и результативности СУИБ и средств управления ИБ в отношении достижения целей ПолИБ;
- выявлении функционирования процедур периодической оценки и проверки соответствия правовым и нормативным требованиям по ОИБ;
- результатах внутренних аудитов СУИБ и их анализе со стороны руководства;
- мерах, принятых в отношении несоответствий, выявленных во время последнего аудита ИБ;
- установлении соответствия между выбранными и внедренными средствами управления ИБ;
- определении введения в действие и результативности средств управления ИБ и установление их эффективности для достижения намеченных целей;
- программах, процессах, процедурах, записях, внутренних аудитах ИБ и анализах эффективности СУИБ с целью обеспечения их прослеживаемости до решений управления, политики и целей СУИБ.

Основными документами внешнего аудита ИБ являются [20]:

1) программа внешнего аудита ИБ, включающая описание деятельности, необходимой для планирования, проведения, контроля, анализа и совершенствования внешних аудитов ИБ;

2) план внешнего аудита ИБ;

3) аудиторское заключение.

Программа аудита ИБ – план деятельности по проведению одного или нескольких аудитов ИБ (обязательно внешних плюс, возможно, внутренних и самооценок), запланированных на конкретный период времени и направленных на достижение конкретной цели.

План аудита ИБ – описание деятельности и мероприятий по какому-либо конкретному аудиту ИБ.

Область аудита ИБ – содержание и границы аудита ИБ. Область аудита ИБ обычно включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются аудиту ИБ, а также охватываемый период времени. Применительно к СУИБ область действия аудита отражает риски ИБ, соответствующие бизнес-требования и бизнес-риски организации.

Аудиторское заключение (заключение по результатам аудита ИБ) – качественная и/или количественная оценки соответствия установленным критериям аудита ИБ, представленные аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.

Выводы аудита ИБ – результат оценки собранных свидетельств аудита ИБ на соответствие критериям аудита ИБ. Выводы аудита ИБ указывают на несоответствие/соответствие и степень соответствия ИБ организации критериям аудита ИБ или возможность улучшения.

Аудитор (***эксперт***) – лицо, обладающее компетентностью для проведения аудита ИБ.

Аудиторская группа – один или несколько аудиторов, проводящих аудит ИБ, при необходимости поддерживаемые техническими экспертами.

Технический эксперт – лицо, предоставляющее аудиторской группе свои знания и/или опыт по специальным вопросам, включая ИБ.

2.5.1. Принципы проведения внешнего аудита ИБ

Проведение внешнего аудита ИБ основывается на ряде принципов, следование которым является предпосылкой для обеспечения объективных заключений по результатам внешнего аудита ИБ. Эти принципы делают внешний аудит ИБ результативным и надежным методом поддержания политики руководства и контроля, обеспечивая информацией, на основе которой организация может улучшать свои характеристики. Принципы должны быть признаны и соблюдены всеми сторонами, участвующими во внешнем аудите ИБ.

К принципам внешнего аудита ИБ [5, 6, 20, 28–32] относят:

Независимость – основа беспристрастности при проведении внешнего аудита ИБ и объективности при формировании заключения по результатам аудита ИБ. Аудиторы должны быть независимы в своей деятельности, неответственны за деятельность, которая подвергается аудиту ИБ, и свободны от предубеждений и конфликтов интересов. Аудиторы сохраняют объективное мнение во время всего процесса внешнего аудита ИБ с целью обеспечения того, что в основе выводов и заключений находятся только свидетельства аудита. Аудиторы проверяющей внешней организации должны назначаться исходя из принципа независимости от руководства проверяемых подразделений.

Полнота – необходимое условие для формирования объективных заключений по результатам аудита ИБ. Аудит ИБ должен охватывать все области ИБ, соответствующие аудиторскому заданию. Кроме того полнота

аудита ИБ определяется достаточностью предоставленных материалов, документов и уровнем их соответствия поставленным задачам.

Оценка на основе свидетельств аудита ИБ – основа для достижения надежных и воспроизводимых (повторяемых) заключений внешнего аудита ИБ в процессе систематического аудита ИБ. Свидетельство аудита ИБ основано на выборках существующей информации, поскольку аудит осуществляется в ограниченный период времени и с ограниченными ресурсами. Соответствующее использование выборок не дает стопроцентной гарантии соответствия требованиям и тесно связано с доверием, с которым относятся к заключениям по результатам аудита. Повторяемость заключений по результатам внешнего аудита ИБ повышает доверие к нему. Для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми.

Достоверность свидетельств аудита ИБ – основа получения достоверных и полных заключений внешнего аудита ИБ. Доверие к фактам, полученным при опросе сотрудников проверяемых подразделений, повышается при подтверждении данных фактов из различных источников. Доверие к фактам, полученным при наблюдении за деятельностью проверяемых подразделений в области ОИБ, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов.

Необходимость понимания аудитором деятельности проверяемой организации – условие получения достоверных и полных заключений внешнего аудита ИБ. При проведении внешнего аудита ИБ аудитор должен понимать деятельность проверяемой организации в достаточной степени, чтобы идентифицировать и правильно оценивать события, процессы, относящиеся к области ИБ, с учетом возможностей применения методов и способов оценки рисков ИБ, которые могут оказывать существенное влияние на достоверность проверяемых данных, на ход проведения проверки или на выводы, содержащиеся в аудиторском заключении.

Компетентность, этичность и беспристрастность – основа профессионализма. Доверие к процессу внешнего аудита ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения. Компетентность базируется на личных качествах аудитора и способности применять на практике свои знания и опыт. Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, осмотрительность. Профессиональная осмотрительность заключается в прилежании и умении принимать правильные решения при проведении внешнего аудита ИБ и соответствует важности выполняемого задания и доверительности со стороны заказчиков и других заинтересованных сторон. Беспристрастность означает обязательство представлять правдивые и точные отчеты. Выводы внешних аудитов ИБ, заключения по результатам аудита и записи отражают правдиво и точно

деятельность по аудиту. Неразрешенные проблемы или разногласия между аудиторской группой и проверяемой организацией отражают в отчетах (актах).

Ответственность за соответствие требованиям несет проверяемая организация, а за оценку достаточности объективных свидетельств, являющихся основанием для принятия решений, и сами принимаемые решения – аудиторская организация.

Открытость – принцип доступности и раскрытия соответствующей информации: аудиторская организация должна обеспечить открытый доступ или своевременно раскрывать соответствующую неконфиденциальную информацию в отношении процесса проведения аудита и его результатах определенным заинтересованным сторонам.

Конфиденциальность – аудиторская организация должна обеспечивать конфиденциальность частных сведений о проверяемой организации и заказчике аудита ИБ.

Реагирование на жалобы – в случае признания обоснованными жалобы сторон соответствующим образом учитываются, рассматриваются и для их разрешения прикладываются надлежащие усилия, то есть реагирование на жалобы должно быть результативным.

2.5.2. Управление программой внешнего аудита ИБ

Программа внешнего аудита ИБ, как отмечается в стандарте ISO/IEC 27007:2011 [7], основывается на выявленных рисках ИБ для организации. Она разрабатывается самой проверяемой организацией. В зависимости от размера, вида деятельности и сложности организации эта программа может включать один и более аудитов, которые могут иметь различные цели. Может быть создано больше одной программы аудита ИБ.

Программа внешнего аудита ИБ включает все мероприятия, необходимые для планирования, организации и проведения внешних аудитов ИБ, а также для обеспечения ресурсами, необходимыми для эффективного и рационального проведения аудитов в определенные временные рамки.

В программе внешнего аудита ИБ определяются ее задачи. Для этого принимается во внимание следующее:

- установленные требования по ОИБ;
- риски ИБ для организации;
- показатели эффективности ОИБ;
- деятельность по мониторингу и анализу СУИБ;
- строгость следования организацией своим политикам и задачам и выполнению установленных процедур;
- эффективность реализации и поддержания процессов и средств управления СУИБ, а также их выполнение согласно ожиданиям.

Примеры задач программы внешнего аудита ИБ: проверка соответствия определенным правовым, нормативным требованиям и договор-

ным обязательствам и их влияние на ИБ; подтверждение выбора адекватной обработки рисков ИБ организации; оценка адекватности установления и удовлетворения требований по ОИБ; оценка постоянной актуальности задач СУИБ; подтверждение эффективности реализации средств управления для снижения рисков ИБ; проверка применения и полноты измерений и мер измерений в области ИБ; мониторинг и анализ деятельности СУИБ; анализ совершенствований СУИБ и т. п. Этим задачам могут быть присвоены соответствующие приоритеты, основанные на оценке рисков ИБ и бизнес-требованиях с учетом направлений деятельности СУИБ в организации.

Содержание программы внешнего аудита ИБ зависит в первую очередь от размера и сложности СУИБ, численности персонала и временных работников, количества используемых ИС и ИТ, рисков ИБ для самой СУИБ, критичности активов в области действия СУИБ.

Выдержка из возможной программы аудита УНБ приведена в Приложении 1 [33].

Программа внешнего аудита ИБ требует постоянного контроля, анализа и совершенствования.

Процедуры программы внешнего аудита ИБ включают в себя следующее:

- планирование и составление планов–графиков аудитов;
- обеспечение компетентности аудиторов по ИБ и руководителей аудиторских групп;
- подбор соответствующих аудиторских групп и распределение ролей и ответственности;
- проведение аудитов;
- выполнение действий по результатам аудита, если требуется;
- поддержание записей по программе внешнего аудита ИБ;
- мониторинг показателей результативности программы;
- отчетность перед руководством организации по всей проделанной работе по программе.

Управление программой внешнего аудита ИБ должно выполняться в рамках цикла PDCA (рис. 2.4) [9, 10, 25].

На *этапе планирования* разрабатывается программа внешнего аудита ИБ. При этом определяются цели и объем внешнего аудита ИБ, ответственные за его проведение, ресурсы и процедуры.

Для определения целей необходимо рассмотреть следующее:

- приоритеты руководства;
- коммерческие намерения;
- требования стандартов (внешних и внутренних);
- законодательные требования, требования регламентов и требования, предусмотренные договорными обязательствами;
- потребности заинтересованных сторон;
- риски организации.

