Основы безопасности информационных технологий

Основы безопасности межсетевого взаимодействия

Содержание лекции

- Введение
- Сетевое и межсетевое взаимодействие
- Системная классификация угроз
- Понятие информационной безопасности
- Политика безопасности
- Сетевая политика безопасности
- Эшелонированная оборона

Определения

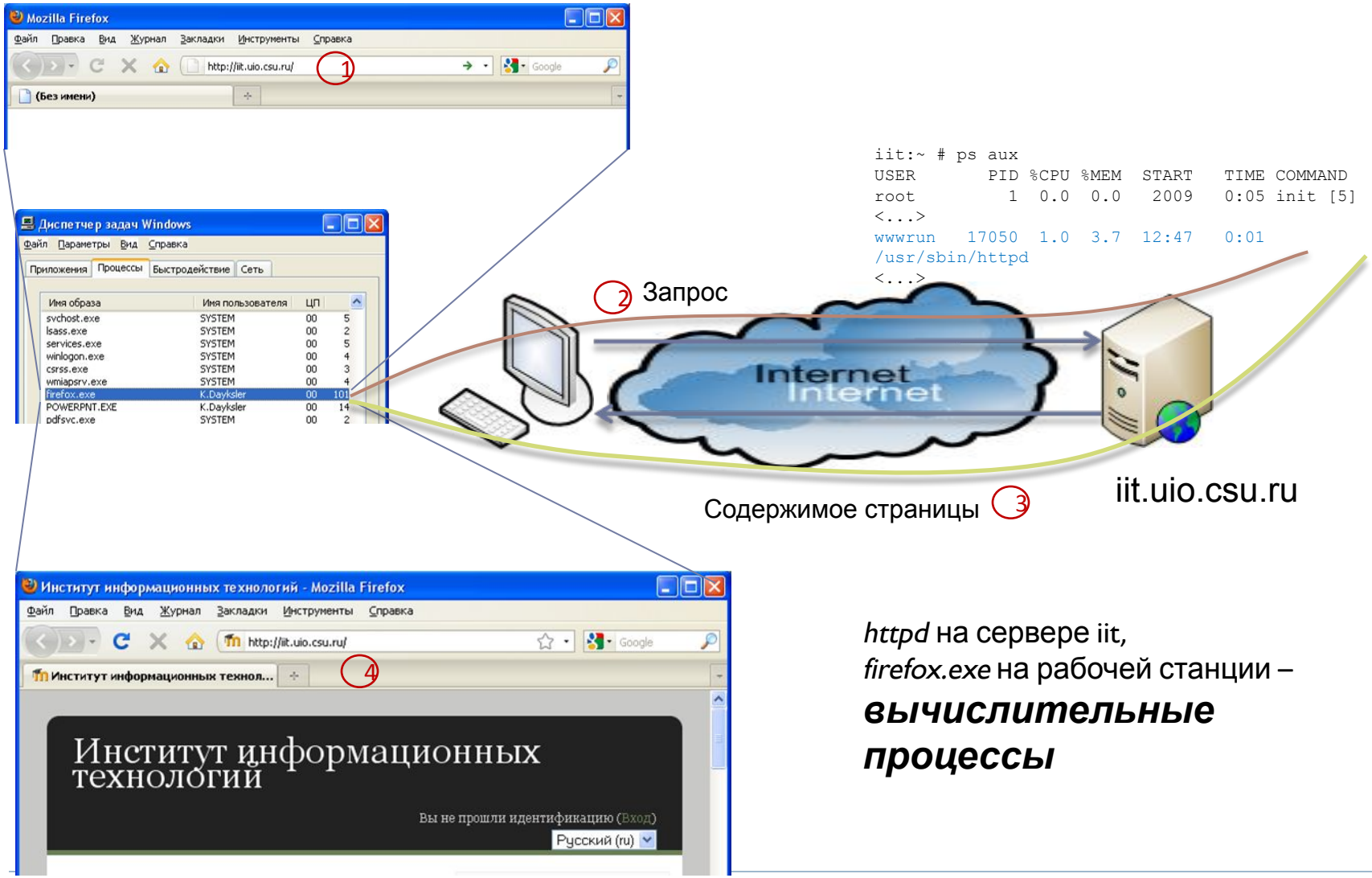
Корпоративная сеть (интранет) — это сеть на уровне компании, в которой используются программные средства, основанные на стеке протоколов TCP/IP.

