ЗАЩИТА ИНФОРМАЦИИ

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, подделки, несанкционированного копирования, блокирования информации и т.п.

Основные причины повреждений электронной информации:

- Неумышленная ошибка человека – 52%
- Умышленные действия человека – 10%
- Отказ техники – 10%
- Повреждения в результате пожара – 15%
- Повреждения водой – 10%
- Прочие причины – 3%

Умышленные действия:

- 81% – текущий кадровый состав учреждений
- 13% – совершенно посторонние люди
- 6% – бывшие работники этих же учреждений

Информацию защищают от:

- Физической утраты;
- Нежелательного изменения, удаления, порчи пользователем;
- Удаления, изменения, порчи в результате использования бракованного программного обеспечения;
- Порчи, изменения, удаления компьютерными вирусами и подобными им программами;
- Несанкционированного изменения, просмотра, удаления посторонними лицами

Физическая утрата

- Выход из строя (износа, поломки) носителя информации
- Кража компьютера и/или носителя информации
- Нарушение правил эксплуатации вычислительной техники и носителей информации
- Стихийное бедствие (пожар, наводнение и т.п.)

Меры по предотвращению физической утраты информации:

- Резервное копирование ценной информации;
- Хранение и установка вычислительной техники (и носителей информации) в охраняемых и защищенных от внешних воздействий помещениях;
- Строгое соблюдение правил хранения и эксплуатации вычислительной техники и носителей информации

Нежелательное удаление, изменение, порча информации пользователем

- Невнимательность при работе с компьютером
- Случайное нажатие клавиш

Для предотвращения нежелательного удаления, изменения, порчи информации пользователем следует:

- Быть внимательным при работе с компьютером;
- По возможности исключить случайное нажатие клавиш;
- Создавать резервные копии важных данных;
- Настроить используемое программное обеспечение таким образом, чтобы перед удалением, внесением изменений в информацию обязательно выводился запрос на подтверждение

Утрата информации в результате использования плохого программного обеспечения

- использование бракованного программного обеспечения и программ, содержащих ошибки и недоработки

СЛЕДУЕТ:

- создавать резервные копии ценной информации
- использовать лицензионное программное обеспечение
- использовать "проверенные временем" программы

Предотвращение воздействия со стороны компьютерных вирусов

- Антивирусные программы
- Аппаратные средства защиты
- Сочетание программных и аппаратных методов защиты

Предотвращение доступа к информации посторонних лиц

- Использование различных паролей и кодов доступа
- Установка программного обеспечения, предоставляющего широкие возможности по защите информации

