Принципы обеспечения компьютерной безопасности

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

1. Основные понятия и положения компьютерной безопасности.

2. Защита информации в компьютерных системах.

3. Защита от вредоносного программного обеспечения.

4. Принципы обеспечения сетевой безопасности.

ЛИТЕРАТУРА

Основная литература

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В.К. Новиков, С.Б. Вепрев ; Академия СК РФ. – Москва : ЮНИТИ-ДАНА, 2019. – 287 с.

2. Основы информационной безопасности в органах внутренних дел : учеб. пособие / сост. А.Б. Сизоненко, С.Г. Клюев, В.Н. Цимбал. - Краснодар : Краснодарский университет МВД России, 2016. – 122 с..

ЛИТЕРАТУРА

Основная литература

3. Костюченко, К.Л. Основы информационной безопасности в органах внутренних дел : учеб. пособие / К. Л. Костюченко, С. В. Мухачев. – Екатеринбург: Уральский юридический институт МВД России, 2015. – 155 с.

1. Основные понятия и положения компьютерной безопасности

Компьютерная безопасность -

состояние защищенности (безопасность) информации (данных) в компьютерных системах и

безотказность (надежность) функционирования компьютерных систем.

«Компьютерная система» (КС)

человеко-машинная система, представляющая совокупность электронно-программируемых технических средств обработки, хранения и представления данных,

программного обеспечения (ПО), реализующего информационные технологии осуществления каких-либо функций,

и информации (данных).

Таким образом, **компьютерная система представляет собой совокупность** следующих компонентов:

- информационных массивов, представленных на различных машинных носителях (**данных**);

- технических средств обработки и передачи данных (**оборудования**);

Компьютерная система представляет собой совокупность следующих компонентов:

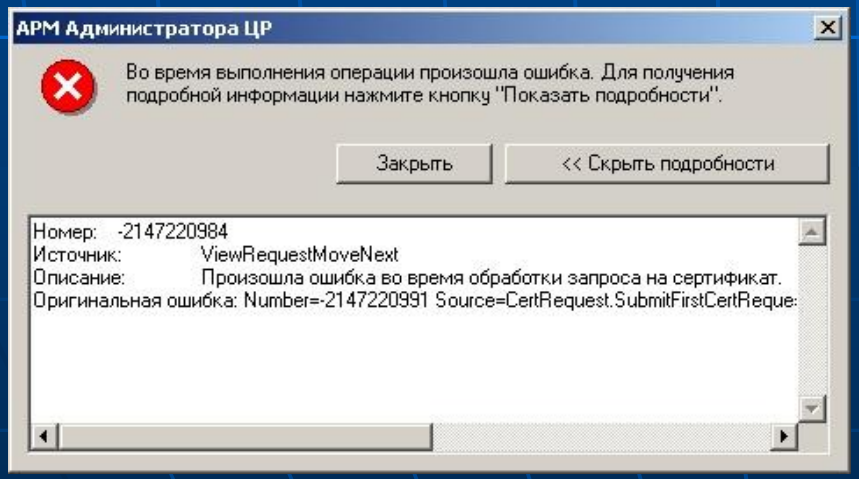
- программных средств, реализующих соответствующие методы, алгоритмы и технологию обработки информации (**программ**);

- обслуживающего персонала и пользователей системы (**персонала**).

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Случайные угрозы:

- сбои и отказы в работе технических средств;

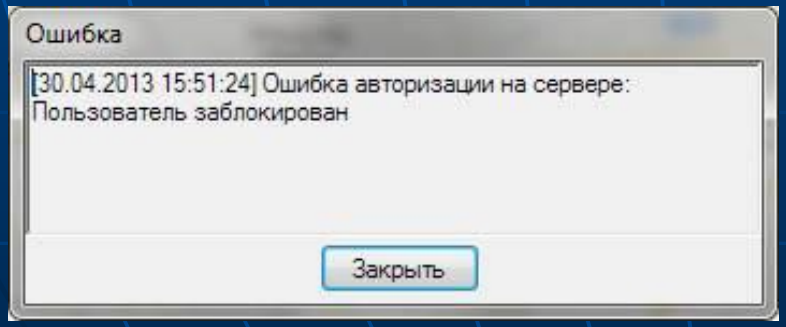


Сбой **- это временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции**

Отказ **- это необратимое нарушение работоспособности какого-либо элемента системы, приводящее к невозможности вы полнения им своих функций.**

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

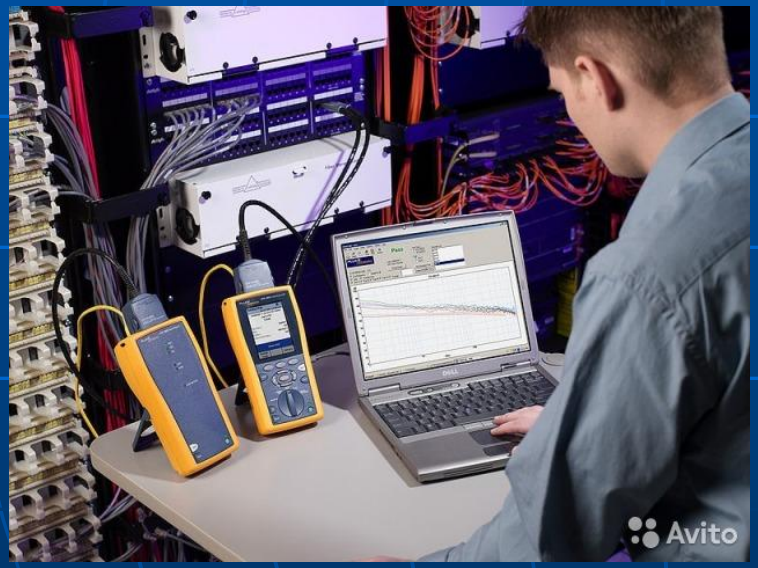
Случайные угрозы:



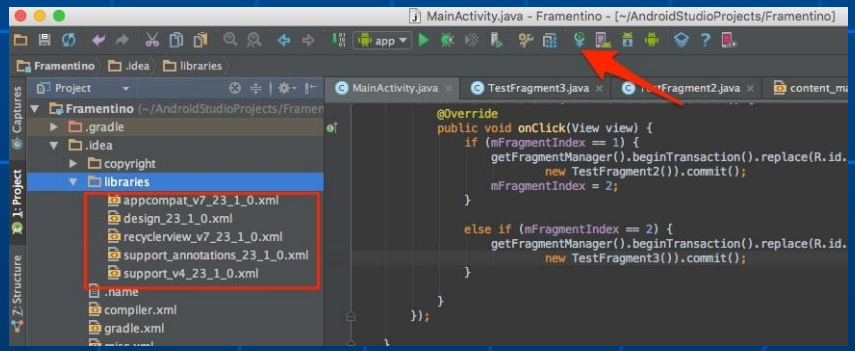
- **ошибки обслуживающего персонала и пользователей;**

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Случайные угрозы:



- ошибки при разработке КС;



Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Случайные угрозы:

- **стихийные бедствия и аварии.**

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Преднамеренные угрозы :

- традиционный шпионаж и диверсии;

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Преднамеренные угрозы :

- **электромагнитные излучения и наводки;**

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Преднамеренные угрозы :

- **модификация структур КС;**

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Преднамеренные угрозы :

- **несанкционированный доступ к информации;**

Несанкционированный доступ **- доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.**

Причины несанкционированного доступа к информации:

- ошибки конфигурации;

- слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников);

Причины несанкционированного доступа к информации:

- ошибки в программном обеспечении;

- злоупотребление служебными полномочиями;

- прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС;

- использование клавиатурных шпионов, вирусов и троянов.

Все искусственные угрозы безопасности в КС можно подразделить на случайные и преднамеренные.

Преднамеренные угрозы :

- **вредоносное программное обеспечение.**

2. Защита информации в компьютерных системах

Защита информации представляет собой принятие

правовых,

организационных и

технических мер.

Правовые меры включают в себя разработку нормативных правовых актов, регламентирующих отношения в информационной сфере, а также устанавливающих ответственность за нарушения в ней

Правовые меры направлены на решение следующих вопросов:
- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий по доступу к информации;
- права должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя.

Организационные меры ориентированы на людей, а не на технические средства.

Они включают в себя:
- мероприятия, осуществляемые при проектировании компьютерных систем и их обслуживании;
- мероприятия по регламентации допуска сотрудников к ресурсам системы;
- мероприятия, осуществляемые при подборе и обучении персонала;
- организацию работы с документами и носителями информации (учет, использование, хранение, уничтожение);
- организацию охраны и пропускного режима.

Технические меры основаны на использовании различных электронных устройств и специальных программ.

Направления, по которым они реализуются:
- идентификация и аутентификация субъектов и объектов системы;
- разграничение доступа к ресурсам;
- резервное копирование;
- криптографическая защита информации;
- защита от несанкционированного копирования;
- защита от вредоносных программ;
- регистрация и оперативное оповещение о событиях, происходящих в системе (в том числе об атаках) и т.д.

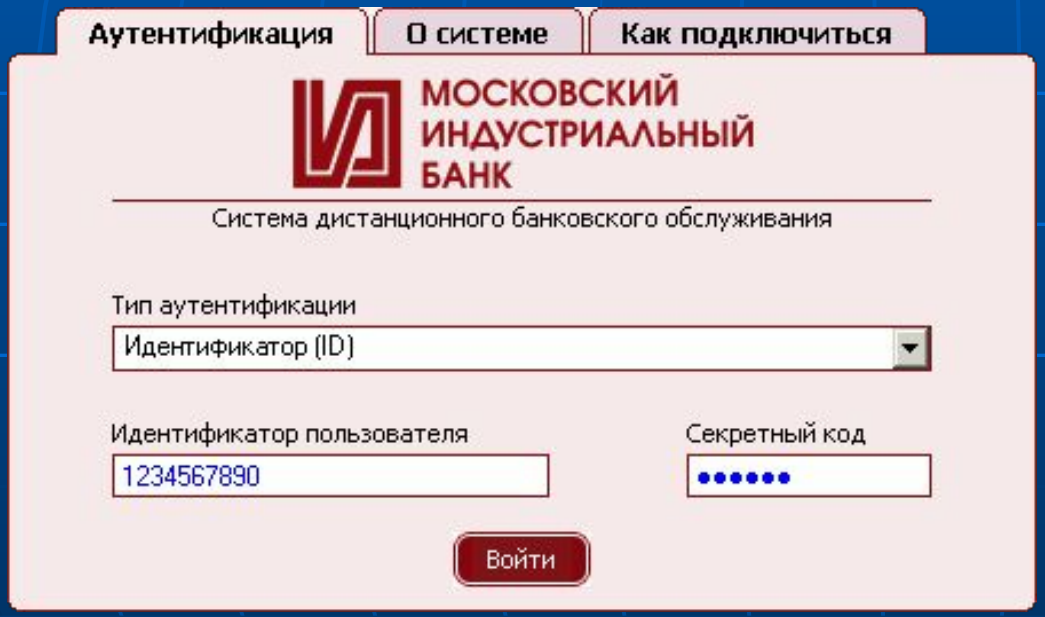
Идентификация и аутентификация в компьютерных системах

