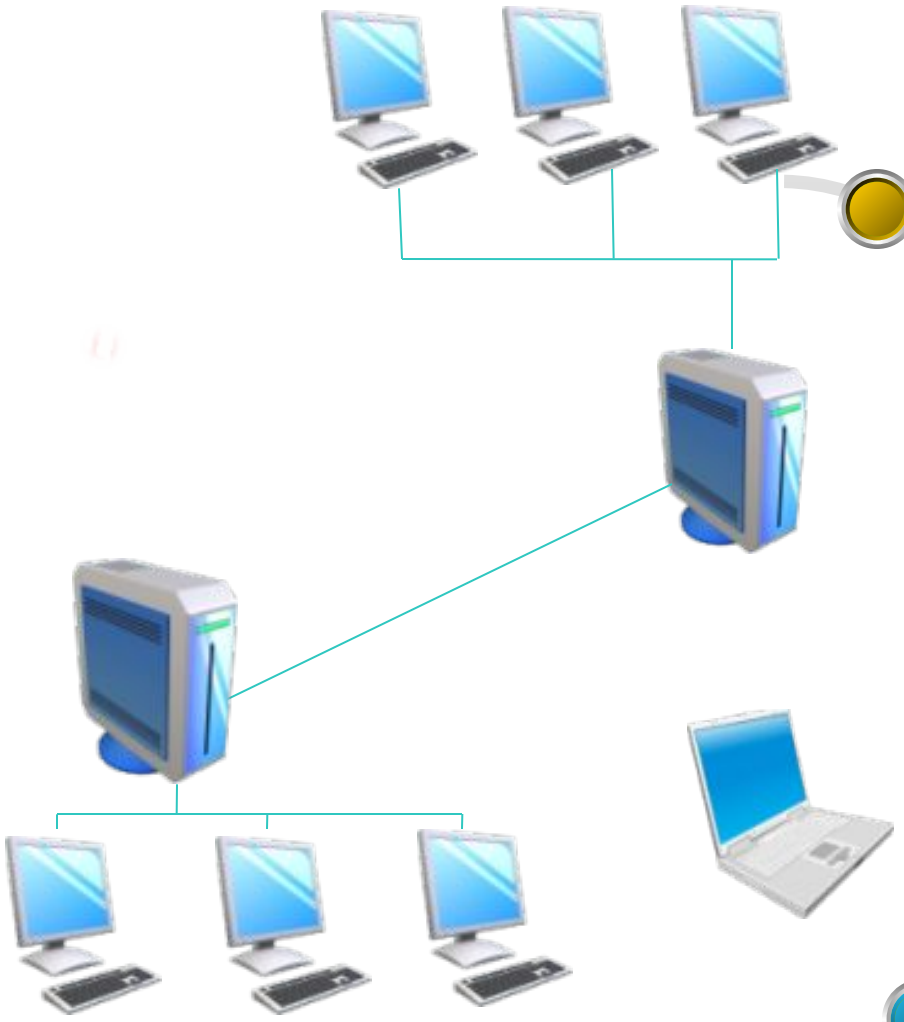
# КСЗИ «Панцирь-К»

## ЗАЩИТА

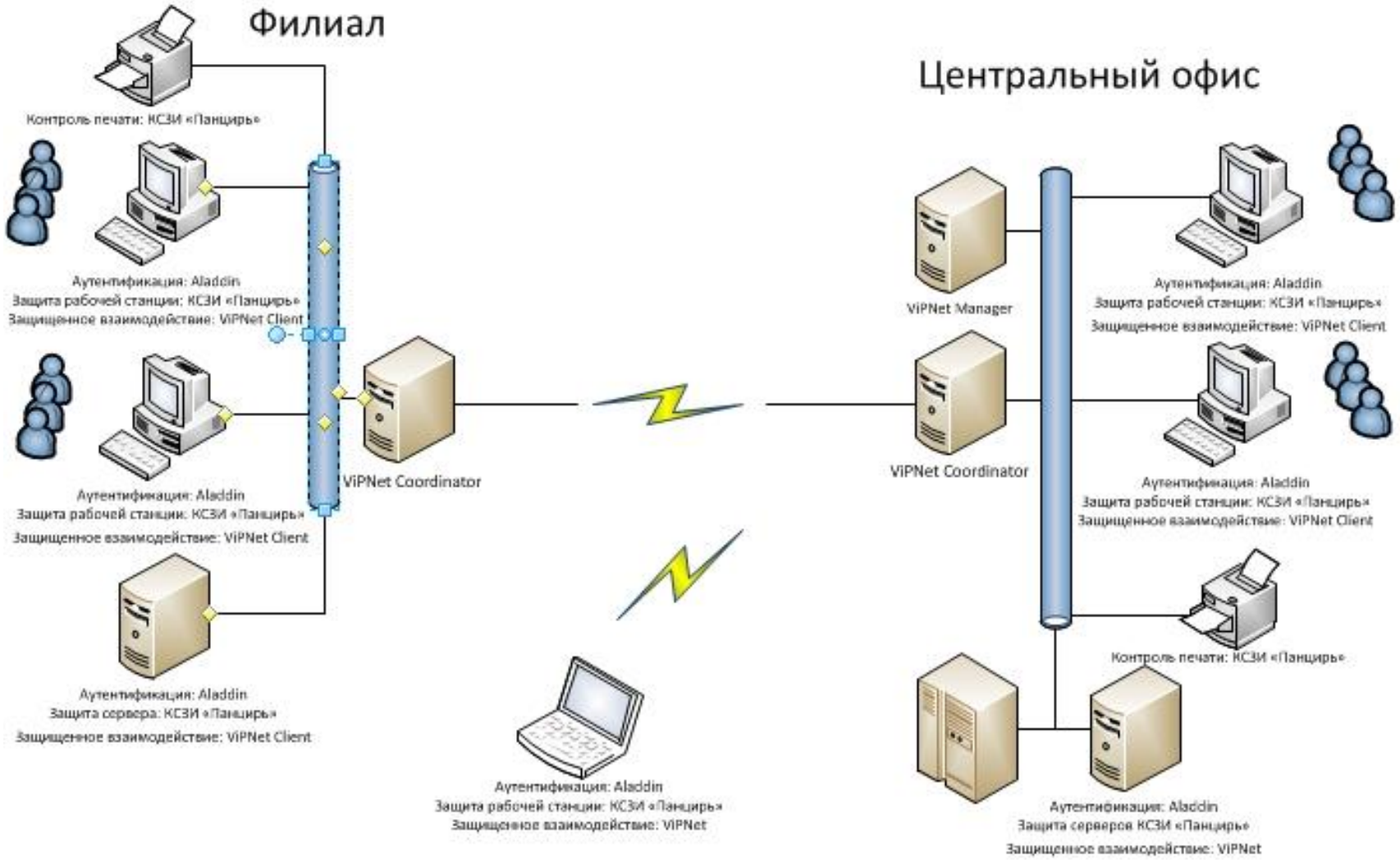
**конфиденциальной информации и персональных данных**

# Общие сведения



- «Панцирь-К» - это комплексная система защиты информации.
- Реализована программно и имеет как автономное, так и сетевое решение.
- Обеспечивает эффективную защиту от НСД
- Реализует возможность шифрования данных
- Функционирует под управлением ОС Windows 2000/XP/2003/Vista/2008

# Вариант комплексного решения



# Дополнительная информация

1

КСЗИ «Панцирь-К» имеет сертификат ФСТЭК России на соответствие 5 классу СВТ и 4 уровню контроля НДВ

