Учебный курс

Обеспечение информационной безопасности с помощью антивируса Касперского

Лекция 1

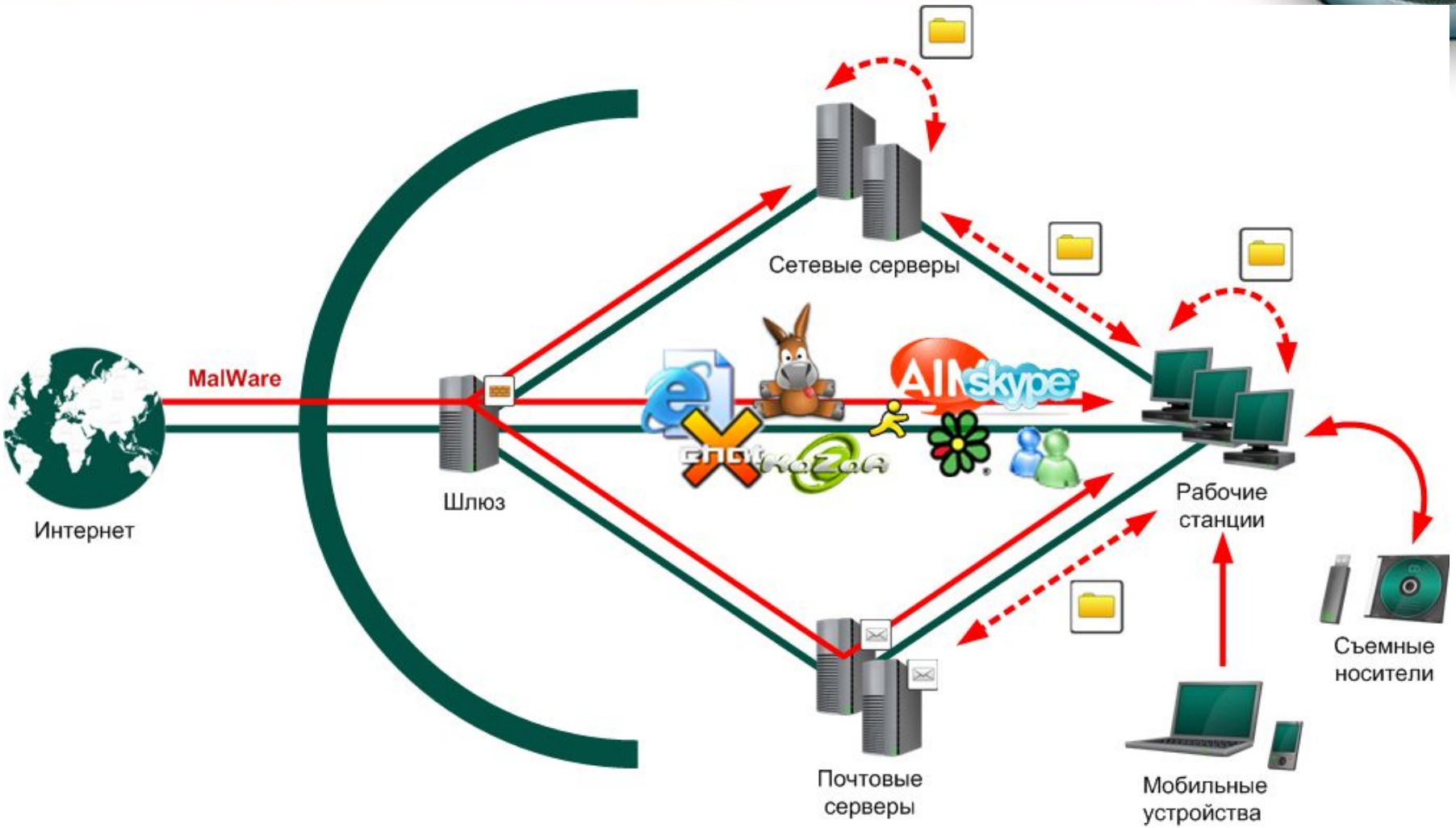
Классификация вредоносных программ. Методы защиты