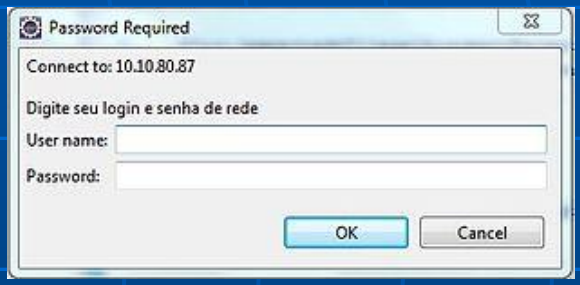
Идентификация **– это присвоение индивидуальных имен, номеров (идентификаторов) субъектам и объектам системы, а также их распознавание (опознавание) по присвоенным им уникальным идентификаторам.**

Аутентификация **– это проверка (подтверждение) подлинности идентификации субъекта или объекта системы.**

Аутентификация пользователей осуществляется:

- путем проверки знания ими паролей;





Аутентификация пользователей осуществляется:

- путем проверки владения ими какими-либо специальными устройствами с уникальными признаками;

Аутентификация пользователей осуществляется:

- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Правила составления пароля:

- при составлении пароля необходимо использовать цифры, символы алфавита различного регистра, спецсимволы;
- длина пароля должна составлять не менее 8 символов;
- нельзя использовать слова и их производные;
- следует систематически менять пароли;
- нельзя использовать одинаковые пароли на различных сервисах;
- нельзя использовать функцию автозаполнения для сохранения паролей.

Разграничение доступа

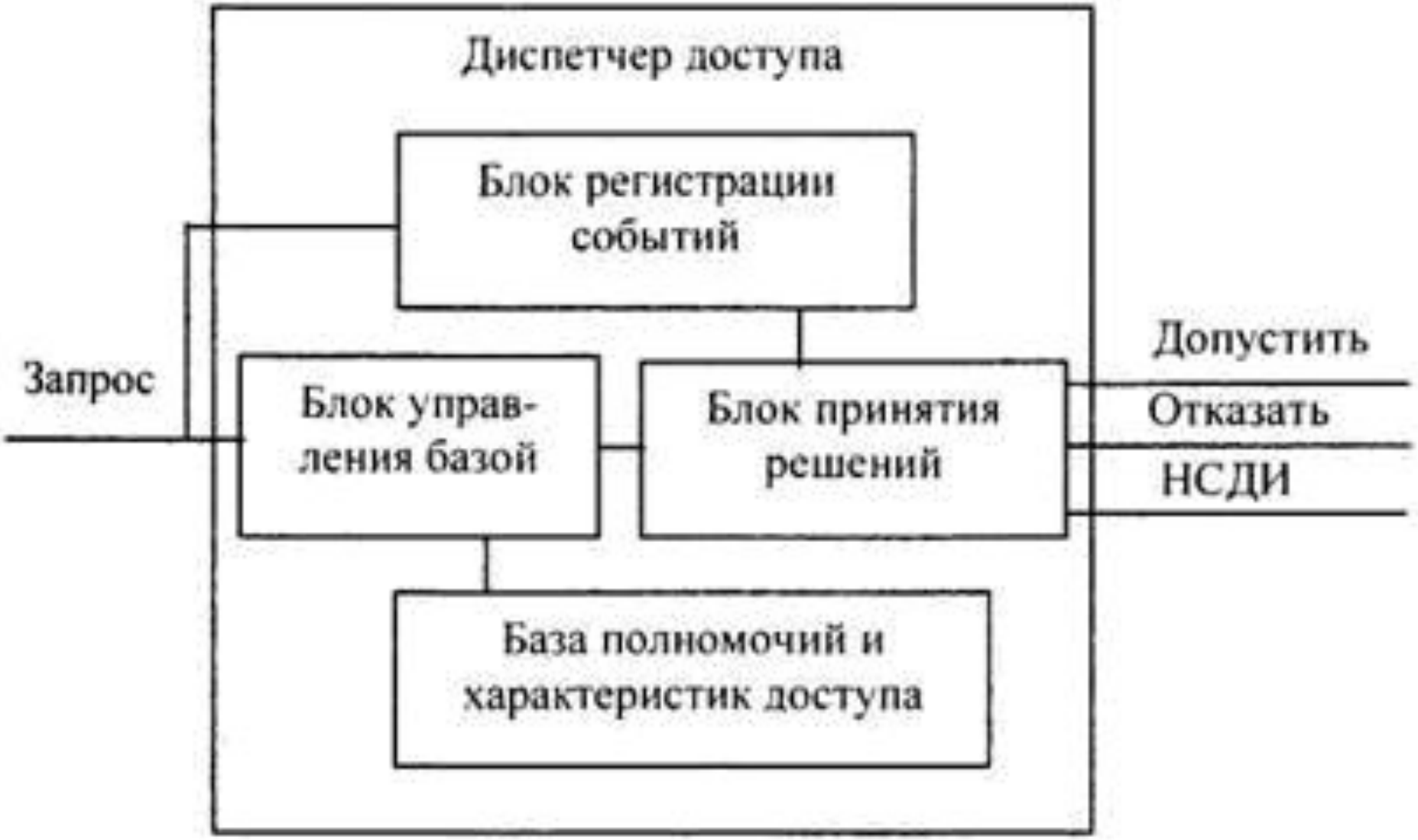
Модели разграничения доступа:

дискреционная
(избирательная)

и

полномочная
(мандатная).

Разграничение доступа



Резервное копирование

Резервное копирование – это процесс создания копии информации, хранящейся на компьютере или ином электронном устройстве, с целью обеспечения возможности восстановления данной информации в случае ее повреждения или разрушения.

Данный метод обеспечивает возможность быстрого восстановления данных в случае их повреждения или разрушения.

Методы резервного копирования:

- полное резервное копирование;
- инкрементальное (инкрементное) резервное копирование;
- дифференциальное резервное копирование.

