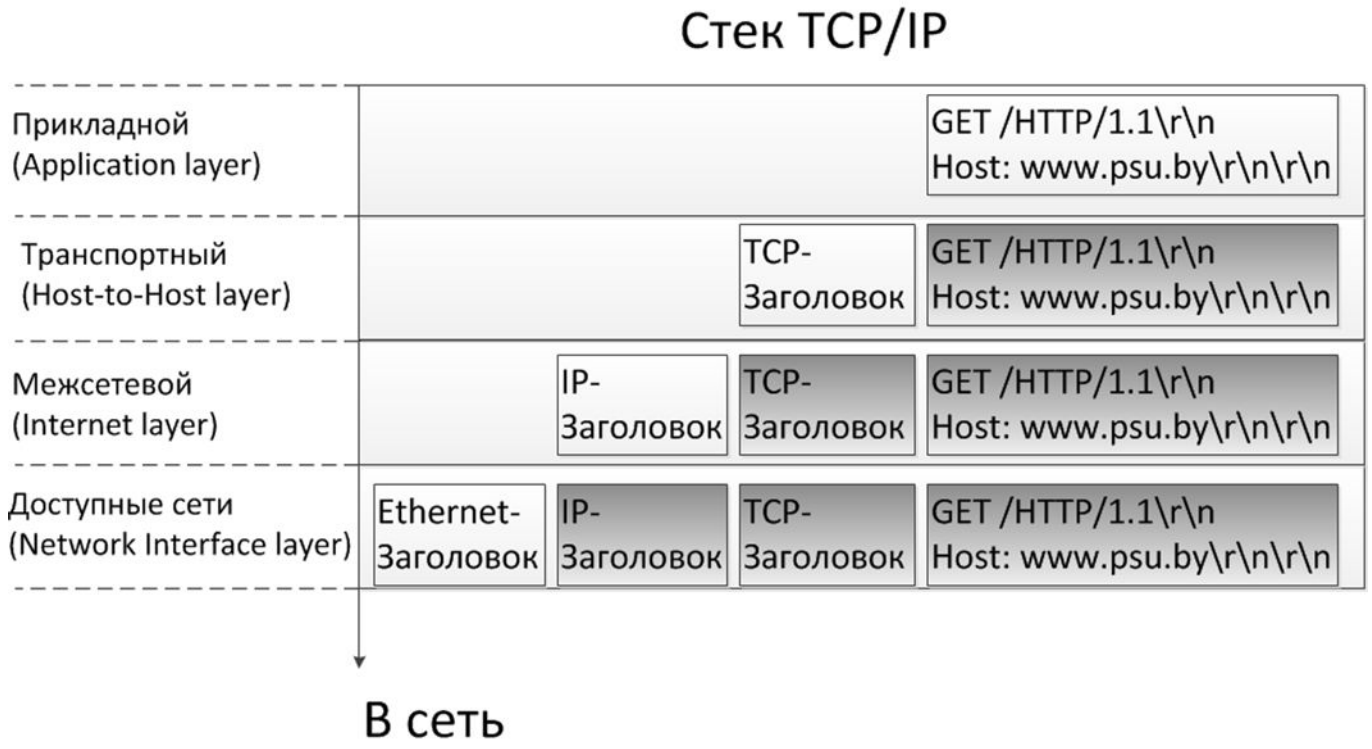
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ

Защита информационных ресурсов компьютерных систем и сетей

Виды атак в IP-сетях

Подслушивание (sniffing) – подключение к линиям связи
Парольные атаки
Изменение данных
«Угаданный ключ»
Подмена доверенного субъекта – хакер выдает себя за санкционированного пользователя (подмена IP-адреса)
Перехват сеанса – хакер переключает установленное соединение на новый хост
Посредничество в обмене незашифрованными ключами
«Отказ в обслуживании»
Атаки на уровне приложений – использование слабостей системного ПО (HTTP, FTP)
Злоупотребление доверием
Вирусы и приложения типа «троянский конь»
Сетевая разведка – сбор информации о сети

Инкапсуляция



Причины уязвимости IP-сетей

1. Аутентификация отправителя осуществляется исключительно по его IP-адресу.
2. Процедура аутентификации выполняется только на стадии установления соединения — в дальнейшем подлинность принимаемых пакетов не проверяется.
3. Важнейшие данные, имеющие отношение к системе, передаются по сети в незашифрованном виде.

«Врожденные слабости» служб Интернет:

Врожденные слабости» служб Интернет

- простой протокол передачи электронной почты SMTP;
- программа электронной почты Sendmail;
- служба сетевых имен DNS;
- служба эмуляции удаленного терминала Telnet;
- всемирная паутина WWW;
- протокол передачи файлов FTP.

Интернет

это всемирная сеть сетей, которая использует для взаимодействия стек протоколов TCP/IP.

Основные причины уязвимости IP-сетей

1. Сеть Internet разрабатывалась как открытая и децентрализованная сеть с изначальным отсутствием политики безопасности.
2. Большая протяженность линий связи и уязвимость основных служб.
3. Модель «клиент — сервер», на которой основана работа в Internet, не лишена слабостей и лазеек в продуктах отдельных производителей.
4. Информация о существующих и используемых средствах защиты доступна пользователям.
5. Существует возможность наблюдения за каналами передачи данных.
6. Средства управления доступом сложно конфигурировать, настраивать и контролировать.
7. Использование большого числа сервисов, информационных служб и сетевых протоколов, освоение которых одному человеку в лице администратора сети практически недоступно.
8. Недостаток в специалистах по защите информации в Internet.
9. Существует потенциальная возможность обойти средства обнаружения отправителя информации либо посетителя Web-узла с помощью использования виртуальных IP-адресов.

