Роль аудита информационной безопасности

Директор Департамента информационной безопасности ОАО МГТС
А.А. Хрусталев

Москва,

МГТС МТС

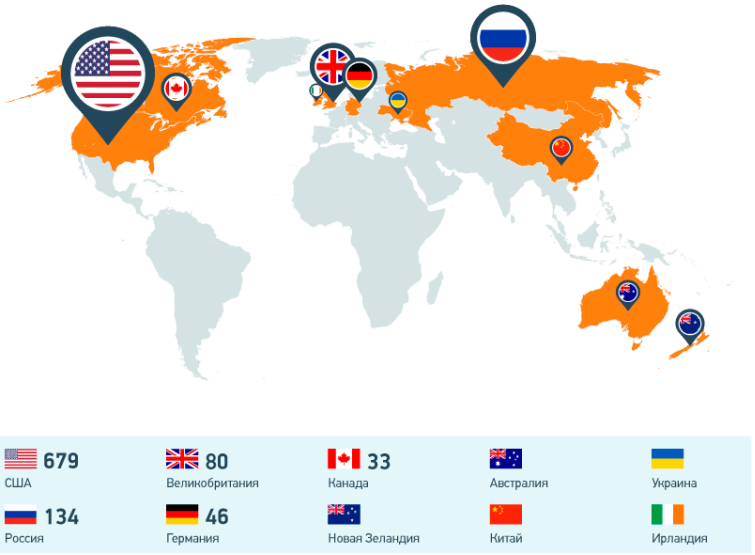
Что такое аудит ИБ

Аудит ИБ организации: Систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации.

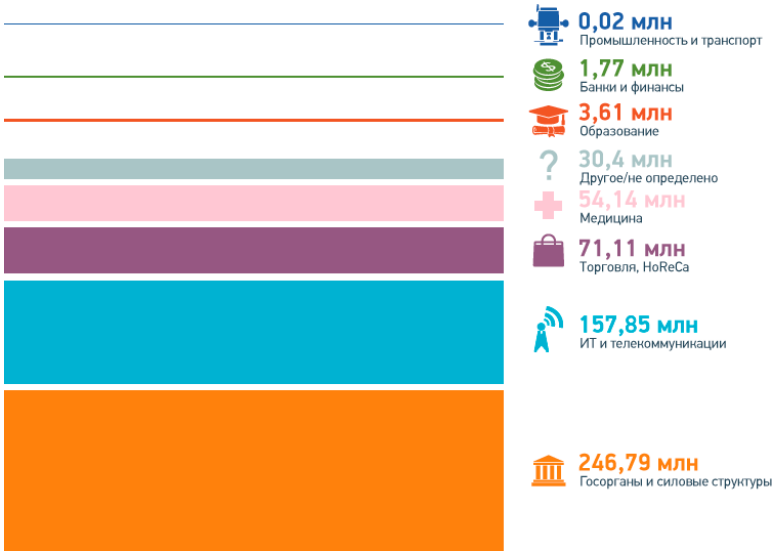
ГОСТ Р 53114-2008

Зачем проводить аудит в компании

Россия занимает 2-ое место в мире по уровню утечек



Основные сферы деятельности откуда происходят утечки



1143
случая утечки в 2013 году

на 22,3%
больше, чем в 2012 году

Как показало исследование InfoWatch за 1 полугодие 2014 года было зарегистрировано 654 случая утечки конфиденциальной информации (3,5 инцидента в день), что на 32% превышает аналогичный показатель за прошлый год.

Проведение регулярного аудита систем информационной безопасности позволит:

- Предотвратить утечку конфиденциальной информации из компании;
- Выявить наиболее узкие места в компании с точки зрения информационной безопасности;
- Повысить культуру информационной безопасности среди сотрудников компании.

Основные предпосылки проведения аудита ИБ

Основными предпосылками проведения аудита ИБ являются:

- Получение объективной информации о защищенности информационных активов, оценка эффективности действующих систем защиты;
- Оценка соответствия систем защиты (получение сертификата соответствия) требованиям международных и отечественных стандартов, отраслевым нормативным документам;
- Контроль функционирования ИС и деятельности персонала (регулярная деятельность).