Криптографическое преобразование информации

Криптография **– это раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.**

Криптоанализ **– это раздел прикладной математики, изучающий модели, алгоритмы, программные и аппаратные средства криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст.**

К криптографическим методам зашиты в общем случае относятся:

- шифрование (дешифрование) информации;
- формирование и проверка цифровой подписи электронных документов.

Защита программного обеспечения от несанкционированного использования и копирования

- *Ввод пароля (серийного номера)*
- *Счетчик возможных установок*
- *Проверка наличия CD/DVD-диска*
- *Привязка к параметрам компьютера и активация*
- *Проверка наличия электронного ключа*
- *Использование подхода SaaS*
- *Сетевая защита*
- *Защита программного кода от исследования*
-

3. Защита от вредоносного программного обеспечения.

Вредоносная программа – программа, используемая для осуществления **несанкционированного доступа** к информации и (или) **воздействия на информацию или ресурсы** автоматизированной информационной системы

273 статья УК РФ определяет вредоносное программное обеспечение как компьютерные программы либо иную компьютерную информацию, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Основные признаки заражения вредоносным ПО:

- прекращение работы или неправильная работа программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов (нереальные значения);

Основные признаки заражения вредоносным ПО:

- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- существенное увеличение сетевого трафика;

Основные признаки заражения вредоносным ПО:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Причины, по которым антивирус не справился со своей задачей:

- ***антивирус был отключен пользователем;***
- ***антивирусные базы были слишком старые;***
- ***были установлены слабые настройки защиты;***

- *вирус использовал технологию заражения, против которой у антивируса не было средств защиты;*
- *вирус попал на компьютер раньше, чем был установлен антивирус, и смог обезвредить антивирусное средство;*
- *это был новый вирус, для которого еще не были выпущены антивирусные базы.*

Основные виды вредоносного ПО:

- вирусы,
- черви,
- троянские программы,
- прочие вредоносные программы.

Вирус **– это программа или часть программного кода, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы или системные области компьютера.**

Как правило вирусы заражают отдельную рабочую станцию, и не могут самостоятельно распространяться между ними.

Черви **(вирусы-репликаторы) – это вредоносные программы, которые способны самостоятельно распространяться в локальных и глобальных вычислительных сетях.**

В отличие от вирусов черви не заражают локальные файлы на компьютере, а создают и распространяют свои копии, которые не всегда совпадают с оригиналом.

Троянские программы **– это вредоносные программы, которые замаскированы под обычное прикладное ПО.**

Они не способны распространяться самостоятельно, поэтому для них важно спровоцировать пользователя запустить исполняемый файл троянской программы.

Классификация вредоносных программ по вредоносной нагрузке:

- **вредоносные программы, создающие помехи в работе ЭВМ;**
- **вредоносные программы, предназначенные для кражи данных, шпионажа, мошенничества и вымогательства;**
- **вредоносные программы, предназначенные для инсталляции иных вредоносных программ;**
- **вредоносные программы для прочей незаконной деятельности;**
- **программы, не являющиеся истинно вредоносными**

Методы защиты компьютерных систем от вредоносных программ

Организационные методы *направлены в первую очередь на* ***пользователя компьютера.*** *Их цель состоит в том, чтобы изменить поведение пользователя, ведь не секрет, что часто вредоносные программы попадают на компьютер из-за необдуманных действий пользователя. Простейший пример организационного метода -* ***разработка правил работы за компьютером****, которые должны соблюдать все пользователи.*

Методы защиты компьютерных систем от вредоносных программ

***Программно-технические методы**, наоборот, направлены на изменения в компьютерной системе. Большинство программно-технических методов состоит в использовании дополнительных средств защиты, например, антивирусных программ.*

Принципы действия антивирусных программ:

1. **Реактивная защита** – защита от известных угроз с использованием знаний об участках кода и других уникальных особенностях существующих вредоносных программ.
2. **Проактивная защита** – защита от новых вредоносных программ, основанная на знании неуникальных особенностей кода и поведения, характерных для деструктивного ПО.

4. Принципы обеспечения сетевой безопасности.

Методы воздействия нарушителей на сети:

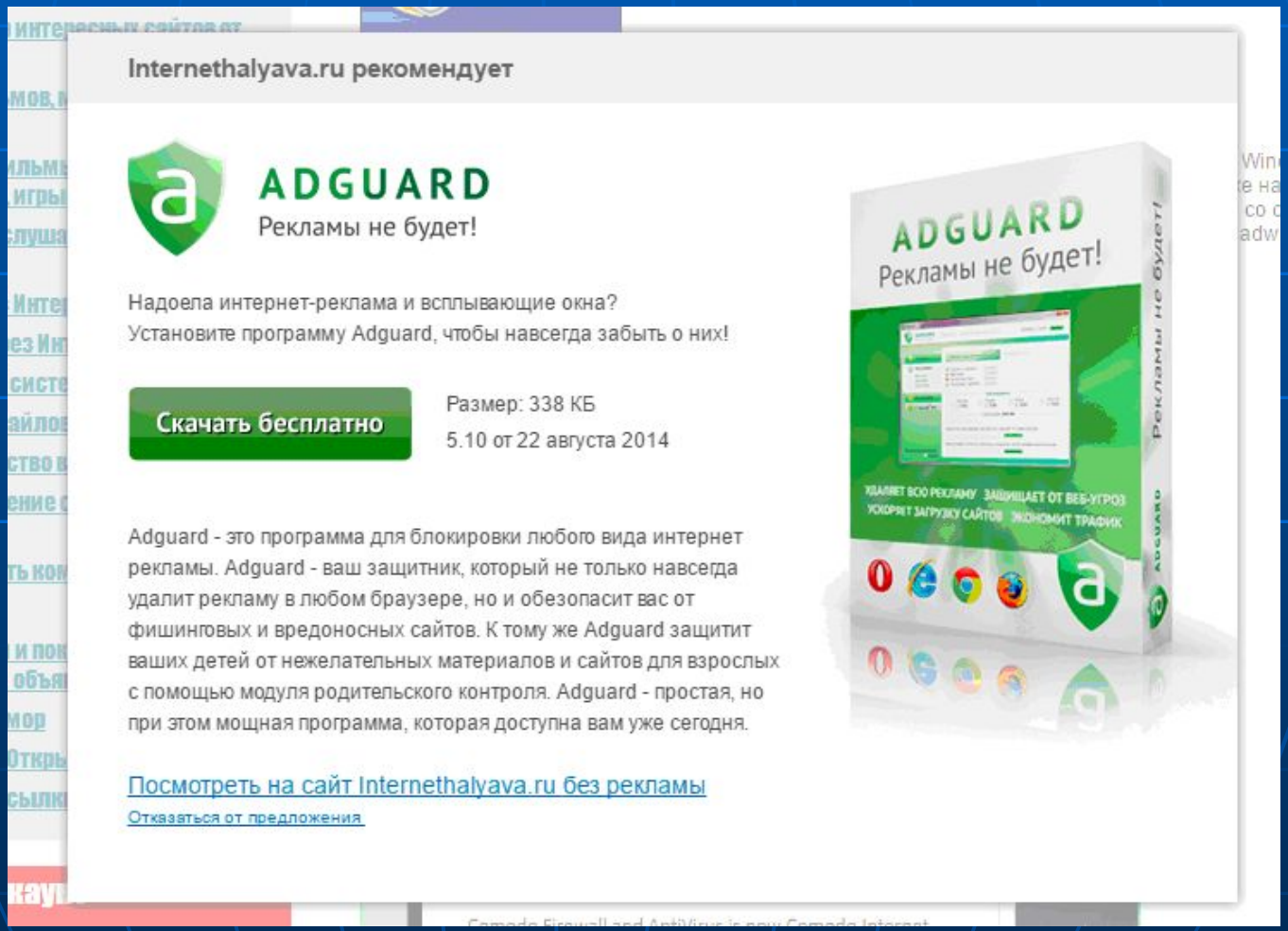
- пассивные методы:
  - прослушивание каналов связи.
- активные методы:
  - подавление каналов связи;
  - сетевые атаки.

Виды сетевых атак:

- **подмена IP-адресов;**
- **просмотр (сканирование) портов;**
- **«отказ в обслуживании» (DoS** от *Denial of Service*) **;**
- **атака прикладного уровня;**

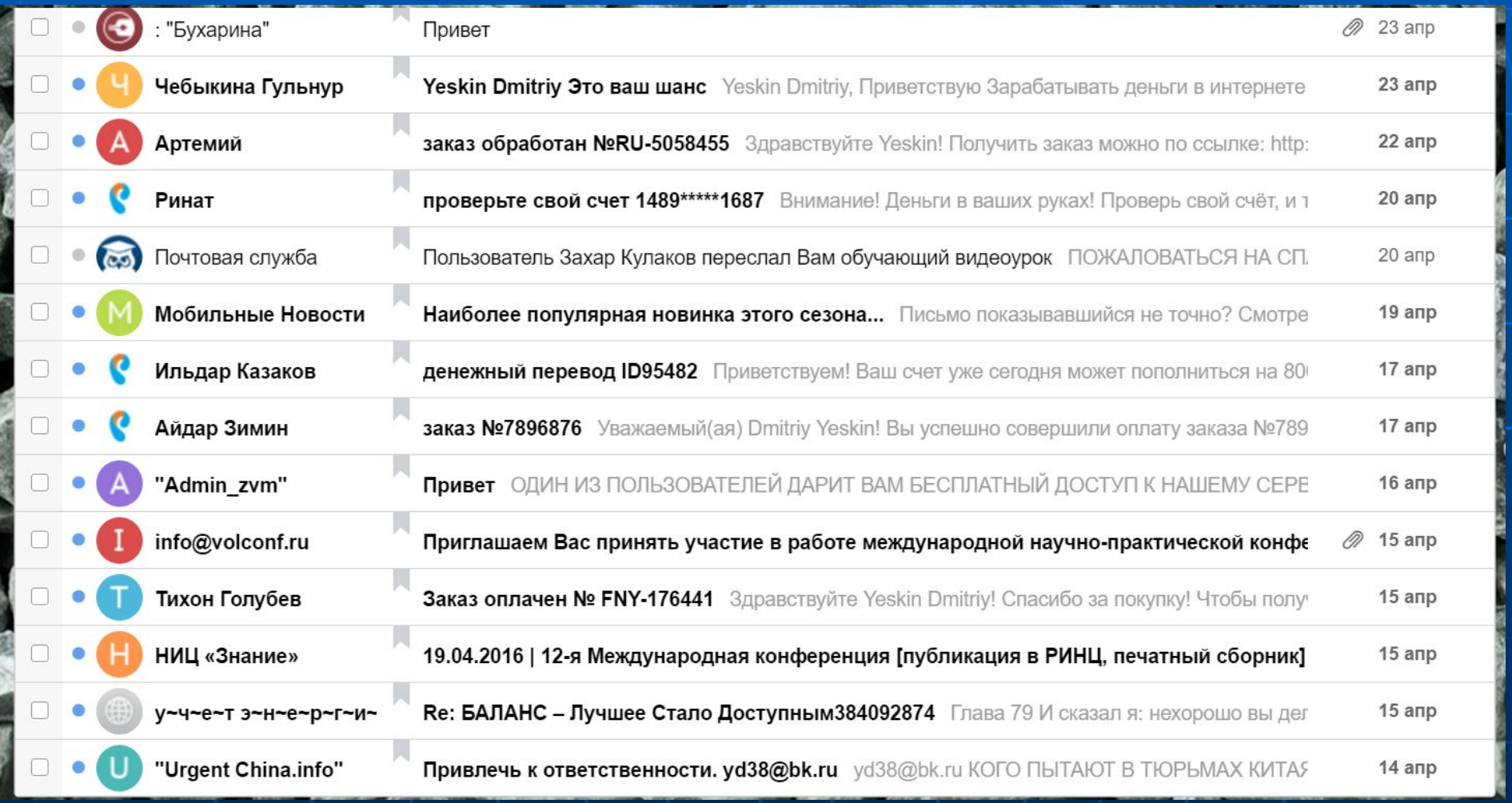
Виды сетевых атак:

- внедрение «троянских коней;



Виды сетевых атак:

- внедрение «троянских коней»;



Виды сетевых атак:

- *Phishing* (*password* harvesting *fishing*) – атака, направленная на получение паролей, PIN-кодов и пр.

Письмо ↑ предыдущее следующее ↓

Ответить | Ответить всем | Переслать | Удалить | Это спам | Переместить

Пример фишинг-сообщения

От кого: **Администрация Альфа-Банка** <admin@alfabank.ru>

Кому:

Уважаемый клиент!

На Ваш текущий счет был получен перевод в размере 200000 (двести тысяч) руб. В соответствии с пользовательским соглашением Альфа-Банка, Вам необходимо подтвердить этот перевод. Для подтверждения платежа просим Вас зайти в интернет-банк Альфа-Клик и следовать инструкциям виртуального консультанта.
Если подтверждение не будет получено в течение 24 часов, платеж будет возвращен отправителю.

Для входа в интернет-банк Альфа-Клик, перейдите по данной ссылке >>

С уважением, администрация Альфа-Банка.

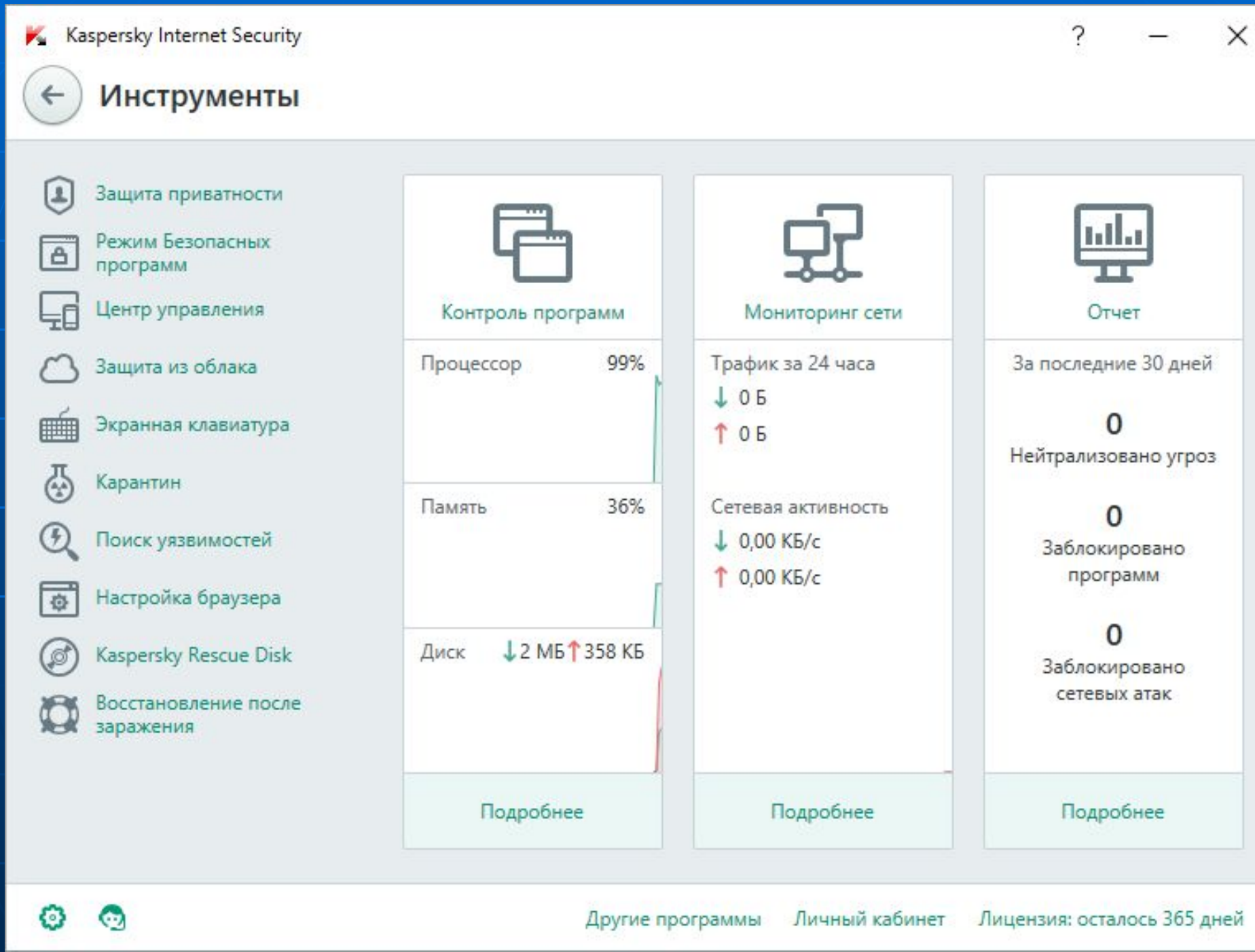
Основные средства защиты информации в системах передачи данных:

- межсетевые экраны;
- частные виртуальные сети (VPN);
- средства анализа защищенности;
- системы обнаружения вторжений.

