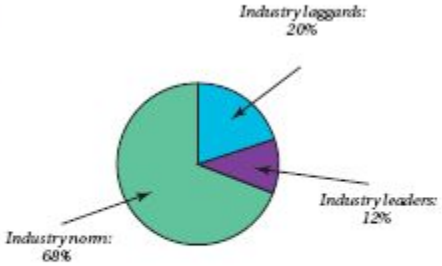
Лекция 1

Актуальность задачи обеспечения информационной безопасности данных

Размер проблемы потери данных

	Performance classification	Confirmed annual losses of sensitive data
●	Industry laggards	22
■	Industry norm	6
◆	Industry leaders	Less than 2

N: 201



Population experiencing losses

Figure 1: Sensitive data loss results
Source: IT Policy Compliance Group, 2007

Организации различаются по частоте возникновения проблемы потери данных.

- В 10-12% организаций возникает чувствительная потеря данных менее 2 раз в год;
- В 68% организаций возникает чувствительная потеря данных 6 раз в год;
- У 20% организаций возникают чувствительная потери данных 22 и более раз в год.

Наиболее ценные данные

- Клиетские
- Финансовые
- Корпоративные
- Работников
- Безопасность IT

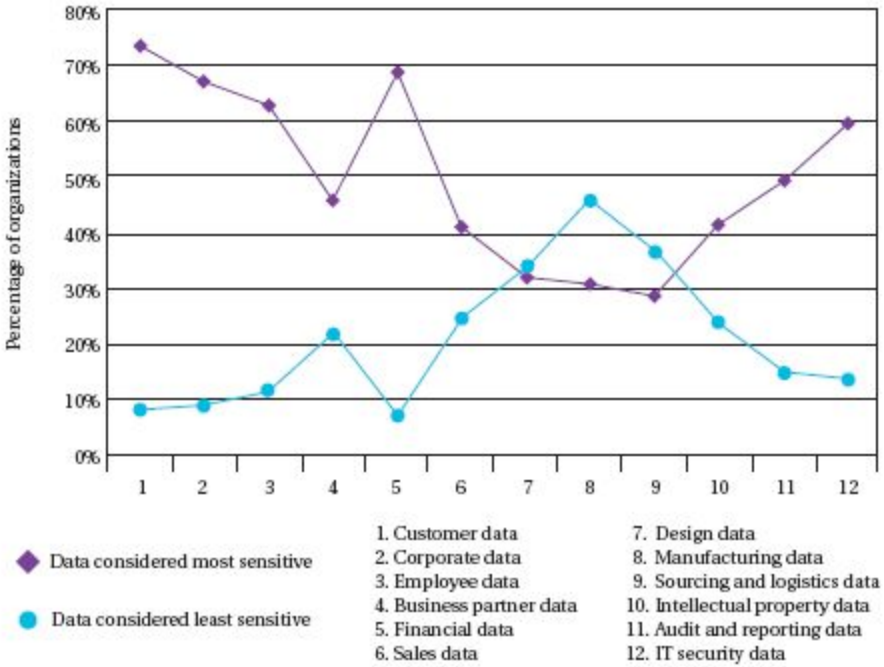
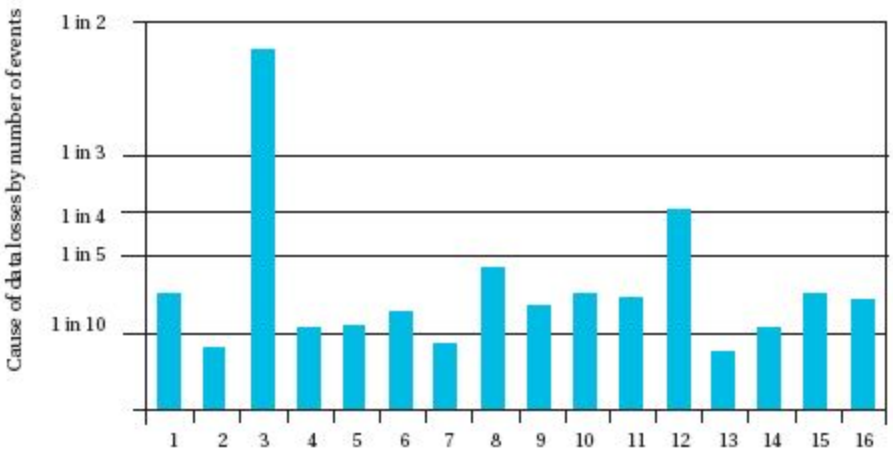


Figure 2: Least and most sensitive data
Source: IT Policy Compliance Group, 2007

Причины потерь данных

- Ошибки пользователей
- Нарушения политики безопасности
- Атаки из интернет, взломы и т.д.