2

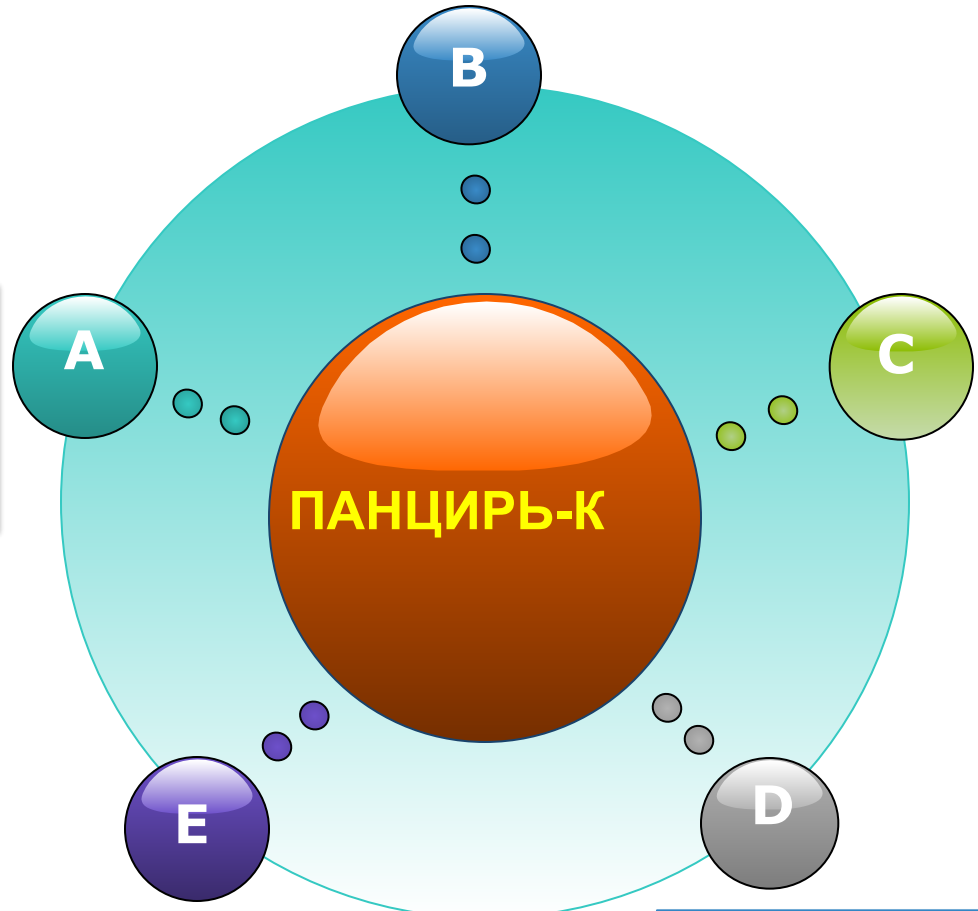
Выполняет все требования к классу защищенности 1Г для АС

3

Выполняет все требования по защите от НСД для ИСПДн 1 класса (В соответствии с приказом ФСТЭК России №58 от 05.02.2010г)

# Возможности КСЗИ

Разграничение и аудит действий пользователей и приложений




Идентификация и аутентификация: Console, flash, eToken USB, …

Контроль целостности

Шифрование: 3DES, AES, DES, ГОСТ 28147-89 …

Гарантированное удаление

# Назначение КСЗИ

КСЗИ «Панцирь-К» предназначена для решения актуальных задач защиты конфиденциальной информации, персональных данных и системных ресурсов:

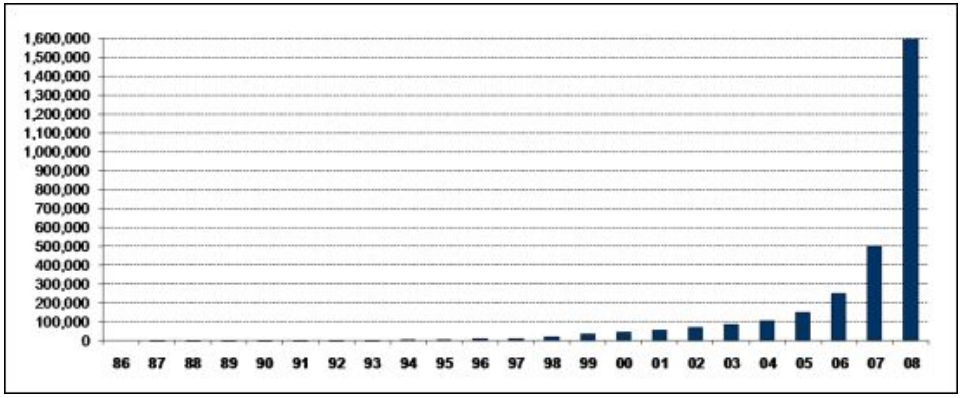
1. Защита от внешних угроз - обеспечивается эффективное противодействие атакам со стороны хакеров
2. Защита от внутренних угроз - обеспечивается эффективное противодействие атакам со стороны инсайдеров (санкционированных пользователей)
3. Защита от вирусных атак, вредоносных, шпионских и любых иных деструктивных программ.
4. Защита от атак на ошибки программирования в системном и прикладном ПО (эксплойты)
5. Защита как от известных, так и потенциально возможных атак на защищаемые ресурсы, обеспечивает устранение архитектурных недостатков защиты современных ОС семейства Windows

# Авторизация пользователей

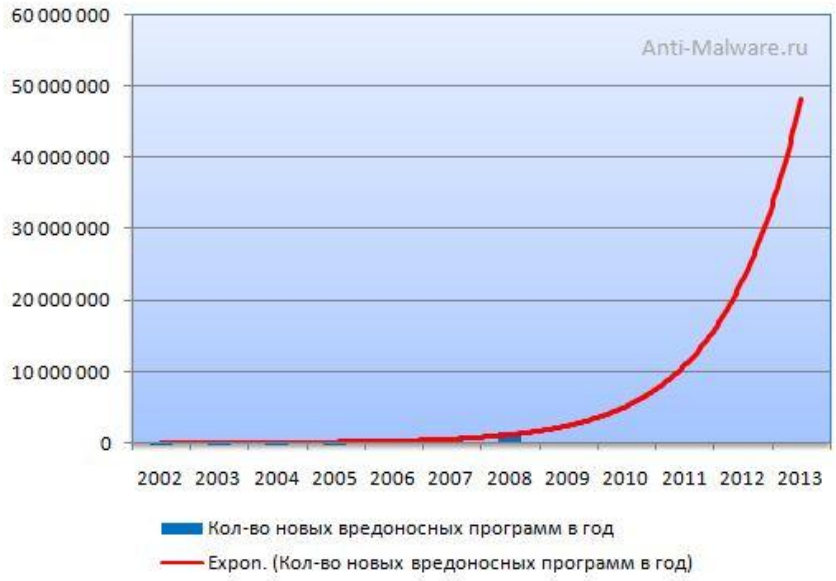
Возможность использования аппаратных решений для авторизации пользователей при входе в систему (в том числе для двухфакторной авторизации) и при доступе к критичным файловым объектам:

- Aladdin eToken USB
- Aladdin eToken смарт-карта
- И др. …


# Угрозы вредоносного ПО

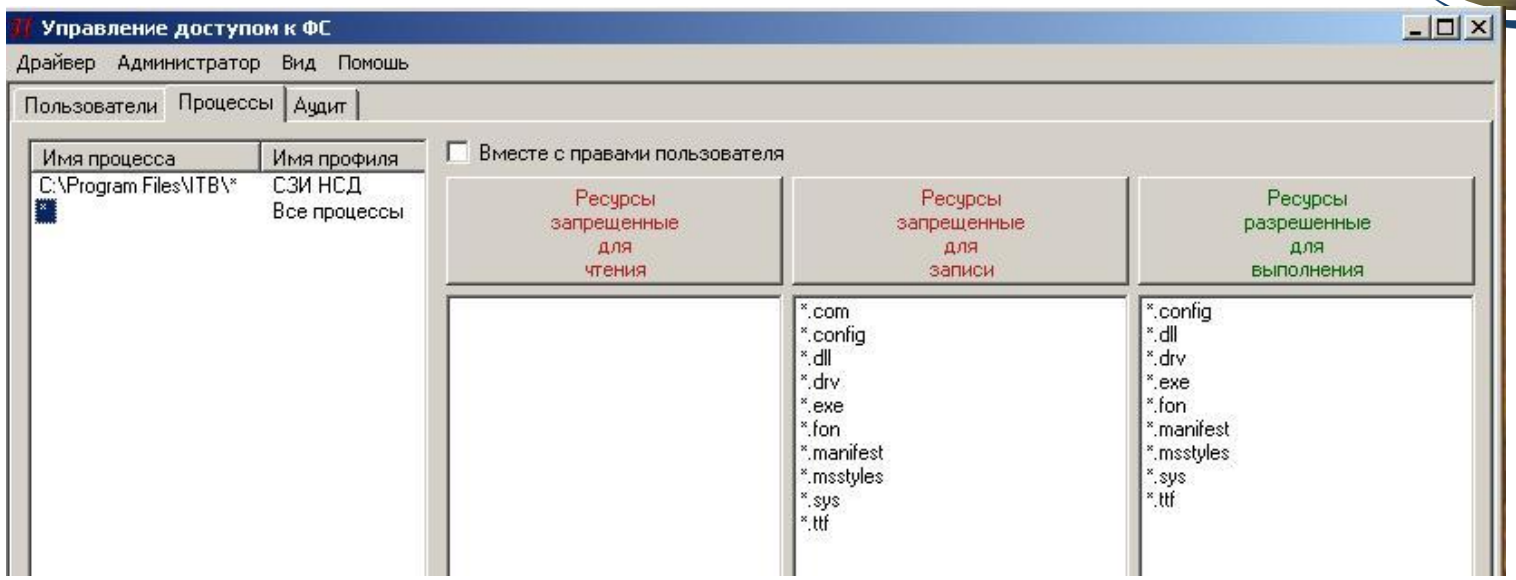



| Временной период | Кол-во обнаружений | Кол-во добавленных сигнатур |
|---|---|---|
| 1987 – 2006 | 250 000 | 250 000 |
| 2007 | 500 000 | 250 000 |
| 2008 | 1 500 000 | 1 000 000 |




Независимые тесты компонентов эвристического анализа показывают, что уровень обнаружения новых вредоносных программ составляет не более чем 40-50 % от их числа

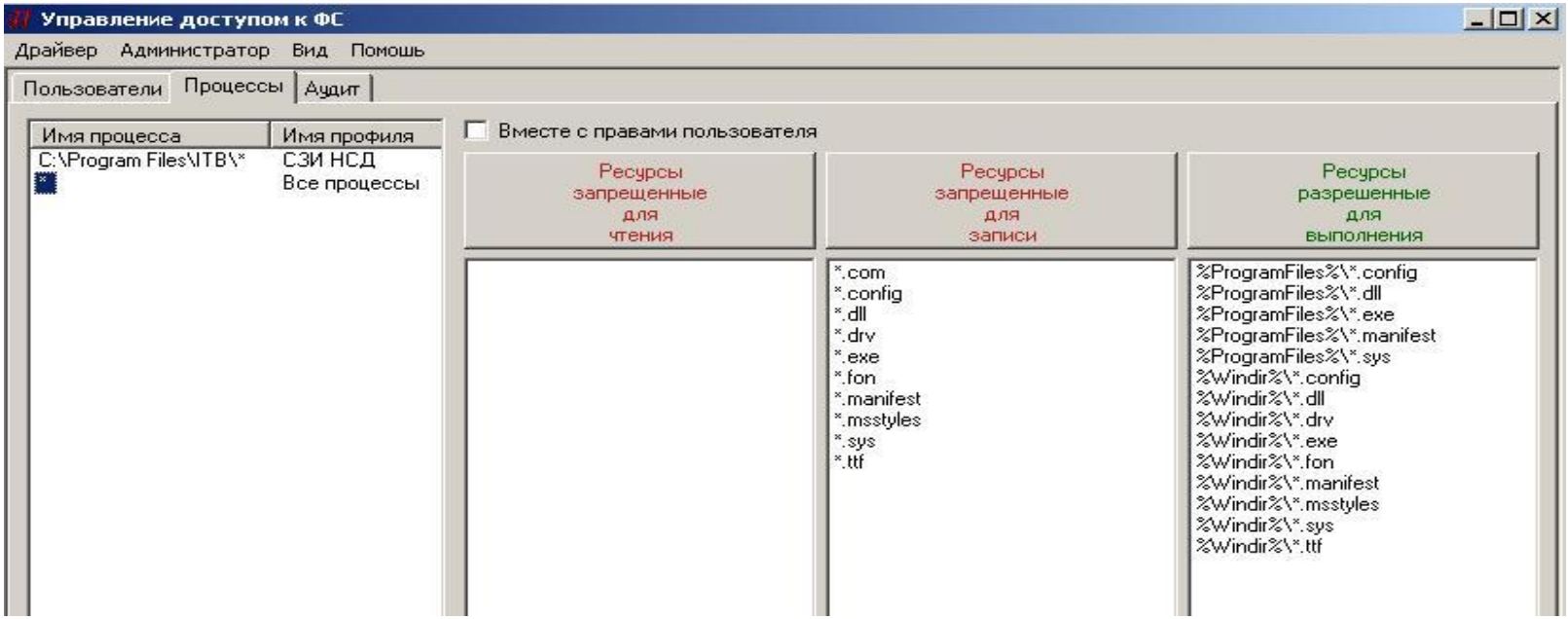
# Защита. Интерфейсы + настройки



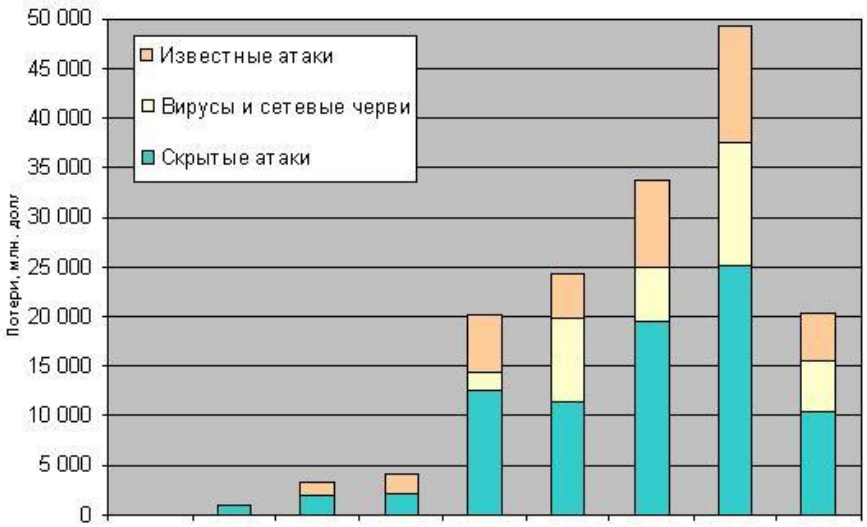

*Главную угрозу современности – внедрение и запуск вредоносного ПО, достаточно просто предотвратить реализацией разграничительной политики доступа к ресурсам, но для решения этой задачи защиты должны использоваться специализированные средства, т.к. требуется кардинальное изменение возможностей и интерфейса механизма разграничения прав доступа к файловым объектам, по сравнению с реализацией данного механизма защиты в современных универсальных ОС*