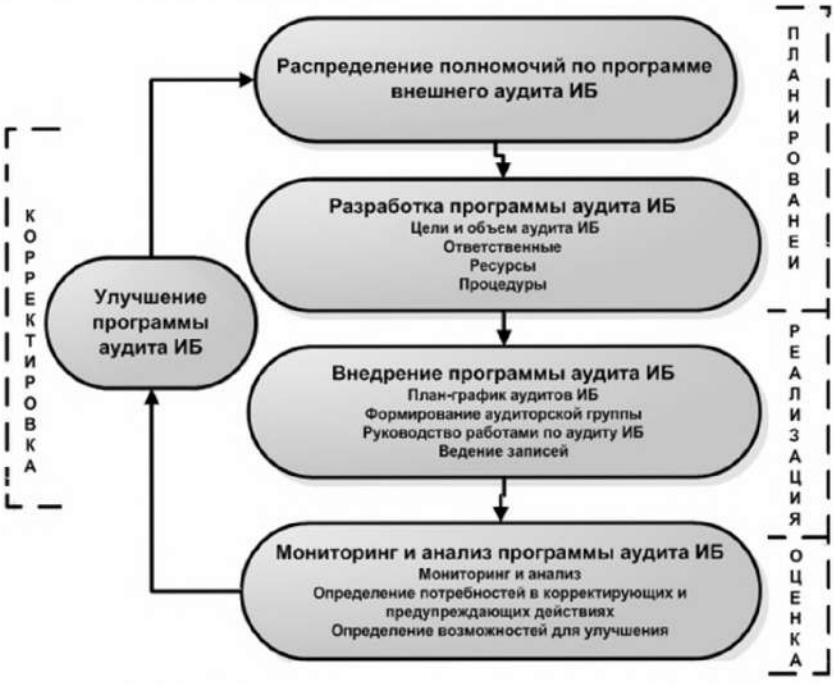

Рис. 2.4. Последовательность процессов управления программой внешнего аудита ИБ

Примерами целей различных программ внешнего аудита ИБ являются следующие: содействие улучшению СУИБ, обеспечение выполнения требований к сертификации СУИБ на соответствие стандарту ISO/IEC 27001 или проверка соответствия требованиям по ОИБ ПолИБ организации.

Объем программы внешнего аудита ИБ зависит от размера, вида деятельности, сложности структуры проверяемой организации, а также:

- области, цели и продолжительности каждого осуществляемого аудита;
- частоты проводимых аудитов;
- количества, важности, комплексности, степени сходства, местоположения подразделений, подлежащих аудиту;
- стандартов, законодательных, нормативных и контрактных требований и другие критериев аудита;
- потребностей организации в оценке полноты и качества выполнения требований, предъявляемых к организации или ее систем ИТ, при возникновении необходимости их аккредитации или регистрации/сертификации;
- заключений по результатам предыдущих аудитов или анализа результатов предыдущих программ аудитов;

- любых проблем, связанных с языком, культурой или социальными вопросами;
- мнений заинтересованных сторон;
- существенных изменений в организации или ее деятельности.

Высшее руководство организации предоставляет полномочия по управлению программой внешнего аудита ИБ. Ответственность за управление этой программой возлагают на одно или нескольких лиц, имеющих представление о принципах аудита ИБ, компетентности аудитора по ИБ и применении методов аудита ИБ. Эти лица также должны обладать навыками управления, техническими и экономическими знаниями в области ИБ. Они должны:

- определять цели и объем программы внешнего аудита ИБ;
- определять ответственность и процедуры, а также гарантировать обеспечение необходимыми ресурсами;
- разрабатывать и внедрять программу;
- вести записи по программе;
- осуществлять мониторинг, анализ и улучшение программы;
- определять потребность программы в ресурсах;
- способствовать принятию решений об обеспечении программы необходимыми ресурсами.

При определении ресурсов для программы учитывают следующее:

- финансовые ресурсы для развития, внедрения, управления и улучшения деятельности по внешнему аудиту ИБ;
- методы проведения аудитов ИБ;
- процессы по достижению и поддержанию компетентности и улучшению деятельности аудиторов по ИБ;
- наличие аудиторов по ИБ и технических экспертов, обладающих компетентностью, требуемой для достижения конкретных целей программы аудита ИБ;
- объем программы;
- время в пути аудиторов по ИБ, обустройство и другие потребности для проведения аудита ИБ.

На *этапе реализации* осуществляется внедрение программы внешнего аудита ИБ. При этом разрабатывается план-график внешних аудитов ИБ, формируется аудиторская группа и проводятся работы по аудиту, осуществляются ведение записей и руководство работами по аудиту. Таким образом, внедрение программы включает в себя следующее:

- доведение программы до участвующих сторон;
- координация и календарное планирование аудитов и другой деятельности, связанной с программой;
- определение и поддержание процесса оценки аудиторов по ИБ и их непрерывного профессионального роста;
- формирование аудиторских групп;

- предоставление необходимых ресурсов аудиторским группам;
- проведение аудитов в соответствии с программой;
- управление записями по аудиту ИБ;
- анализ и утверждение отчетов по аудиту ИБ и их рассылка заказчикам аудитов ИБ и заинтересованным сторонам;
- действия по результатам аудита ИБ, если это требуется.

Записи по программе внешнего аудита ИБ хранятся защищенным образом и включают в себя следующее:

- записи, связанные с отдельными аудитами ИБ: планы аудита, отчеты (акты) по аудиту, отчеты о несоответствиях, отчеты по корректирующим и предупреждающим действиям, отчеты о действиях по результатам аудита, если это требуется;
- результаты анализа программы;
- записи о персонале, привлекаемом к аудиту ИБ: оценка компетентности аудитора по ИБ и его деятельности, выбор аудиторской группы, поддержание и повышение компетентности.

На *этапе оценки* осуществляются мониторинг внедрения программы внешнего аудита ИБ и через определенные интервалы времени ее анализ достижения целей, определяются потребности в корректирующих и предупреждающих действиях, определяются возможности для улучшения программы. Руководство проверяемой организации информируется о результатах анализа.

Показатели деятельности по внешнему аудиту ИБ обычно используются для мониторинга следующих характеристик:

- возможности аудиторской группы реализовать план внешнего аудита ИБ;
- соответствие программам аудитов ИБ (в частности достижение целей аудита) и планам-графикам;
- отчеты и заключения по результатам аудита ИБ;
- обратная связь от заказчиков аудита ИБ, проверяемых организаций и аудиторов.

Анализ программы внешнего аудита ИБ традиционно охватывает следующие вопросы:

- результаты мониторинга и установленные тенденции;
- соответствие процедурам программы;
- выявление потребностей и ожиданий заинтересованных сторон;
- записи по программе;
- альтернативные или новые методики в области аудита ИБ;
- согласованность действий аудиторских групп в сходных ситуациях.

На *этапе корректировки* производится (при необходимости) улучшение программы внешнего аудита ИБ. Это касается, например, пересмотра и корректировки сроков проведения аудитов ИБ и необходимых ресурсов, улучшения методов подготовки свидетельств аудита ИБ и т. п.

2.5.3. Этапы проведения внешнего аудита ИБ

Суммируя имеющиеся требования стандартов [5, 6, 9, 10, 20, 25] и лучшие практики в этой области, выделим следующие этапы осуществления работ по проведению внешнего аудита ИБ:

- организация проведения аудита;
- анализ документации;
- подготовка к проведению аудита на месте его проведения;
- проведение аудита на месте;
- подготовка, утверждение и рассылка отчета по аудиту;
- завершение аудита;
- выполнение действий по результатам аудита.

Рассмотрим все эти этапы более подобно.

Организация проведения внешнего аудита ИБ

Организация проведения внешнего аудита ИБ включает в себя следующие действия:

- определение целей, области и критериев аудита;
- согласование и заключение договора на проведение аудита;
- формирование аудиторской группы;
- назначение руководителя аудиторской группы;
- установление начального контакта с проверяемой организацией;
- определение возможности аудита.

Содержание договора на проведение аудита ИБ может иметь особенности, но, как правило, в нем указывается следующие сведения:

- область аудита;
- ответственность руководства проверяемой организации за подготовку и предоставление необходимых свидетельств аудита;
- требования к отчету аудита;
- порядок взаимодействия представителей проверяющей и проверяемой организаций;
- порядок сбора необходимых свидетельств аудита;
- цена проведения аудита;
- порядок привлечения к работе по каким-либо вопросам аудита ИБ других проверяющих организаций и/или технических экспертов;
- необходимые ограничения ответственности проверяющей организации.

В аудиторской организации для проведения внешнего аудита ИБ подбирается аудиторская группа. Руководством аудиторской организации назначается руководитель аудиторской группы, ответственный за проведение аудита ИБ организации. При наличии только одного аудитора он выполняет все предусмотренные обязанности руководителя аудиторской группы.

При определении размера и состава аудиторской группы учитываются следующие факторы:

- цели, область, критерии аудита и его ориентировочная продолжительность;
- общая компетентность и уровень квалификации аудиторской группы;
- необходимость исполнения принципов проведения аудита ИБ;
- законодательные, регламентирующие, контрактные требования и требования органов аккредитации/сертификации, если это применимо;
- способность членов аудиторской группы к совместной работе и к эффективному взаимодействию с проверяемой организацией;
- понимание социальных и культурных особенностей проверяемой организации (это может быть достигнуто либо собственным опытом аудитора, либо с помощью эксперта).

Если в определенной области (по определенному вопросу) знаний аудиторской группы недостаточно, то недостающие знания и умения обычно восполняются включением в группу технических экспертов (как внутренних, так и внешних), работающих под руководством аудитора.

И заказчик, и проверяемая организация имеют право потребовать замены членов аудиторской группы по объективным причинам (член аудиторской группы работал ранее в проверяемой организации или же оказывал ей услуги по консалтингу, предыдущее неэтичное поведение). Причины доводятся до сведения руководителя аудиторской группы и ответственного за управление программой аудита ИБ, которые согласовывают с заказчиком аудита и проверяемой организацией решение по замене членов аудиторской группы.

Для взаимодействия с аудиторской группой руководством проверяемой организации назначаются лица, на которых возлагается ответственность за своевременность, достоверность и полноту предоставления запрошенной аудиторами информации в объеме, не выходящем за пределы их полномочий и условий, определенных договором.

Руководитель аудиторской группы устанавливает неофициальный или официальный первоначальный контакт с проверяемой организацией со следующими целями:

- определение каналов связи с представителями проверяемой организации;
- подтверждение полномочий на проведение аудита;
- предоставление информации по предполагаемым срокам аудита и составу аудиторской группы;
- запрос доступа к необходимым документам проверяемой организации;
- определение применимых правил техники безопасности на месте проведения аудита;
- подготовка мероприятий аудита;
- согласование присутствия со стороны проверяемой организации наблюдателей и необходимости в сопровождающих для аудиторской группы.

В самом начале процесса внешнего аудита ИБ аудиторская организация определяет его осуществимость на основании таких факторов:

- достаточность и соответствие информации для составления плана аудита;
- готовность к сотрудничеству со стороны проверяемой организации;
- наличие времени и соответствующих ресурсов.