В 1993 году создана рабочая группа IP Security Working Group, разработан набор протоколов IPSec, основанных на современных технологиях шифрования и электронной цифровой подписи данных.

Проблемы информационной безопасности существенно зависят от типа информационных систем и сферы их применения.

Особенности информационных систем распределенного типа:

1. Территориальная разнесенность компонентов системы и как следствие наличие обмена информацией между ними.

2. Широкий спектр способов представления, хранения и передачи информации.

3. Интеграция данных различного назначения в единых базах данных и наоборот, размещение данных в различных узлах сети.

4. Использование режимов распределенной обработки данных.

5. Одновременное участие в процессах обработки информации большого количества пользователей с разными правами доступа.

6. Использование разнородных программно-технических средств обработки и систем телекоммуникаций.

Инциденты с безопасностью в Интернете

- Внутренний инцидент - инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом

- Внешний инцидент - инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом

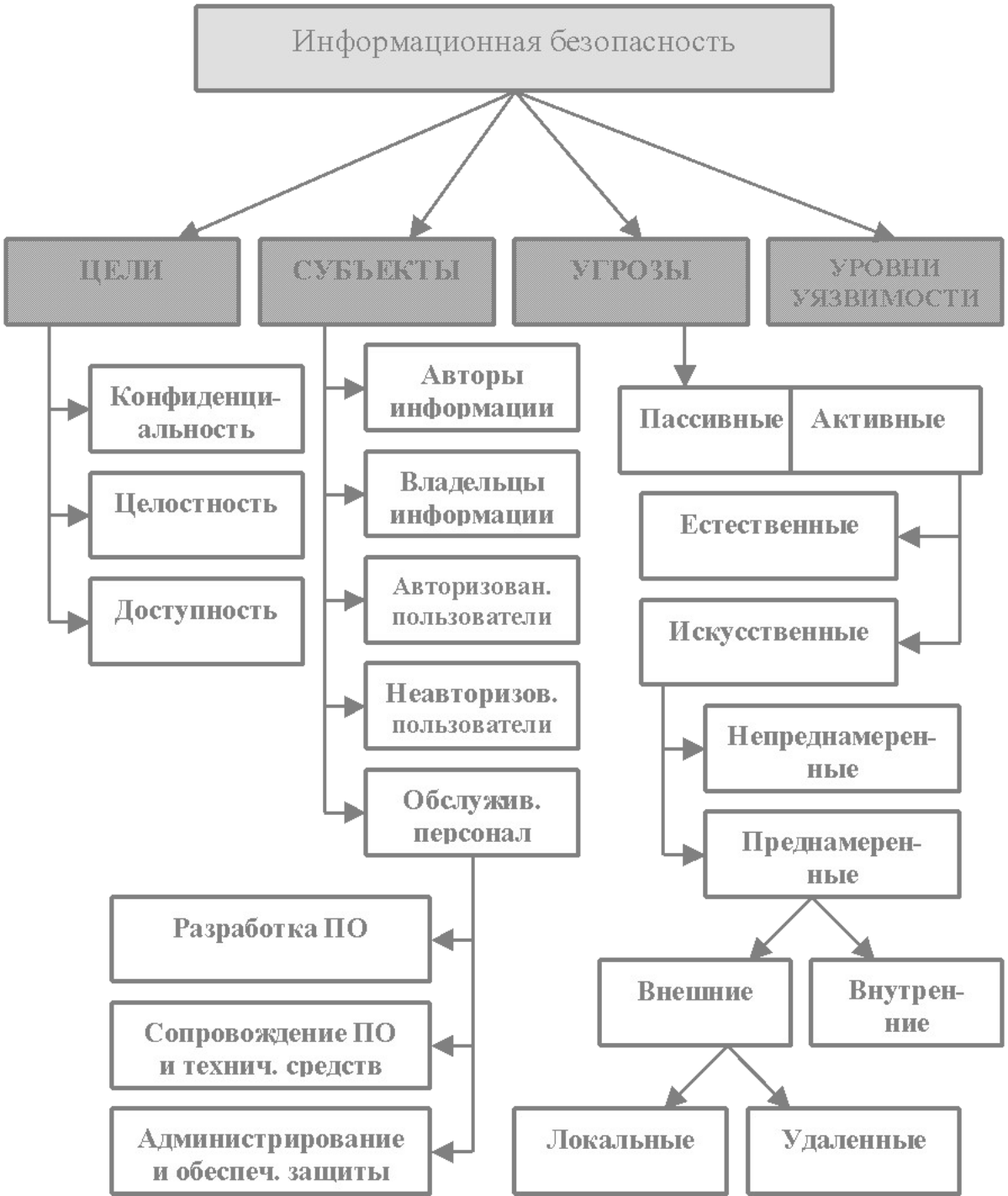
Внутренний инцидент

- утечка конфиденциальной информации;
- неправомерный доступ к информац
- удаление информации;
- компрометация информации;
- саботаж;
- мошенничество с помощью ИТ;
- аномальная сетевая активность;
- аномальное поведение бизнес-приложений;
- использование активов компании в личных целях или в мошеннических операциях.

Внешний инцидент

- мошенничество в системах ДБО;
- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- неправомерное использование корпоративного бренда в сети Интернет;
- фишинг;
- размещение конфиденциальной/провокационной информации в сети
- Интернет;
- взлом, попытка взлома, сканирование портала компании;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации;
- анонимные письма (письма с угрозами).

