



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





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 СІО : 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



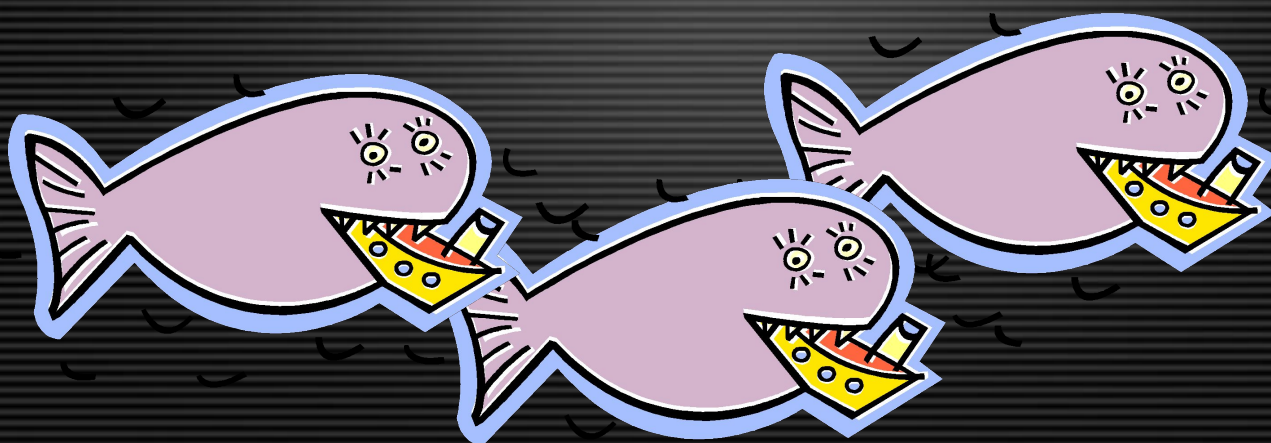
Конфиденциальность



Целостность



Доступность





Гексада Паркера



Конфиденциальность



Целостность



Доступность



Управляемость



Подлинность



Полезность

R

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



S
T
R
I
D
E

- **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



Возможность получения доступа из любого компьютера, подключенного к глобальной сети



Низкая стоимость сенсорных устройств



Тотальная оцифровка информации



3 тенденции последних десятилетий



Возможность получения доступа из любого компьютера, подключенного к глобальной сети



Низкая стоимость сенсорных устройств



Тотальная оцифровка информации



3 тенденции последних десятилетий



Возможность получения доступа из любого компьютера, подключенного к глобальной сети



Низкая стоимость сенсорных устройств



Тотальная оцифровка информации



3 тенденции последних десятилетий



Возможность получения доступа из любого компьютера, подключенного к глобальной сети



Низкая стоимость сенсорных устройств



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

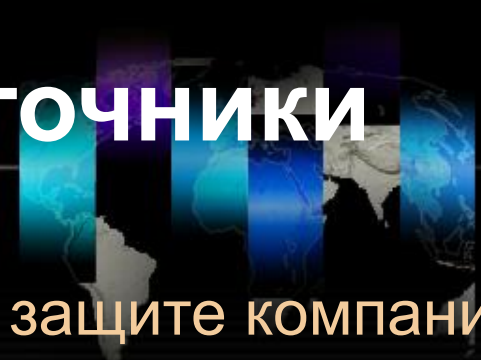
Криптография



- 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.

A world map is shown in the background, overlaid with four vertical bands of color: red/pink, orange, cyan, and blue. The map is rendered in a light, semi-transparent style.

Спасибо за внимание!

Вопросы?