Если аудит ИБ неосуществим, то по результатам консультаций с проверяемой организацией заказчику аудита предлагается альтернативный вариант.

Анализ документации

Этап анализа документов проверяемой организации проводится аудиторской группой для определения соответствия положений, отраженных в документации организации, критериям аудита ИБ. Анализ всегда должен учитывать размер, тип и сложность организации, а также цели и область аудита ИБ.

Проверка и анализ документов могут проводиться на всех этапах аудиторской проверки и позволяют аудитору получить свидетельства аудита ИБ, обладающие наибольшей полнотой по сравнению с другими методами получения свидетельств аудита ИБ. Однако эти свидетельства аудита ИБ имеют различную степень достоверности в зависимости от их характера и источника, а также от эффективности внутреннего контроля организации за процессом подготовки и обработки представленных документов.

Документация может содержать следующие сведения:

- информацию, касающуюся организационно-правовой формы и организационной структуры проверяемой организации;
- выдержки или копии необходимых юридических документов, соглашений и протоколов;
- действующие в организации политики;
- информацию о процессах организации;
- информацию о применяемых в организации средствах, в том числе это может быть: аппаратные диаграммы, чертежи и модели; программная документация; спецификации интерфейсов; рабочие инструкции; учебники для тренировки персонала; описание процедур сопровождения; вопросы снятия с эксплуатации;
- отчеты по предыдущим внешним и внутренним аудитам ИБ;
- любая другая документация, в которой отражаются вопросы, регламентируемые положениями действующих стандартов и нормативов в области ИБ.

Например, при внешнем аудите ИБ организации в целом она готовит для проверки следующие документы [24]:

- документы, подтверждающие внедрение в организации выработанной ПолИБ и, в частности, наличие документированного подхода к оценке рисков ИБ и управлению ими в рамках всей организации;
- описание организационной инфраструктуры ИБ на местах – распределение обязанностей сотрудников по ОИБ;
- обоснование выбора средств защиты для рассматриваемой системы;
- документацию на процессы обслуживания и администрирования ИБ;
- документацию с описанием подходов к оценке рисков ИБ и управлению ими;
- документацию по подготовке периодических проверок, касающихся оценки рисков ИБ, и управлению ими;
- описание процедуры принятия уровня остаточного риска ИБ с документированным выводом о реализации необходимых средств защиты, степени их тестирования и корректности работы с ними;
- документацию по СУИБ и реестр средств управления ИБ в ведомости соответствия (англ. *Statement of Applicability*);
- результаты оценки рисков ИБ по всем ИС;
- описание мер для противодействия выявленным рискам ИБ.

Аудиторам, детально оценивающим одну из ИС организации, потребуется следующая документация по этой системе:

- ПолИБ, документация по СУИБ и ведомость соответствия, отражающая реальное состояние оцениваемой системы;
- документация по проведенной оценке рисков ИБ;
- документация по средствам управления ИБ;
- доказательства эффективности принятых контрмер и результаты их тестирования;
- структурная схема ИС;
- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений;
- другая проектная и рабочая документация на ИС;
- схема информационных потоков;
- описание структуры комплекса технических средств ИС;
- описание структуры ПО;
- описание структуры информационного обеспечения;
- размещение компонентов ИС и т. д.

Если документация признана аудиторами неадекватной, то руководитель аудиторской группы сообщает об этом заказчику аудита ИБ и проверяемой организации. Далее аудиторская группа принимает решение, может ли аудит ИБ быть продолжен или приостановлен до момента решения всех вопросов по документации.

Подготовка к проведению внешнего аудита ИБ на месте

Этап подготовки к внешнему аудиту ИБ на месте его проведения включает в себя распределение работ в аудиторской группе и подготовку рабочей документации.

Руководитель аудиторской группы готовит план аудита ИБ, который облегчит составление графика и координацию действий при проведении аудита ИБ. В плане отражается следующее:

- цель аудита;
- критерии аудита;
- область аудита, включая идентификацию организационных и функциональных единиц и процессов, подлежащих проверке;
- дата и место, где должны осуществляться действия по аудиту на месте;
- ожидаемое время и продолжительность действий по аудиту на месте, включая совещания с руководством проверяемой организации и совещания аудиторской группы;
- роли и обязанности членов аудиторской группы и сопровождающих лиц;
- методы аудита (например, возможно применение сетевых технологий, включая телеконференции, интернет-совещания, интерактивную связь на базе интернет-технологий и удаленный электронный доступ к документации СУИБ и/или процессам СУИБ);
- описание деятельности и мероприятий по проведению аудита ИБ на месте;
- распределение ресурсов при проведении аудита,

И при необходимости дополнительно:

- перечень представителей проверяемой организации, которые будут сопровождать аудиторскую группу;
- разделы отчета;
- техническое обеспечение (поездки, оборудование на месте и т. д.);
- рассмотрение вопросов конфиденциальности;
- сроки и цели последующих аудитов ИБ.

План аудита ИБ анализируется аудиторской группой и предоставляется проверяемой организации до начала проведения аудита ИБ на месте.

Любые возражения со стороны проверяемой организации должны быть разрешены совместно руководителем аудиторской группы, проверяемой организацией и заказчиком аудита ИБ. Пересмотренный план аудита ИБ согласуется со всеми вовлеченными сторонами до продолжения аудита.

Консультируясь с аудиторской группой, ее руководитель устанавливает ответственность каждого члена группы за проверку конкретных процессов, функций, площадок, областей или действий. Такие назначения должны учитывать необходимость выполнения принципов аудита ИБ и эффективность использования аудитором ресурсов, а также раз-

личные роли и обязанности аудиторов и экспертов. В процессе аудита ИБ для достижения его цели в распределение обязанностей могут вноситься изменения.

Члены аудиторской группы анализируют информацию, относящуюся к распределению обязанностей при проведении аудита ИБ, и готовят документы, необходимые для регистрации результатов, например:

- контрольные листы и планируемые выборки анализируемой во время аудита ИБ информации;
- формы для регистрации данных, таких как подтверждающие свидетельства, выводы аудита ИБ и протоколы совещаний.

Документы составляются и систематизируются таким образом, чтобы отвечать обстоятельствам каждого конкретного аудита ИБ и потребностям аудитора в ходе ее проведения. Они войдут в состав рабочей документации, которая может быть создана самой аудиторской организацией или получена от проверяемой организации или от других лиц.

Состав, количество и содержание документов, входящих в рабочую документацию аудита ИБ, определяются аудиторской организацией исходя из сложности деятельности проверяемой организации и состояния системы внутреннего аудита и/или мониторинга ИБ. Рабочая документация обычно включает следующие основные документы:

- информацию, касающуюся организационно-правовой формы и организационной структуры проверяемой организации;
- выдержки или копии необходимых юридических документов, соглашений и протоколов;
- план проведения аудита ИБ;
- описания использованных аудиторской организацией процедур и их результатов;
- объяснения, пояснения и заявления проверяемой организации;
- копии переписки с другими аудиторскими организациями, экспертами и прочими лицами в связи с проводимым аудитом ИБ;
- описания системы внутреннего аудита и/или мониторинга ИБ;
- аналитические документы аудиторской организации.

Рабочие документы могут быть собраны в виде данных, записанных на бумаге, электронных носителях, путем микрофильмирования или другими способами.

Рабочие документы, включая записи по результатам их использования, хранятся, по крайней мере, до окончания аудита ИБ. Документы, содержащие конфиденциальную или запатентованную информацию, хранятся в течение всего времени членами аудиторской группы с соблюдением соответствующих требований по ОИБ.

Проведение внешнего аудита ИБ на месте

Этап проведения аудита ИБ на месте включает следующие мероприятия:

- проведение предварительного совещания;
- обмен информацией во время аудита ИБ;
- назначение ролей и обязанностей сопровождающих и наблюдателей;
- сбор свидетельств аудита ИБ;
- оценка свидетельств аудита ИБ;
- проведение заключительного совещания.

Перед началом проведения аудита ИБ на месте проводится вступительное совещание с участием аудиторской группы и лиц, ответственных за функции или процессы, подлежащие проверке. Цели совещания обычно таковы:

- подтверждение плана аудита ИБ;
- краткое изложение действий по аудиту;
- подтверждение каналов обмена информацией между аудиторской группой и представителями проверяемой организации;
- предоставление возможностей проверяемой организации задать вопросы.

Совещание с руководителем аудиторской группы в качестве председателя должно быть официальным, и должен быть составлен список присутствующих.

В зависимости от области и сложности аудита ИБ может возникнуть необходимость в официальных мероприятиях для обеспечения связи между аудиторской группой и проверяемой организацией в процессе проведения аудита.

Аудиторская группа периодически проводит совещания для обмена информацией, оценки хода аудита ИБ и, при необходимости, перераспределения обязанностей между аудиторами, а руководитель группы доводит до сведения проверяемой организации и заказчика аудита информацию о ходе аудита и любых возникающих проблемах. Свидетельства, собранные во время аудита ИБ и выявляющие критические для ИБ проверяемой организации уязвимости, немедленно доводятся до сведения проверяемой организации и, если возможно, заказчика аудита.

Если имеющееся свидетельство аудита ИБ указывает на то, что цель аудита недостижима, то руководитель аудиторской группы сообщает причины этого заказчику аудита и проверяемой организации для определения дальнейших действий. Эти действия могут включать повторное подтверждение или изменение плана аудита ИБ, либо изменение цели или области аудита, либо прекращение аудита.

Любая необходимость изменения области аудита ИБ, которая может стать очевидной по мере выполнения аудита на месте, анализируется и утверждается заказчиком аудита и проверяемой организацией.

Аудиторскую группу могут сопровождать сопровождающие и наблюдатели, но они не являются ее членами и не должны влиять или вмешиваться в проведение аудита ИБ. Если сопровождающие были на-

значены проверяемой организацией, то они должны помогать аудиторской группе и действовать по просьбе руководителя аудиторской группы. В их обязанности может входить следующее:

- установление контактов и времени для опроса;
- организация посещений конкретных мест в организации;
- обеспечение ознакомления и соблюдения членами аудиторской группы правил, касающихся техники безопасности на месте и охранных процедур;
- выступление в качестве свидетеля по поручению проверяемой организации;
- разъяснение или помощь в сборе информации.

В процессе проведения аудита ИБ информация, относящаяся к цели, области и критериям аудита, включая информацию по взаимодействию функций, видов деятельности и процессов, собирается методом соответствующей выборки и должна быть проверяема. Только тогда она может стать свидетельством аудита ИБ, подлежащим обязательной регистрации.

