Практические аспекты проведения аудита информационной безопасности

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

ДиалогНаука

О компании «ДиалогНаука»

- Создано в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest
- В настоящее время ДиалогНаука позиционируется как системный интегратор в области информационной безопасности

Членство в ассоциациях

- Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ)
- Ассоциации документальной электросвязи (АДЭ)
- Сообщество ABISS (Association of Banking Information Security Standards)
- Сертифицированный партнер BSI Management Systems
- Ассоциация системной интеграции и разработки информационных и управляющих систем «СИРИУС»

Основные направления деятельности

- проведение аудита информационной безопасности
- разработка системы управления безопасностью в соответствии с ISO 27001
- разработка Политик информационной безопасности и других нормативных документов, регламентирующих вопросы защиты информации
- проектирование, разработка и внедрение комплексных систем обеспечения информационной безопасности
- поставка программного и аппаратного обеспечения в области защиты информации
- техническое сопровождение поставляемых решений и продуктов

Лицензии компании «ДиалогНаука»

- Лицензия ФСТЭК на деятельность по разработке и (или) производству средств защиты конфиденциальной информации. Серия КИ 0029. Номер 001412. Регистрационный номер 0284 от 20 июня 2006 г.
- Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации. Серия КИ 0029. Номер 001411. Регистрационный номер 0486 от 20 июня 2006 г.
- Лицензия ФСБ на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем. Регистрационный номер 3237 П от 15 июня 2006 г.
- Лицензия ФСБ на осуществление технического обслуживания шифровальных (криптографических) средств. Регистрационный номер 3238 Х от 15 июня 2006 г.
- Лицензия ФСБ на распространение шифровальных (криптографических) средств. Регистрационный номер 3239 П от 15 июня 2006 г.
- Лицензия ФСБ на предоставления услуг в области шифрования информации. Регистрационный номер 3240 У от 15 июня 2006 г.

Услуги по проведению аудита информационной 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 обоснования инвестиций в направление информационной безопасности

Конечные потребители результатов аудита

Внутренние пользователи:

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

Внешние пользователи:

- Акционеры компании
- Регулирующие органы
- Страховые компании
- Клиенты компании

Варианты проведения аудита

- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности Интернет-систем (penetration testing)
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001 (ISO17799)
- Оценка соответствия стандарту Банка России
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка и анализ рисков информационной безопасности
- Комплексный аудит информационной безопасности

Инструментальный анализ защищенности

- Анализ средств защиты информации
- Анализ безопасности сетевой инфраструктуры
- Анализ безопасности общесистемного программного обеспечения
- Анализ безопасности прикладного программного обеспечения

Penetration Testing

Исходные данные

- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

Собираемая информация

- Топология сети
- Используемые ОС и версии ПО
- Запущенные сервисы
- Открытые порты, конфигурация и т.д.

! С помощью этой информации можно успешно осуществить атаку на АС с целью проникновения

Аудит СУИБ по стандарту ISO 27001

1. **Политика безопасности**
2. **Организационные меры безопасности**
3. **Учет и категорирование информационных ресурсов**
4. **Кадровые аспекты ИБ**
5. **Физическая защита информационных ресурсов**
6. **Управление технологическим процессом**
7. **Управление доступом**
8. **Закупка, разработка и сопровождение компонент ИС**
9. **Управление инцидентами в области информационной безопасности**
10. **Обеспечение непрерывности работы и восстановления**
11. **Соответствие нормативным и руководящим документам**

Аудит наличия конфиденциальной информации

- Аудит наличия конфиденциальной информации представляет собой независимый и документированный процесс поиска и анализа конфиденциальных сведений в сети Интернет при помощи средств конкурентной разведки
- Поиск информации осуществляется: на форумах, в блогах, в электронных СМИ, в гостевых книгах, на досках объявлений, в дневниках, конференциях и т.д.
- По результатам проведённого поиска проводится выдача «оценочной» информации в виде отчёта. Отчёт содержит следующую информацию:
  1. область поиска (где осуществлялся поиск);
  2. найденная конфиденциальная информация;
  3. где найдена конфиденциальная информация;
  4. рекомендации по устранению (удалению) найденной конфиденциальной информации в Интернете

Оценка и анализ рисков безопасности

- Идентификация информационных активов
- Формирование каталога возможных угроз безопасности
- Оценка уровня вероятности реализации угроз безопасности
- Оценка уровня ущерба, который может быть нанесен в случае реализации угрозы
- Определение интегрального значения риска безопасности
- Анализ рисков безопасности

Комплексный аудит безопасности

- Учитывает организационные и технологические аспекты защищённости автоматизированной системы компании
- Предполагает проведение оценки рисков информационной безопасности
- Учитывает требования российского законодательства и рекомендации международных стандартов
- При необходимости может включать в себя инструментальное обследование организации

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

Дальнейшие действия по результатам

Результаты аудита являются **основой** для проведения дальнейших работ по повышению информационной безопасности:

- ★ Совершенствование организационно-правового обеспечения Заказчика (разработка Политики безопасности, должностных инструкций, регламентов и т.д.)
- ★ Проектирование, разработка, внедрение и сопровождение систем защиты, устраняющих уязвимости, выявленные в процессе проведения аудита безопасности
- ★ Обучение персонала Заказчика

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

Спасибо за внимание!

ЗАО «ДиалогНаука»

Тел.: (495) 980-67-76
Факс: (495) 980-67-75

vas@dialognauka.ru
www.dialognauka.ru

ДиалогНаука