Межсетевой экран (Firewall, Brandmauer) - это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

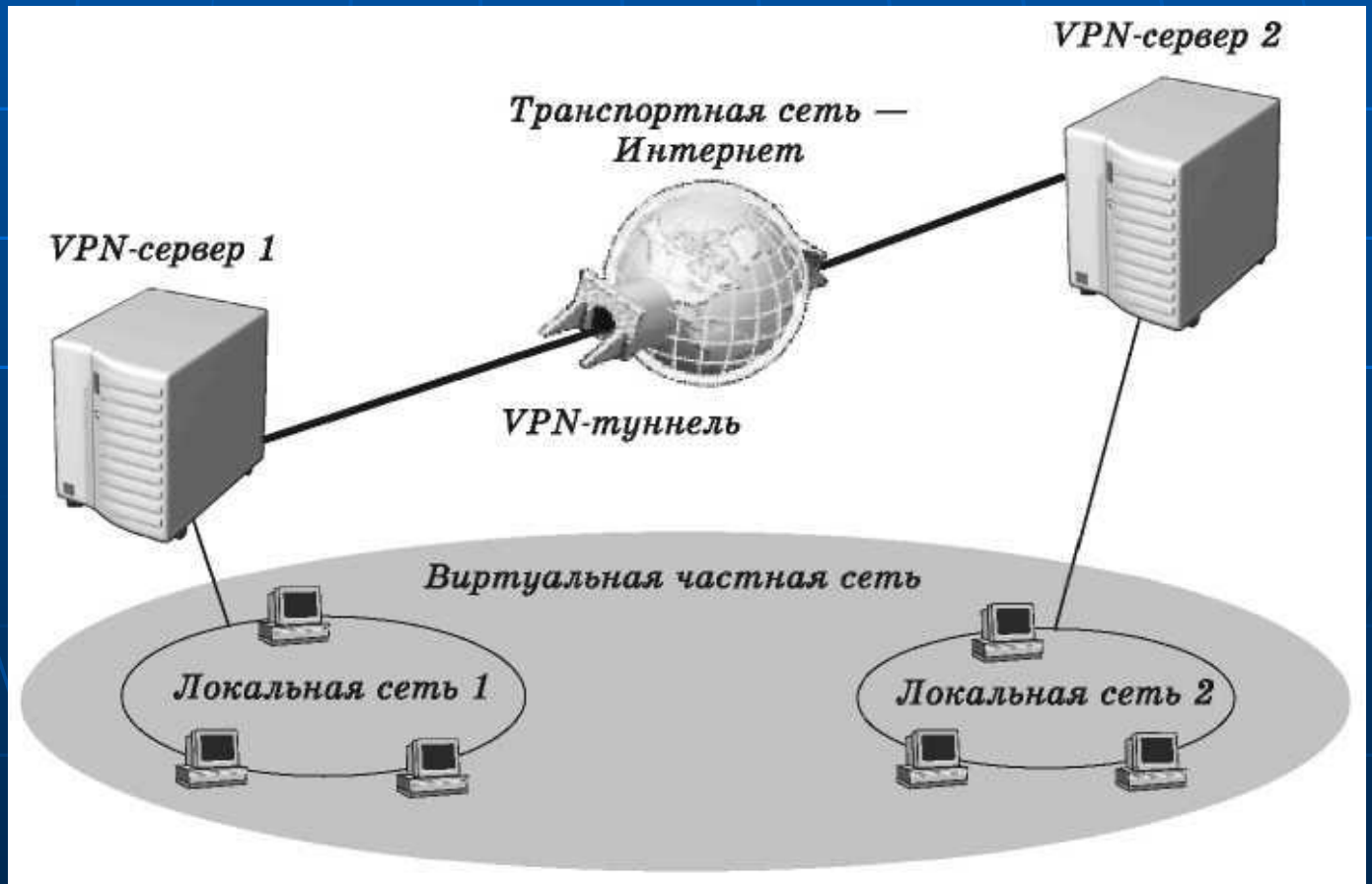
Проблемы, не решаемые МЭ:

- не защищает узлы сети от проникновения через «Чёрный ход» или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь от утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов.