Выделяют следующие виды свидетельств аудита ИБ:

- внутренние – информация, полученная от проверяемой организации в письменном или устном виде,
- внешние – информация, полученная от третьей стороны в письменном виде (обычно по письменному запросу аудиторской организации);
- смешанные – информация, полученная от проверяемой организации в письменном или устном виде и подтвержденная третьей стороной в письменном виде.

К основным источникам свидетельств аудита ИБ относят:

1) документы проверяемой организации и третьих лиц, относящиеся к ОИБ организации;

2) устные высказывания и письменные ответы сотрудников проверяемой организации в процессе проводимых опросов;

3) результаты наблюдений аудиторов за деятельностью организации в области ОИБ.

Качество свидетельств аудита ИБ зависит от их источников. Наиболее ценными считаются свидетельства, полученные аудиторской организацией непосредственно в результате исследования деятельности организации по ОИБ. Наблюдение за деятельностью проверяемых подразделений представляет собой отслеживание аудитором процедур или процессов в проверяемых подразделениях, выполняемых другими лицами (в том числе персоналом организации). Информация считается достоверной только в том случае, если она получена непосредственно в момент выполнения проверяемых процедур или функционирования процессов [20]. Основная часть анализа средств управления ИБ, используемых в рамках СУИБ, состоит из серии испытаний (тестов), проведенных аудиторами или по их просьбе. Во время этих испытаний осу-

ществляется сбор доказательств реализации и функционирования средств управления ИБ для последующего их рассмотрения в сравнении с ожидаемыми результатами, полученными на основе соблюдения определенных требований, стандартов или общепризнанных лучших практик. Например, один из тестов может касаться средств борьбы со злонамеренным ПО посредством проверки, на всех ли компьютерах (или их некоторой выборке) установлено соответствующее антивирусное ПО. Более интересны исследования, в процессе которых доказательства могут быть собраны в электронном виде, например, с помощью SQL-запросов к БД доказательств, полученных от систем или БД управления активами.

Также часто применяется интервьюирование отдельных лиц или групп лиц, которое может проводиться на всех этапах аудиторской проверки [20]. Интервьюированию могут подвергаться следующие категории опрашиваемых: руководство, владельцы активов, сотрудники службы и подразделений ИБ, сотрудники отдела кадров, преподаватели, операторы ИС, сетевые и системные администраторы, администраторы сайтов, сотрудники отдела физической защиты, пользователи, работники проверяемых подразделений. Интервью могут проводиться в отношении репрезентативной выборки лиц или всех причастных сторон. Они бывают разных видов: обобщенные (по самым общим вопросам), сфокусированные на специфической области и подробные.

В качестве примера приведем наиболее часто встречающиеся вопросы опросов при сборе свидетельств аудита ИБ, проводимого для ИС различных организаций. Кто является владельцем информации? Кто является пользователем (потребителем) информации? Кто является провайдером услуг? Какие услуги и каким образом предоставляются конечным пользователям? Какие основные виды приложений функционируют в ИС? Количество и виды пользователей, использующих эти приложения? Из каких компонентов (подсистем) состоит ИС? Функциональность отдельных компонентов? Где проходят границы системы? Какие точки входа имеются? Как ИС взаимодействует с другими системами? Какие каналы связи используются для взаимодействия с другими ИС? Какие каналы связи используются для взаимодействия между компонентами системы? По каким протоколам осуществляется взаимодействие? Какие программно-технические платформы используются при построении системы?

Результаты устных опросов оформляются в виде протокола или краткого конспекта, в котором обязательно указаны фамилия, имя, отчество сотрудника аудиторской группы, проводившего опрос, фамилия, имя, отчество опрашиваемого лица, а также представлены их подписи. Для проведения типовых опросов готовятся бланки с перечнями интересующих вопросов. Письменная информация по итогам устных опросов приобщается аудиторской группой к другим рабочим документам ауди-

торской проверки. Однако результаты устного опроса следует проверять, так как опрашиваемый может выражать свое субъективное мнение. Хорошей практикой является проведение перекрестных опросов сотрудников организации (то есть опрос различных лиц).

Сбор информации на этапе аудита ИБ на месте осуществляется и на основе анализа предоставленных на месте документов.

Для примера конкретизируем, что в первую очередь включает в себя внешний аудит ИБ интранета, являющийся комбинацией документального и технического аудита ИБ в определенном выше понимании [15]:

- анализ архитектуры интранета, анализ используемых ОС, сетевых протоколов и служб, специализированных подсистем и приложений, СЗИ и т. п.;
- анализ ядра автоматизированных бизнес-процессов (задач, решаемых с использованием интранета);
- анализ и выделение существующих уровней секретности информации;
- выделение основных объектов хранения информации;
- определение существующих механизмов доступа к объектам хранения информации;
- составление схемы информационных потоков с точки зрения категорий секретности информации и топологии интранета;
- выявление наиболее опасных внутренних и внешних угроз ИБ для данного объекта и анализ возможностей их успешной реализации;
- проведение тестов на проникновение (англ. *Penetration Testing*), в результате которых осуществляется поиск и использование обнаруженных уязвимостей с применением различных моделей нарушителей ИБ как изнутри, так и снаружи по отношению в информационной среде организации;
- оценку текущего уровня защищенности интранета в соответствии с необходимыми применимыми требованиями по ОИБ и, при необходимости, обоснование его повышения.

Аудиторы должны проявлять достаточную степень профессионального скептицизма в отношении собираемых свидетельств аудита ИБ, принимая во внимание возможность наличия различного вида нарушений при ОИБ в проверяемых подразделениях организации.

По степени достоверности (от наибольшей к наименьшей) свидетельства аудита ИБ делятся следующим образом:

1) от третьей стороны в письменном виде;

2) от проверяемой организации и подтвержденные третьей стороной в письменном виде;

3) полученные в ходе проведения аудиторских процедур (наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т. д.);

4) в форме документов;

5) в устной форме.

Определение достаточности свидетельств аудита ИБ зависит от следующего:

- степени аудиторского риска, то есть вероятности принятия неверного решения аудиторской организацией;
- наличия свидетельства от независимого источника (третьих лиц) как более достоверного, чем полученное непосредственно от сотрудников проверяемой организации;
- получения свидетельства аудита на основе данных системы внутреннего аудита и/или мониторинга ИБ, достоверность которых определяется состоянием самой этой системы;
- получения информации в результате самостоятельного анализа или проверки аудиторской организацией как более достоверной, чем сведения, полученные от других лиц;
- получения свидетельств аудита в форме документов и письменных показаний как более достоверных, чем показания в устной форме;
- возможности сопоставления выводов, сделанных в результате использования свидетельств, полученных из различных источников.

Собранные свидетельства аудита ИБ оцениваются с точки зрения критериев аудита для формирования выводов аудита ИБ. Их оценка проводится на основе постоянного и непрерывного накопления и обобщения федеральным органом исполнительной власти, ответственным в пределах своих полномочий за нормативно-методологическое обеспечение деятельности в области аудита ИБ, соответствующего мирового опыта, а также лучших практик отечественных организаций, аккредитованных на право осуществления деятельности по аудиту ИБ.

Выводы аудита ИБ могут указывать на соответствие или несоответствие критериям аудита ИБ. Выводы аудита ИБ о несоответствии критериям аудита ИБ и подтверждающие их свидетельства аудита ИБ рассматриваются и анализируются аудиторами совместно с представителем проверяемой организации для получения подтверждения того, что свидетельства аудита ИБ верны и несоответствия понятны. Нерешенные вопросы обязательно документально фиксируются.

До заключительного совещания аудиторская группа проводит совещание со следующими целями:

- проанализировать выводы аудита ИБ и любую другую соответствующую информацию, собранную в процессе аудита, с точки зрения целей аудита;
- согласовать заключения по результатам аудита ИБ, с учетом элемента неопределенности, свойственного процессу аудита ИБ;
- подготовить рекомендации для проверяемой организации по результатам проведенного аудита ИБ;
- обсудить последующий аудит ИБ, если это было включено в план аудита ИБ.

Правильно подготовленное заключение по результатам аудита ИБ охватывает следующие вопросы:

- степень соответствия проверяемой организации критериям аудита ИБ;
- оценка системы внутреннего аудита и/или мониторинга ИБ проверяемой организации;
- способность со стороны руководства обеспечить постоянную пригодность, адекватность, результативность этой системы и ее совершенствование.

Аудиторской группой может быть подготовлено четыре типа заключений:

- безусловно положительное;
- условно положительное;
- отрицательное;
- отказ от выражения заключения.

В случае если по результатам аудита ИБ сформировано аудиторское заключение, отличное от безусловно положительного, обязательно излагаются причины, приведшие к составлению данного заключения.

Отказ от выражения заключения возможен в случаях, когда ограничение области аудита было настолько существенно и глубоко, что аудитор не мог получить достаточные доказательства и, следовательно, был не в состоянии провести оценку показателей, отражающих соответствие ИБ организации критериям аудита ИБ.

Заведомо ложное аудиторское заключение признается таковым только по решению суда.

По окончании аудита ИБ проводится заключительное совещание под председательством руководителя аудиторской группы. При проведении аудита ИБ в малой организации заключительное совещание может состоять только из доведения до сведения выводов аудита и заключения по результатам аудита. В других случаях совещание должно быть официальным с ведением протокола и списка присутствующих.

На совещании выводы аудита ИБ и заключения по результатам аудита представляются таким образом, чтобы они были понятны и признаны проверяемой организацией. Участниками заключительного совещания должны быть представители проверяемой организации, а также могут быть заказчик аудита и другие стороны. В случае возникновения в процессе аудита ситуаций, которые могут отразиться на надежности заключений по результатам аудита, руководитель аудиторской группы сообщает об этом проверяемой организации.

Любые разногласия в отношении выводов аудита и/или заключений по результатам аудита ИБ между аудиторской группой и проверяемой организацией должны быть обсуждены и, если возможно, разрешены. В противном случае все мнения обязательно документально фиксируются.

На совещании также представляются рекомендации по улучшению состояния ИБ проверяемой организации.

Подготовка, утверждение и рассылка отчета по внешнему аудиту ИБ

По завершении проверки аудиторская группа предоставляет установленным получателям отчет по результатам проведения аудита ИБ, ответственность за подготовку и содержание которого несет руководитель аудиторской группы.

