

## **1 Цели аудитов информационной безопасности, их классификации по типам**

Аудит состояния информационной безопасности на предприятии представляет собой экспертное обследование основных аспектов информационной безопасности, их проверку на соответствие определенным требованиям. В некоторых случаях под аудитом информационной безопасности подразумевается проверка защищенности отдельных элементов информационной инфраструктуры предприятия (сегментов его сети, отдельных серверов, баз данных, Интернет-сайтов и пр.) и надежности средств защиты информации (межсетевых экранов, систем обнаружения вторжений и пр.). Однако мы в дальнейшем исходим из того, что аудит информационной безопасности является комплексным (по возможности, исчерпывающим) исследованием всех аспектов информационной безопасности (как технических, так и организационных) в контексте всей хозяйственной деятельности предприятия с учетом действующей политики информационной безопасности, объективных потребностей предприятия и требований, предъявляемых третьими лицами (государством, контрагентами и пр.).

Различают два основных вида аудита: внутренний (проводимый исключительно силами сотрудников предприятия) и внешний (осуществляемый сторонними организациями).

Целями аудита могут быть:

- установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации;
- проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности;

- контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности;

- сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам).

Одной из стратегических задач, решаемых при проведении аудита информационной безопасности и получении соответствующего сертификата, является демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов, что может быть особенно важно при осуществлении сделок, предполагающих обмен конфиденциальной информацией, имеющей большую стоимость (финансовыми сведениями, конструкторско-технологической документацией, результатами НИОКР и пр.).

В том случае, если аудит является внутренним, группу аудиторов необходимо сформировать из числа таких специалистов, которые сами не являются разработчиками и администраторами используемых информационных систем и средств защиты информации и не имели отношения к их внедрению на данном предприятии.

Как правило, предприятие может прибегать к помощи внешних аудиторов с целью:

- повышения объективности, независимости и профессионального уровня проверки;

- получения заключений о состоянии информационной безопасности и соответствии международным стандартам от независимых аудиторов.

Компании, специализирующиеся на проведении аудитов, могут осуществлять проверки состояния информационной безопасности на соответствие таким общепризнанным стандартам и требованиям, как:

- ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий);
- ISO 17799 (BS 7799): Code of Practice for Information Security Management (Практические правила управления информационной безопасностью);
- BSI\IT: Baseline Protection Manual (Руководство базового уровня по защите информационных технологий Агентства информационной безопасности Германии);
- COBIT: Control Objectives for Information and related Technology (Основные цели для информационных и связанных с ними технологий);
- Требованиям Руководящих документов ФСТЭК РФ, ФСБ или других государственных органов и других документов (таких как SAC, COSO, SAS 55/78).

При этом организация, осуществляющая внешний аудит, должна отвечать определенным требованиям:

- иметь право (лицензию) на выдачу заключений о соответствии определенным требованиям (например, аккредитацию UKAS – United Kingdom Accreditation Service);
- сотрудники должны иметь право доступа к информации, составляющей государственную и военную тайну (если такая информация имеется на проверяемом предприятии);
- обладать необходимыми программными и аппаратными средствами для исчерпывающей проверки имеющегося у предприятия программного и аппаратного обеспечения.

## **2 Этапы аудита**

Основными этапами проведения аудита являются:

- инициирование проведения аудита;
- непосредственно осуществление сбора информации и проведение обследования аудиторами;
- анализ собранных данных и выработка рекомендаций;
- подготовка аудиторского отчета и аттестационного заключения.

Аудит должен быть инициирован руководством предприятия с достаточно четко сформулированной целью на определенном этапе развития информационной системы или системы обеспечения информационной безопасности предприятия (например, после завершения одного из этапов внедрения). В случае если аудит не является комплексным, на начальном этапе необходимо определить его непосредственные границы:

- перечень обследуемых информационных ресурсов и информационных систем (подсистем);
- перечень зданий, помещений и территорий, в пределах которых будет проводиться аудит;
- основные угрозы, средства защиты от которых необходимо подвергнуть аудиту;
- элементы системы обеспечения информационной безопасности, которые необходимо включить в процесс проверки (организационное, правовое, программно-техническое, аппаратное обеспечение);

Основная стадия – проведение аудиторского обследования и сбор информации – как правило, должно включать в себя:

- анализ имеющейся политики информационной безопасности и другой организационной документации;
- проведение совещаний, опросов, доверительных бесед и интервью с сотрудниками предприятия;

- проверку состояния физической безопасности информационной инфраструктуры предприятия;
- техническое обследование информационных систем – программных и аппаратных средств (инструментальная проверка защищенности).

