САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А.Бонч-Бруевича

# Дипломная работа: «Анализ способов и средств обеспечения информационной безопасности пользователей услуг Интернет»

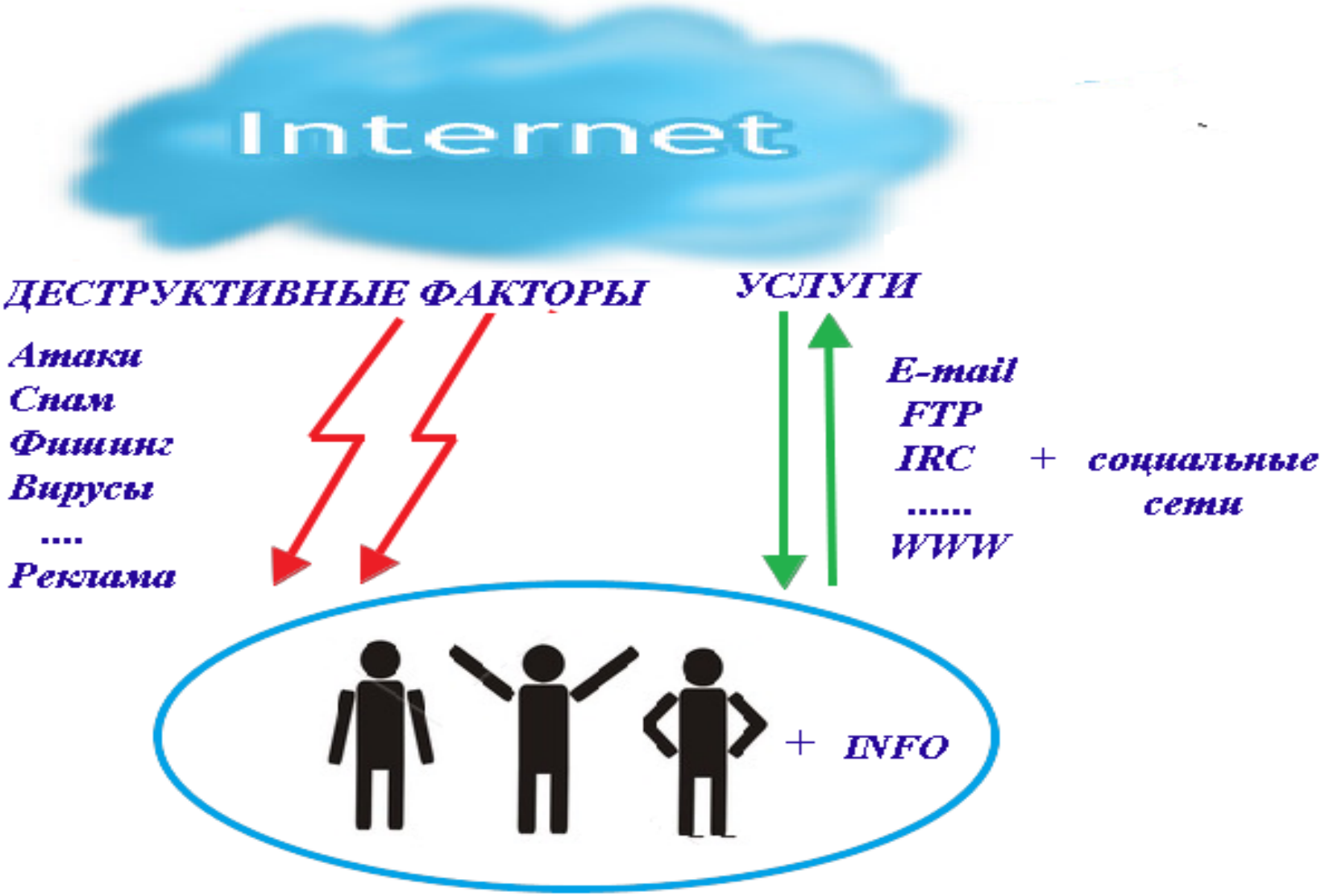

Подготовила: студентка гр. СУ-61
Володченко Марина Александровна

СПб, 2011г.

