Технологии и продукты Microsoft в обеспечении ИБ

Лекция 1. Введение

Цели

- Изучить фундаментальные свойства оцифрованной информации
- Выявить причины появления киберпреступности
- Рассмотреть примеры нерешенных проблем
- Понять причины, по которым совершенная защита информации невозможна
- Оценить роль криптографии в обеспечении информационной безопасности

Эпиграф

«Все любят разгадывать других, но никто не любит быть разгаданным»

Франсуа VI де Ларошфуко

Рост количества атак

137529
73359
52658
21756
9859
2573
1334
252
6

Инсайдеры
Распределенные атаки
Атаки типа «SQL Injection»
Атаки типа «format string»
Stealth - сканирование
Атаки типа «переполнение буфера»
Атаки на общедоступные Web-сервисы
Атаки типа «отказ в обслуживании»
Автоматизированное сканирование
Перехват данных
Подмена субъекта соединения
«Троянские кони»
Перебор паролей
Вирусы

1980 г. 1985 г. 1990 г. 1995 г. 2000 г. 2005 г. 2008 г.

Что защищать?

- **Бизнес-процессы компании**
- **Информация** (коммерческая тайна, персональные данные, служебная тайна, банковская тайна и др.)
- **Прикладное программное обеспечение** (АБС, почтовые системы, комплексы ERP и др.)
- **Общесистемное программное обеспечение** (операционные системы, СУБД и др.)
- **Аппаратное обеспечение** (серверы, рабочие станции, жёсткие диски, съёмные носители и др.)
- **Телекоммуникационное обеспечение** (каналы связи, коммутаторы, маршрутизаторы и др.)

Безопасность и финансовый хаос

- Человеческий фактор
  - Злые инсайдеры
  - Уволенные по сокращению сотрудники
- Потеря оборудования
  - Кража ноутбуков
  - Кража систем хранения
- **Обеспечение ИБ!**

Задача CIO : как выбрать подходящую стратегию обеспечения информационной безопасности *в условиях ограниченного бюджета и растущих рисков НСД к информационным активам?*

Тенденции рынка ИБ

- Появление нормативной базы в области информационной безопасности
- Изменение приоритетов
- Появление новых решений, ориентированных на противодействие внутренним угрозам безопасности

Базовые определения

- **Инсайдер** - сотрудник компании, являющийся нарушителем, который может иметь легальный доступ к конфиденциальной информации
- В результате действий инсайдера конфиденциальная информация может попасть в посторонние руки
- Действия могут быть как умышленные, так и совершенные по неосторожности

Инциденты в России

- База данных проводок ЦБ РФ
- База данных абонентов МТС и МГТС
- Базы данных ГУВД, ГИБДД, ОВИР
- База данных Налоговой Службы
- База данных Пенсионного Фонда
- База данных Таможенной Службы
- База данных кредитных бюро

Каналы утечки информации

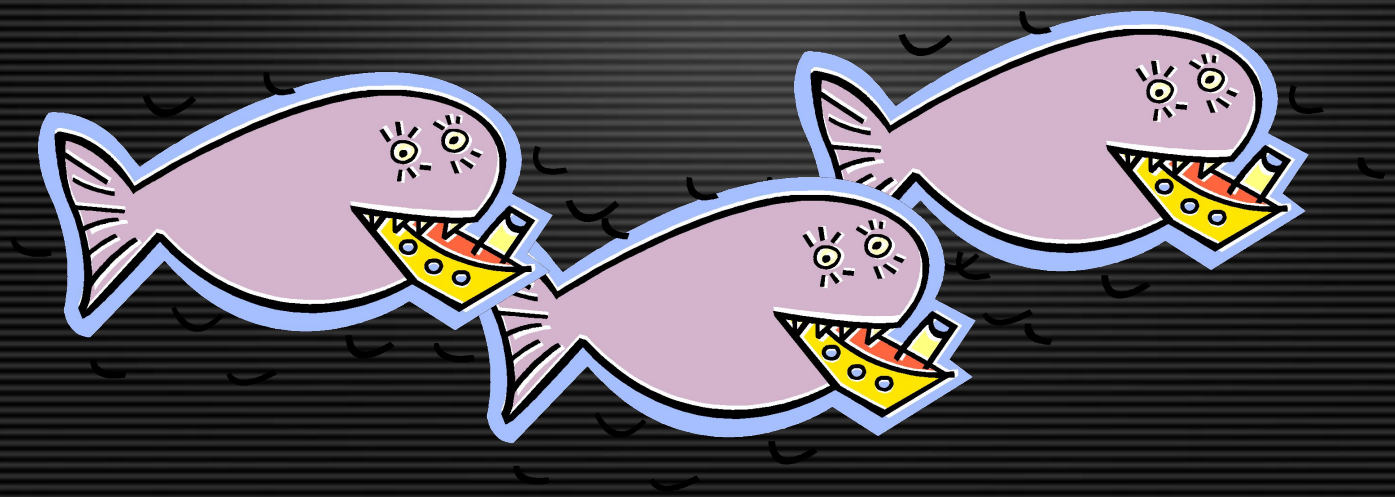
- Мобильные накопители (USB, CD, DVD)
- Ноутбуки, мобильные устройства
- Электронная почта
- Интернет (форумы, веб-почта и т.д.)
- Печатающие устройства