# Самозапускающееся вредоносное ПО

«Исследователи McAfee также установили, что за 30 дней самозапускающееся вредоносное ПО заразило более 27 млн. файлов. Данное ПО использует особенности Windows, позволяющие запускать приложения автоматически, не требуя от пользователя даже клика мышкой для активации программы. Оно наиболее часто распространяется через Usb - flash drive и другие устройства для внешнего хранения информации. Количество обнаружений данного ПО превзошло даже показатели печально известного червя Conficker на 400%, что делает самозапускающееся вредоносное ПО угрозой №1 во всем мире»



# Сетевая атака – одна из актуальнейших угроз современности

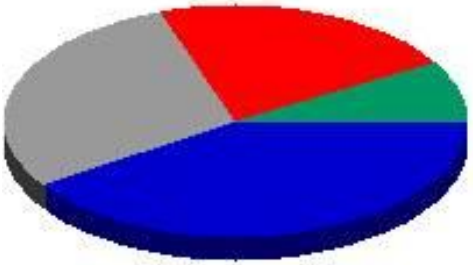



Только за первый квартал 2008 года финансовые потери в мировом масштабе сравнялись с потерями за весь 2004 год и составили почти 50 % от всей суммы потерь за 2007 год.

Это наглядно показывает неспособность классических антивирусных программ справляться с данным видом атак.

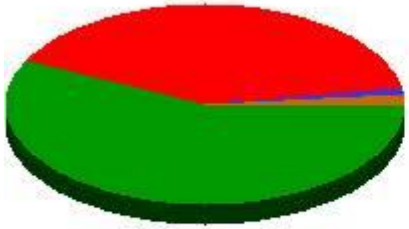
# Сетевая атака – одна из актуальнейших угроз современности

Общая статистика по уязвимостям




www.SecurityLab.ru

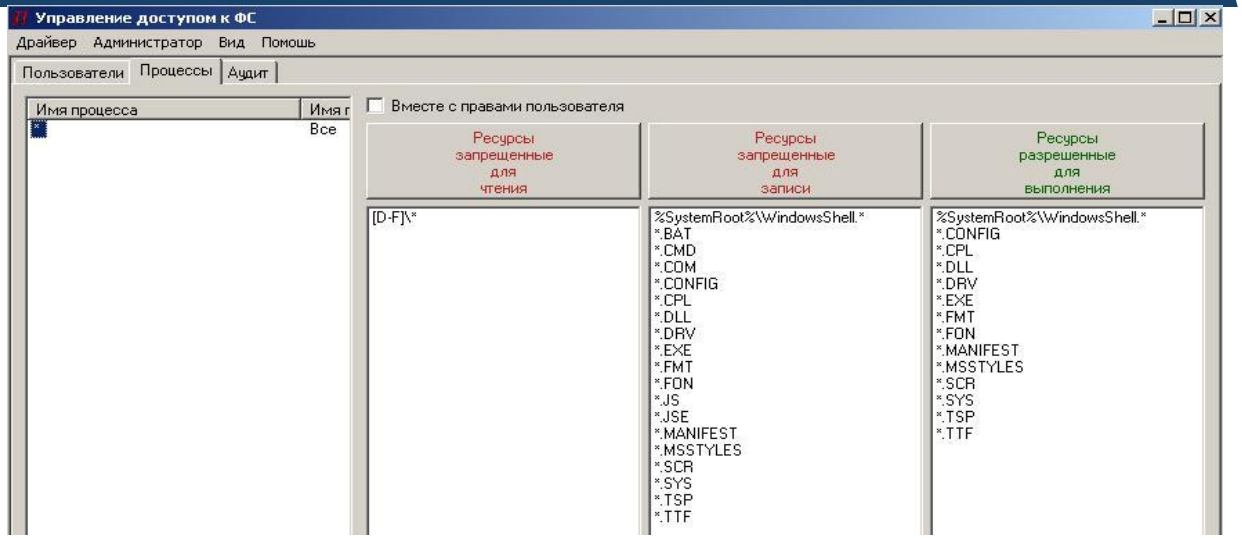

Наличие исправлений

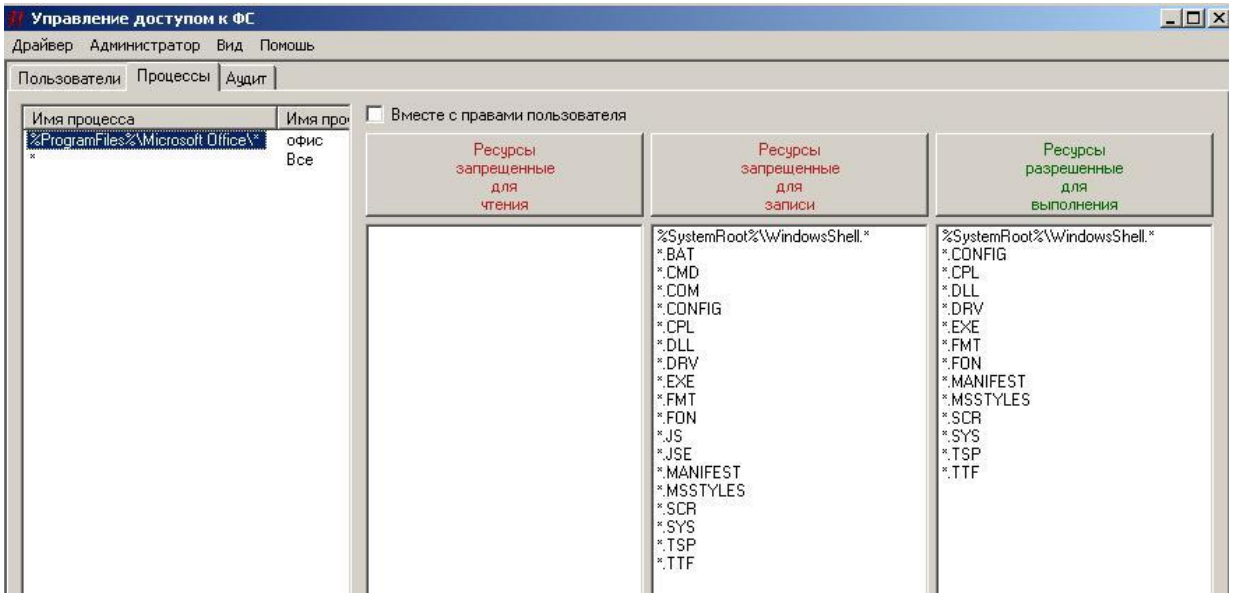



www.SecurityLab.ru

Всего исправлено 57.58% уязвимостей, исправления отсутствуют для 39.91% уязвимостей.

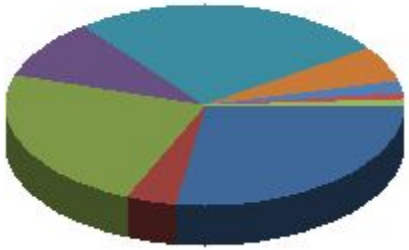
# Защита от сетевых атак реализацией разграничительной политики доступа к ресурсам



# Защита от атак на уязвимости ОС и приложений

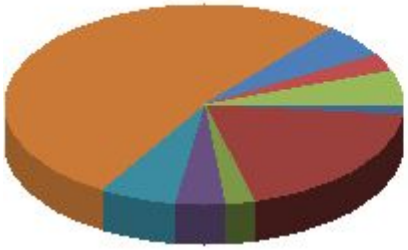
Типы уязвимостей в компонентах ОС



www.SecurityLab.ru

- Отказ в обслуживании (27.62%)
- Раскрытие важных данных (3.81%)
- Повышение привилегий (23.81%)
- Обход ограничений безопасности (9.52%)
- Компрометация системы (25.71%)
- Спуфинг атака (5.71%)
- Раскрытие системных данных (1.9%)
- Межсайтовый скриптинг (0.95%)
- Неавторизованное изменение данных (0.95%)