**Цель работы:**

оказать помощь пользователям услуг Интернет в обоснованном выборе эффективных способов и средств защиты персонального компьютера и локальных сетей от различных деструктивных факторов со стороны глобальной сети.

# Взаимодействие пользователей с сетью Интернет



# Интернет и безопасность

**Информационная безопасность** — это *состояние* защищённости информационной среды, *защита информации* представляет собой *деятельность* по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Безопасность информации (при применении информационных технологий)** (англ. *IT security*) — состояние защищенности информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

# Нормативные документы в области защиты информации

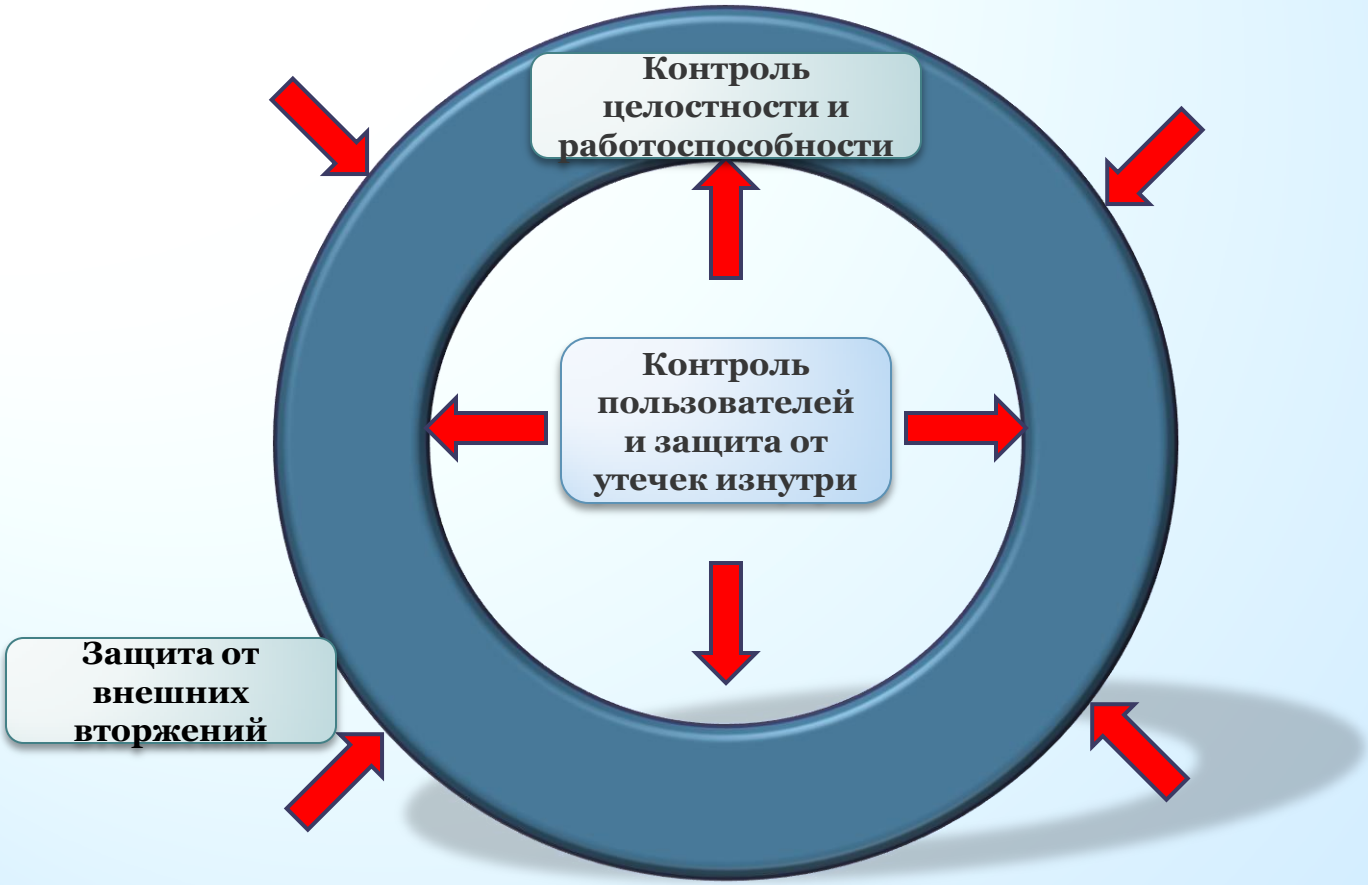
**Федеральные Законы в области защиты информации**