Отчет должен предоставлять полные, точные, четкие и достаточные записи по аудиту ИБ и должен включать в себя:

- сведения об аудиторской организации;
- сведения о руководителе и членах аудиторской группы;
- сведения о проверяемой организации;
- сведения о заказчике аудита ИБ;
- продолжительность и место проведения аудита ИБ;
- цель аудита ИБ;
- область аудита ИБ, в частности идентификацию проверенных организационных и функциональных единиц или процессов и охваченный период времени;
- критерии и выводы аудита ИБ;
- степень доверия к внутренним аудитам ИБ;
- заключения по результатам аудита ИБ;
- выводы по результатам аудита ИБ и рекомендации по улучшению ИБ организации;
- документально оформленную совокупность анкет, содержащих критерии и выводы аудита ИБ, сделанные по каждому из рассмотренных критериев аудита ИБ;
- лист рассылки отчета по результатам аудита ИБ.

Также отчет может содержать:

- план аудита ИБ на месте;
- перечень представителей со стороны проверяемой организации, которые сопровождали и опрашивались аудиторской группой при проведении аудита;
- краткое изложение процесса аудита ИБ, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам аудита;
- подтверждение, что цель аудита ИБ достигнута в области аудита в соответствии с планом аудита;
- любые неохваченные области, входящие в область аудита ИБ;
- любые неразрешенные разногласия между аудиторской группой и проверяемой организацией;
- при необходимости, согласованные планы последующих аудитов;

- заполненные опросные листы, перечни контрольных вопросов, результаты наблюдений, журналы регистрации, замечания аудиторов и т. п.;
- заявление о конфиденциальном характере содержания отчета.

Отчет по результатам аудита ИБ выпускается в согласованные сроки. Если это невозможно, то причины задержки доводятся до сведения заказчика аудита ИБ, и тогда согласуется новая дата выпуска отчета.

Утвержденный отчет подлежит рассылке получателям, определенным заказчиком аудита ИБ.

Отчет по результатам проведения аудита ИБ является собственностью заказчика аудита. Члены аудиторской группы и все получатели отчета должны учитывать и обеспечивать конфиденциальность содержания отчета.

Завершение внешнего аудита ИБ

Внешний аудит ИБ считается завершенным, если все процедуры, предусмотренные планом аудита ИБ, выполнены, и утвержденный отчет разослан установленным получателям.

Документы, имеющие отношение к внешнему аудиту ИБ, хранят или уничтожают на основании соглашения между участвующими сторонами в соответствии с процедурами программы аудита, соглашением между сторонами, действующим законодательством, нормативными требованиями и договорными обязательствами.

Если это не предусмотрено законом, аудиторская группа и ответственные за управление программой аудита ИБ не должны раскрывать содержимого документов и другой информации, полученной во время аудита, или отчетов по аудиту любой другой стороне без ясного разрешения заказчика аудита и, где это требуется, разрешения проверяемой организации. Если необходимо раскрыть содержание документов аудита, заказчик аудита и проверяемая организация информируются об этом как можно скорее.

Выполнение действий по результатам внешнего аудита ИБ

В заключении по результатам внешнего аудита ИБ может быть указано на необходимость корректирующих, предупреждающих действий или действий по улучшению. Такие действия обычно разрабатываются и проводятся проверяемой организацией в течение согласованного срока и не рассматриваются как часть аудита. Проверяемая организация информирует заказчика аудита о статусе таких действий.

Выполнение и результативность корректирующего действия также проверяются. Данная проверка может быть частью очередного внешнего или внутреннего аудита ИБ.

Программа внешнего аудита ИБ может предусматривать выполнение определенных действий после аудита членами аудиторской группы, что добавит ценности аудиту, учитывая опыт аудиторов. В таких случаях

следует позаботиться об обеспечении независимости при проведении последующих аудитов.

2.5.4. Компетентность аудиторов ИБ

Доверие к аудиту ИБ зависит от компетентности аудиторов в вопросах ИБ [5, 6, 9, 10, 25]. Во время аудита аудиторы ИБ должны продемонстрировать следующее:

- личные качества (порядочность, открытость, тактичность, наблюдательность, проницательность в оценке ситуации, готовность к различным ситуациям, упорство в достижении цели, решительность в своевременном принятии решений, самостоятельность);
- способность применить знания и навыки по принципам, процедурам и методам аудита ИБ, всем вопросам управления ИБ и СУИБ и ссылочным документам, организационным моментам, применяемым законам, техническим регламентам и другим требованиям по ОИБ;
- образование, опыт работы, подтверждение обучения на аудитора ИБ и опыт проведения аудита ИБ.

Оценка аудиторов ИБ и руководителей аудиторских групп планируется, реализуется и отражается в протоколах в соответствии с процедурами программы аудита ИБ с целью обеспечения объективных, последовательных, достоверных и надежных результатов. Процесс оценки выявляет потребности в обучении и приобретении аудиторами ИБ других необходимых навыков.

Оценка аудиторов ИБ происходит на следующих этапах:

- начальное оценивание лиц, желающих стать аудиторами ИБ;
- оценивание аудиторов во время процесса формирования аудиторской группы;
- постоянное оценивание характеристик аудитора ИБ с целью идентификации потребностей, необходимых для поддержания и улучшения его знаний и навыков.

Процесс оценки включает четыре основных этапа:

1) идентификация личных качеств, знаний и навыков для соответствия потребностям программы аудита ИБ с учетом размера, вида деятельности и сложности проверяемой организации, целей и объема программы аудита, требований сертификации/регистрации и аккредитации, роли процесса аудита ИБ для руководства проверяемой организации, уровень конфиденциальности, требуемый в программе аудита ИБ, сложность проверяемой СУИБ;

2) определение критериев оценки: количественных (опыт работы в годах, образование, количество проведенных аудитов, количество часов обучения аудиту) или качественных (демонстрируемые личные качества, знания или характеристики навыков при обучении или при нахождении на рабочем месте);

3) выбор соответствующего метода оценки;
4) проведение оценки.

Собранную информацию о персонале сравнивают с критериями. Если персонал не соответствует критериям, указывают на необходимость дополнительного обучения, опыта работы и/или участия в аудите ИБ, после чего проводят повторную оценку.

Требования, предъявляемые к уровню квалификации аудиторской группы, обычно следующие:

- наличие базового образования – высшего технического по специальностям, связанным с ИБ, системами ИТ, вычислительной техникой или по другим специальностям, которые могут иметь отношение к рассматриваемой области. Образование должно быть получено в учебном учреждении РФ, имеющем государственную аккредитацию, или иностранного государства, дипломы которого имеют юридическую силу в РФ;
- наличие практического опыта, который определяется стажем работы в режиме полной занятости в области ИТ не менее четырех лет и из них в области ИБ не менее двух лет из последних пяти лет в качестве руководителя, аудитора или специалиста аудиторской организации, оказывающей аудиторские услуги в области ИБ; руководителя или сотрудника службы/подразделения организации, отвечающей за обеспечение ее ИБ; научного работника или преподавателя по профилю, связанному с ИБ;
- наличие опыта, касающегося всего процесса оценки ИБ и приобретенного посредством участия, как минимум, в четырех аудитах общей продолжительностью, по крайней мере, 20 дней, включая проверку документации и анализ рисков ИБ, оценку реализации и составления отчета о результатах аудита ИБ;
- наличие специального профессионального образования, включающего обучение не менее пяти дней в учебно-методических центрах и организациях по обучению и переподготовке аудиторов и стажировку в аудиторской организации; программа этого обучения должна включать вопросы аудита ИБ и управления им;
- поддержание знаний и навыков в области ИБ и аудита соответственно современным требованиям путем постоянного повышения профессионального уровня;
- знание законов, зарубежных и отечественных стандартов, инструкций и других нормативных актов, вносимых в них дополнений и изменений, относящихся к области ИБ в целом и СУИБ и управлению рисками ИБ в частности;
- свободное владение деловым русским языком в объеме, необходимом для изучения нормативных актов, проверки документации, ведения рабочей документации, делового общения с клиентами и со-

ставления аудиторского заключения и отчета по результатам проведения аудита ИБ.

Аудиторы СУИБ должны знать и понимать следующие процессы проведения аудита и объекты СУИБ:

- программирование и планирование аудита СУИБ;
- тип и методология аудита СУИБ;
- аудиторский риск;
- знание законодательных и нормативных требований в отдельной области ИБ;
- анализ процессов ИБ;
- цикл PDCA для постоянного совершенствования СУИБ;
- принципы, методы и процессы управления, применимые в СУИБ;
- средства управления СУИБ и их реализация;
- анализ эффективности и результативности СУИБ и средств управления;
- политики и процедур ИБ;
- материальные и нематериальные информационные активы;
- бизнес-процессы;
- интеллектуальная собственность;
- идентификация угроз ИБ;
- идентификация уязвимостей и понимание вероятности их использования, влияния, уменьшения и контроля;
- риски ИБ; методы управления рисками ИБ; обработка рисков ИБ;
- перехват в телекоммуникациях и мониторинг данных (например, электронная почта);
- злоупотребление компьютером, сбор электронных данных;
- обработка инцидентов ИБ;
- анализ влияния на бизнес;
- обеспечение непрерывности бизнеса (ОНБ);
- инспекция рабочих мест;
- защита данных и конфиденциальность;
- средства криптографической защиты информации (СКЗИ);
- электронная цифровая подпись (ЭЦП);
- МЭ и виртуальные частные сети (ВЧС);
- тесты на проникновение и т. д.

Также аудиторы ИБ должны обладать знаниями и умениями в следующих областях:

1. Принципы, процедуры и методы аудита, позволяющие выбирать такие способы работы, которые соответствуют различным аудитам и обеспечивают последовательное и систематичное проведение аудитов. Аудитор должен уметь:

- применять принципы, процедуры и методы аудита;
- результативно планировать и организовывать работу;
- проводить аудит в согласованные сроки;

- расставлять приоритеты и концентрироваться на важных вопросах;
- собирать информацию путем результативных опросов, наблюдений и анализа документов, включая записи и данные;
- понимать применимость и последствия использования метода выборки для аудита;
- проверять точность собранной информации;
- подтверждать достаточность и соответствие свидетельств аудита для обоснования наблюдений и заключений по результатам аудита;
- оценивать факторы, которые могут повлиять на надежность наблюдений и заключений по результатам аудита;
- использовать рабочие документы для регистрации действий по аудиту;
- подготавливать отчеты по аудиту;
- обеспечивать конфиденциальность и безопасность информации;
- результативно общаться самостоятельно, используя знание языка или через переводчика.

2. Система управления и справочные документы, позволяющие аудитору понять объем аудита и применить критерии аудита. Знания и умения в этой области:

- применение систем управления для различных организаций;
- взаимодействие между составными элементами системы управления;
- стандарты, применимые процедуры или другие документы системы управления, используемые как критерии аудита;
- понимание различия между справочными документами и приоритетности тех или иных документов;
- применение справочных документов к различным ситуациям в процессе аудита;
- информационные системы и технологии утверждения, рассылки и управления документами, данными и записями.