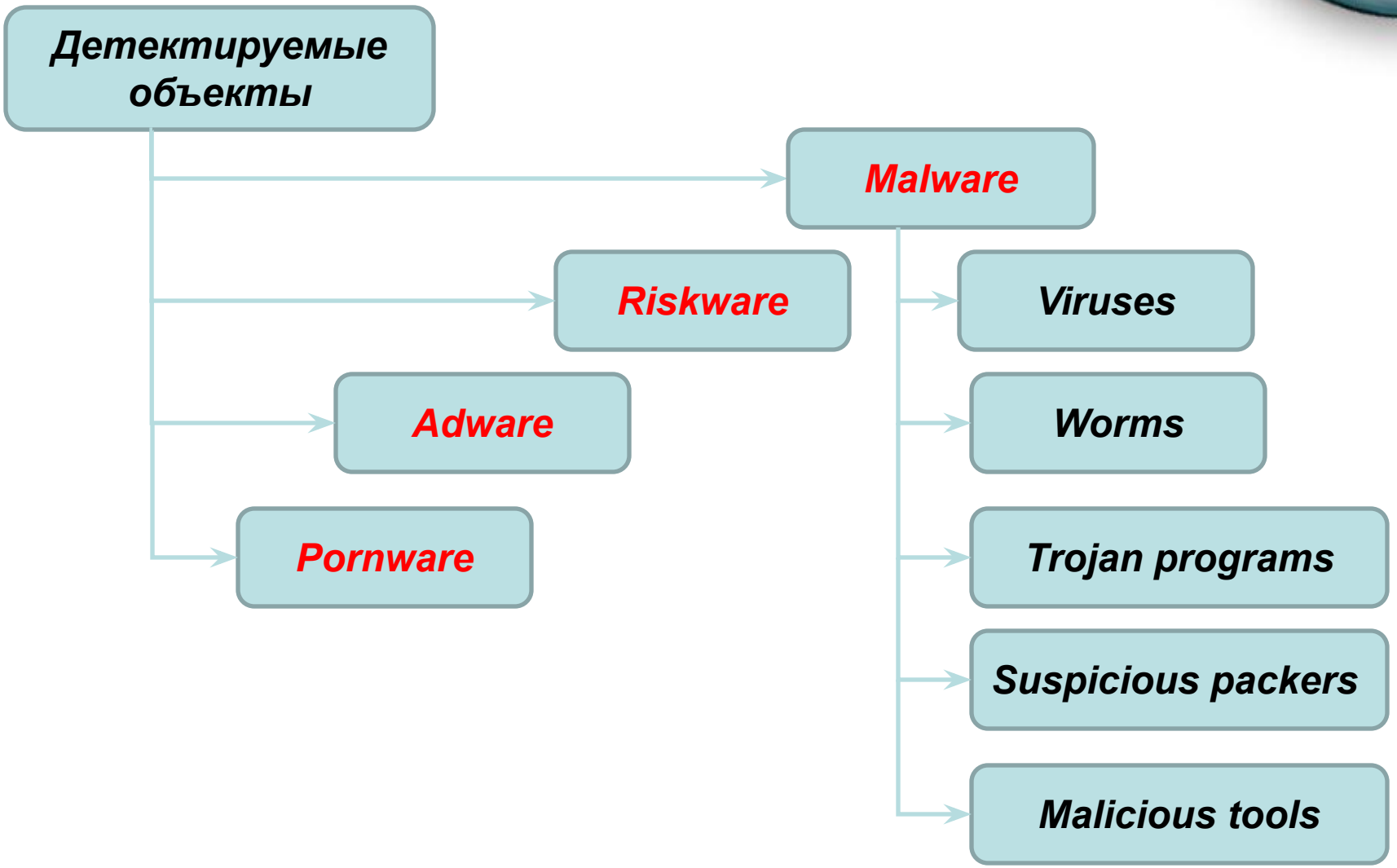
Лекции читает

методист образовательных программ Лаборатории Касперского

Яшутина Ольга Александровна

Типичная схема заражения




Детектируемые объекты
Malware
Riskware
Adware
Pornware
Viruses
Worms
Trojan programs
Suspicious packers
Malicious tools

Вредоносная программа

Статья 273 УК РФ трактует термин «**вредоносные программы для ЭВМ**» следующим образом: «... программы для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети...»

Корпорация **Microsoft** трактует термин Malware следующим образом: «**Malware** – это сокращение от «malicious software», обычно используемое как общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу, или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и т.д.»

Классические вирусы

Классические вирусы - программы, распространяющие свои копии по ресурсам локального компьютера с целью последующего запуска своего кода при каких-либо действиях пользователя и дальнейшего внедрения в другие ресурсы компьютера.

Различаются между собой по следующим основным признакам:

- среда обитания;
- способ заражения.

Классификация вирусов

- По среде обитания
  - Файловые вирусы
  - Загрузочные вирусы
  - Макро-вирусы
  - Скриптовые вирусы

Классификация вирусов

Способы заражения

- Перезаписывающие (overwriting)
- Паразитические (parasitic)
- Заражающие объектные модули (OBJ)
- Вирусы-компаньоны (companion)
- Заражающие библиотеки компиляторов (LIB)
- Вирусы-ссылки (link)
- Заражающие исходные тексты программ

Сетевые черви

Сетевые черви - программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры сети.

Троянские программы

Троянские программы - программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Malicious tools (Вредоносные утилиты)

Malicious tools - программы, разработанные для автоматизированного создания вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п.