Модель информационной безопасности



Специфические виды угроз для компьютерных сетей

- несанкционированный обмен информацией между пользователями;

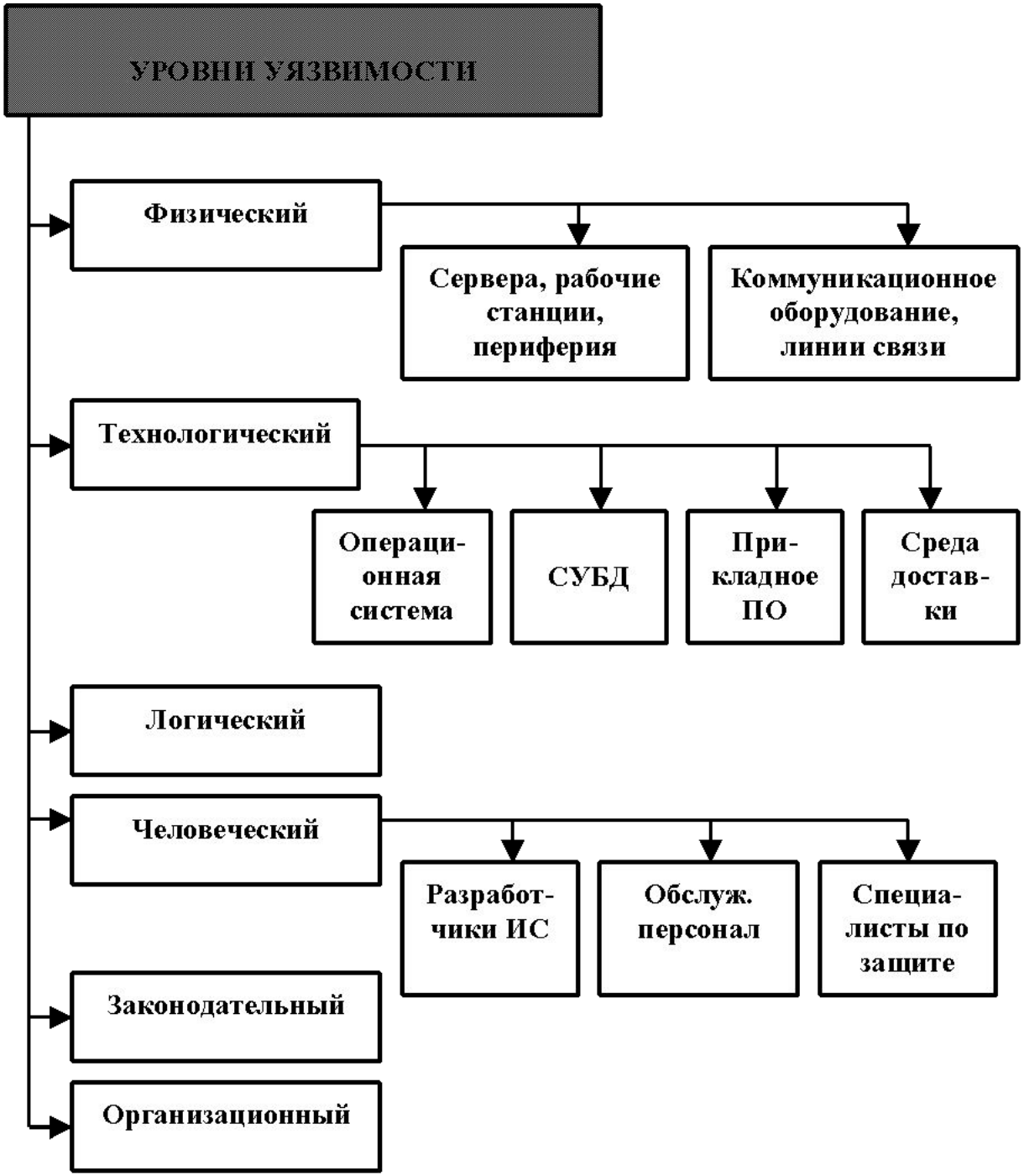
- несанкционированный межсетевой доступ к информационным и техническим ресурсам сети;

- отказ от информации, т.е. непризнание получателем (отправителем) этой информации факта ее получения (отправления);

