

Принципы аудита безопасности информационных систем

Содержание

- А что такое «Аудит ИБ»? Базовые понятия
- Стандарты и нормативы
- Почему проводится аудит ИБ? Каковы ожидания от аудита? Предпосылки аудита ИБ
- А кто проводит аудит ИБ?
- Цели аудита ИБ
- А как проводят аудит ИБ? Этапы аудита ИБ
- Виды аудита ИБ
- А как выглядит правильный отчет об аудите ИБ?
Аудиторское заключение
- А как правильно использовать результаты аудита ИБ?
Дорожная карта по итогам аудита ИБ

Базовые понятия

Аудит, аудиторская проверка

— процедура независимой оценки деятельности организации, системы, процесса, проекта или продукта.

Согласно Федеральному закону от 30.12.2008 №307-ФЗ «Об аудиторской деятельности», аудит — это «независимая проверка бухгалтерской (финансовой) отчетности аудируемого лица в целях выражения мнения о достоверности такой отчетности».



Информационная безопасность

— защищенность информации и поддерживающей ее информационной инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, наносящих ущерб владельцам или пользователям этой информации и поддерживающей ее информационной инфраструктуре

Базовые понятия

Аудит информационной безопасности

— это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании» («Консалтинг и аудит в сфере ИТ 2004». CNews Analytics).

Аудит ИБ – это комплекс мероприятий.

«Какова реальная ситуация с ИБ?»

«Как реальная ситуация с ИБ соотносится с требованиями?»

