ДиалогНаука

Практика проведения аудитов информационной безопасности на крупных предприятиях

Виктор Сердюк, к.т.н., CISSP
Генеральный директор
ЗАО «ДиалогНаука»

ДиалогНаука

Когда проводить аудит безопасности?

ЦЕЛЬ: Получить независимую и объективную оценку текущего уровня информационной безопасности

- Перед внедрением комплексной системы безопасности для подготовки ТЗ на её разработку и создание
- После внедрения комплексной системы безопасности для оценки уровня её эффективности
- Для приведения системы информационной безопасности в соответствие установленным требованиям (международные стандарты или требования российского законодательства)
- Для систематизации и упорядочивания существующих мер защиты информации
- Для проверки эффективности работы подразделений компании, ответственных за обеспечение ИБ
- Для обоснования инвестиций в направление информационной безопасности

ДиалогНаука

Конечные потребители результатов аудита

Внутренние пользователи:

- Руководство компании
- Подразделение информационной безопасности
- Служба безопасности
- Подразделение автоматизации предприятия
- Служба внутреннего контроля/аудита

Внешние пользователи:

- Акционеры компании
- Регулирующие органы
- Клиенты компании

ДиалогНаука

Внешний и внутренний аудит безопасности

Внутренний аудит:

- Проводится внутренними подразделениями компании (отделом ИБ, отделом ИТ или службой внутреннего контроля)
- Рекомендуется проводить не реже 1 раза в квартал

Внешний аудит:

- Проводится с привлечением внешней организации
- Рекомендуется проводить не реже 1 раза в год

ДиалогНаука

Варианты проведения аудита

- Тест на проникновение (penetration testing)
- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта PCI DSS
- Оценка соответствия стандарту Банка России
- Оценка соответствия требованиям Федерального закона «О персональных данных»
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка и анализ рисков информационной безопасности
- Комплексный аудит информационной безопасности

ДиалОгНаука

Основные этапы работ

- Заключение соглашения о неразглашении (NDA)
- Разработка регламента, устанавливающего порядок и рамки проведения работ
- Сбор исходной информации об автоматизированной системе компании
- Анализ собранной информации с целью выявления технологических, эксплуатационных уязвимостей, а также недостатков организационно-правового обеспечения
- Подготовка отчётных материалов
- Презентация и защита результатов проекта

ДиалогНаука

Структура регламента

- Состав рабочих групп от Исполнителя и Заказчика, участвующих в процессе проведения аудита
- Описание ролей участников рабочей группы и зоны их ответственности
- Порядок обмена информацией по проекту
- Порядок проведения совещаний по проекту

ДиалогНаука

Состав исходных данных

- Информация об организационной структуре компании
- Организационно-распорядительная и нормативно-методическая документация по вопросам информационной безопасности
- Информация об ИТ-активах, влияющих на бизнес-процессы компании
- Информация об аппаратном, общесистемном и прикладном обеспечении хостов
- Информация о средствах защиты, установленных в компании
- Информация о топологии автоматизированной системы компании

ДиалОгНаука

Методы сбора исходных данных

- Предоставление опросных листов по определённой тематике, самостоятельно заполняемых сотрудниками Заказчика
- Интервьюирование сотрудников Заказчика, обладающих необходимой информацией
- Анализ существующей организационно-технической документации, используемой Заказчиком
- Использование специализированных программных средств

ДиалогНаука

Критерии оценки безопасности

- Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности
- Требования действующего российского законодательства (РД ФСТЭК, СТР-К, ГОСТы)
- Требования отраслевых стандартов (СТО БР ИББС 1.0, базовый уровень информационной безопасности операторов связи)
- Рекомендации международных стандартов (ISO 17799, OCTAVE)
- Рекомендации компаний-производителей программного и аппаратного обеспечения (Microsoft, Oracle, Cisco и т. д.)

ДиалогНаука

Структура итогового отчёта

- Границы проведения аудита безопасности
- Описание АС Заказчика
- Методы и средства проведения аудита
- Результаты инструментального анализа защищенности
- Результаты оценки соответствия требованиям международного стандарта ISO27001
- Результаты оценки рисков безопасности
- Результаты внешнего обследования (penetration testing)
- Рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности
- План мероприятий по реализации рекомендаций в области информационной безопасности

ДиалОгНаука

Продолжительность этапов

Этап	Занимаемое время, %
Подготовительные работы (подписание NDA, подготовка регламента работ и т.д.)	10
Сбор необходимой информации (анкетирование, интервьюирование)	15
Анализ действующей нормативной документации	10
Инструментальное обследование	20
Анализ полученных данных	20
Подготовка отчетных материалов	20
Презентация и защита отчета	5

ДиалогНаука

Преимущества аудита безопасности

- Лучшее понимание руководством и сотрудниками целей, задач, проблем организации в области ИБ
- Осознание ценности информационных ресурсов
- Надлежащее документирование процедур и моделей ИС с позиции ИБ
- Принятие ответственности за остаточные риски

ДиалогНаука

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: vas@DialogNauka.ru