- Федеральный закон РФ № 63-ФЗ от 06 апреля 2011 г. «Об электронной подписи»
- Федеральный закон РФ № 83-ФЗ от 8 мая 2010 г. "О внесении изменений в отдельные законодательные акты РФ в связи с совершенствованием правового положения государственных (муниципальных) учреждений"
- Федеральный закон РФ № 8-ФЗ от 09 февраля 2009 г. «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»
- Федеральный закон РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»
- Федеральный закон РФ № 98-ФЗ от 29 июля 2004 «О коммерческой тайне»
- Закон РФ № 2446-I от 5 марта 1992 года «О безопасности»

**ГОСТы в области защиты информации**

- ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»
- ГОСТ Р 50862–96 «Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость»

# В основе зашиты информационных систем (ИС) лежит подход «тройного кольца» безопасности.



# Способы

**организационные** | **аппаратные** | **программные**


# Средства

- антивирусные и антиспам программы
- прокси-серверы
- брандмауэры
- IDS-системы
- PGP

- цифровые подписи
- протокол SSL/TLS
- протокол IPSec
- хэш-функции
- Mac-коды

# Антивирусные программы

- Это программа для обнаружения компьютерных вирусов, нежелательных (вредоносных) программ и восстановления зараженных файлов, а также для профилактики — предотвращения заражения (модификации) файлов или ОС вредоносным кодом.