Средства защиты информации

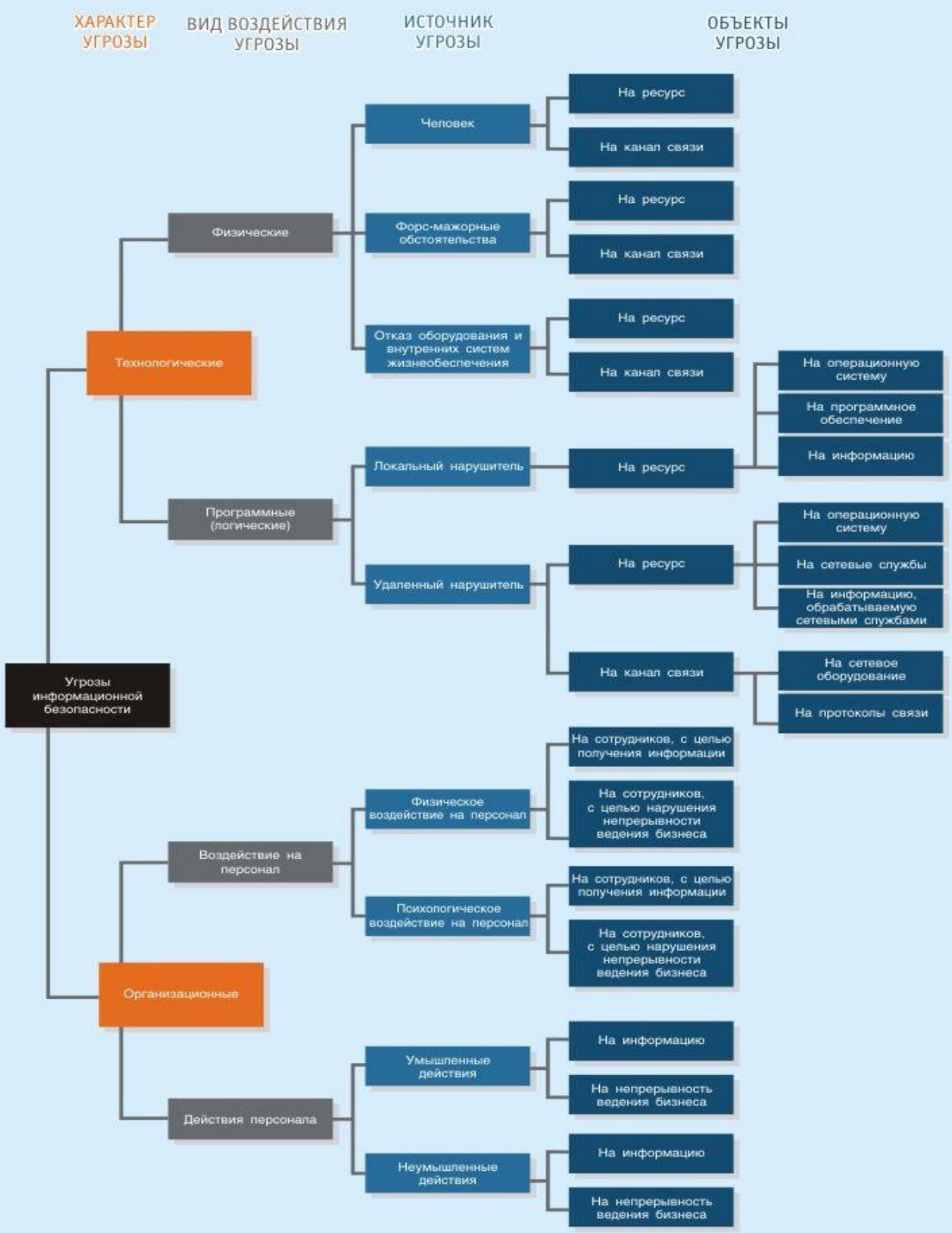
- Технические (аппаратные) средства.
- Программные средства
- Смешанные аппаратно-программные средства
- Организационные средства