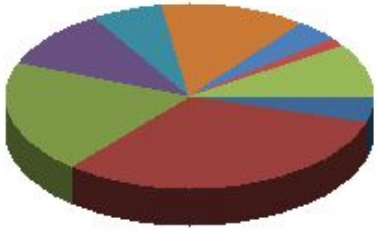
Типы уязвимостей в клиентском ПО



www.SecurityLab.ru

- Раскрытие системных данных (1.77%)
- Отказ в обслуживании (19.15%)
- Межсайтовый скриптинг (2.48%)
- Спуфинг атака (4.26%)
- Раскрытие важных данных (6.03%)
- Компрометация системы (52.48%)
- Обход ограничений безопасности (5.67%)
- Неавторизованное изменение данных (2.48
- Повышение привилегий (5.67%)

Типы уязвимостей в серверных приложениях



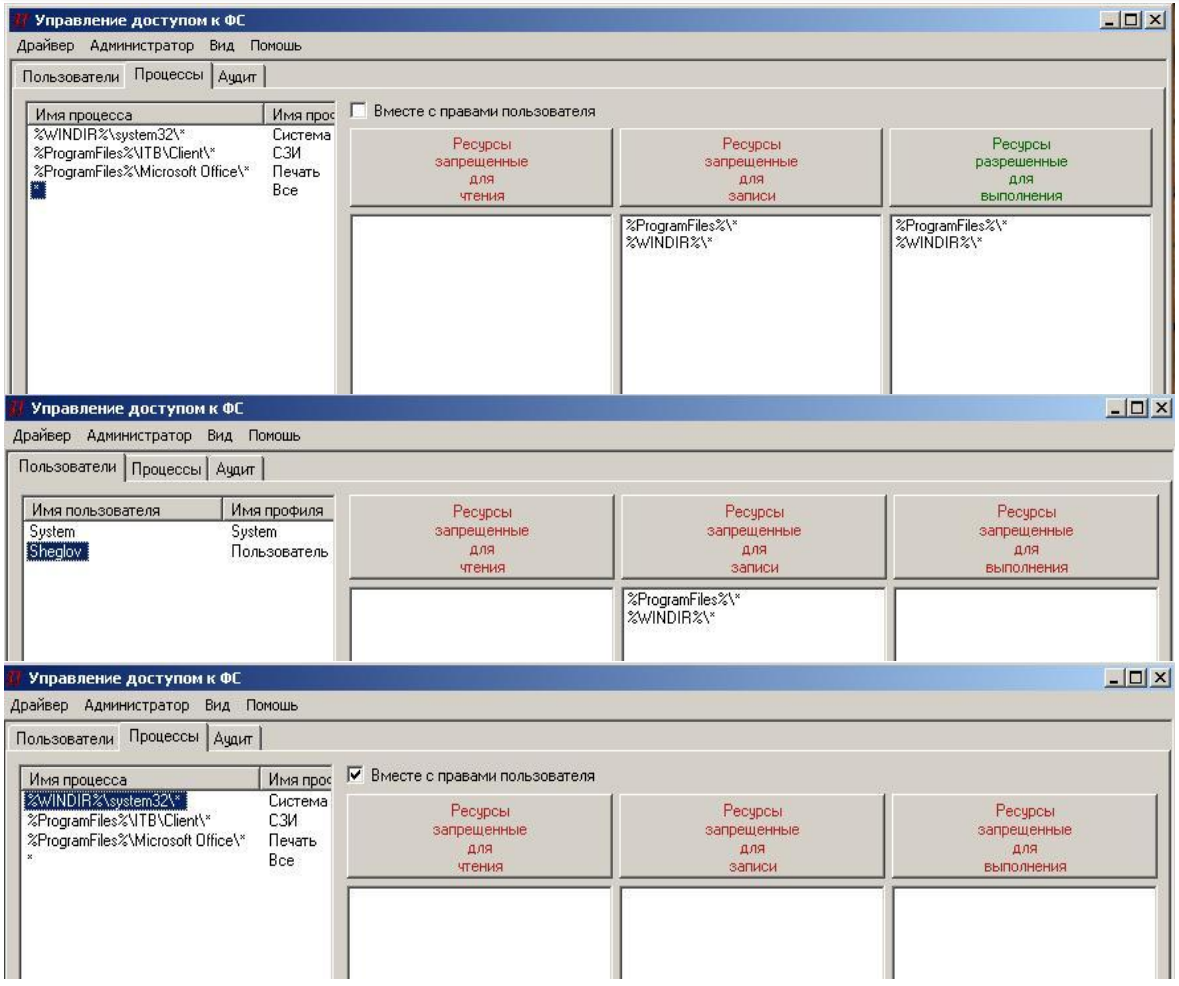
www.SecurityLab.ru

- Неавторизованное изменение данных (4.81%)
- Отказ в обслуживании (31.48%)
- Компрометация системы (20%)
- Межсайтовый скриптинг (10.37%)
- Повышение привилегий (5.93%)
- Обход ограничений безопасности (12.96%)
- Раскрытие системных данных (3.7%)
- Спуфинг атака (1.48%)
- Раскрытие важных данных (9.26%)

Как в ОС, так и в приложениях доминируют следующие уязвимости: отказ в обслуживании, компрометация системы и повышение привилегий.

# Защита реализацией разграничительной политики доступа к ресурсам в общем случае

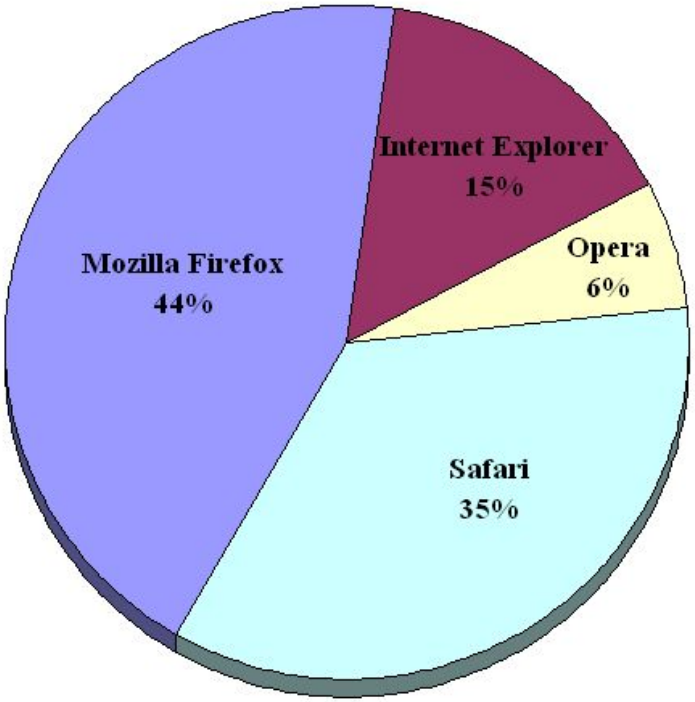
Защита от атак на уязвимости отказа в обслуживании и компрометации системы




Запуск только санкционированных программ, включая приложения и системные процессы – только программ из папок Windows и Program Files (никакие иные программы не могут быть запущены). Это и защита от атак на уязвимости компрометации системы и одновременно предотвращение любой возможности модификации исполняемых файлов и файлов настроек системы и приложений – запрет записи в папки Windows и Program Files - защита от атак на уязвимости отказов обслуживании.