Подходы к моделированию угроз безопасности

- CIA
- Гексада Паркера
- 5A
- STRIDE

3 кита информационной безопасности

1. Конфиденциальность
2. Целостность
3. Доступность



Гексада Паркера

1. Конфиденциальность
2. Целостность
3. Доступность
4. Управляемость
5. Подлинность
6. Полезность

5A

- Authentication (who are you)
- Authorization (what are you allowed to do)
- Availability (is the data accessible)
- Authenticity (is the data intact)
- Admissibility (trustworthiness)

Модель угроз информационной безопасности STRIDE

Spoofing
Притворство

Tampering
Изменение

Repudiation
Отказ от ответственности

Information Disclosure
Утечка данных

Denial of Service
Отказ в обслуживании

Elevation of Privilege
Захват привилегий

Экскурс в историю

- Неприкосновенность частной жизни
- Управление идентичностью
- Проблема защиты авторского права
- Новое преступление XX века

Оцифрованная информация

- Отчуждаемость
- Воспроизводимость
- Неуничтожимость
- Возможность быстрого поиска

Новые технологии

- Портативные и дешевые устройства хранения с высокой плотностью записи
- Распространение Wi-fi
- Социальные сети: поколение Y
- Новое поколение хакеров
- RFID
- Все передается через цифровые каналы

3 тенденции последних десятилетий

1. Возможность получения доступа из любого компьютера, подключенного к глобальной сети
2. Низкая стоимость сенсорных устройств
3. Тотальная оцифровка информации

3 тенденции последних десятилетий

1. **Возможность получения доступа из любого компьютера, подключенного к глобальной сети**
2. **Низкая стоимость сенсорных устройств**
3. **Тотальная оцифровка информации**

3 тенденции последних десятилетий

1. Возможность получения доступа из любого компьютера, подключенного к глобальной сети
2. Низкая стоимость сенсорных устройств
3. Тотальная оцифровка информации

3 тенденции последних десятилетий

1. Возможность получения доступа из любого компьютера, подключенного к глобальной сети
2. Низкая стоимость сенсорных устройств
3. Тотальная оцифровка информации

Почему совершенная защита невозможна

- Взгляд на обеспечение ИБ как дополнительную функцию
- Нестабильность программного обеспечения
- Компьютер – система из множества компонентов, поставляемых различными вендорами
- Человеческий фактор

Уязвимости

Вызов нового тысячелетия

- Необратимый процесс развития технологий
- Регулируемость деятельности в сети Интернет
- Терроризм
- ВЧЕРА: Защита материальных ценностей
- СЕГОДНЯ и ЗАВТРА: Защита нематериальных ценностей

Примеры нерешенных проблем

- Истинность данных
- Актуальность данных
- Доверие к результатам работы поисковых систем
- Удаление персональных данных из Интернета

Криптография

- Свобода слова ☺
- Защита интеллектуальной собственности
- Шифрование
- Управление идентичностью
- Цифровая подпись кода
- Доверенная платформа
- Разграничение доступа
- Построение VPN
- Гарантированное уничтожение информации
- Защита от физической кражи носителя информации

Использованные источники

- **Сердюк В.А.** Комплексный подход к защите компании от угроз информационной безопасности // Презентация, ДиалогНаука, 2008
- **Сердюк В.А.** Современные методы и средства защиты от внутренних нарушителей // Презентация, ДиалогНаука, 2008
- **Сердюк В.А.** Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007.
- **Holtzman D.** PRIVACY LOST: How Technology Affects Privacy //Interop'2008 Moscow
- **Holtzman D.** Privacy Lost: How Technology is Endangering Your Privacy. Josey-Bass, 2006 , 352 p.


Спасибо за внимание!
Вопросы?