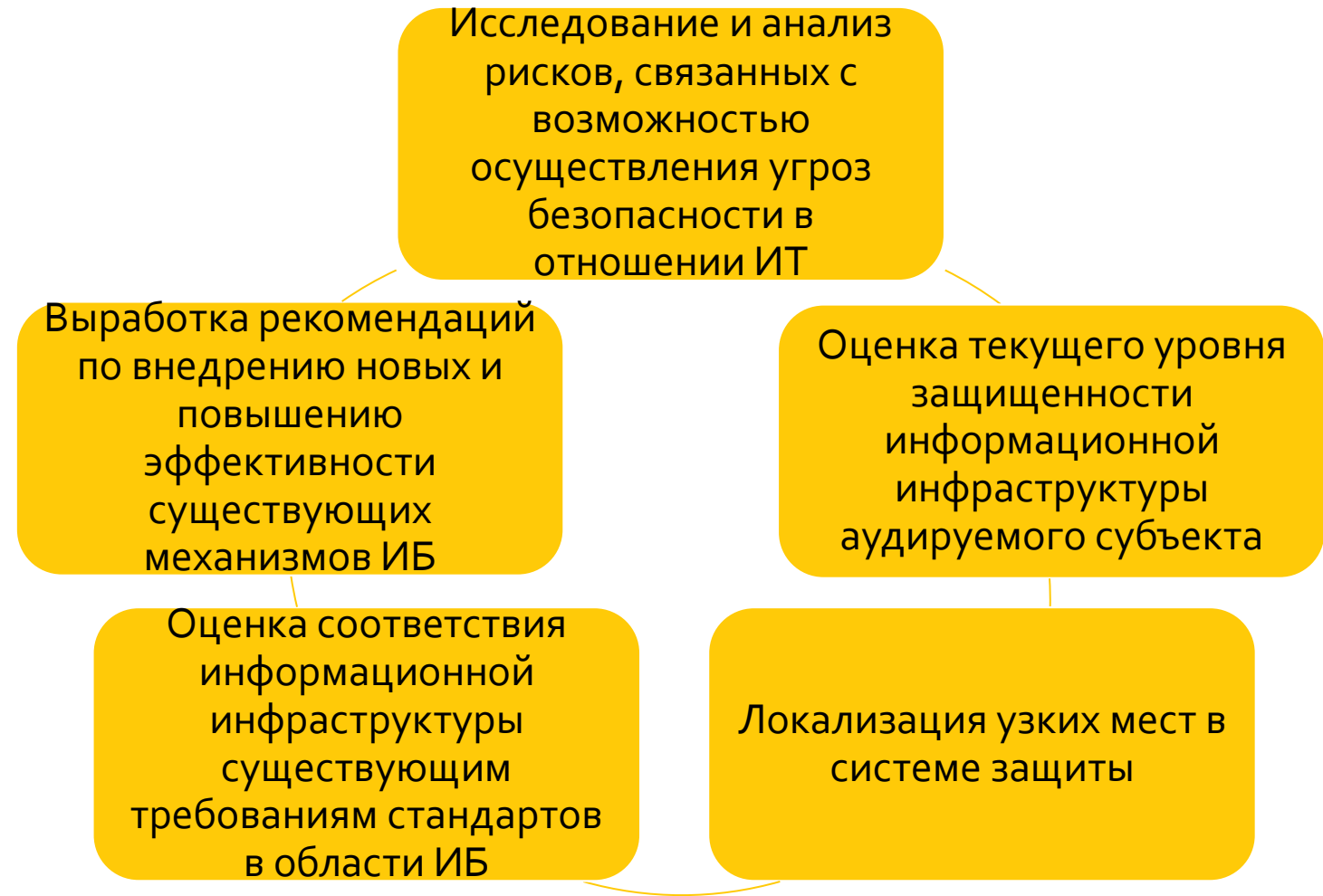
Государственные стандарты РФ

- ГОСТ Р 50922-2006 — Защита информации (ЗИ). Основные термины и определения.
- ГОСТ Р 50.1.053-2005 — Информационные технологии (ИТ). Основные термины и определения в области технической защиты информации.
- ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-99 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р ИСО/МЭК 15408-1-2008 — ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.
 - Часть 1. Введение и общая модель.
 - Часть 2. Функциональные требования безопасности.
 - Часть 3. Требования доверия к безопасности.
- ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий». Сфера приложения— защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
- ГОСТ Р ИСО/МЭК 17799 — «ИТ. Практические правила УИБ». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
- ГОСТ Р ИСО/МЭК 27001 — «ИТ. Методы безопасности. СУИБ. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
- ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

Между-народные стандарты:

- Стандарт COBIT (Control Objectives for Information and Related Technologies)
- BS 7799-1:2005 — Британский стандарт BS 7799 1-я часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила УИБ). Служит практическим руководством по созданию СУИБ
- BS 7799-2:2005 — Британский стандарт BS 7799 2-я часть. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация СУИБ). Используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
- BS 7799-3:2006 — Британский стандарт BS 7799 3-я часть. Новый стандарт в области управления рисками информационной безопасности
- ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента ИБ».
- ISO/IEC 27000 — Словарь и определения.
- ISO/IEC 27001:2005 — «Информационные технологии — Методы обеспечения безопасности — СУИБ — Требования».
- ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. Дата выхода — 2007 год.
- ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
- German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты IT).
- Стандарт WebTrust. Применим для подтверждения высокого уровня защищенности системы электронной коммерции и web-сервисов.

Зачем проводить аудит ИБ? Цели



Чего мы ожидаем?

- Объективную информацию
- Оценку соответствия требованиям
- Рекомендации по повышению эффективности

Что аудируют?



*Ценность (важность) ресурса определяется величиной ущерба наносимого в случае нарушения ИБ:

данные были изменены, удалены или стали недоступны;

аппаратно-программные средства были разрушены или повреждены;

нарушена целостность программного обеспечения и пр.

Кто проводит аудит ИБ?

- «Мы – ИБ-консультанты»

ИТ-интеграторы и специализированные организации

- «Мы – сами с усами»

внутренний контроль, специалисты УК холдинга

- «Мы – частные эксперты»

гуру, авторитеты, «партнер посоветовал»

Желательно, чтобы специалисты-аудиторы имели соответствующую квалификацию, как правило, подтвержденную:

- международными сертификатами CISA и CISM,
- сертификатами Гостехкомиссии РФ,
- сертификатами ведущих производителей оборудования и программного обеспечения, включая:
 - Microsoft Certified Systems Engineer (MCSE): Security,
 - CheckPoint Certified Security Expert (CCSE),
 - Cisco Certified Internetwork Expert (CCIE).

Когда проводят аудит ИБ?

- ➔ При наступлении критических ситуациях, когда защита уже была нарушена;
- ➔ При расширении компании, слиянии, поглощении, присоединении другими предприятиями;
- ➔ При смене стратегии, концепции курса бизнеса или руководства;
- ➔ В случаях изменений в международном законодательстве или в правовых актах внутри отдельно взятой страны;
- ➔ В случаях серьезных изменения в информационной инфраструктуре.

Первый этап аудита ИБ

1. Подготовка к проведению аудита ИБ:

- ❖ выбор объекта аудита (фирма, отдельные здания и помещения, отдельные системы или их компоненты);
- ❖ составление команды аудиторов-экспертов и распределение зон ответственности;
- ❖ определение объема и масштаба аудита и установление конкретных сроков работы;
- ❖ формирование программы проверки;
- ❖ сбор «первички».

«Первичка»

- ВНД: политика ИБ, защиты информации, парольная. регламенты АИС и др.
- структурные и функциональные схемы;
- схемы информационных потоков;
- описание комплекса аппаратных средств информационной инфраструктуры;
- описание автоматизированных функций;
- описание основных технических решений;
- проектную и рабочую документацию на информационную инфраструктуру
- описание структуры программного обеспечения.

«Первичка»

- о владельцах информации и пользователях (потребителях) информации;
- о провайдерах услуг;
- о характере и путях предоставления услуг конечным потребителям;
- об основных видах функционирующих приложений;
- о существующих компонентах (элементах) информационной инфраструктуры и их функциях;
- о масштабе и границе информационной инфраструктуры;
- о входах в информационную систему (ИТ-процессы);
- о взаимодействии с другими системами (каналы связи);
- о протоколах взаимодействия;
- об аппаратно-программных платформах используемых в информационной инфраструктуре.

Второй этап аудита ИБ

2. Проведение аудита:

- ❖ общий анализ состояния безопасности объекта аудита;
- ❖ регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз;
- ❖ оценка результатов проверки;
- ❖ составление отчета о результатах проверки по отдельным составляющим.