3. Организационные аспекты, позволяющие аудитору понимать производственную ситуацию: размер, структура, функции и взаимоотношения в организации; общие бизнес-процессы и относящаяся к ним терминология.

4. Соответствующие законы, правила и другие документы, позволяющие аудитору работать с учетом и пониманием требований, которые применимы к проверяемой организации. Знания и умения в этой области должны охватывать:

- местные, региональные и национальные кодексы, законы и правила;
- контракты и соглашения;
- международные договоры и конвенции;
- другие требования, с которыми согласилась организация.

Также можно выделить профессиональные умения аудитора ИБ:

- тщательно готовиться перед началом каждого этапа аудита ИБ;

- проводить начальное и заключительное совещание (особенно важно для главного аудитора);
- собирать информацию без проявления агрессивности или запугивания (хороший аудитор заставляет проверяемых вести себя непринужденно);
- осуществлять сбор объективных данных с минимальной суетой, используя визуальные наблюдения, анализ выбранной документации и интервью;
- проводить опрос самых различных по уровню и рангу сотрудников организации;
- подтверждать свои выводы конкретными свидетельствами и документами;
- указывать (устно) при первой возможности проверяемым на выявленный отказ процесса системы управления, идентифицируя соответствующие обстоятельства, включая вовлеченных лиц, но не делая утверждения о виновности людей;
- определять статус несоответствия с обоснованием своих утверждений перед руководством проверяемого подразделения;
- осуществлять подготовку изложенных понятно, объективно и непредвзято письменных отчетов о несоответствии, которые могут быть поняты даже человеком, не участвовавшим в проверке, через длительный период времени после его написания;
- добиваться согласия и конструктивного отношения к обнаруженным несоответствиям, а также планирования реалистичных корректирующих действий и разработки графиков их осуществления (на бланке регистрации несоответствий представитель проверяемого подразделения расписывается в том, что он ознакомлен и согласен с выявленным несоответствием; после этого на следующей части бланка представитель подразделения формулирует (составляет план) и указывает срок выполнения корректирующих действий, а аудитор своей подписью подтверждает, что план достаточен для устранения обнаруженных несоответствий);
- записывать все ключевые факты, имеющие отношение к проверке, в окончательном отчете (вместе с бланками регистрации несоответствий);
- пользоваться правами аудитора, данными ему по статусу, при решении спорных вопросов, когда не удается достичь единого мнения с проверяемыми.

Кроме перечисленных требований к уровню квалификации и профессиональным умениям, каждый аттестованный аудитор должен ежегодно проходить курс повышения квалификации и систематически самостоятельно повышать свою квалификацию путем:

- изучения законов, стандартов, инструкций и других нормативных актов, вносимых в них дополнений и изменений;

- изучения зарубежного и отечественного опыта по организации и методике проведения аудита ИБ;
- участия в семинарах, конференциях, симпозиумах;
- разработки пособий, монографий по вопросам теории и практики аудита ИБ;
- участия в работе над правилами (стандартами), методиками, программами учебных курсов по аудиту ИБ.

Требования к руководителям аудиторских групп еще более расширены, например за счет обладания ими знаниями и качествами, необходимыми для управления процессом аудита, опыта участия, по крайней мере, в трех полных аудитах СУИБ и умения эффективно общаться в письменной и устной формах.

2.5.5. Взаимоотношения представителей аудиторской группы и проверяемых организаций

Целью общения представителей аудиторской организации (аудиторов) с представителями проверяемого подразделения является оптимизация аудиторских процедур и обеспечение достижения целей аудита ИБ с максимально возможной эффективностью. В процессе такого общения на всех этапах проведения аудита ИБ они должны демонстрировать честность, открытость, желание обсуждать и по возможности разрешать возникшие разногласия [5, 6, 20, 23].

Хорошими практиками являются направления следующих документов:

1) официального предложения со стороны проверяемой организации или заказчика аудита, например государственного надзорного органа, аудиторской организации о заключении договора на проведение аудита ИБ;

2) письма от аудиторской организации о проведении аудита ИБ руководству проверяемой организации до заключения договора на проведение аудита ИБ с целью согласования условий предстоящего договора.

Аудиторское задание на проведение аудита ИБ оформляется договором в соответствии с требованиями законодательства РФ. В нем фиксируются критерии аудита ИБ, по которым должно быть выражено мнение аудиторской организации.

Аудиторская организация информирует проверяемую организацию обо всех мероприятиях, проводимых в рамках аудиторской проверки.

В процессе проведения аудита ИБ руководитель аудиторской группы периодически доводит до сведения проверяемой организации и заказчика аудита информацию о ходе аудита ИБ и любых возникающих проблемах. Свидетельства, собранные при проведении аудита ИБ, которые выявляют критические для ИБ проверяемой организации уязвимости (по мнению руководителя аудиторской группы), немедленно доводятся до сведения проверяемой организации и, если необходимо, до сведения заказчика аудита ИБ.

Если имеющееся свидетельство аудита ИБ (или его отсутствие) указывает на то, что цель аудита ИБ недостижима, то для определения дальнейших действий руководитель аудиторской группы сообщает причины заказчику аудита ИБ и проверяемой организации. Эти действия касаются изменения цели или областей аудита ИБ или прекращения аудита ИБ.

При подготовке к проведению аудита ИБ и в процессе его проведения аудиторская группа вправе самостоятельно принимать решение об источниках, методах получения и достоверности свидетельств аудита ИБ, необходимых для составления заключения по результатам аудита ИБ, если иное не оговорено в договоре на проведение аудита ИБ.

Аудиторская организация несет ответственность за достоверность заключения по результатам аудита ИБ и соблюдение конфиденциальности сведений и документов, получаемых и составляемых в ходе аудиторской проверки (за исключением случаев, прямо предусмотренных действующим законодательством РФ). При необходимости требования по использованию документов проверяемой организации и отчета по аудиту ИБ определяются договором на проведение аудита ИБ.

Аудиторская организация должна гарантировать знание ею технологических и правовых вопросов, относящихся к СУИБ организации, которую она оценивает. Она должна обладать эффективной системой для анализа компетентности в сфере управления ИБ, применимой по отношению ко всем техническим областям, в которых оно действует. В состав аудиторской организации должны входить специалисты, обладающие достаточной компетентностью для управления программой внешнего аудита ИБ, а в аудиторской группе, проводящей конкретный аудит, должно быть достаточное число аудиторов, включая руководителей групп и технических специалистов, для выполнения всего объема работ.

Аудитор в группе при выполнении аудита отвечает:

- за выполнение требований аудита и проведение аудита в соответствии с процедурами и согласованным планом аудита;
- проведение аудита в определенной области, не выходя за пределы поставленных задач;
- сообщение и пояснение требований аудита проверяемой стороне, оказание помощи в понимании требований документации, содержащей указание на критерии аудита;
- эффективное планирование и выполнение возложенных обязанностей;
- сбор и анализ свидетельств аудита, необходимых для сопоставления с критериями аудита;
- регистрацию данных наблюдений в ходе аудита;
- внимание ко всем ситуациям, в которых оценка соответствия требует детального изучения;
- устный и письменный отчет о наблюдениях, выполненных в ходе аудита;

- проверку эффективности корректирующих действий, выполненных по результатам аудита, по требованию клиента;
- сотрудничество с руководителем аудиторской группы и его поддержку;
- сохранение и систематизацию документации, относящейся к аудиту;
- сохранение конфиденциальности;
- этичное поведение.

Проверяемая организация обеспечивает предоставление аудиторской организации всей необходимой для проведения аудита ИБ информации.

Руководство проверяемой организации несет ответственность за достоверность и полноту предоставляемой аудиторской организации информации, а также любые ограничения возможности осуществления аудиторской организацией своих обязательств.

Факты невыполнения аудиторской организацией вышеперечисленных требований сообщаются в органы, контролирующие их деятельность, и заказчику аудита ИБ.

Факты невыполнения требований руководством проверяемой организации указываются в отчете об аудите ИБ и могут служить основанием для прекращения процесса аудита ИБ.

2.6. Анализ СУИБ со стороны высшего руководства организации

В соответствии со стандартами [1, 2, 14] руководство по утвержденному графику периодически, но не менее одного раза в год, проводит анализ СУИБ организации в целях обеспечения ее полной пригодности, адекватности, эффективности и результативности. Результаты анализа содержат предложения по изменению СУИБ и оценку их реализации в интересах обеспечения выполнения требований политики и целей ОИБ. Результаты таких проверок фиксируются документально, а записи сохраняются в течение установленного времени.

Входные данные для анализа СУИБ со стороны руководства включают в себя следующее:

- результаты предыдущих аудитов и анализа СУИБ;
- результаты взаимодействия с заинтересованными сторонами;
- методы, средства или процедуры, которые могут быть использованы в организации совершенствования функционирования и повышения результативности и эффективности СУИБ;
- правовое обоснование предупреждающих и корректирующих действий;
- уязвимости или угрозы ИБ, которые не были адекватно учтены в процессе предыдущей оценки рисков ИБ;
- результаты количественной оценки эффективности и результативности СУИБ;

- последующие действия, вытекающие из предыдущего анализа со стороны руководства;
- любые изменения, которые могли бы повлиять на СУИБ;
- рекомендации по улучшению СУИБ.

В организации утверждается перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СУИБ. В частности, в указанный перечень документов входят:

- отчеты с результатами мониторинга ИБ и контроля защитных мер;
- отчеты с результатами анализа функционирования СУИБ;
- отчеты с результатами аудитов ИБ;
- отчеты с результатами самооценок ИБ;
- документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СУИБ;
- документы, содержащие информацию о новых выявленных уязвимостях и угрозах ИБ;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СУИБ, осуществленных руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СУИБ, например изменения в законодательстве РФ;
- документы, содержащие информацию по выявленным инцидентам ИБ;
- документы, подтверждающие выполнение требуемой деятельности по управлению и обеспечению ИБ, например выполнение планов обработки рисков ИБ;
- документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

В свою очередь, анализ функционирования СУИБ основан на следующем:

- результаты мониторинга ИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов и самооценок ИБ;
- данные об угрозах ИБ, возможных нарушителях ИБ и уязвимостях;
- данные об изменениях внутри организации, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации;
- данные об изменениях вне организации, например, данные об изменениях в законодательстве РФ и в договорных обязательствах организации.

Анализ функционирования СУИБ включает в себя следующие мероприятия:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по управлению ИБ в организации, требованиям законодательства РФ, требованиям стандартов, договорным обязательствам организации;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по управлению ИБ, требованиям ПолИБ организации;
- оценку адекватности модели угроз организации существующим угрозам ИБ;
- оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска ИБ;
- проверку адекватности используемых защитных мер требованиям внутренних документов организации и результатам оценки рисков ИБ;
- анализ отсутствия разрывов в технологических процессах ОИБ, а также несогласованности в использовании защитных мер.