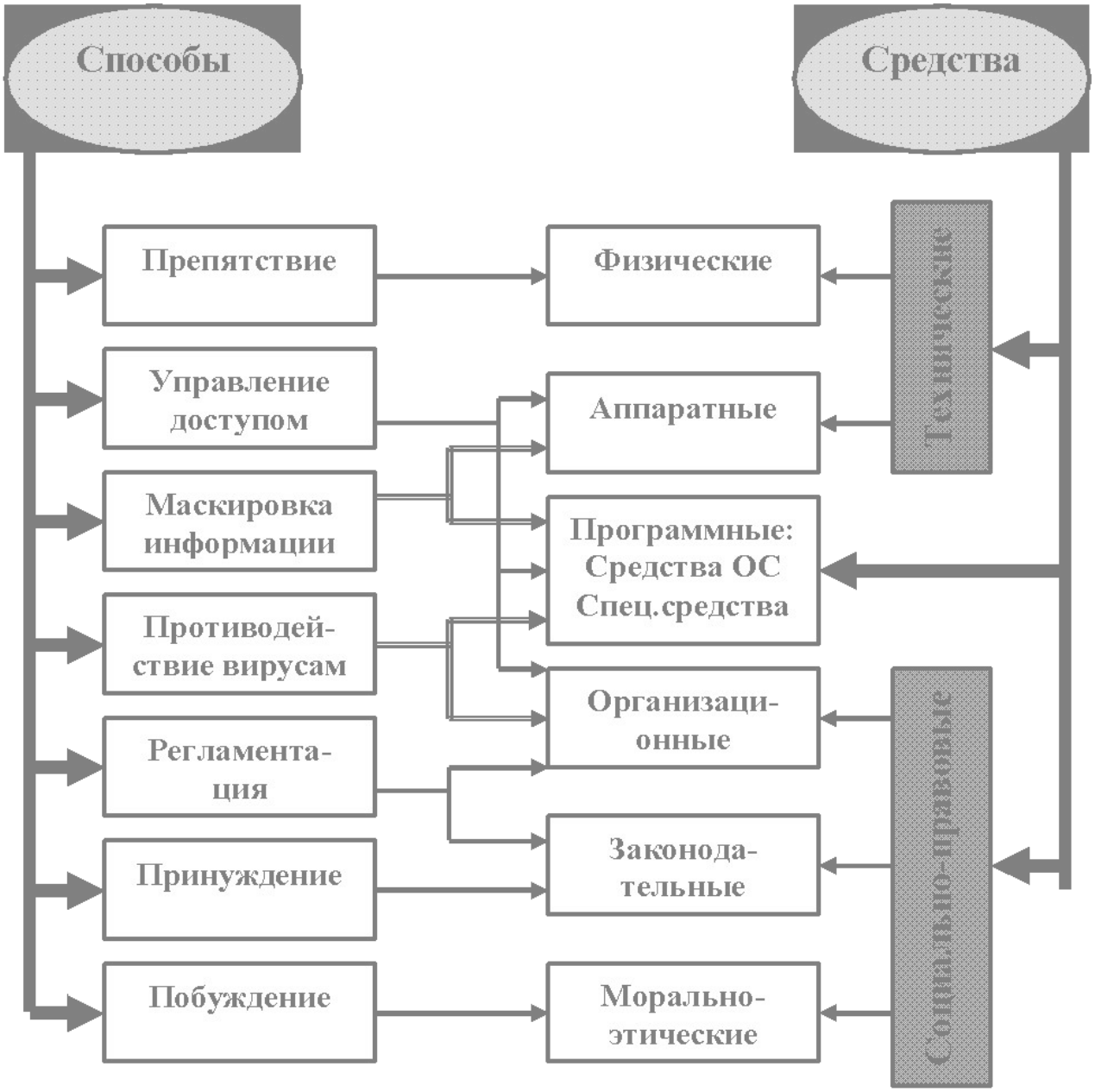
- отказ в обслуживании, который может сопровождаться тяжелыми последствиями для пользователя, обратившегося с запросом на предоставление сетевых услуг;

- распространение сетевых вирусов.

Модель информационной безопасности



Способы и средства защиты информации в сетях



Защита от компьютерных вирусов

Компьютерный вирус - это специально написанная программа, которая может "приписывать" себя к другим программам и выполнять различные нежелательные для пользователя действия на компьютере.

Черви – это независимые программы, размножающиеся путем копирования самих себя через компьютерную сеть.

Троянские кони (троян) – это программы, которые запускаются на компьютере не зависимо от согласия пользователя.

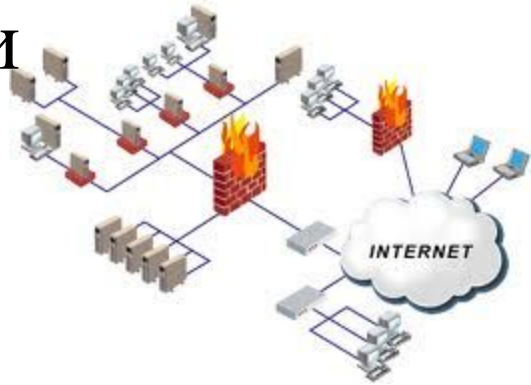
Смешанные коды – это сравнительно новый класс вредоносных программ, сочетающий в себе свойства вирусов, червей и троянов.

Жизненный цикл вируса:

1. Внедрение
2. Инкубационный период
3. Репродуцирование (саморазмножение)
4. Деструкция (искажение и/или уничтожение информации).

Целесообразность использование брандмауэра

- Защита от уязвимых мест в службах
- Управляемый доступ к систем сети



- Концентрированная безопасность
- Повышенная конфиденциальность
- Протоколирование и статистика использования сети и попыток проникновения
- Претворение в жизнь политики

Классификация компьютерных вирусов

Симптомы заражения вирусами:

1. Подозрительная активность диска.
2. Беспричинное замедление работы компьютера.
3. Подозрительно высокий трафик в сети.
4. Изменение размеров и имен файлов.

Классические антивирусные средства основаны на анализе сигнатур вирусов.

Перспективным считается принцип отслеживания отклонений поведения программ и процессов от эталонного (например система Cisco Security Agent, разработанная компанией Cisco System).

В России наиболее распространенными средствами антивирусной защиты являются продукты и технологии компаний:
«Доктор WEB» (www.doctorweb.com)
«Лаборатория Касперского» (www.kaspersky.ru).

Методы защиты сетей

Парольная защита

Требования к паролю:

- в качестве пароля не может использоваться слово из какого бы то ни было языка;
- длина пароля не может быть менее 8 символов;
- один и тот же пароль не может быть использован для доступа к разным ресурсам;
- старый пароль не должен использоваться повторно;
- пароль должен меняться как можно чаще.

Идентификация - процедура распознавания пользователя (процесса) по его имени.

Аутентификация - процедура проверки подлинности пользователя, аппаратуры или программы для получения доступа к определенной информации или ресурсу.