Прежде чем приступить собственно к аудиту информационной безопасности, аудиторам (в частности, если проводится внешний аудит) необходимо ознакомиться со структурой предприятия, его функциями, задачами и основными бизнес-процессами, а также с имеющимися информационными системами (их составом, функциональностью, процедурами использования и ролью на предприятии). На начальном этапе аудиторы принимают решения о том, насколько глубоко и детально будут исследованы отдельные элементы информационной системы и системы защиты информации. Также необходимо заранее скоординировать с пользователями информационных систем процедуры проверки и тестирования, требующие ограничения доступа пользователей (такие процедуры по возможности должны проводиться в нерабочее время или в периоды наименьшей загрузки информационной системы).

Качественный анализ действующей на предприятии политики безопасности является отправной точкой для проведения аудита. Одна из первых задач комплексного аудита – установление того, в какой степени действующая политика соответствует объективным потребностям данного предприятия в безопасности, могут ли действия в рамках данной политики обеспечить необходимый уровень защищенности информации и средств ее обработки, хранения и передачи. Это, в свою очередь, может потребовать проведения дополнительной оценки значимости основных информационных активов предприятия, их уязвимости, а также существующих рисков и угроз. Анализ политики также может включать оценку таких ее характеристик, как:

Тема 2.7 – Аудит информационной безопасности  
(Управление информационной безопасностью)

- полнота и глубина охвата всех вопросов, а также соответствие содержания политик нижнего уровня целям и задачам, установленным в политиках верхнего уровня;
- понятность текста политики для людей, не являющихся техническими специалистами, а также четкость формулировок и невозможность их двойного толкования;
- актуальность всех положений и требований политики, своевременность учета всех изменений, происходящих в информационных системах и бизнес-процессах.

После проверки основных положений политики безопасности в процессе аудита могут быть изучены (проверены) действующие классификации информационных ресурсов по степени критичности и конфиденциальности, а также другие документы, имеющие отношение к обеспечению информационной безопасности:

- организационные документы подразделений предприятия (положения об отделах, должностные инструкции);
- инструкции (положения, методики), касающиеся отдельных бизнес-процессов предприятия;
- кадровая документация, обязательства о неразглашении сведений, данные сотрудниками, свидетельства о прохождении обучения, профессиональной сертификации, аттестации и ознакомлении с действующими правилами;
- техническая документация и пользовательские инструкции для различных используемых программных и аппаратных средств (как разработанных самим предприятием, так и приобретенных у сторонних поставщиков): межсетевых экранов, маршрутизаторов, операционных систем, антивирусных средств, систем управления предприятием и пр.

Основная работа аудиторов в процессе сбора информации заключается в изучении фактически предпринимаемых мер по обеспечению защиты информационных активов предприятия, таких как:

- организация процесса обучения пользователей приемам и правилам безопасного использования информационных систем;
- организация работы администраторов информационных и телекоммуникационных систем и систем защиты информации (правильность использования программных и аппаратных средств администрирования, своевременность создания и удаления учетных записей пользователей, а также настройки их прав в информационных системах, своевременность замены паролей и обеспечение их соответствия требованиям безопасности, осуществление резервного копирования данных, ведение протоколов всех производимых в процессе администрирования операций, принятие мер при выявлении неисправностей и пр.);
- организация процессов повышения квалификации администраторов информационных систем и систем защиты информации;
- обеспечение соответствия необходимых (в соответствии с политикой безопасности и должностными обязанностями) прав пользователей информационных систем и фактически имеющихся;
- организация назначения и использования специальных («суперпользовательских») прав в информационных системах предприятия;
- организация работ и координации действий при выявлении нарушений информационной безопасности и восстановлении работы информационных систем после сбоев и нападений (практическое выполнение «аварийного плана»);
- предпринимаемые меры антивирусной защиты (надлежащее использование антивирусных программ, учет всех случаев заражения, организация работы по устранению последствий заражений и пр.);

Тема 2.7 – Аудит информационной безопасности  
(Управление информационной безопасностью)

- обеспечение безопасности приобретаемых программных и аппаратных средств (наличие сертификатов и гарантийных обязательств, поддержка со стороны поставщика при устранении выявленных недостатков и пр.);
- обеспечение безопасности самостоятельно разрабатываемого программного обеспечения (наличие необходимых требований в проектной документации информационных систем, качество программной реализации механизмов защиты и пр.);
- организация работ по установке и обновлению программного обеспечения, а также контроля за целостностью установленного ПО;
- предпринимаемые меры по обеспечению учета и сохранности носителей информации (дисков, дискет, магнитных лент и пр.), а также по их безопасному уничтожению после окончания использования;
- эффективность организации взаимодействия сотрудников предприятия – пользователей информационных систем – со службой информационной безопасности (в частности, по вопросам реагирования на инциденты и устранения их последствий).