ПРОБЛЕМЫ ЗАЩИТЫ ЛОКАЛЬНЫХ СЕТЕЙ

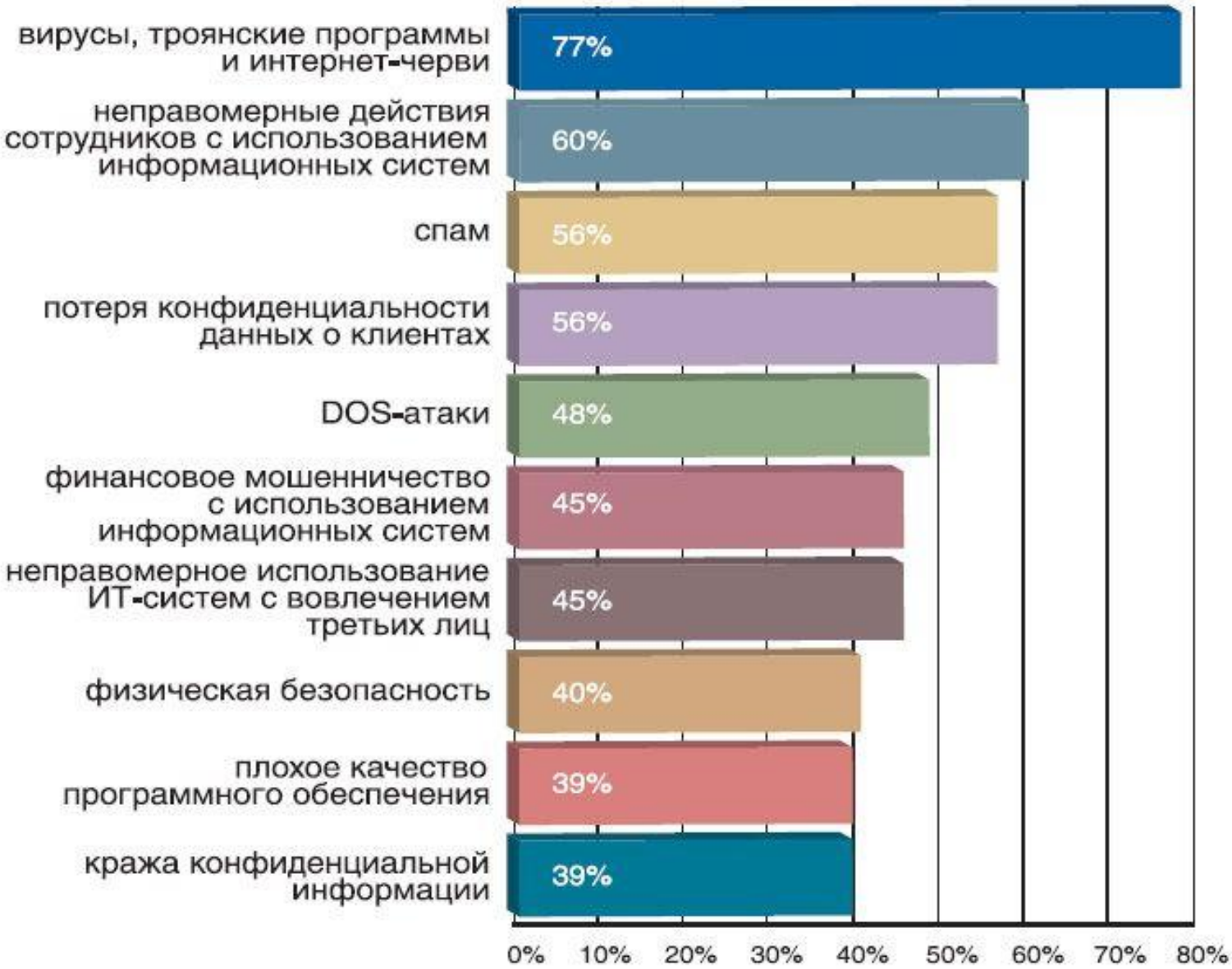
- Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц
- Значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть
- Неидеальны встроенные средства защиты информации даже в таких известных и "мощных" сетевых ОС, как Windows NT или Netware