В организации определяется и утверждается руководством план выполнения деятельности по контролю и анализу СУИБ. В частности, указанный план содержит положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации.

Также документально определяются роли, связанные с подготовкой информации, необходимой для анализа СУИБ руководством, и назначаются ответственные за выполнение указанных ролей.

Выходные данные анализа СУИБ со стороны руководства включают в себя все решения и действия, направленные на следующее:

- повышение эффективности и результативности СУИБ;
- обновление планов оценки и обработки рисков ИБ;
- модификацию процедур и средств управления ИБ с целью обеспечить реагирование на внутренние или внешние события, которые могут оказать воздействие на СУИБ, включая изменения бизнес-требований, влияющих на существующие бизнес-процессы требований по ОИБ, требований законов и нормативных документов, договорных обязательств, уровней риска и/или критериев принятия рисков ИБ;
- потребности в ресурсах;
- совершенствование способов оценки функционирования средств управления ИБ.

В целом по результатам анализа СУИБ со стороны руководства необходимо реализовать тактические или стратегические улучшения СУИБ [14].

К *тактическим улучшениям СУИБ* отнесем корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СУИБ организации и не требующие пересмотра корпоративной и частных ПолИБ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа «планирование» СУИБ. Примеры решений по тактическим улучшениям СУИБ:

- пересмотр процедур выполнения отдельных видов деятельности по управлению ИБ;
- пересмотр процедур эксплуатации отдельных видов защитных мер;
- пересмотр процедур обнаружения и обработки инцидентов ИБ;
- уточнение описи информационных активов;
- пересмотр программы обучения и повышения осведомленности персонала;
- пересмотр планов ОНБ;
- пересмотр планов обработки рисков ИБ;
- вынесение санкций в отношении персонала;
- пересмотр процедур мониторинга ИБ и контроля защитных мер;
- пересмотр программ аудитов ИБ;
- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по управлению ИБ и эксплуатации защитных мер;
- ввод новых или замена используемых защитных мер.

К *стратегическим улучшениям СУИБ* отнесем корректирующие или превентивные действия, связанные с пересмотром корпоративной и частных ПолИБ организации, с последующим выполнением соответствующих тактических улучшений СУИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа «планирование» СУИБ. Примеры решений по стратегическим улучшениям СУИБ:

- уточнение/пересмотр целей и задач управления ИБ организации;
- изменение области действия СУИБ;
- уточнение описи типов информационных активов;
- пересмотр моделей угроз и нарушителей ИБ;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

2.7. Инструментальные средства проверки ИБ

Инструментальные средства проверки ИБ обеспечивают сбор и хранение большого количества информации и гибкую фильтрацию данных, их анализ, сопоставление и соответствующие возможности визуализации результатов. Их применение позволяет эффективно реагировать на выявленные события и инциденты ИБ, разрабатывать и проверять выполнение плана мероприятий по текущему состоянию ИБ в организации.

Согласно стандарту ISO/IEC 27008:2011 [8] в ходе внешней и внутренней проверки СУИБ могут использовать три основных метода: обследование, интервью и испытания (тесты). Обследование в меньшей степени, а тестирование в большей базируются на применении признанных для этих целей инструментальных средств. При использовании таких средств аудиторы должны продемонстрировать (предоставить доказательства) генерации ими достоверных результатов [11, 12].

Кроме этого, для максимизации эффективности и минимизации влияния на ИБ и на нормальное функционирование исследуемых систем в процессе тестирования необходимо предусматривать защитные меры для операционной среды и используемых инструментальных средств. Защита также требуется для поддержания целостности исследуемых систем и предотвращения неправильного использования инструментальных средств.

С целью предотвратить любое возможное неправильное использование или компрометацию доступ к инструментальным средствам проверки ИБ, то есть ПО или файлам данных, необходимо защищать. Такие инструментальные средства обязательно отделяют от систем разработки и систем операционной среды, а также не хранят эти средства в библиотеках магнитных лент или пользовательских областях, если не обеспечен соответствующий уровень дополнительной защиты.

Основными объектами тестирования с помощью инструментальных средств проверки ИБ являются механизмы (АО, ПО, прошивки и т. д.) и процессы (весь жизненный цикл систем, сервисов и т. п.). При этом тестированию подлежат:

- механизмы контроля доступа, идентификации, аутентификации и анализа;
- управление привилегированным доступом пользователей;
- механизмы авторизации;
- конфигурационные настройки безопасности;
- ключевые компоненты ИС;
- функции резервирования ИС;
- возможности СЗИ и СОВ по обнаружению вторжений, оповещению и ответному реагированию на них;
- средства и алгоритмы шифрования и хеширования;
- возможности реагирования на инциденты ИБ;
- возможности планов ОНБ и учений по ним;
- устройства систем контроля и управления доступом (СКУД);
- эшелонированность защитных мер.

В стандарте ISO/IEC 27008:2011 [8] рассматривается шесть методов тестирования ИБ в информационной среде организации, для чего применяются соответствующие инструментальные средства (рис. 2.5):

Тестирование «вслепую» (англ. *Blind Testing*) – проверяющий исследует объект без каких-либо предварительных знаний о его характери-

стиках, помимо общедоступной информации. Объект подготовлен к исследованию при заранее известных деталях этого исследования. Такое исследование в первую очередь проверяет навыки проверяющего. Широта и глубина тестирования соответствуют только знаниям проверяющего и разрешенному использованию объекта. Таким образом, это исследование имеет ограниченное применение при оценке защищенности и его следует избегать. Метод также называют *этическим взломом/хакингом* (англ. *Ethical Hacking*).

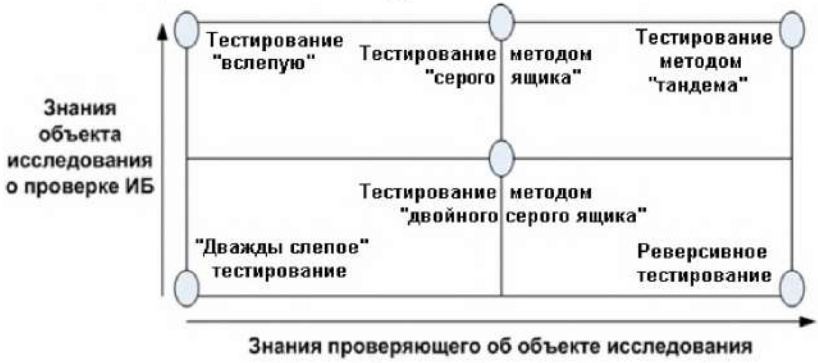

Рис. 2.5. Методы тестирования ИБ

«Дважды слепое» тестирование (англ. *Double Blind Testing*) – проверяющий исследует объект без каких-либо предварительных знаний о его характеристиках, помимо общедоступной информации. Объект не уведомлен заранее об области или направлении исследования. Метод тестирует готовность объекта к неизвестным видам воздействий.

Тестирование методом «серого ящика» (англ. *Gray Box Testing*) – проверяющий исследует объект с ограниченными знаниями о его защите и активах и полным знанием направлений допустимого исследования. Объект подготовлен к исследованию при заранее известных деталях этого исследования. Метод тестирует навыки проверяющего. Характер теста – разрешенное использование. Широта и глубина зависят от качества информации, предоставляемой проверяющему перед тестом, а также от его знаний. Таким образом, это исследование имеет ограниченное применение при оценке защищенности и его следует избегать. Метод также называют *тестированием уязвимостей* (англ. *Vulnerability Test*), которое чаще всего инициировано объектом как самооценка деятельности.

Тестирование методом «двойного серого ящика» (англ. *Double Gray Box Testing*) – проверяющий исследует объект с ограниченными знаниями о его защите и активах и полным знанием направлений допустимого исследования. Объект уведомлен заранее об области и времени, но не направлении исследования. Метод тестирует готовность объекта

к неизвестным видам воздействий. Широта и глубина зависит от качества информации, предоставляемой проверяющему перед тестом, а также от его знаний. Это исследование также называют *тестирование методом «белого ящика»* (англ. *White Box Testing*).

Тестирование методом «тандема» (англ. *Tandem Testing*) – проверяющий и объект готовы к исследованию, заранее зная все детали исследования. Этим методом тестируют защиту и средства управления объекта. Однако он не может протестировать готовность объекта к неизвестным видам воздействий. Характер теста – тщательность/доскональность, поскольку аудитор знает все тесты и реакцию на них. Широта и глубина зависят от качества информации, предоставляемой проверяющему перед тестом, а также от его знаний. Метод известен как внутреннее исследование (англ. *In-House Review*), а аудитор часто сам играет активную роль в процессе обеспечения ИБ.

Реверсивное тестирование (англ. *Reversal Testing*) – проверяющей исследует объект, зная все его процессы и защиту, но сам объект не знает ничего о том, что, как или когда проверяющий будет тестировать. Характер теста – исследование готовности объекта к неизвестным видам и направлениям воздействий. Широта и глубина зависят от качества информации, предоставляемой проверяющему перед тестом, а также от его знаний и творческого подхода к процессу исследования. Метод часто называют *«упражнением красной команды»* (англ. *Red Team exercise*).

При проведении перечисленных методов тестирования проверяемая организация может быть проинформирована о факте и времени проведения тестов (метод «White Hat Testing») или не проинформирована вообще (метод «Black Hat Testing»).

Специализированное инструментальное обеспечение, используемое при различных проверках ИБ, представляет собой динамические системы, самостоятельно следящие за событиями в информационной среде организации и фиксирующие аномалии в ее работе, предупреждающие администратора о возникающих угрозах ИБ, анализирующие полученную информацию, восстанавливающие разрушенные данные и пресекающие несанкционированную активность. Помимо централизованной системы управления и системы разбора и корреляции событий, регистрируемых СЗИ, это инструментальное обеспечение может включать следующие технические средства и интегрированные решения [15, 25]:

1. Средства автоматизации анализа выполнения требований по ОИБ:

- системы анализа защищенности (САЗ), или сканирующее ПО (англ. *scanning software*), или сканеры безопасности (англ. *security scanners*) (в публикациях по ИБ они называется именно так, хотя представляется, что более точным является перевод «сканеры защищенности»);

- СОВ и системы предотвращения вторжений (СПВ) (включая системы-ловушки).

2. Средства автоматизации процесса оценки рисков ИБ (они уже упоминались ранее во второй части серии учебных пособий).