Цели аудита ИБ

Цели аудита ИБ:

- Анализ возможности осуществления угроз безопасности по отношению к информационным системам
- Определение уровня защищенности ИС и выявление слабых мест в системе защиты;
- Формирование рекомендаций по повышению эффективности механизмов безопасности ИС;
- Оценка полноты выполнения законодательных требований, стандартов, нормативных документов

Чем руководствоваться при проведении аудита ИБ

- Законы РФ
- Руководящие документы ФСБ и ФСТЭК
- Международные стандарты и рекомендации (ISO/IEC);
- Государственные стандарты РФ
- Отраслевые стандарты и рекомендации (СТО БР ИББС, NIST, NERC, PCI DSS);
- Рекомендации (Best Practice) на основе мирового опыта;
- Нормативные акты и стандарты компании.

Основные формы аудита для ИС

1. **Первичный аудит** – проводится на этапе формирования бизнес-требований к внедряемой ИС. Основная цель – формирование концепции ИБ в рамках данной ИС для решения проблем реализации требований нормативных документов.

2. **Проектный аудит** – проводится на этапе формирования функциональных и технических требований к внедряемой ИС. Основная цель – формирование конкретных требований к ИС по обеспечению безопасности, определение необходимых средств защиты.

3. **Аттестационный аудит** – проводится после завершения работ по построению ИС. Основная цель – подтверждение соответствия принятых мер в части ИБ требуемым стандартам.

4. **Плановый аудит** – проводится на протяжении всего жизненного цикла ИС. Основная цель – контроль (подтверждение) уровня ИБ ИС, проверка соблюдения пользователями ИС политик безопасности.

Аудит собственными силами:

Плюсы	Минусы
1. Ясное понимание происходящих процессов и специфики ИС; 2. Сведения о системе и итогах аудита не покидают Компанию; 3. Отсутствуют финансовые затраты.	1. Отсутствие квалифицированного персонала и обширного опыта в сфере аудита; 2. Недостаток времени у сотрудников; 3. Субъективность оценки.

Аудит внешними силами

Плюсы	Минусы
1. Независимая оценка; 2. Наличие обширного опыта в сфере аудита 3. Высокий уровень экспертизы.	1. Сведения о системе и итогах аудита находятся у Подрядчика; 2. Сложность выбора Подрядчика; 3. Высокая стоимость работ.

Виды аудита информационной безопасности:

1. Документальная проверка

✓ Проверка нормативных документов по вопросам информационной безопасности организации на соответствие международным стандартам, рекомендациям и практикам ИБ.

2. Анализ конфигураций ИС

✓ Анализ конфигураций оборудования, настроек ИС и сервисов.

3. Инструментальный аудит

✓ Выявление уязвимостей программного и аппаратного обеспечения систем средствами автоматизированной проверки.

4. Тест на проникновение

✓ Анализ уязвимостей и моделирование атак злоумышленника.

Этапы проведения аудита ИБ

1. Планирование
   - ✓ Определение целей и средств аудита;
   - ✓ Формирование задания на аудит, определение критериев для оценки ИБ.

2. Сбор данных, проведение проверки
   - ✓ Анализ документации по вопросам ИБ, изучение ИТ и ИБ инфраструктуры (в том числе программно-технических средств обеспечения ИБ), анализ организационных мер обеспечения ИБ, инструментальная проверка, моделирование атак злоумышленника.

3. Анализ и обработка результатов
   - ✓ Обобщение результатов, анализ угроз и оценка рисков ИБ;
   - ✓ Оценка возможного ущерба;
   - ✓ Формирование отчета.

4. Повышение эффективности ИБ
   - ✓ Разработка мер по устранению недостатков или усовершенствованию ИБ;
   - ✓ Составление план-графика проведения работ. Проведение мероприятий;
   - ✓ Анализ итогов и планирование нового аудита ИБ.

Главная задача информационной системы – обеспечение пользователей информацией. Главная задача аудита ИБ – проверка и контроль соблюдения процессов и требований по безопасности в информационной системе. При этом не стоит забывать, что наиболее эффективным является комплексный подход к аудиту – проверки требований к техническим и программным средствам защиты недостаточно. Не менее важной составляющей является проверка достаточности организационных мер защиты. Информационная безопасность должна быть обеспечена как на техническом, так и на организационно-административном уровне.

Спасибо за внимание