Виды аудита ИБ согласно между- народной классификации

Экспертная проверка состояния защищенности информации и информационных систем

- основывается на личном опыте экспертов, ее проводящих

Аттестация систем и мер безопасности

- на предмет соответствия международным стандартам (ISO 17799) и гос. правовым документам, регулирующим эту сферу деятельности

Анализ защищенности информационных систем

- с применением технических средств, направленный на выявление потенциальных уязвимостей в программно-аппаратном комплексе

Экспертный аудит ИБ

Экспертный аудит представляет собой сравнение состояния ИБ с «идеальным» описанием, которое базируется на:

- **требованиях**, которые были предъявлены руководством в процессе проведения аудита;
- **описании «идеальной» системы безопасности**, основанном на «Best Practices»

3 столпа экспертного аудита:

1. Ключевой этап экспертного аудита - анализ проекта ИС, топологии сети и технологии обработки информации. В ходе анализа выявляются недостатки существующей топологии сети, снижающие уровень защищенности ИС.

2. Проводится анализ информационных потоков предприятия, позволяющий спроектировать систему обеспечения ИБ, которая будет соответствовать принципу разумной достаточности.

3. В рамках экспертного аудита производится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции.

Аудит ИБ на соответ- ствие стандартам

При проведении аудита ИБ на соответствие стандартам состояние ИБ сравнивается с неким абстрактным описанием, приводимым в стандартах.

Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

- степень соответствия проверяемой ИС выбранным стандартам;
- степень соответствия собственным внутренним требованиям компании в области ИБ;
- количество и категории полученных несоответствий и замечаний;
- рекомендации по построению или модификации системы обеспечения ИБ, позволяющие привести ее в соответствие с рассматриваемым стандартом;

Инструментальный анализ защищенности АС или «Активный аудит»

Активный аудит - это исследование состояния защищенности ИС с точки зрения некоего злоумышленника, обладающего высокой квалификацией в области ИТ.

Активный аудит представляет собой сбор информации о состоянии системы сетевой защиты с помощью специального ПО и специальных методов. В процессе проведения данного вида аудита моделируется как можно большее количество таких сетевых атак, которые может выполнить злоумышленник.

Результатом активного аудита является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации сети заказчика.

По завершении данного вида аудита выдаются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить опасные уязвимости и тем самым повысить уровень защищенности ИС от действий злоумышленника при минимальных затратах на ИБ.

Третий этап аудита ИБ

3. Завершение аудита:

- ❖ разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности фирмы;
- ❖ составление итогового отчета.

Аудиторское заключение (1)

Раздел	Описание
Название	отличающее аудиторский отчет от иных отчетных документов
Адресат	указывает на субъект, которому представляется аудиторский отчет (например, совету директоров и пр.)
Вводный раздел (Краткая справка)	<p>В нем необходимо отразить цель и задачи аудирования. В этом разделе приводят краткую информацию о :</p> <ul style="list-style-type: none">• назначении и основных функциях как информационной инфраструктуры в целом, так и ее отдельных элементов;• группы задач, решаемых инфраструктурой;• классификацию ИТ пользователей;• структуру и состав комплекса аппаратно-программных средств;• виды информационных ресурсов;• структуру информационных потоков;

Аудиторское заключение (2)

Раздел	Описание
Раздел, раскрывающий масштаб (границы) проведения аудита	<ul style="list-style-type: none">• Список обследуемых физических, программных и информационных ресурсов.• Площадки (помещения), попадающие в границы обследования.• Основные виды угроз безопасности, рассматриваемые при проведении аудита.• Организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты
Раздел раскрывающий характер аудиторского исследования	В нем дается описание примененной методики аудиторского исследования, а также критерии оценки величины вероятного ущерба, оценки критичности ИТ-ресурсов и анализа и оценки рисков.

Аудиторское заключение (3)

Раздел	Описание
Выводы по результатам исследования	Здесь четко и аргументировано формулируются основные выводы, полученные на основании аудита
Рекомендации	В этом разделе раскрываются рекомендуемые предложения (контрмеры) как по организационным аспектам аудируемого субъекта и в частности информационной безопасности, так и аппаратно-программным средствам.
Дата составления отчета	
Подпись аудитора	<ul style="list-style-type: none">Аудиторский отчет подписывается от имени аудирующего субъекта, так как именно он принимает на себя всю ответственность за проведение аудита в целом

Дорожная карта по итогам аудита ИБ

Мероприятия на стадии аудита ИБ

Аудит ИБ

Результаты
аудита ИБ

Презентация
и обсуждение
результатов

Назначение
ответственных
лиц

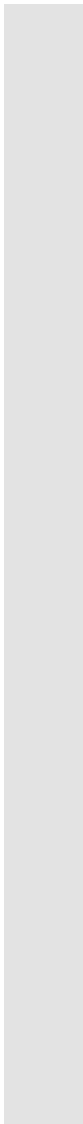

Оценка
достижения
успеха

Контроль и
учет
мероприятий

Исполнение
мероприятий

Формирова-
ние плана
мероприятий

Дальнейшая активность



Рассмотрим пример
аудиторского отчета



Спасибо за внимание!