Криптографические методы защиты

Привязка программ и данных к конкретному компьютеру (сети или ключу)

Способы аутентификации

- Аутентификация по многоразовым паролям
- Аутентификация по одноразовым паролям
- Многофакторная аутентификация

Методы защиты сетей

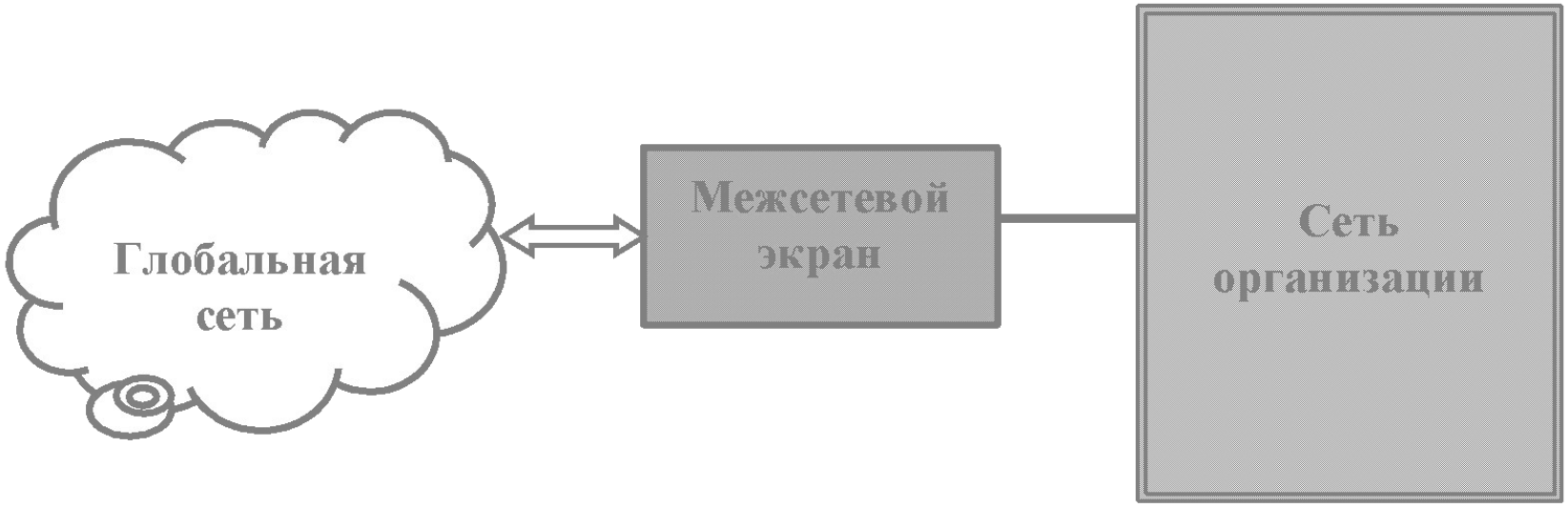
Разграничение прав доступа пользователей к ресурсам сети