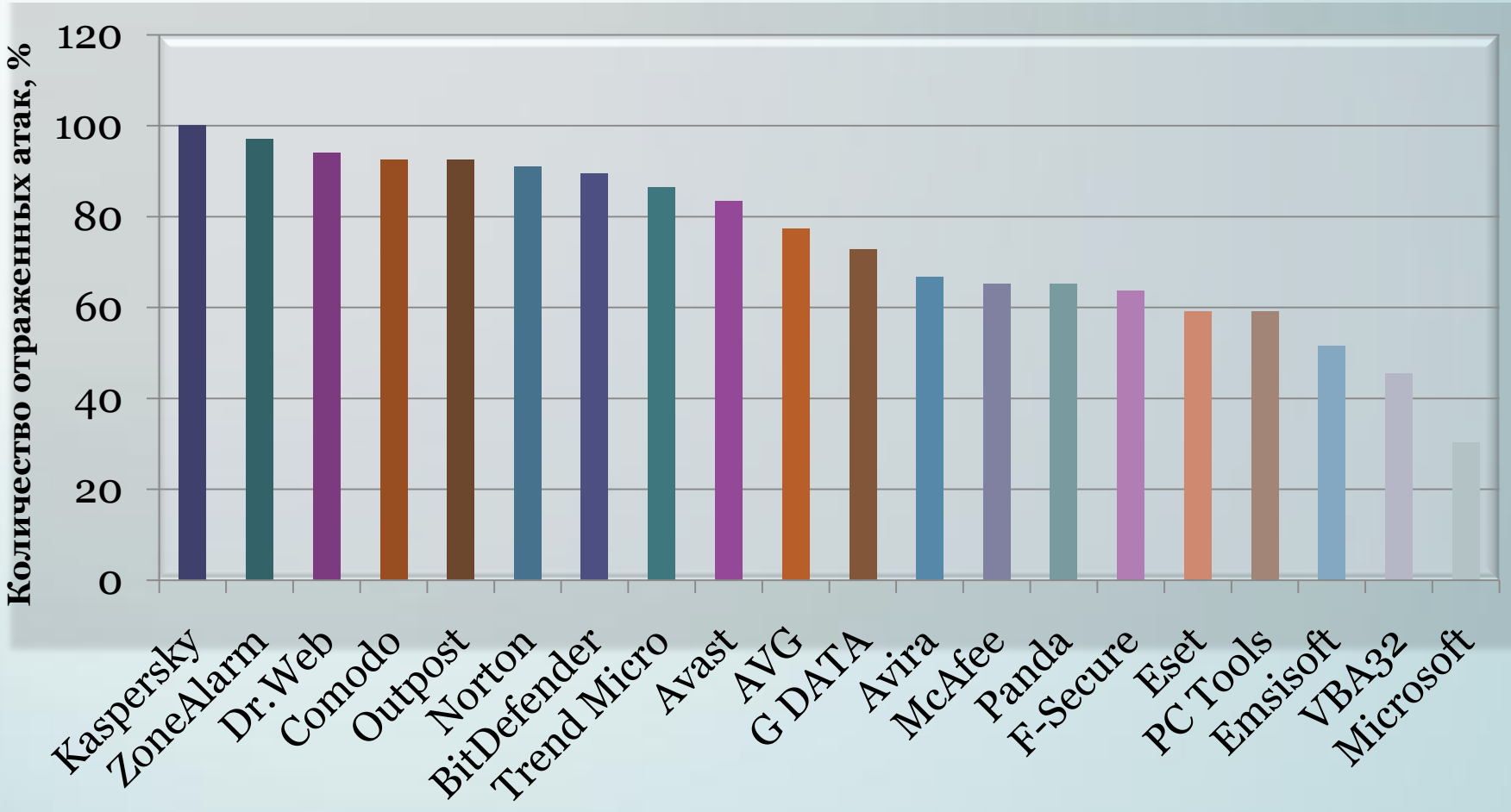
**Классификация антивирусов по принципу их действия**

- Сканеры
- Ревизоры
- Мониторы
- Иммунизаторы


**Критерии оценки антивирусов:**

- Объем антивирусной базы;
- Скорость реакции на появление новых вирусов;
- Степень задействования ресурсов компьютера;
- Эвристический анализ;
- Корректное лечение вирусов.

# Результаты теста самозащиты современных антивирусных программ на платформе ОС Windows 7



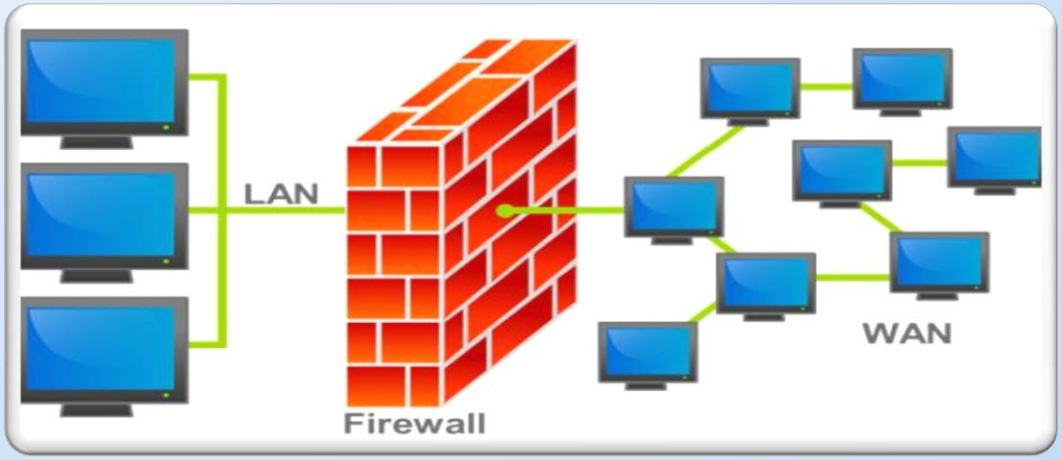

Источник: Anti-Malware,2011г.