СПЕЦИАЛИЗИРОВАННЫЕ ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

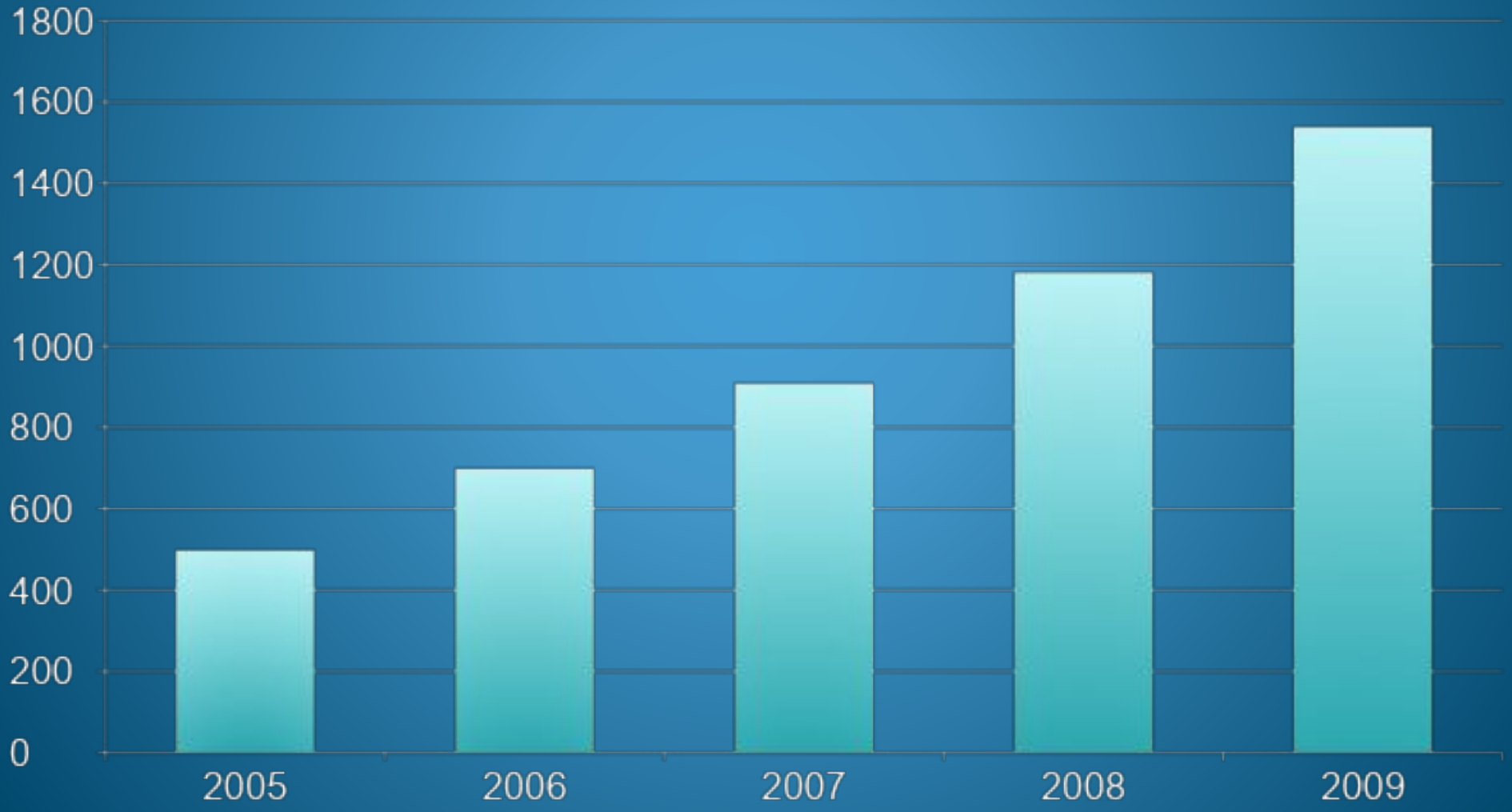
- Firewalls - брандмауэры
- Proxy-servers


ХАРАКТЕР УГРОЗЫ
ВИД ВОЗДЕЙСТВИЯ УГРОЗЫ
ИСТОЧНИК УГРОЗЫ
ОБЪЕКТЫ УГРОЗЫ
Угрозы информационной безопасности
Технологические
Физические
Человек
На ресурс
На канал связи
Форс-мажорные обстоятельства
На ресурс
На канал связи
Отказ оборудования и внутренних систем жизнеобеспечения
На ресурс
На канал связи
Программные (логические)
Локальный нарушитель
На ресурс
На операционную систему
На программное обеспечение
На информацию
Удаленный нарушитель
На ресурс
На операционную систему
На сетевые службы
На информацию, обрабатываемую сетевыми службами
На канал связи
На сетевое оборудование
На протоколы связи
Организационные
Воздействие на персонал
Физическое воздействие на персонал
На сотрудников, с целью получения информации
На сотрудников, с целью нарушения непрерывности ведения бизнеса
Психологическое воздействие на персонал
На сотрудников, с целью получения информации
На сотрудников, с целью нарушения непрерывности ведения бизнеса
Действия персонала
Умышленные действия
На информацию
На непрерывность ведения бизнеса
Неумышленные действия
На информацию
На непрерывность ведения бизнеса

