Чернов Алексей Евгеньевич, Студент,
Финансовый университет при Правительстве РФ
Москва
Chernov Alexey Evgenyevich, Student

Научный руководитель:
Резниченко Сергей Анатольевич, к.тех.н., доцент,
доцент кафедры информационной безопасности
Финансового университета при Правительстве РФ
Финансовый университет при Правительстве РФ
Москва

АНАЛИЗ МЕТОДОВ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ANALYSIS OF INFORMATION SECURITY AUDIT METHODS

Аннотация: Аудит информационной безопасности – это процесс оценки уровня защищенности ИТ-инфраструктуры, проводимый на основании целевых показателей информационной безопасности. В данной статье будут рассмотрены методы аудита информационной безопасности.

Abstract: Information security audit is a process of assessing the level of security of the IT infrastructure, conducted on the basis of information security targets. This article will discuss information security audit methods.

Ключевые слова: Аудит, информация, безопасность, методы, анализ.

Keywords: Audit, information, security, methods, analysis.

В ходе аудита обычно проверяют организационно-распорядительные документы (приказы, распоряжения и т.п.), относящиеся к обеспечению информационной безопасности, настройки межсетевых экранов и систем защиты периметра сети, журналы безопасности сетевых серверов и сетевого оборудования и многое другое в зависимости от поставленных перед аудиторами целей. Проведение аудита информационной безопасности позволяет понять, насколько ИТ-инфраструктура компании защищена от внешних угроз и несанкционированного доступа, а также при необходимости – насколько её уровень информационной безопасности соответствует требованиям регуляторов, отраслевых или международных стандартов.

Проведение аудита безопасности информационных систем может потребоваться в различных ситуациях:

- Перед выбором средства защиты информации – чтобы сформулировать релевантные требования к функциональным возможностям продукта и выявить слабые места сетевого периметра, а также оценить текущий уровень безопасности компании. Результаты аудита помогут с цифрами в руках обосновать выбор того или иного средства защиты информации и аргументировать саму необходимость покупки средства.
- После внедрения приобретённого технического решения – чтобы оценить эффективность защиты и при необходимости скорректировать её.
- Аудит информационной безопасности потребуется для проведения сертификации на соответствие стандартам – PCI DSS, СТО БР ИББ, GDPR, ГОСТ Р 57580.1-2017, ISO/IEC 27001:2005 и другим.
- Аудит информационной безопасности предприятия поможет разобраться в существующих средствах защиты и привести всё к единому стандарту.

• Проведение ИБ-аудита необходимо, чтобы расследовать инцидент, связанный с кибератакой, утечкой данных или другим нарушением информационной безопасности.

Цели проведения аудита информационной безопасности:

В зависимости от перечисленных ситуаций цели аудита ИБ условно можно разделить на внутренние и внешние.

Внутренние:

• расследование ИБ-инцидентов,

• определение уровня осведомлённости пользователей в области информационной безопасности и разработка плана обучения и тренировки их навыкам безопасного поведения,

• разработка или корректировка нормативных документов в сфере защиты информации,

• разработка требований к уровню защищенности ИТ-инфраструктуры для последующей реализации комплекса мер сотрудниками ИТ-подразделения.

Внешние:

• определение текущего уровня защищённости компании,

• формирование перечня рисков, которые могут угрожать безопасности,

• выявление слабых мест в защите сетевого периметра,

• оценка соответствия компании ИБ-стандартам,

• разработка рекомендаций по внедрению новых и доработке имеющихся средств защиты.

Методы аудита информационной безопасности:

1. Активный или инструментальный аудит (пентест):

Этот метод имитирует действия злоумышленников в ходе реальных кибератак. Например, аудиторы информационной безопасности могут попытаться взломать интернет-магазин компании или систему онлайн-банкинга, если проводится исследование сети кредитной организации. Также проверяются на уязвимости системы управления контентом, которые используются на сайте заказчика (Битрикс, Вордпресс, Друпал и т.п.)

В ходе активного аудита информационной безопасности может быть проведено тестирование сетевого периметра, которое выявляет открытые сетевые порты и уязвимые сетевые сервисы, а также предприняты попытки с их помощью проникнуть в сеть компании.

В ходе инструментального аудита информационной безопасности может быть проведён стресс-тест корпоративной сети, имитирующий реальную атаку на отказ в обслуживании. Он даст понимание того, что будет происходить в случае реального нападения, и разработать стратегию проактивной защиты от DDoS.

2. Экспертный аудит информационной безопасности:

Проводится экспертами-аудиторами, которые изучают состояние информационной безопасности компании и сравнивают его с эталонным описанием, в качестве которого может выступать, например, перечень требований, выдвинутых руководством компании, либо представление об идеальной системе безопасности в соответствии с мнением экспертов.

3. Аудит на соответствие стандартам:

Проведение такого аудита ИБ сводится к сравнению характеристик информационной безопасности компании с требованиями конкретных стандартов, например, PCI DSS или ГОСТ Р ИСО/МЭК 27001. По результатам такого аудита составляется официальный отчёт, содержащий:

• уровень соответствия безопасности информационной системы компании выбранному стандарту;

• замечания и несоответствия, отсортированные по категориям;

• рекомендации аудиторов по приведению системы обеспечения ИБ в соответствие с требованиями стандарта.

4. Комплексный аудит информационной безопасности:

Может включать в себя любые комбинации перечисленных методов аудита.

Этапы проведения аудита информационной безопасности:

1. Разработка регламента проведения аудита ИБ

На этом этапе определяется, что и каким образом будет проверяться, назначается состав рабочих групп и ответственные. Обычно в регламент включают:

- список информационных активов,
- состав рабочей группы и перечень ответственных,
- модель угроз информационной безопасности и категории нарушителей,
- расписание проведения инструментального аудита информационной безопасности и стресс-тестирования сетевого периметра.

2. Сбор исходных данных

На этом этапе команда аудиторов изучает сеть компании и собирает информацию в соответствии с регламентом. Действия аудиторов не ограничиваются исключительно запуском программ и могут включать опрос сотрудников и анализ нормативных документов.

3. Анализ собранных данных

Команда аудиторов обобщает собранные сведения и формирует аудиторское заключение, в котором описывает состояние сети компании. В зависимости от поставленных задач и полученных результатов аудиторы могут также разработать рекомендации по повышению уровня защищённости сетевой инфраструктуры.

Список литературы:

1. международный стандарт ISO/IEC 27001:2005
2. стандарт COBIT
3. стандарт PCI DSS