# Межсетевой экран

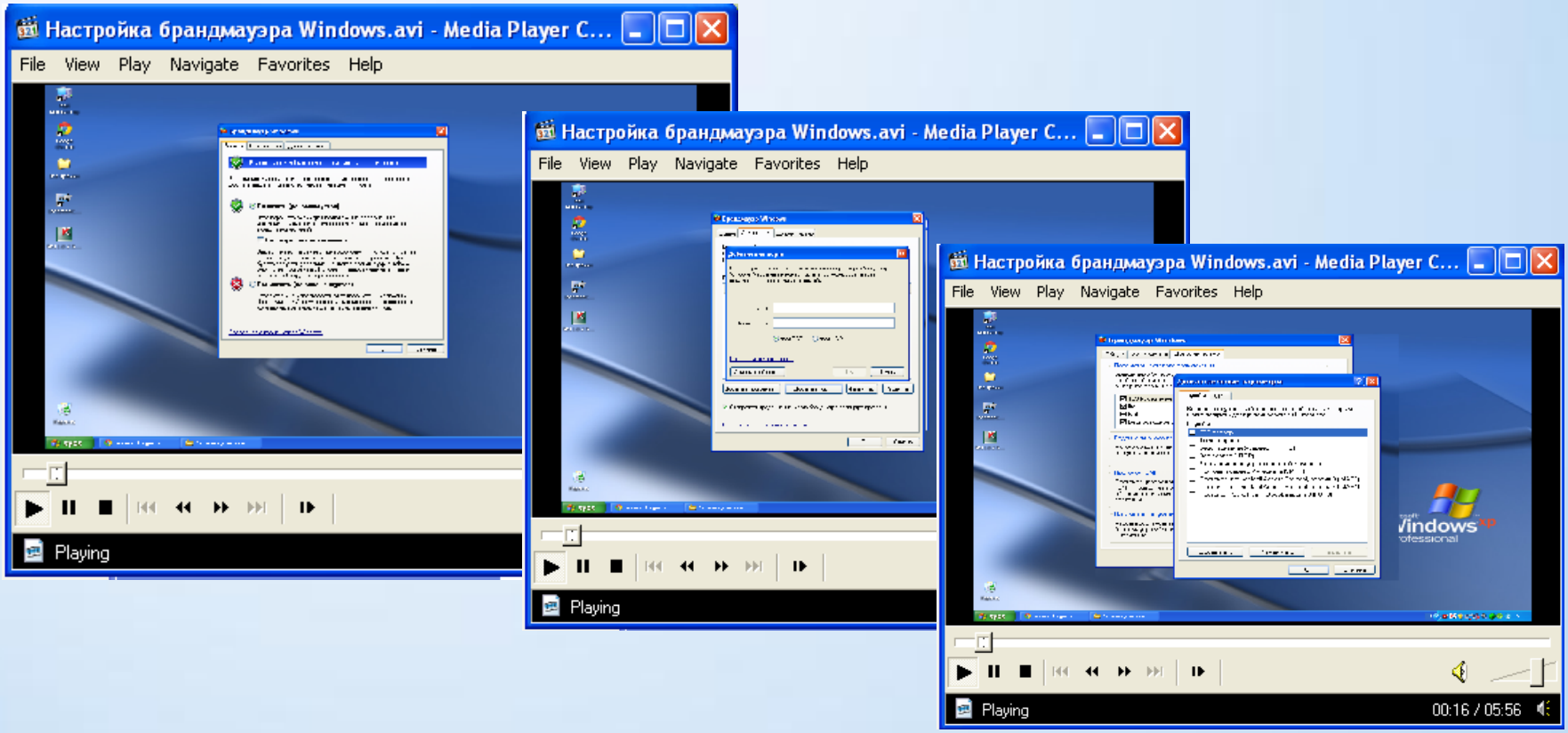
- **специализированный программно-аппаратный комплекс, обеспечивающий защиту локальной сети от вторжений со стороны глобальной сети в точке их соединения.**

**Межсетевой ЭКРАН**

- **фильтрующие маршрутизаторы**
- **шлюзы сеансового уровня**
- **шлюзы прикладного уровня**



В ходе моей дипломной работы разработан обучающий видео-курс по настройке брандмауэра в ОС Windows XP.