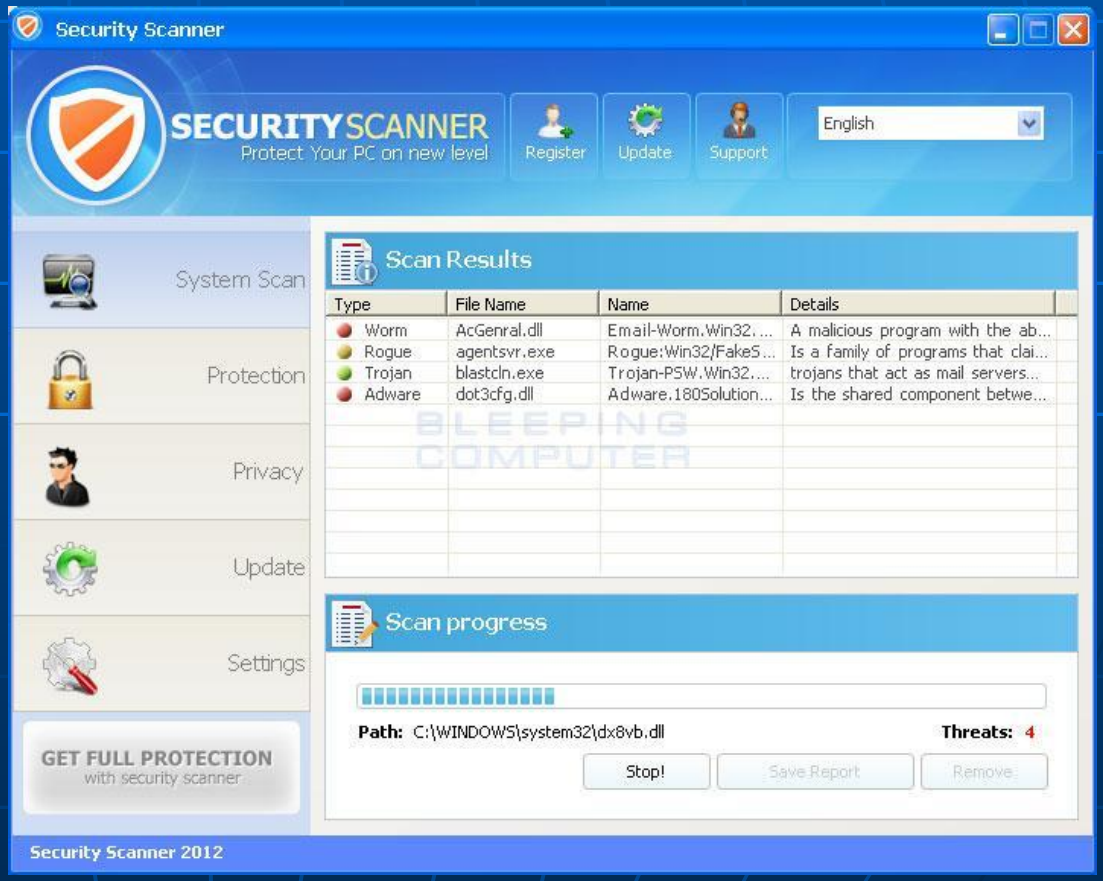

Kaspersky Internet Security
Инструменты
Защита приватности
Режим Безопасных программ
Центр управления
Защита из облака
Экранная клавиатура
Карантин
Поиск уязвимостей
Настройка браузера
Kaspersky Rescue Disk
Восстановление после заражения
Контроль программ
Процессор 99%
Память 36%
Диск ↓2 МБ ↑358 КБ
Подробнее
Мониторинг сети
Трафик за 24 часа
↓ 0 Б
↑ 0 Б
Сетевая активность
↓ 0,00 КБ/с
↑ 0,00 КБ/с
Подробнее
Отчет
За последние 30 дней
0
Нейтрализовано угроз
0
Заблокировано программ
0
Заблокировано сетевых атак
Подробнее
Другие программы
Личный кабинет
Лицензия: осталось 365 дней


COMODO
Internet Security Premium
УЛУЧШИТЬ
Под защитой
Задачи
Антивирус
Кумулятивное сканирование
Предыдущее обновление:
1 час назад
Сканировать
Перетащите файлы сюда
Обнаружено угроз: 0
Авто-Sandbox
Отключён
HIPS
Отключён
Viruscope
Включён
Заблокировано вторжений: 0
Изолировано в Sandbox: 0
Фаервол
Безопасный режим
11
Входящие
281
Исходящие
chrome.exe 60.65%
svchost.exe 24.60%
explorer.exe 11.49%
Сетевых вторжений: 0
Игровой режим
Под защитой
Сканирование
Обновление
Виртуальный рабочий стол
Карантин
Онлайн-поддержка

Виртуальная частная сеть (VPN - Virtual Private Network) - это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия.

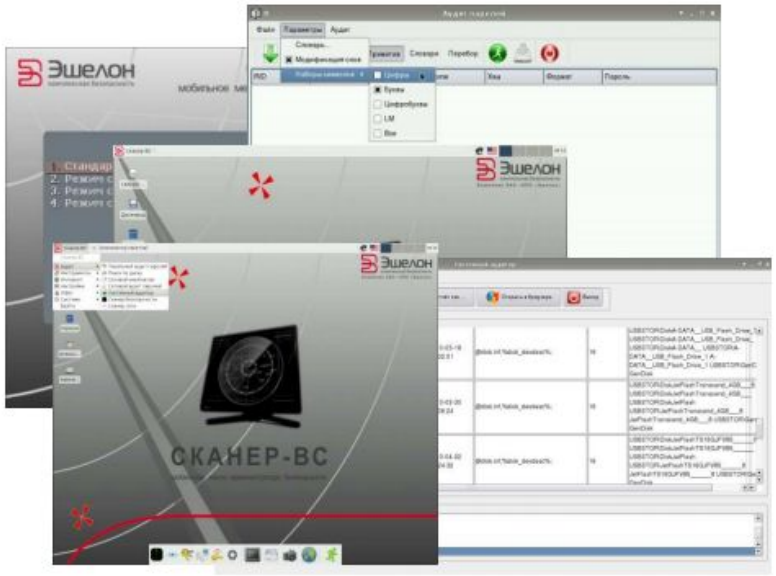


Средства анализа защищенности (сканеры безопасности / security scanners), помогают определить факт наличия уязвимости на узлах корпоративной сети и своевременно устранить их.



Сертифицированное средство защиты информации

Средство анализа защищенности Сканер-ВС



- определение топологии и ресурсов сети
- поиск уязвимостей
- поиск остаточной информации в памяти
- локальный аудит паролей ОС
- перехват и анализ сетевого трафика
- аудит ПО и аппаратной конфигурации
- аудит паролей к сетевым сервисам

НЕ ТРЕБУЕТ УСТАНОВЛЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

- Анализ защищенности рабочих станций пользователей
- Анализ защищенности серверов и сетевого оборудования
- Анализ защищенности веб-сайтов
- Анализ защищенности внешнего периметра организации
- Инвентаризация узлов в сети

Система обнаружения вторжений (Intrusion Detection System / IDS) - программное или аппаратное средство, предназначенное для выявления фактов несанкционированного доступа в компьютерную систему или сеть либо несанкционированного управления ими.

Компоненты системы обнаружения атак:

- Модуль слежения.
- Подсистема обнаружения атак.
- База знаний.
- Хранилище данных.
- Графический интерфейс.
- Подсистема реагирования.
- Подсистема управления компонентами.