(Средства подготовки отчетов и некоторые другие составляющие в данном учебном пособии не рассматриваются.)

При этом важно отметить, что значительное внимание уделяется комплексу организационно-правовых мероприятий в данной области, например политике и процедурам реагирования на атаки и последующего восстановления систем.

Инструментальные средства автоматизации анализа выполнения требований по ОИБ (критериев аудита ИБ) позволяют следующее:

- автоматизировать процесс оценки степени выполнения требований по ОИБ с учетом их важности;
- оценивать эффективность различных вариантов защитных мер;
- автоматизировать процессы анализа идентифицированных и зафиксированных системами мониторинга ИБ, используемых в проверяемых организациях, внештатных действий пользователей и инцидентов ИБ;
- генерировать отчеты с результатами выполнения различных процедур.

Многие из САЗ умеют находить следующие проблемы в защите информационной среды организации [15]:

- уязвимости проектирования, реализации и эксплуатации;
- уязвимость в реальном масштабе времени;
- уязвимость во внутренней и внешней сетях;
- уязвимость сервисов, программ и устройств (например, модемных пулов) для удаленного доступа;
- подверженность сетевым атакам (DoS, спуффинга и т. п.) и попытками НСД;
- наличие незащищенных сетевых соединений и точек доступа в интранет;
- уязвимость АО из-за неправильных настроек (например, маршрутизаторов);
- уязвимость на сетевом уровне (в сетевых протоколах и сервисах);
- уязвимость на уровне ОС, например, в исходном коде ОС, в ее конфигурационных файлах (конфигураций «по умолчанию»), в системном реестре для ОС Windows, заданные значения ключей системного реестра Windows, права доступа к файлам и каталогам; уязвимость учетных записей; механизмов идентификации и аутентификации, средств мониторинга, аудита и т.п);
- уязвимость на уровне прикладного ПО – серверного и клиентского (например, веб-браузеров и почтовых программ, Web- и FTP-

серверов, неправильную настройку БД, редко используемые сервисы, конфигурации «по умолчанию» и т. п.);
- уязвимость МЭ, прокси-серверов, антивирусных программ и других СЗИ;
- уязвимость к подбору пароля;
- целостность заданных файлов;
- неустановленные или неизвестные обновления (patch, hotfix или Service Pack);
- уязвимость сравнением эталонных значений с текущими;
- новые уязвимости вскоре после их обнаружения.

На основе результатов анализа защищенности можно предпринять следующие действия:
- при запуске сканеров с различными учетными записями, соответствующими привилегиям разных пользователей, можно определить, куда эти пользователи могут проникнуть санкционировано, а куда – нарушая требования по ОИБ;
- произвести корректировку ошибочных настроек и конфигураций подсистем;
- заменить (где это возможно) устаревшие, уязвимые версии обеспечения на более новые, защищенные;
- для ПО и АО, которое пока нельзя заменить более новыми версиями, установить обновления в соответствии с найденными уязвимостями;
- провести мероприятия по снижению вероятности использования уязвимости, которая не может быть устранена немедленно (например, в силу проблем совместимости некоторых подсистем);
- проверить правильность устранения уязвимостей;
- внести необходимые изменения в архитектуру среды, систем, сетей и сервисов с целью учета внесенных изменений и обновлений;
- пересмотреть ПолИБ с учетом последних изменений в информационной среде организации, внести в нее поправки и заново утвердить у руководства;
- повысить квалификацию персонала – как администраторов, так и пользователей отдельных систем, сетей или сервисов;
- провести другие мероприятия, направленные на повышение защищенности среды.

Сканирование необходимо для подтверждения ОИБ и реализации в информационной среде организации механизма превентивной (предупреждающей) защиты, но не достаточно для качественной проверки ИБ, поскольку сканеры, как правило, ищут заранее известные уязвимости, которые внесены в их базы знаний (сигнатур уязвимостей). В результате остается неразрешенный вопрос: если при сканировании не выявлены уязвимости, то их нет на самом деле или их не было на момент проверки в базе сканера? Кроме того, при сканировании всегда остается веро-

ятность нежелательного влияния на элементы среды и, например, существенное увеличение трафика в исследуемом сегменте или даже выведения из строя сканируемого узла или отдельной службы. И, что немаловажно, сканером может воспользоваться не только администратор ИБ, но и злоумышленник, пытающийся выявить уязвимые участки среды для последующего входа и взлома систем.

Основные функции, выполняемые СОВ по соблюдению требований по ОИБ, можно свести к следующим [15]:

- регистрация событий, имеющих отношение к нарушению ИБ (искажение информации, DoS-атака, изменение прав доступа конкретного пользователя в его учетной записи и т. п.);
- оповещение о подозрительных событиях/действиях в сети и выявление нарушенного процесса функционирования систем;
- в случае обнаружения вторжения осуществляются как пассивные (информирование), так и активные действия (завершение соединения);
- по возможности локализации места воздействия злоумышленника.

При этом СОВ решают следующие основные задачи:

- анализ информационных потоков;
- контроль системных конфигураций;
- контроль доступа к файлам;
- контроль доступа к ресурсам;
- анализ данных от сетевого оборудования;
- анализ эффективности настроек и резервирование функций МЭ;
- антивирусная защита;
- распознавание шаблонов атак и анализ аномальных действий;
- контроль неблагонадежных сотрудников;
- контроль действий администратора;
- сбор доказательств для расследования инцидентов ИБ и т. п.

Основные функции СПВ – анализ событий и трафика и предотвращение попыток НСД в режиме реального времени на всех семи уровнях модели взаимодействия открытых систем (включая прикладной) и блокировка или завершение нежелательных сетевых соединений и многое другое. СПВ появились из двух технологий – обнаружение вторжений и межсетевое экранирование. Сначала СПВ, работающая в режиме in-line на скорости передачи данных, анализирует весь трафик и определяет, какой пропускать. СПВ осуществляет всесторонний («глубокий») анализ (англ. *deep packet inspection или application intelligence*) данных, находящихся в проходящих через нее пакетах, а не только их заголовков.

СОВ, как и САЗ, по выполняемым функциям можно отнести сразу к нескольким подсистемам программно-аппаратных СЗИ – это система управления доступом, подсистема регистрации и учета и подсистема

контроля целостности (в той или иной мере эти функции более или менее полно реализованы в зависимости от типа системы).

Проверка выполнения требований по ОИБ требует технической помощи специалиста и включает, в частности, практическое исследование ОС для обеспечения уверенности в том, что защитные меры функционирования АО и ПО были внедрены правильно [11, 12]. Данную проверку следует осуществлять опытному системному инженеру вручную или при необходимости при помощи соответствующих инструментальных средств, генерирующих отчеты с техническими подробностями для последующего анализа.

Проверка выполнения требований по ОИБ также включает тестирование на наличие попыток НСД к системе, которое может быть выполнено независимыми экспертами. Данное тестирование полезно для обнаружения уязвимостей в системе и проверки эффективности защитных мер при предотвращении НСД, использующего эти уязвимости. Особую осторожность следует проявлять в случаях, когда тест на проникновение может привести к компрометации защиты системы и непреднамеренному использованию других уязвимостей.

Любая техническая проверка выполнения требований по ОИБ должна выполняться только компетентными, авторизованными лицами либо под их наблюдением.

Как отмечалось во второй части серии учебных пособий, инструментальные средства автоматизации оценки рисков ИБ позволяют осуществлять следующие действия:

- анализировать выполнение ПолИБ в организации;
- оценивать риски ИБ с использованием подходов и методик, принятых в организации (для негосударственных организаций, обрабатывающих конфиденциальную информацию, не являющуюся собственностью государства) или утвержденных уполномоченным Федеральным органом исполнительной власти в области технической защиты информации (для государственных и негосударственных организаций, обрабатывающих конфиденциальную информацию, являющуюся собственностью государства);
- идентифицировать и оценивать варианты обработки рисков ИБ;
- вырабатывать рекомендации по методам и средствам снижения рисков ИБ при сборе, обработке, хранении конфиденциальной информации при использовании в организации различных систем ИТ;
- вырабатывать и предоставлять обоснования для выбора защитных мер;
- генерировать отчеты по результатам оценки рисков ИБ.

Примеры современных САЗ и СОВ/СПВ приведены соответственно в приложениях 2 и 3.

Выводы

В главе рассматриваются процессы группы проверки СУИБ, включающие мониторинг ИБ (как результата процессов управления ИБ), самооценку ИБ, внутренние и внешние аудиты ИБ, анализ СУИБ со стороны руководства организации. Именно эти процессы являются логическим завершением в цикле непрерывного улучшения процессов управления ИБ и СУИБ в целом за счет определения и реализации необходимых корректирующих и предупреждающих действий в отношении СУИБ.

Мониторинг, в основе которого лежит постоянное наблюдение за эффективностью и результативность существующих защитных мер или процессов СУИБ, является очень гибким инструментом, позволяющим осуществлять сколь угодно детальный контроль над работой каждого процесса. Исходя из текущих значений установленных показателей, можно получить объективную информацию о функционировании процессов и защитных мер. Мониторинг позволяет наглядно увидеть улучшается или ухудшается ситуация в рамках процессов управления ИБ и функционирования защитных мер. Таким образом, появляется возможность выделять процессы, которые работают неэффективно, наблюдать за ними и устранять причины их неэффективной работы.

Самооценка ИБ, проводимая организацией своими силами по инициативе руководства для определения соответствия ИБ критериям аудита ИБ, является хорошей практикой проверки уровня ИБ, выявления недостатков СУИБ и подготовки к аудитам ИБ. На ее основе организация может выработать и затем реализовать основанные на длительно накапливаемых фактах рекомендации, касающиеся улучшения всей деятельности по управлению ИБ.

За счет знания внутренними аудиторами особенностей своей организации и отсутствия предубежденного отношения сотрудников проверяемых подразделений к ним результаты внутреннего аудита ИБ также весьма ценны. Они служат основой входных данных для анализа СУИБ со стороны руководства и дают полезную информацию независимым экспертам при проведении внешних аудитов ИБ.

В основе внешнего аудита ИБ лежит стремление руководства организации с помощью проведения независимой и компетентной оценки определить истинный уровень организации работ в области ИБ и степень соответствия ИБ организации установленным критериям аудита ИБ.

Не менее одного раза в год руководство организации должно проводить анализ своей СУИБ в целях обеспечения ее полной пригодности, адекватности и результативности. Результаты анализа должны содержать оценку выполнения требований ПолИБ в организации и конкретные и выполнимые предложения по изменению СУИБ. Устранение несоответствий и непрерывное улучшение СУИБ и отдельных ее процессов осуществляется за счет процесса управления корректирующими или предупреждающими действиями.