Использование заложенных в ОС возможностей защиты

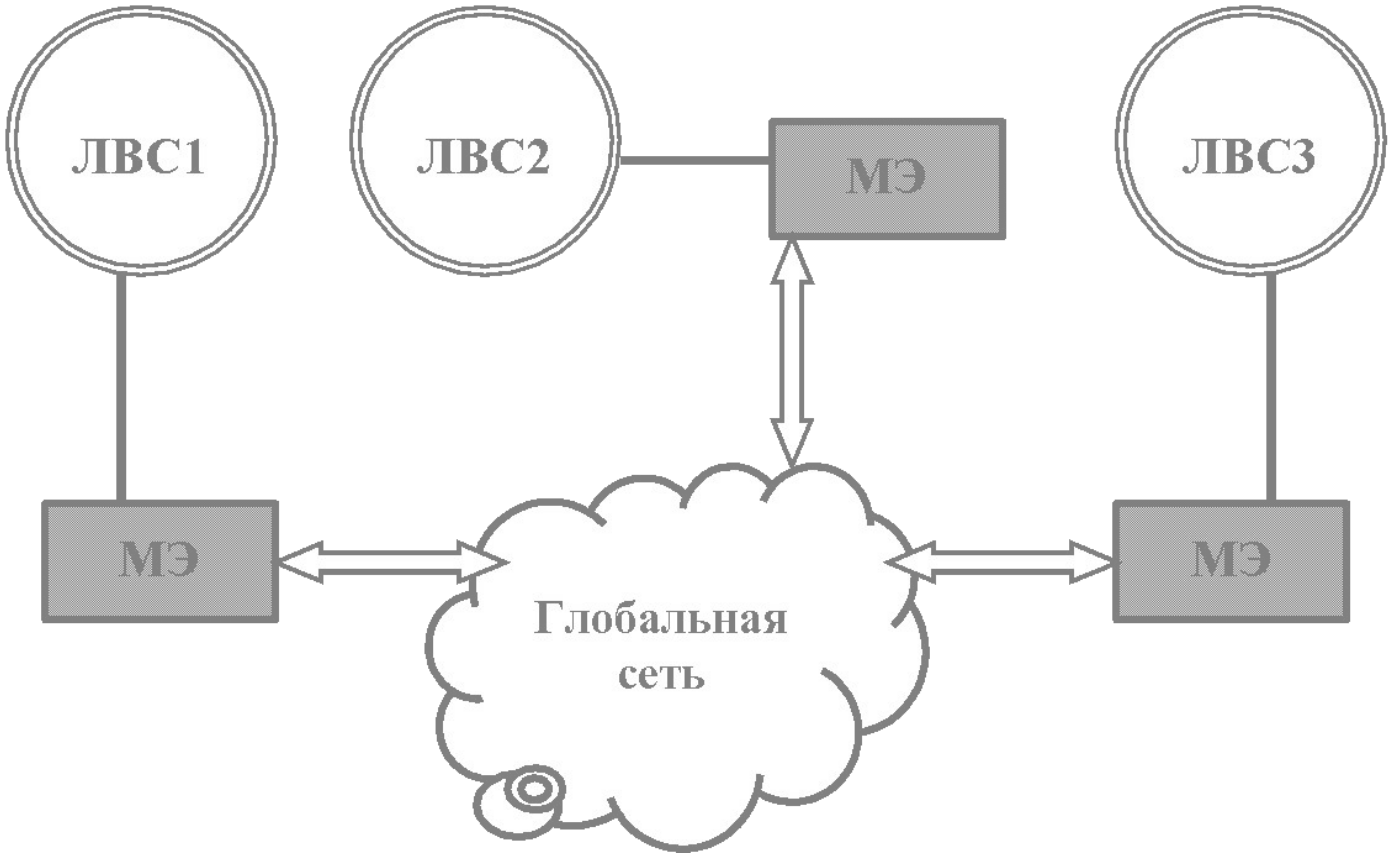
Архитектурные методы защиты

- физическая изоляция закрытого сегмента внутренней сети, содержащего конфиденциальную информацию, от внешней сети;
- функциональное разделение внутренней сети на подсети, при котором в каждой подсети работают пользователи, объединенные по профессиональным интересам;
- сеансовое (кратковременное) подключение внутренней сети к сегменту сети, подключенному к Internet, с помощью коммутатора или моста

Межсетевой экран (брандмауэр, firewall) - это программная или программно-аппаратная система межсетевой защиты, позволяющая разделить две (или более) взаимодействующие сети и реализовать набор правил, определяющих условия прохождения пакетов из одной сети в другую.



Методы защиты сетей

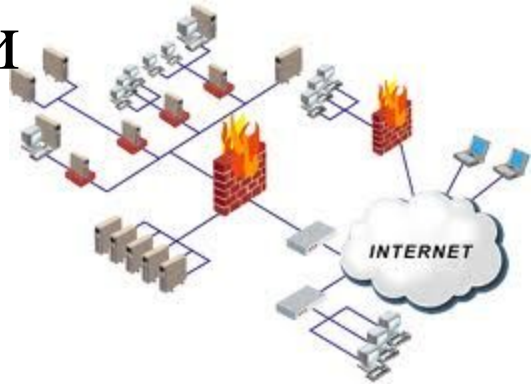


Брандмауэр

это подход к безопасности; он помогает реализовать политику безопасности, которая определяет разрешенные службы и типы доступа к ним, и является реализацией этой политики в терминах сетевой конфигу

Целесообразность использование брандмауэра

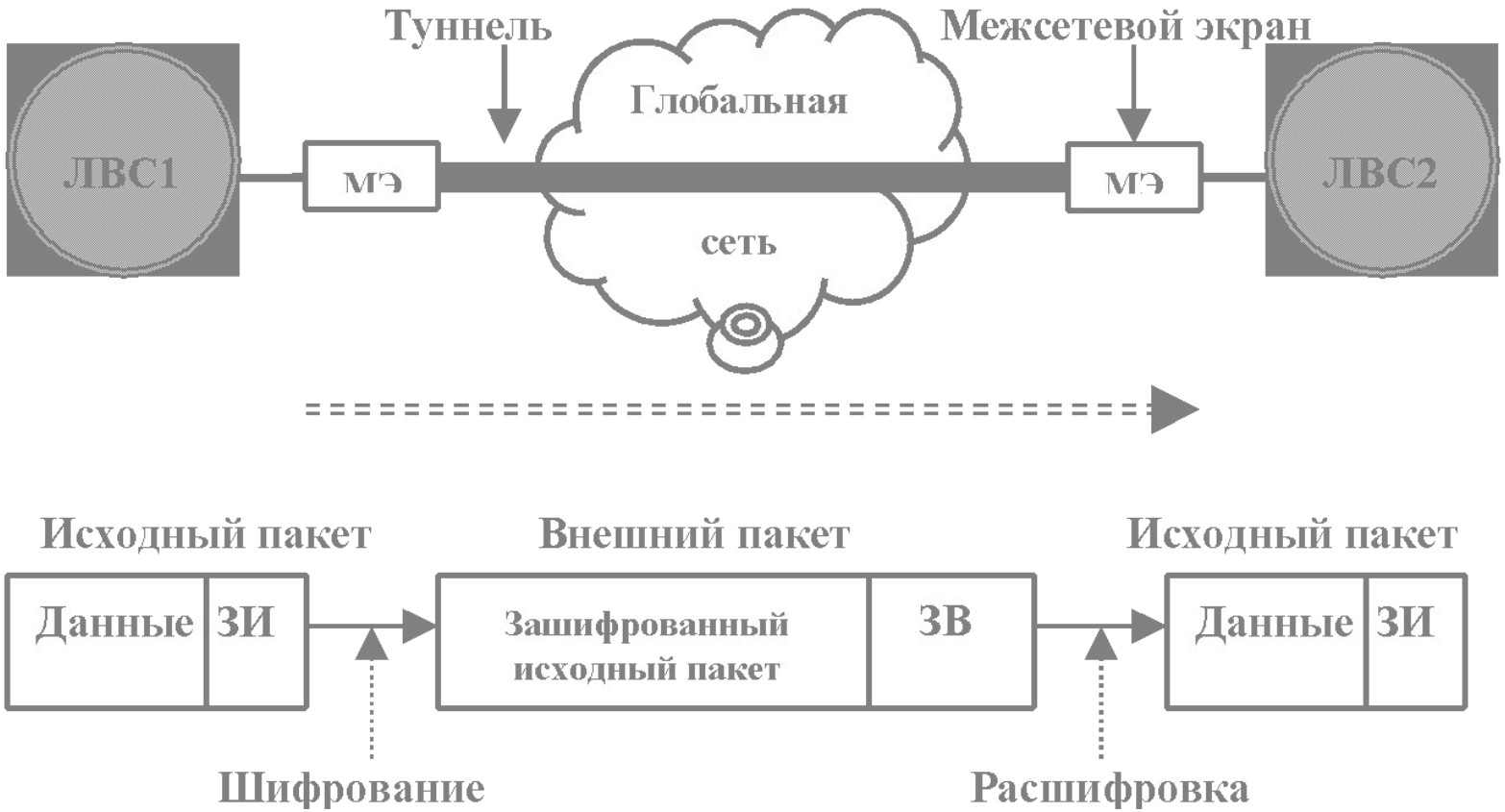
- Защита от уязвимых мест в службах
- Управляемый доступ к систем сети