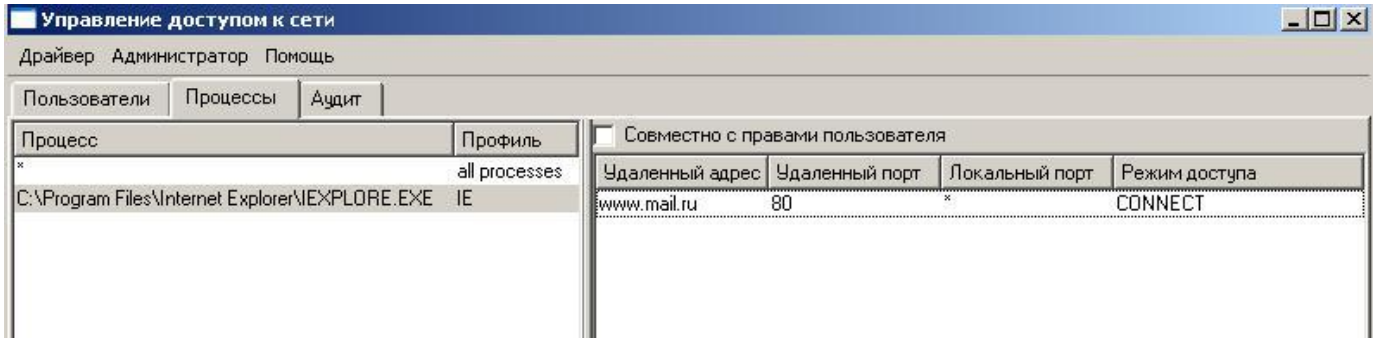
# Атаки на системные ресурсы

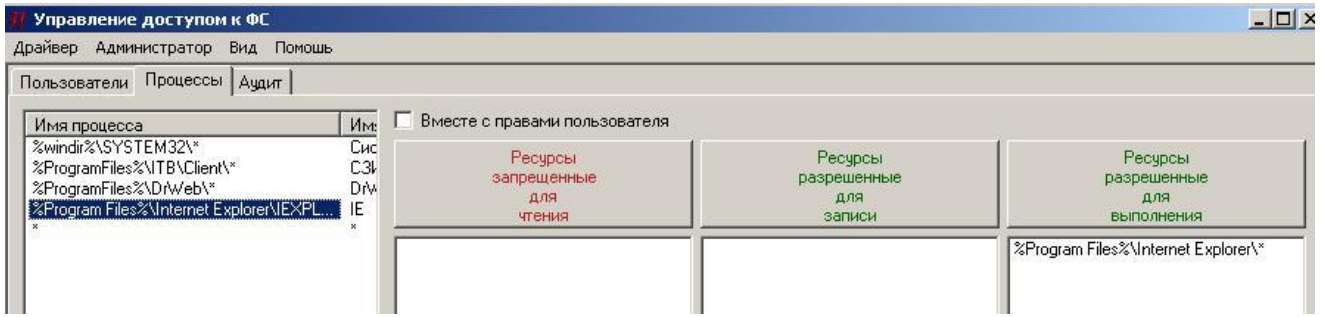
Статистика обнаруженных уязвимостей в интернет - браузерах

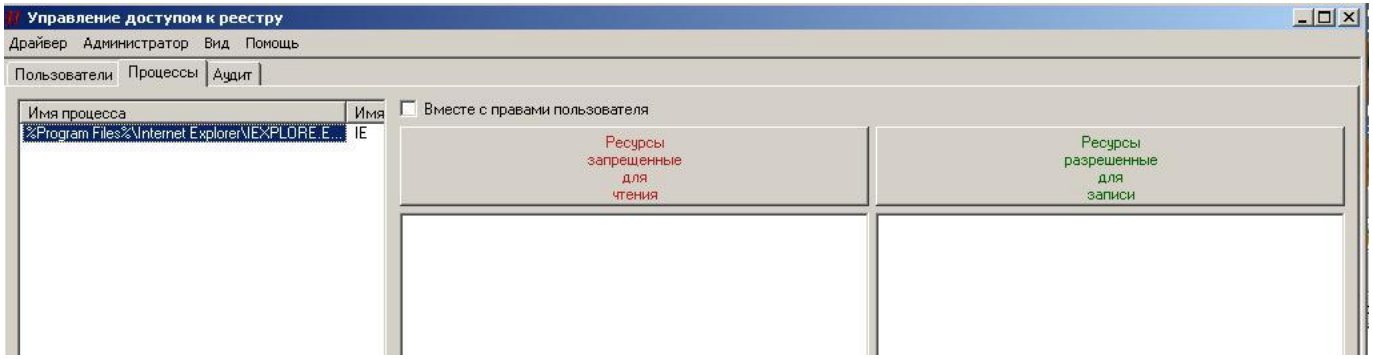



Использование следующих браузеров в настоящее время несет наибольшую опасность: это Microsoft Internet Explorer, который интегрирован в операционные системы, как следствие, в настоящее время лидирует по популярности, и Mozilla Firefox, который также довольно популярен и имеет наибольшее количество обнаруженных уязвимостей