Одним из важных направлений аудиторской проверки является контроль того, насколько своевременно и полно положения и требования политики безопасности и других организационных документов доводятся до персонала предприятия. В том числе, необходимо оценить, насколько систематически и целенаправленно осуществляется обучение персонала (как при занятии должностей, так и в процессе работы), и, соответственно, дать оценку тому, в какой мере персонал понимает все предъявляемые к нему требования, осознает свои обязанности, связанные с обеспечением безопасности, а также возможную ответственность, которая может наступить при нарушении установленных требований.

В процесс проведения интервью, совещаний и бесед с персоналом необходимо включить как можно больше сотрудников предприятия, имеющих

хотя бы какое-то отношение к информационным системам и процедурам обработки информации: администраторов и разработчиков информационных систем, операторов и других пользователей, вспомогательный персонал и пр. При непосредственной работе с персоналом аудиторам необходимо выяснить особенности протекания отдельных бизнес-процессов, роли отдельных сотрудников в этих процессах и их потенциальные возможности влиять на информационную безопасность. Также необходимо оценить, в какой мере сотрудники фактически выполняют свои обязанности в отношении обеспечения информационной безопасности.

Одной из важных задач аудита может быть установление того, насколько предприятие способно противодействовать внутренним угрозам в лице сотрудников, целенаправленно действующих, чтобы нанести тот или иной ущерб предприятию и имеющих для этого различные возможности. В частности, для этого могут быть исследованы:

- процедуры отбора и принятия новых сотрудников на работу, а также их предварительной проверки;
- процедуры контроля за деятельностью сотрудников (отслеживания их действий);
- процедуры регистрации пользователей и назначения им прав в информационных системах;
- распределение функций между различными сотрудниками и минимизация их привилегий, а также возможное наличие избыточных прав у некоторых пользователей и администраторов.

### **3 Проверка состояния физической безопасности информационной инфраструктуры**

Проверка состояния физической безопасности информационной инфраструктуры, как правило, включает в себя:

- проверку того, чтобы наиболее важные объекты информационной инфраструктуры и системы защиты информации располагались в зонах (частях

зданий, помещениях), имеющих пропускной режим, а также оборудованных камерами видеонаблюдения и другими средствами контроля (электронными замками, средствами биометрической идентификации и пр.);

- проверку наличия и работоспособности технических средств, обеспечивающих устойчивую работу компьютерного и телекоммуникационного оборудования: источников бесперебойного энергоснабжения, кондиционеров (там, где это необходимо) и пр.;

- проверку наличия и работоспособности средств пожарной сигнализации и пожаротушения;

- проверку распределения ответственности за физическое (техническое) состояние объектов информационной инфраструктуры предприятия.

#### **4 Инструментальная проверка защищенности**

Инструментальная проверка защищенности является в основном технической задачей и осуществляется с использованием специализированного программного обеспечения, которое подключается к информационной системе предприятия и автоматически производит сбор всевозможных сведений: версий установленных операционных систем и программного обеспечения, данных об используемых сетевых протоколах, номеров открытых портов, данных о версиях установленных обновлений и пр. К другим направлениям инструментального и технического контроля также относятся такие работы, как:

- непосредственное изучение работы отдельных серверов, рабочих станций и сетевого оборудования соответствующими техническими специалистами, которые могут проверить различные аспекты их функционирования (процедуры загрузки, выполняемые процессы, содержимое конфигурационных файлов и пр.);

- сбор и последующий анализ данных о том, как выполняются процедуры резервного копирования, а также другие необходимые технические процедуры, предусмотренные регламентом;

- проверка качества программного обеспечения, самостоятельно разработанного предприятием (в том числе и путем анализа исходных кодов и проектной документации к нему), выявление ошибок, которые могут стать причиной сбоев, несанкционированных проникновений, разрушения и утечки информации и других инцидентов;
- изучение работы сети (сетевого трафика, загрузки различных сегментов сети и пр.);
- проведение с целью тестирования пробных, контролируемых «нарушений» информационной безопасности (по возможности без нанесения реального вреда и во внерабочее время), таких как атаки типа «отказ в обслуживании» (DoS) или проникновение в определенные базы данных и на определенные серверы, а также использование различных известных уязвимостей с целью выяснения конкретных параметров безопасности, устойчивости и надежности проверяемой информационной системы.