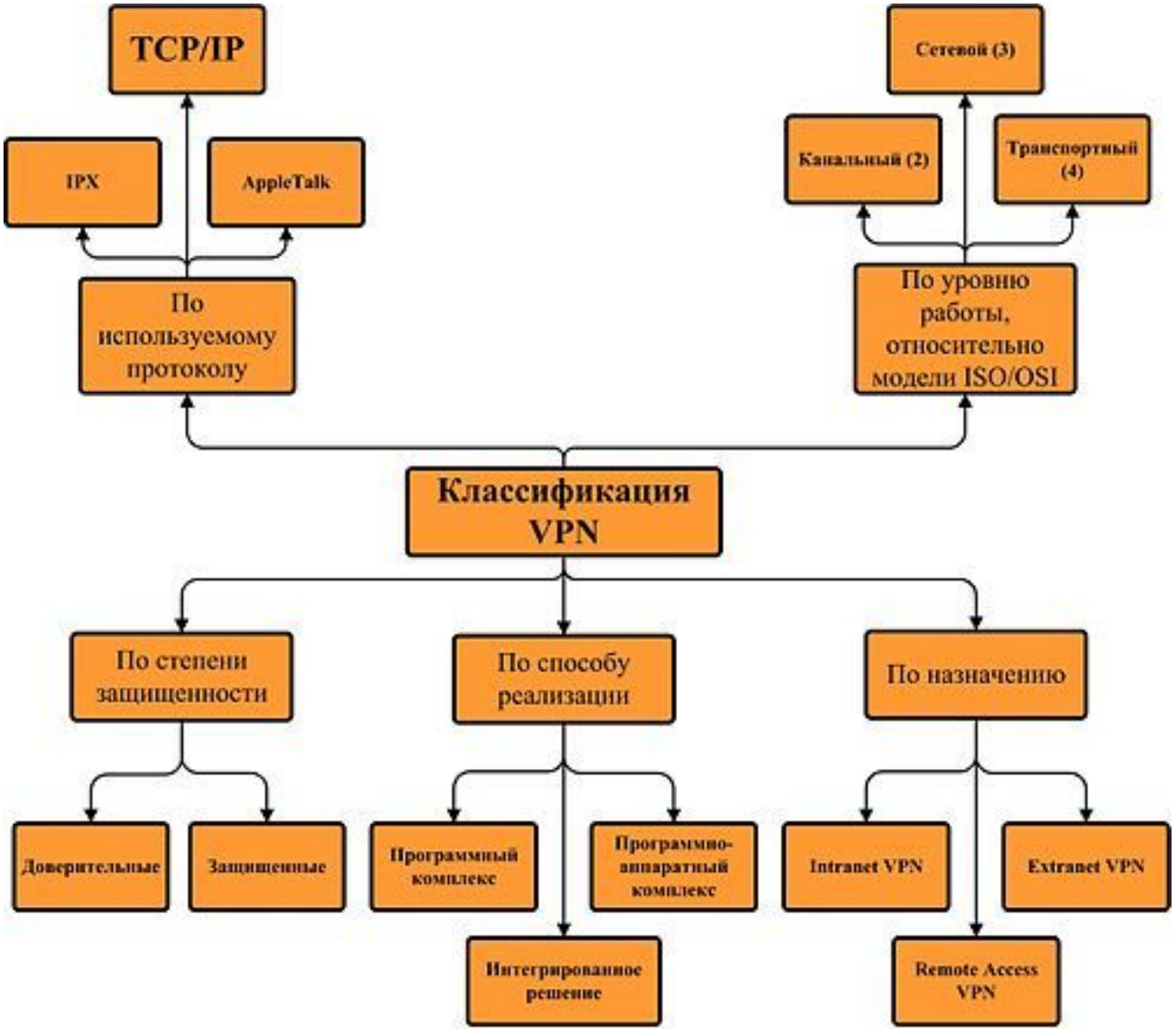
- Концентрированная безопасность
- Повышенная конфиденциальность
- Протоколирование и статистика использования сети и попыток проникновения
- Претворение в жизнь политики

Построение защищенных виртуальных частных сетей VPN (Virtual Private Networks).

Защищенной виртуальной сетью VPN называют соединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность данных.



Классификация VPN



Прокси-сервер

служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сете

Виды рисков:

1. **Хищение услуг.** Злоумышленник может получить доступ к Интернету.
2. **Отказ в услугах.** Хакер может стать источником большого количества запросов на подключение к сети, в результате чего затруднить подключение законных пользователей.
3. **Хищение или разрушение данных.** Злоумышленник, подключившись к сети, может получить доступ к файлам и папкам, а следовательно получить возможность копирования, модификации и удаления.
4. **Перехват контроля над сетью.** Злоумышленник, используя слабые места в системе безопасности, может внедрить троянского коня или назначить такие права доступа, которые могут привести к незащищенности компьютера от атак из сети Интернет.