**Настройка брандмауэра Windows XP**

http://www.youtube.com/watch?v=7JUf6H-Znrw

# Протокол IPSec

- система открытых стандартов, предназначенных для обеспечения защищенных конфиденциальных подключений через IP-сети с использованием криптографических служб безопасности.

Протокол IPSec работает на сетевом уровне модели OSI.

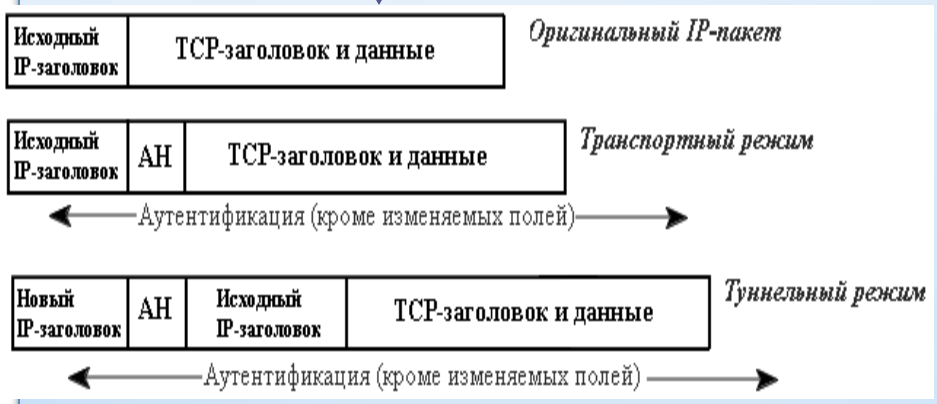
Обеспечивает:

- проверку подлинности источника данных;
- целостность данных;
- конфиденциальность (шифрование).

Существует два режима работы IPSec: транспортный и туннельный режимы.