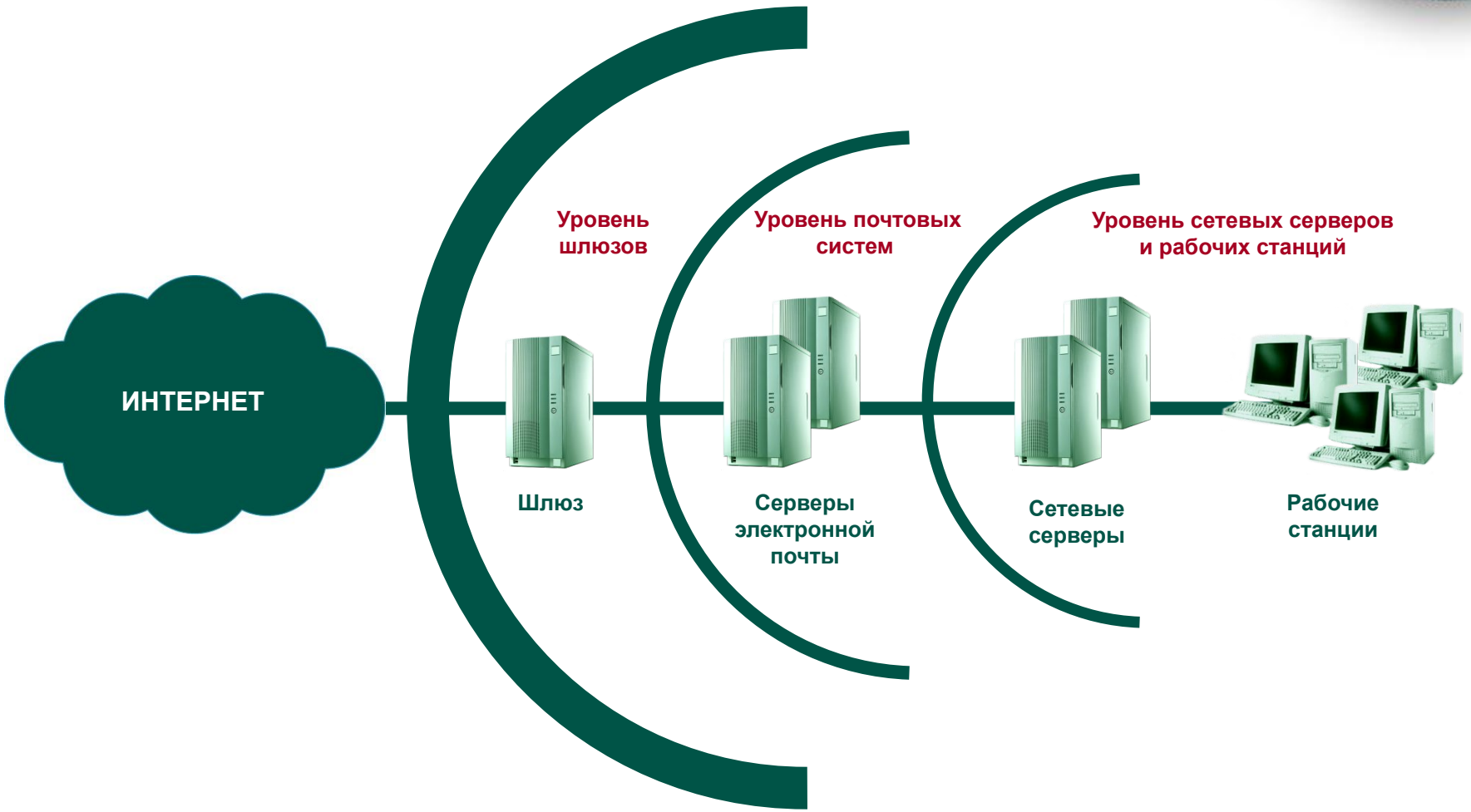
Adware, Pornware, Riskware

Adware - рекламное программное обеспечение, предназначенное для показа рекламных сообщений (чаще всего в виде графических баннеров), перенаправления поисковых запросов на рекламные web-страницы, а также для сбора данных маркетингового характера о пользователе (например, какие тематические сайты он посещает), что позволяет более четко задать аудиторию для рекламной кампании.

Pornware - программы, которые связаны с показом пользователю материалов порнографического характера.

Riskware - это легальные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые в руках злоумышленника способны причинить вред пользователю (вызвать уничтожение, блокирование, модификацию или копирование данных, нарушить работу компьютеров или компьютерных сетей).