Также в процессе аудита может быть проверено ведение журналов (лог-файлов) информационных систем и применение других инструментов сбора и анализа информации, необходимых для обеспечения текущего контроля за соблюдением требований информационной безопасности и своевременного реагирования на инциденты (средств обнаружения вторжений, анализаторов работы локальных сетей и пр.). Информация, накопленная в лог-файлах за время использования информационных систем, является одним из важных объектов анализа в процессе аудита. На основе этих данных могут быть сделаны оценки и выводы относительно соблюдения установленных правил использования информационных систем, эффективности используемых средств защиты информации, поведения пользователей, а также о потенциально возможных проблемах.

## **5 Анализ информации**

Анализ всей информации, полученной в процессе ознакомления с документацией, контроля фактического выполнения всех установленных требований, получения сведений от сотрудников, изучения работы аппаратных средств и программного обеспечения, проверки физической защищенности и проведения инструментальных проверок должен быть произведен с учетом выявленных рисков и потребностей предприятия в информационной безопасности. В частности, такой анализ предполагает выявление конкретных особенностей программных и аппаратных средств, бизнес-процедур, организационных правил и распределений функциональных обязанностей и полномочий, которые могут негативно повлиять на обеспечение информационной безопасности, а также описание причинно-следственных взаимосвязей между выявленными особенностями функционирования предприятия и увеличением рисков нарушения информационной безопасности. Все исследованные обстоятельства, выявленные недостатки и особенности должны быть обобщены, и таким образом должно быть сформировано общее представление о состоянии информационной безопасности на предприятии, отражены основные достоинства и недостатки действующей системы защиты информационных ресурсов, а также обозначены основные приоритеты и направления ее дальнейшего развития и совершенствования.

Результаты анализа могут быть представлены как в виде обобщенных кратких формулировок, характеризующих защищенность информации предприятия (адресованных руководству и собственникам предприятия), так и в виде перечня конкретных замечаний и предложений, относящихся к отдельным участкам работы (адресованных руководителю департамента информационной безопасности, руководителю службы безопасности, функциональным директорам и руководителям структурных подразделений предприятия).

Окончательным результатом анализа и обобщения данных, полученных в процессе аудита, является отчет (заключение), который может включать в себя:

- оценку состояния (уровня) защищенности информационных ресурсов и информационных систем;
- заключения о практическом выполнении требований, предусмотренных политикой информационной безопасности предприятия и иными требованиями, и документами;
- заключение о степени соответствия фактического уровня информационной безопасности требованиям определенных стандартов и нормативных документов;
- предложения по усовершенствованию политики информационной безопасности и реализации дополнительных практических мероприятий в этой сфере (как организационных, так и технических), а также о тех мерах, которые необходимо реализовать для прохождения сертификации на соответствие определенному стандарту (если по результатам проведенного аудита сделан вывод о том, что текущий уровень защищенности информационных ресурсов предприятия не соответствует таким требованиям);
- заключение о степени соответствия политики безопасности предприятия и всего комплекса мер по защите информации требованиям действующего законодательства и ведомственных нормативных актов;
- оценки экономической эффективности вложений в те или иные средства защиты информации, а также организационные мероприятия (отдачи от них);
- количественная (денежная) оценка возможных потерь от тех или иных нарушений, которые могут произойти при существующем уровне обеспечения информационной безопасности, а также расчет необходимых вложений, которые необходимо осуществить для достижения определенного уровня защищенности.

Также по результатам аудита могут быть сформулированы дополнительные рекомендации, касающиеся:

- пересмотра отдельных бизнес-процессов и процедур;

Тема 2.7 – Аудит информационной безопасности  
(Управление информационной безопасностью)

- совершенствования работы с персоналом предприятия;
- внедрения и использования современных технических (программных и аппаратных) средств обработки и защиты информации;
- организации работы по защите информации;
- выбора приоритетов в процессе устранения существующих недостатков.