# В IPSec используются два механизма защиты

защита заголовка IP-пакета шифрование содержимого




# Электронная подпись

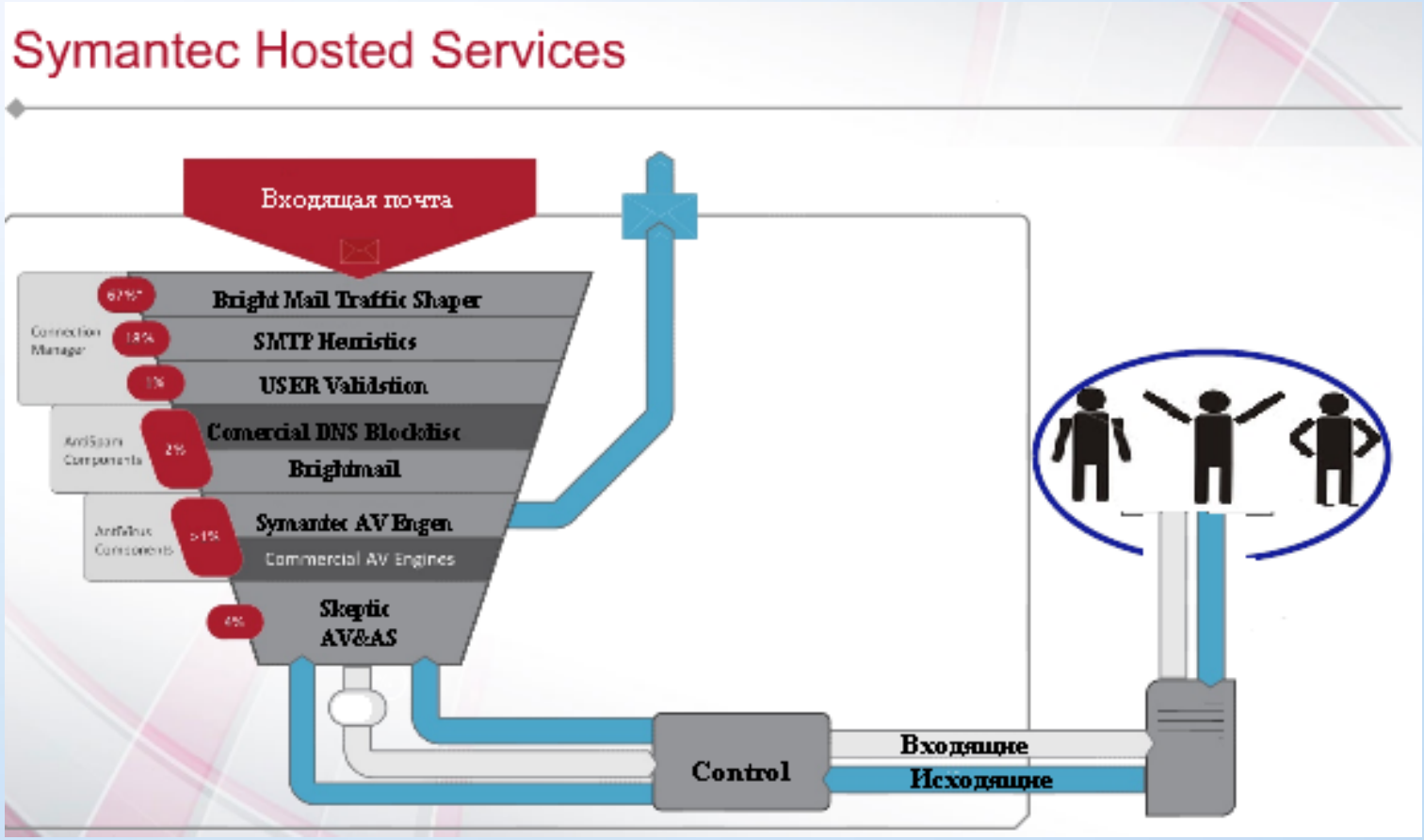
Использование цифровой подписи позволяет осуществить:

- Контроль целостности передаваемого документа.
- Защиту от изменений (подделки) документа.
- Невозможность отказа от авторства и др.


Общепризнанная схема цифровой подписи охватывает три процесса:

- Генерация ключевой пары.
- Формирование подписи.
- Проверка (верификация) подписи.

Компания Symantec предложила новую услугу для обеспечения безопасности информации- Symantec Hosted Services – «облачные» технологии.



# Заключение

Рекомендации, которым следует придерживаться:

- Использовать современные ОС с регулярными обновлениями и лицензионное ПО;
- Работать на ПК под правами пользователя, а не администратора;
- Использовать антивирусные и антиспам-продукты известных производителей с автоматическими обновлениями сигнатурных баз;
- Использовать персональный межсетевой экран и настроить его на прием трафика из достоверных источников;
- Ограничить физический доступ к компьютеру посторонних лиц;
- Не открывать файлы, полученные от ненадёжных источников;
- Использовать внешние носители информации только от проверенных источников;
- Для хранения наиболее важной информации использовать резервное копирование данных и др.

Чтобы защититься от угроз, связанных с сервисами электронной почты и доставки файлов, стоит придерживаться следующим рекомендациям:

- Настраивать антивирусную программу на непрерывную проверку поступающего трафика на наличие вирусов;
- Чтобы исключить перехват паролей доступа, использовать почтовые службы, предоставленными на Web-сайтах, поддерживающих SSL-доступ при регистрации на сайте и имеющих сертификат от доверенных бюро CA;
- Отсылаемые электронные письма шифровать и подписывать своей ЭЦП. Если у Вас нет правомочной подписи, использовать средства PGP и др.