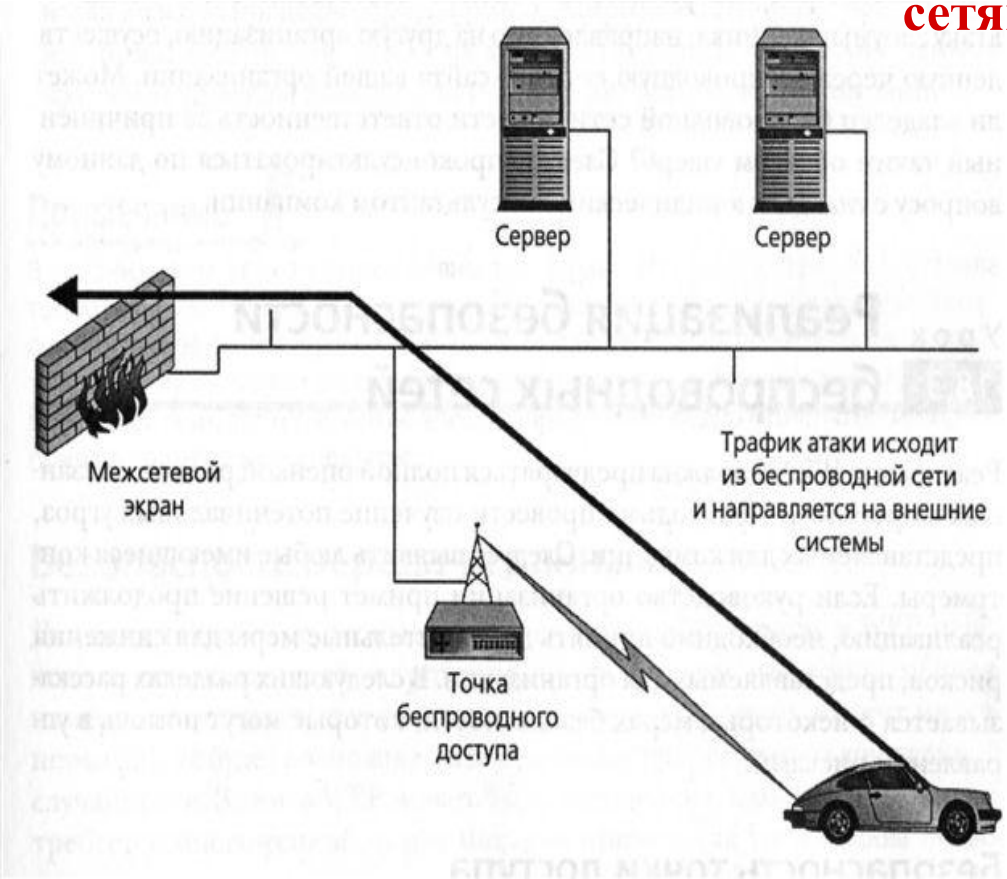
Спецификации беспроводных сетей: группа 802.11x института IEEE.
Web-сайты группы:
www.ieee802.org/11 **www.wi-fi.ogr**

Протокол безопасности уровня передачи данных WEP
(Wired Equivalent Privacy — секретность, эквивалентная проводным сетям)

Беспроводные сети. Проблемы с защитой информации

«На сегодняшний день не предложено ни одного действенного метода защиты для обеспечения полного управления рисками, связанными с беспроводными сетями»

Э. Мэйволд, «Безопасность сетей»



Угрозы безопасности

1. **Несанкционированный доступ к ресурсам корпоративной сети**
2. **Внедрение вредоносных программ**
3. **Использование сети для атак на другие сети**
   (2 уголовных дела в СамГУ)

Дополнительные меры безопасности:

1. Избегать соединения беспроводной сети с проводной ЛВС. Беспроводная точка доступа подключается к маршрутизатору или к интерфейсу брандмауэра.

2. Для реализации беспроводных соединений использовать виртуальные частные сети (VPN).

3. Использовать инструментальные средства сканирования для проверки сети на предмет наличия уязвимых мест в системе безопасности.

4. Регулярно проверять журнал регистрации подключений для контроля всех сетевых подключений.

Нормативная база

Информационная сфера - одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании.

Принятые во второй половине 90-х годов законодательные акты уже не отвечают современному состоянию общественных отношений и реалиям использования информационных технологий и информационно-телекоммуникационных сетей, по отдельным вопросам вступают в противоречие с более поздними актами, тормозят развитие информационного общества.

Нормативная база

Составляющие авторского права

Права

Личные

- Право авторства.
- Право на имя.
- Право на целостность.

Имущественные

- Выпуск в свет.
- Воспроизведение.
- Распространение.
- Иное использование.

Все действия без согласия правообладателя незаконны!

Компьютерное пиратство

- Незаконное копирование
- Интернет-пиратство
- Незаконная установка программ на компьютеры
- Нарушение ограничений лицензии
- Изготовление подделок

Экземпляры программ для ЭВМ или базы данных, изготовленные (введенные в хозяйственный оборот) с нарушением авторских прав, называются **контрафактными**.

Ответственность, предусмотренная законом

Уголовная ответственность	1. непосредственный нарушитель 2. должностное лицо (руководитель)
Административная ответственность	1. непосредственный нарушитель 2. должностное лицо (руководитель) 3. юридическое лицо
Гражданско-правовая ответственность	1. непосредственный нарушитель (суд общей юрисдикции) 2. юридическое лицо (арбитражный суд)

Нормативная база

«Окинавская Хартия глобального информационного общества» 22.07.2000 г.

Информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века.

Основные принципы:

защита прав интеллектуальной собственности на ИТ;

обязательство правительств использовать только лицензированное программное обеспечение;

защиты частной жизни при обработке личных данных.

Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства.

Содействовать использованию бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этом права на интеллектуальную собственность.

Содействие подготовке специалистов в сфере ИТ, а также в нормативной сфере.

Модель отношений субъектов информационных отношений