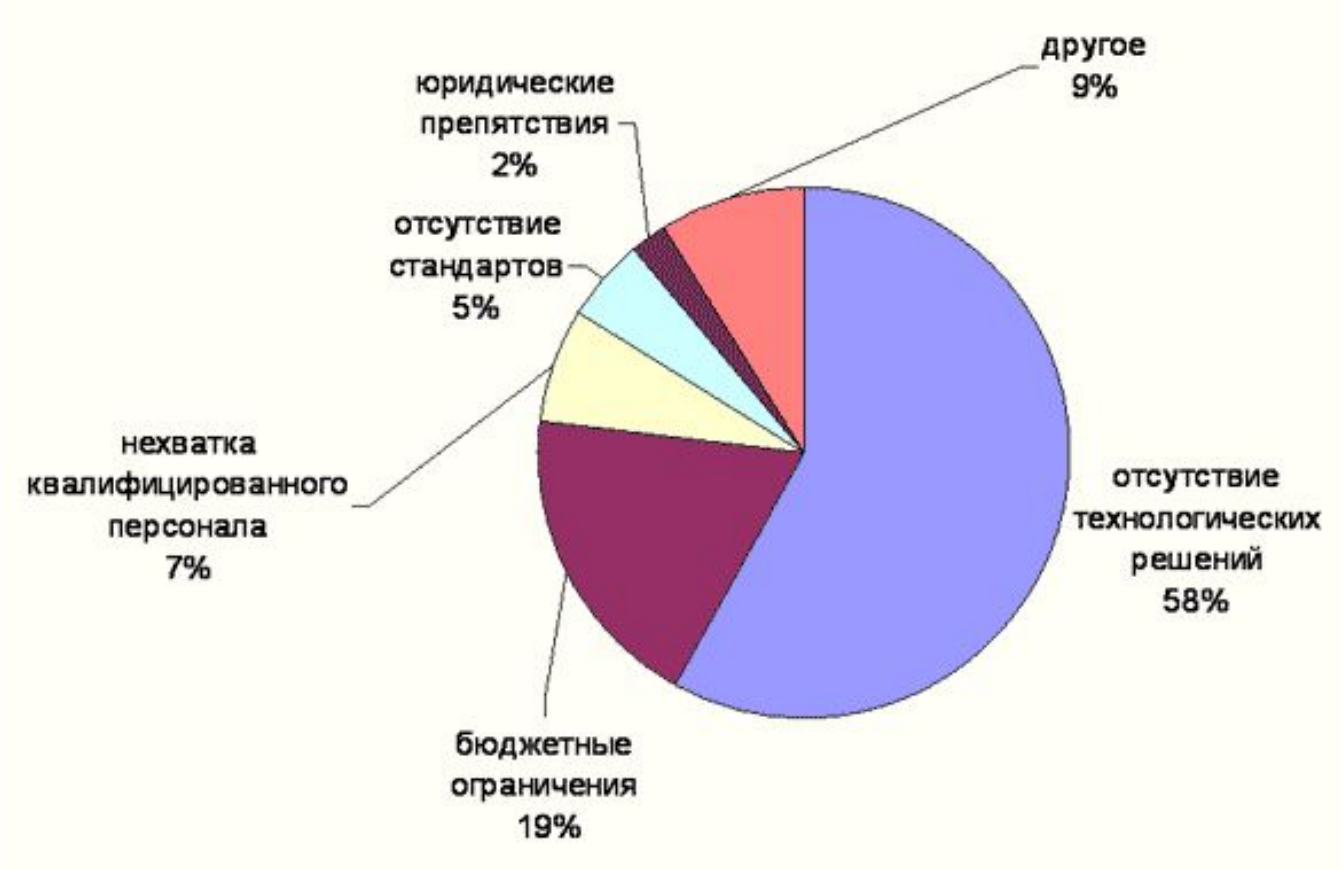
10 главных угроз информационной безопасности



Рост объёма рынка информационной безопасности в России (в млн. $)



Причины, по которым компании не готовы ставить внутренние системы защиты информации



БЛАГОДАРИМ ЗА ВНИМАНИЕ