Экстранет-сеть – *это* интранет-сеть, подключенная к Интернету, т.е. это сеть типа интранет, но санкционирующая доступ к ее ресурсам определенной категории пользователей, наделенной соответствующими полномочиями.

Сетевое и межсетевое взаимодействие

Модель OSI	Модель TCP/IP
Прикладной (Application)	Прикладной (Application)
Представительный (Presentation)	
Сеансовый (Session)	
Транспортный (Transport)	Транспортный (Transport)
Сетевой (Network)	Сетевой (Internetwork)
Канальный (Data link)	Сетевой интерфейс (Data link)
Физический (Physical)	Физическая среда (Physical)

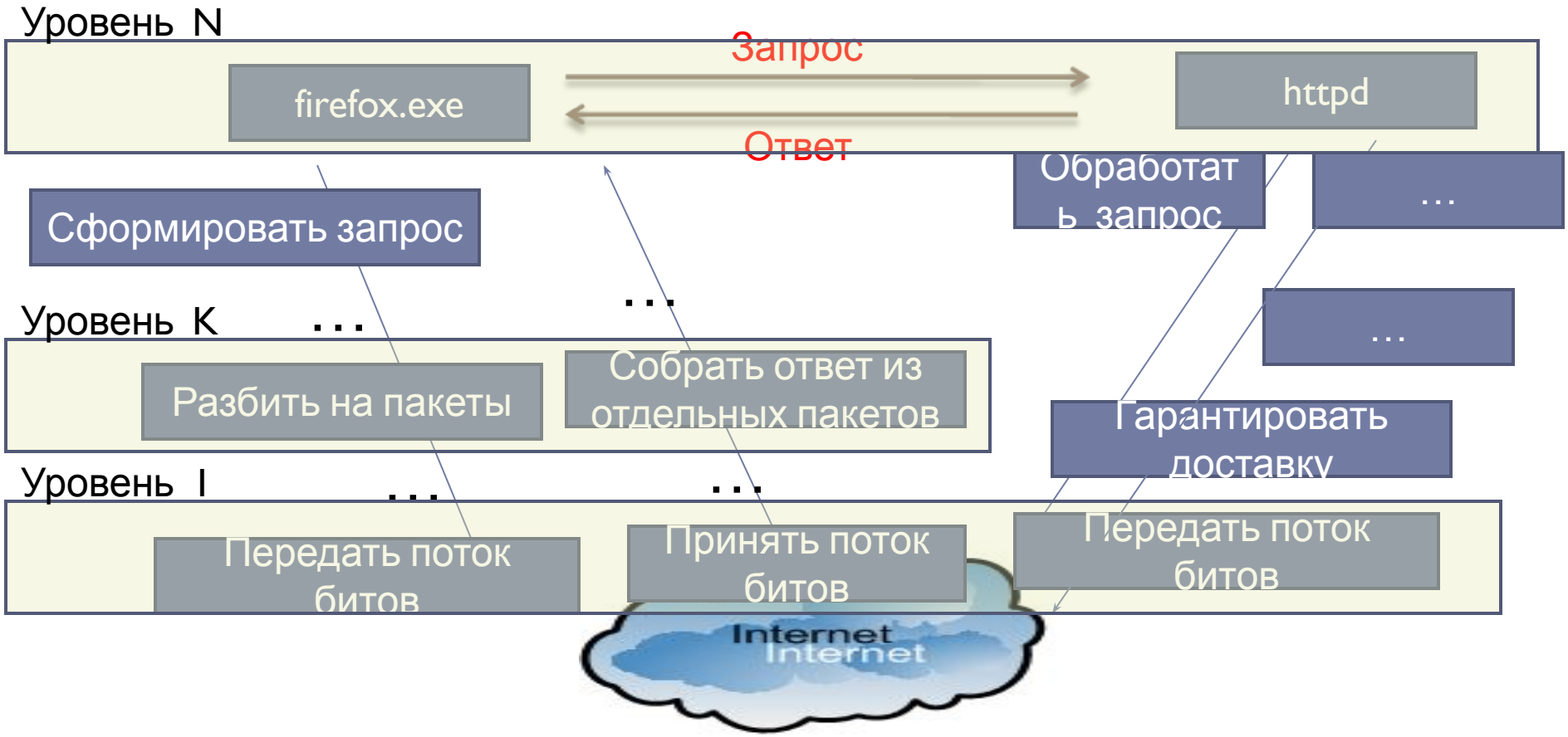
Пример взаимодействия вычислительных процессов