1. Lost or stolen laptops
2. Improperly disposed of computer equipment
3. User errors
4. Improperly transferred backup media
5. Inappropriate access to IT resources
6. Insufficient controls on business procedures
7. Insufficient controls on IT procedures
8. Internet threats, attacks and hacks
9. Employee manipulation and malfeasance
10. Accident and damage to computing equipment
11. Inappropriate usage of IT resources
12. Violation of policies
13. Unauthorized access to IT resourced
14. Insufficient auditing, monitoring and reporting
15. IT vulnerabilities
16. Insufficient IT controls

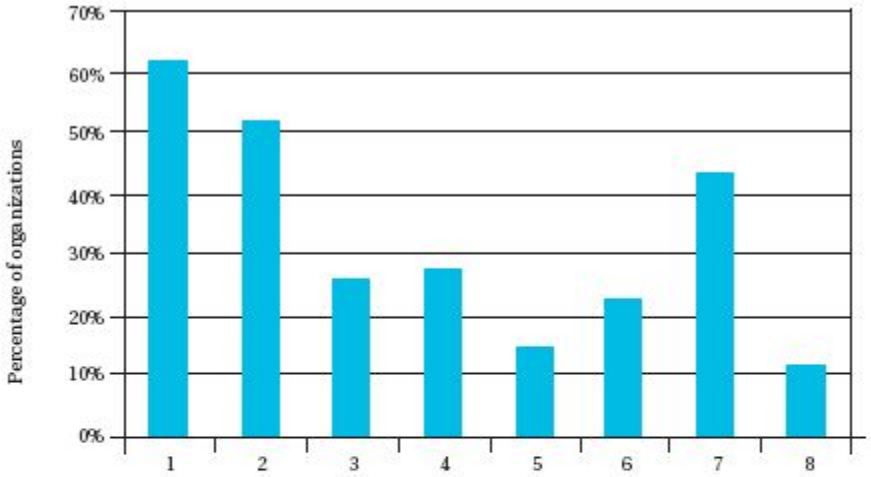
N: 201

Figure 5: Leading causes of data loss

Source: IT Policy Compliance Group, 2007

Источники угроз потери данных

- PC, laptop и мобильные устройства
- E-mail и другие электронные каналы
- Приложения для работы с БД



1. Data residing on PCs, laptops and other mobile devices
2. Data leaking through Email, Instant Messaging and other electronic channels
3. Data residing in centralized storage facilities and devices
4. Data transferred to backup and archive sites
5. Data that has been off-shored or outsourced
6. Data in the hands of business partners and suppliers
7. Data accessible through applications and databases
8. Data in the hands of sales channel partners

Figure 6: Primary conduits for data loss
Source: IT Policy Compliance Group, 2007

Финансовый ущерб от потери данных

- Средняя величина ущерба от потери данных включает:
- Потеря до 8% клиентов
- Соразмерное снижение дохода на 8%
- До 100$ на карточку клиента за оповещение и восстановление удаленных, украденных или уничтоженных данных

Меры по снижению рисков потери данных

Включают:

- регистрация потерь данных;
- выделение критичных данных;
- модификация политик и процедур;
- защита всех данных;
- учет всех возможных каналов потерь данных;
- развитие IT служб;
- еженедельный мониторинг процедур

Преимущества бизнеса от лучшей защиты данных

- Гарантия сохранения бренда и имиджа;
- Снижение проблемы электронных хищений;
- Повышение лояльности клиентов;
- Снижение оттока клиентов;
- Снижение частоты уведомлений и необходимости восстановления данных

Оплата труда специалистов по защите данных

Средний уровень заработной платы, июль 2002 - июль 2003 г.

Позиция	Москва (USD)	Санкт-Петербург (USD)
Администратор баз данных	1000-2500	800-1500
Программист	800-1200	800-1000
Инженер отдела технической поддержки	500-1800	500-1000
Консультант по внедрению SAP R/3	1500-10000	1000-2500
Системный/Сетевой администратор	800-2000	800-1200
Бизнес аналитик	2500-3500	1000-2500
ИТ Менеджер	1500-2500	1500-2500

Epic fail I

24 августа 2010г.

ФСО проверяет информацию о взломе своего почтового сервера

Федеральная служба охраны занялась проверкой информации о взломе сервера службы неизвестными хакерами. Как сообщили в пресс-центре ФСО, официального комментария по этому поводу ведомство пока не дает.

Напомним, что сегодня в ряде СМИ появилась информация о том, что накануне неизвестные хакеры взломали почтовый сервер ФСО. Отмечается, что утечки информации государственной важности не произошло.

Между тем, отмечают журналисты, любой желающий мог получить доступ к почтовому серверу ФСО в течение нескольких часов. По данным СМИ, это стало возможным благодаря взлому системы "Дозор", которая охраняет сервер.

Epic fail II

13.08.10 14:45

Биометрический потоп

Interfax-Russia.ru - Вода из кондиционеров залила серверы в НИИ, изготовляющем 10-летние российские биометрические загранпаспорта. С выдачей документов возникли временные задержки.

Прямые и косвенные последствия аномальной жары в России выражаются в самых различных, порой довольно курьезных ЧП. Так, на днях стало известно, что на ФГУП НИИ "Восход", где изготовляют биометрические загранпаспорта, в результате поломки кондиционеров затопило серверы, на которых хранились файлы Федеральной миграционной службы (ФМС) с десятками тысяч заявок россиян на получение документов.

Литература

1. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий»
2. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации
3. С. Н. *Смирнов*. *Безопасность* систем *баз данных*:Гелиос АРВ,2007.
4. А. М. *Поляков*. *Безопасность Oracle глазами аудитора*: нападение и защита. - М.: ДМК Пресс, 2010.
5. Конноли, Томас др. Базы данных: проектирование, реализация и сопровождение. Теория и практика, 2-е изд. – М.: Издательский дом “Вильямс”, 2000.