Антивирусная защита



Назначение Антивируса Касперского

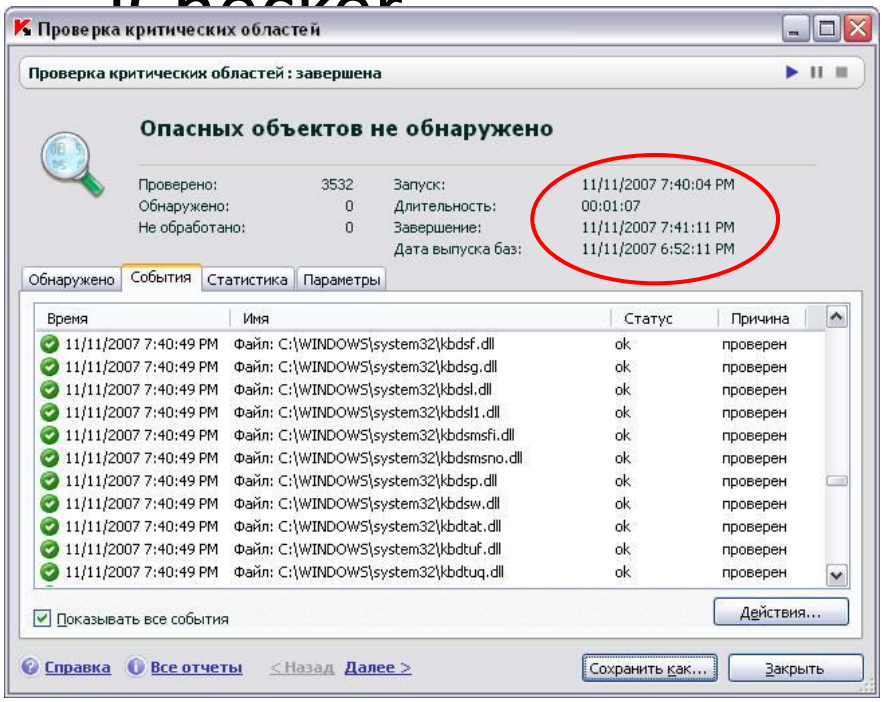
- Защита в режиме реального времени
  - файловой системы
  - электронной почты
  - защита при работе в сети Интернет
  - контроль активности приложений
  - контроль сетевых соединений
  - защита от сетевых атак
- Поиск вредоносных программ
- Обновление сигнатур угроз и компонентов приложения
- Аварийная проверка и восстановление системы

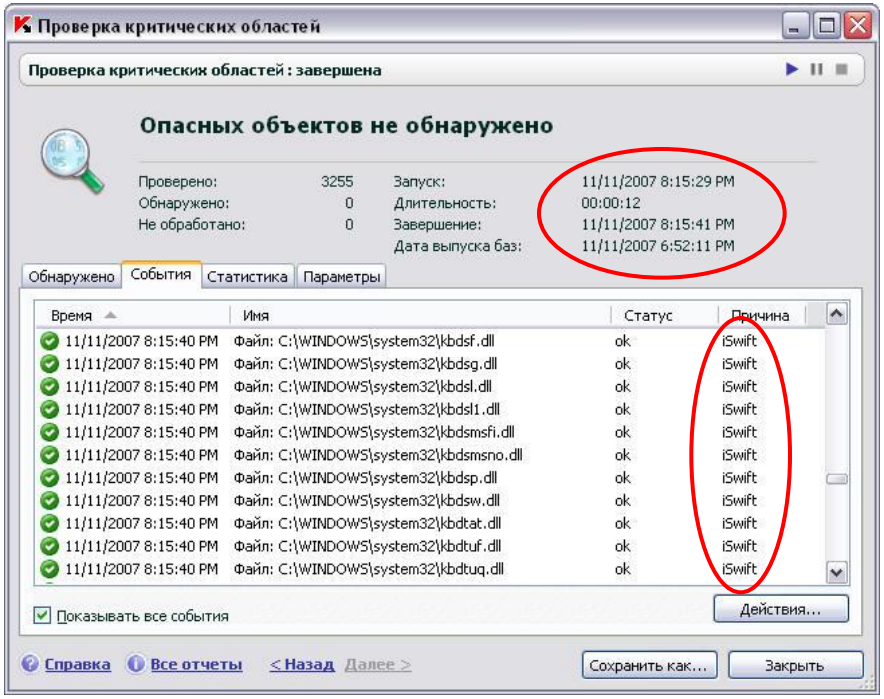
Модули приложения

- Базовый модуль
  - антивирусный сканер
  - компонент загрузки обновлений
- Набор опциональных компонентов
  - Файловый Антивирус
  - Почтовый Антивирус
  - Веб-Антивирус
  - Проактивная защита
  - Анти-Шпион
  - Анти-Хакер
  - Анти-Спам

Скорость работы

Эффективность технологий iSwift и iChecker





- **Существенное ускорение (*12сек* против *1мин 07сек*)**