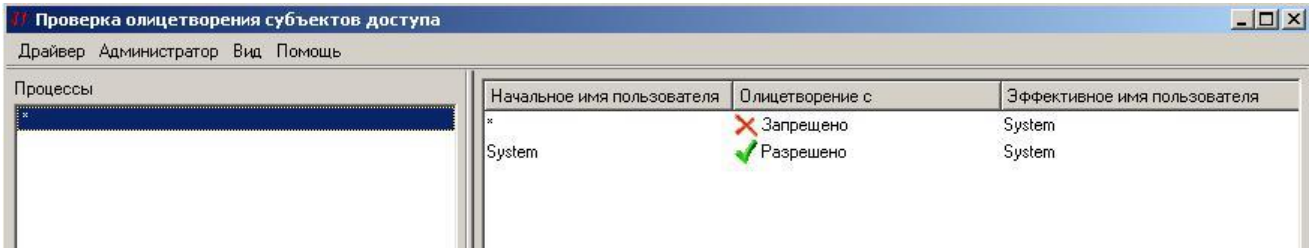
# Разграничения для критичных процессов



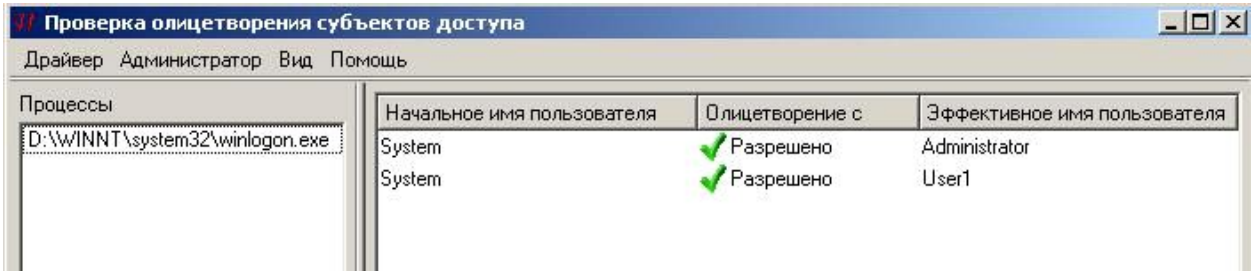



# Атаки на повышение привилегий

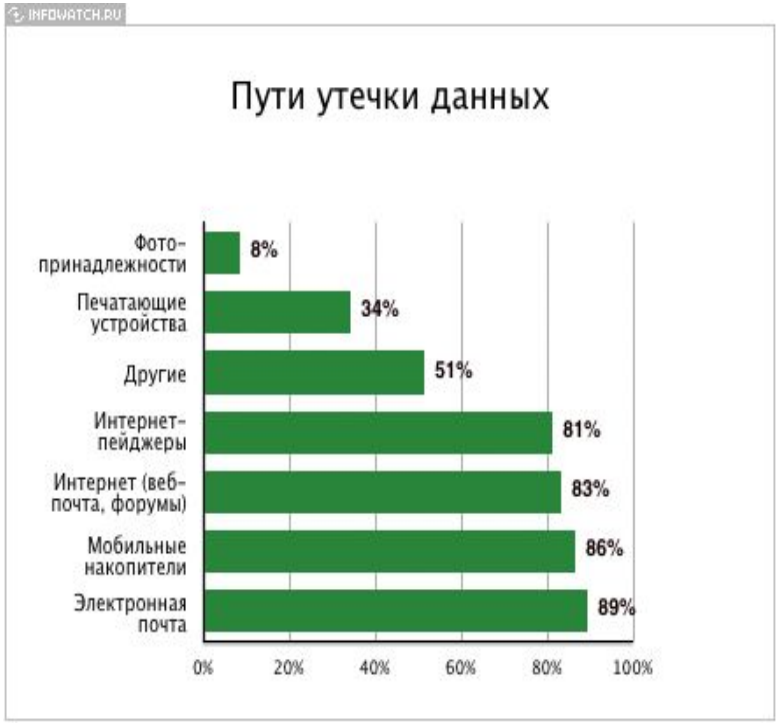



При таких простейших настройках пользователю, несанкционированно повысив свои права до системных, будет не получить доступ к тем ресурсам, к которым разрешен доступ пользователю System и не разрешен доступ пользователю, совершившему несанкционированное олицетворение.




используя данный механизм защиты из состава КСЗИ, можно усилить и механизм идентификации и аутентификации пользователя при входе в систему

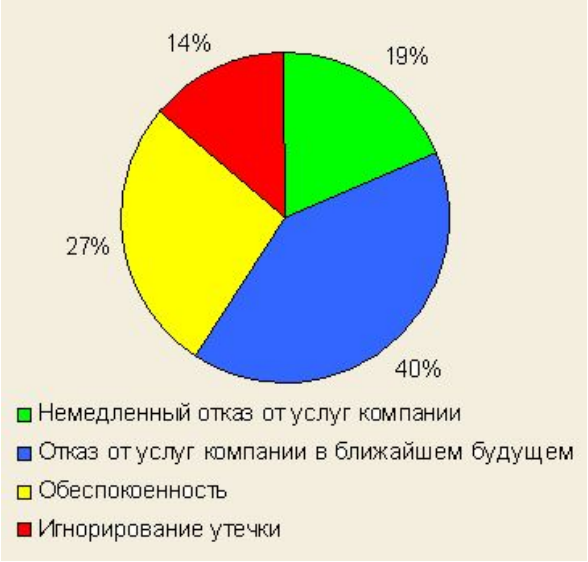
# Портрет инсайдера

# Существующие методы защиты от инсайдерских атак

Для защиты от инсайдерских атак сегодня широко применяются, так называемые, системы предотвращения утечек или DLP-системы. DLP (англ. Data Leak Prevention) -системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы

По оценкам компании Gartner (Hype Cycle of Information Security), эффективность механизмов контентной фильтрации не превышает 80%, а это автоматически означает не менее 20% пропущенных конфиденциальных файлов.



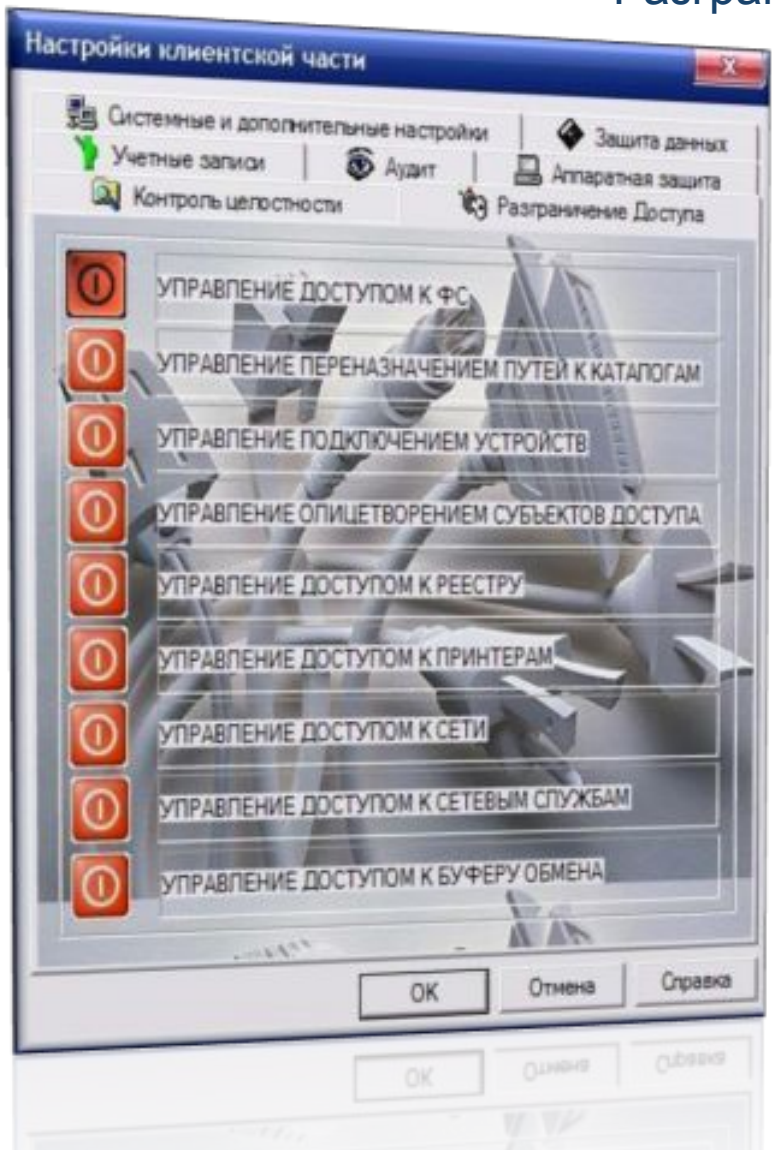
# Состав механизмов

**Технология должна включать:**

- ✔ Управление монтированием устройств на защищаемых компьютерах;
- ✔ Управление запуском приложений на защищаемых компьютерах;
- ✔ Управление обработкой конфиденциальной информации на защищаемых компьютерах (локально, в сети, какими приложениями и т.д.);
- ✔ Управление хранением и передачи защищаемой информации с использованием внешних накопителей;
- ✔ Разграничения по использованию для передачи защищаемой информации по сети (ЛВС, по каналам сети общего использования, какими приложениями, к каким компьютерам – адреса и порты, и т.д.);
- ✔ Управление выдачей конфиденциальной информации на печать (использование локальных и сетевых принтеров);
- ✔ Управление работой с открытой и конфиденциальной информацией на защищаемых компьютерах;
- ✔ И т.д.

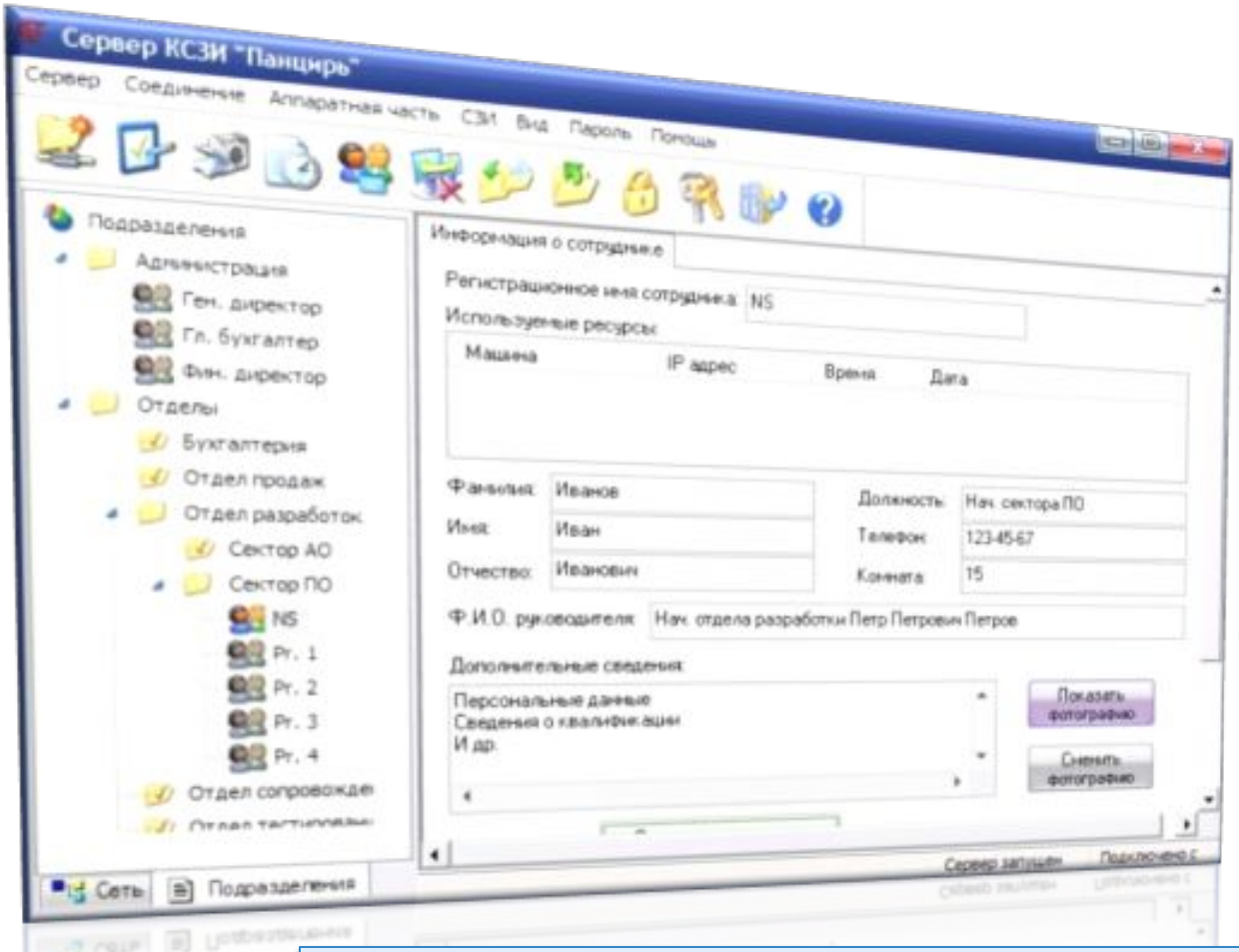
# Механизмы защиты

Разграничения доступа, реализованные в КСЗИ «Панцирь-К»:




- Разграничение доступа к файловой системе
- Разграничение доступа к реестру системы
- Разграничение доступа к сети
- Разграничение доступа к принтерам
- Управление подключением устройств
- Управление переназначением путей к каталогам
- Управление олицетворением
- Управление доступом к буферу обмена
- Управление доступом к сетевым службам

# Удаленное администрирование




- ✔ Система удаленного администрирования клиентских частей КСЗИ
- ✔ Система хранения синхронизации центральной базы КСЗИ
- ✔ Система удаленного управления защищаемым объектом

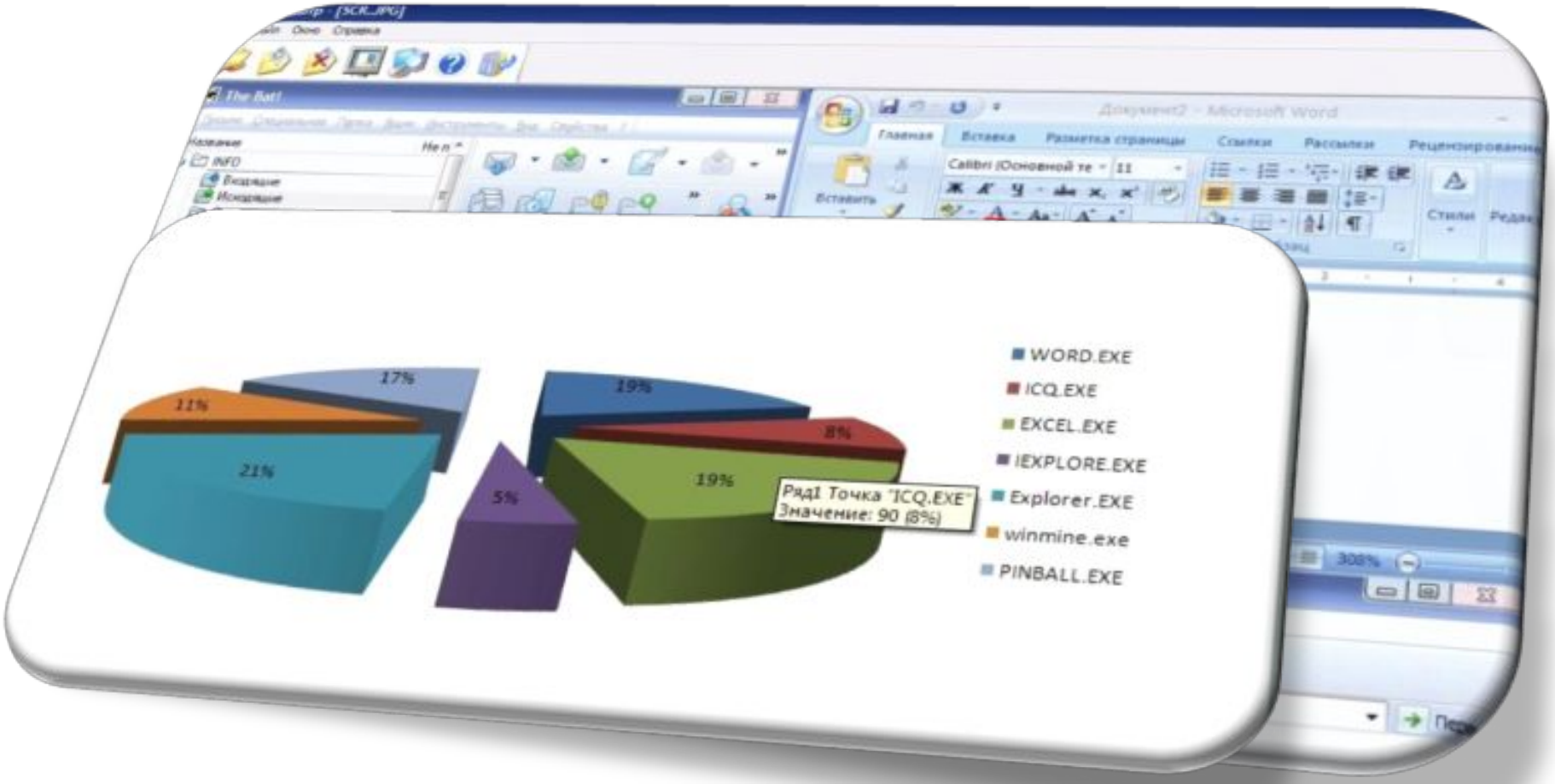
Система удаленного сбора и обработки журналов аудита:

- В реальном времени
- По запросу администратора безопасности

Защищенное взаимодействие клиентских частей КСЗИ с сервером КСЗИ

# Контроль рабочего времени пользователя

- Статистика работы пользователя с приложениями
  - Просмотр снимков экрана в реальном времени или с использованием правил
    - Лог клавиатуры пользователя



# Награды и дипломы