httpd на сервере iit,
firefox.exe на рабочей станции –
вычислительные процессы

Как организовать взаимодействие?

Как организовать взаимодействие?



Системная классификация угроз: общие понятия

Уязвимость (vulnerability) информационной системы – это любая характеристика, использование которой нарушителем может привести к реализации угрозы.

Угроза (threat) информационной системы – это потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы.

Системная классификация угроз

Параметры классификации	Значения параметров	Содержание значения
Виды угроз	Физическая целостность Логическая структура Содержание Конфиденциальность Право собственности	Уничтожение (искажение) Искажение структуры Несанкционированная модификация Несанкционированное получение, утечка информации Присвоение чужого труда
Происхождение угроз	Случайное Преднамеренное	Отказы, сбои, ошибки Стихийные бедствия Побочные влияния Злоумышленные действия людей
Предпосылки появления угроз	Объективное Субъективное	Количественная и качественная недостаточность элементов системы Промышленный шпионаж, недобросовестные сотрудники, криминальные и хулиганствующие элементы, службы других государств
Источники угроз	Люди Технические устройства Модели, алгоритмы, программы Технологические схемы обработки данных Внешняя среда	Пользователи, персонал, посторонние люди Регистрации, ввода, обработки, хранения, передачи и выдачи Общего назначения, прикладные, вспомогательные Ручные, интерактивные, внутримашинные, сетевые Состояние среды, побочные шумы, побочные сигналы

Виды утечки информации

В соответствии с ГОСТ Р 50922—96 рассматриваются три вида утечки формации:

- разглашение;
- несанкционированный доступ к информации;
- получение защищаемой информации разведками.

Канал утечки информации — совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Понятие информационной безопасности

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Уровни обеспечения безопасности

- законодательный
- административный
- процедурный
- программно-технический

Этапы обеспечения безопасности

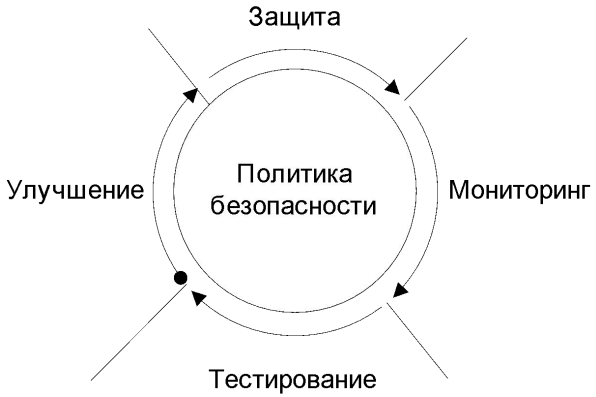
- определение политики ИБ
- определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания
- оценка рисков
- управление рисками
- выбор контрмер, обеспечивающих режим ИБ
- аудит системы управления ИБ

Свойства безопасности

- конфиденциальность
- целостность
- доступность

Политика безопасности

Политика безопасности организации – это документ, описывающий специфические требования или правила, которые должны выполнятся.



Практические шаги определения политики ИБ

- Определение используемых руководящих документов и стандартов в области ИБ
- Определение подходов к управлению рисками
- Определение требований к режиму информационной безопасности
- Структуризация контрмер по уровням
- Определения порядка сертификации на соответствие стандартам в области ИБ
- Определение периодичности проведения совещаний по тематике ИБ на уровне руководства

Разделы политики безопасности

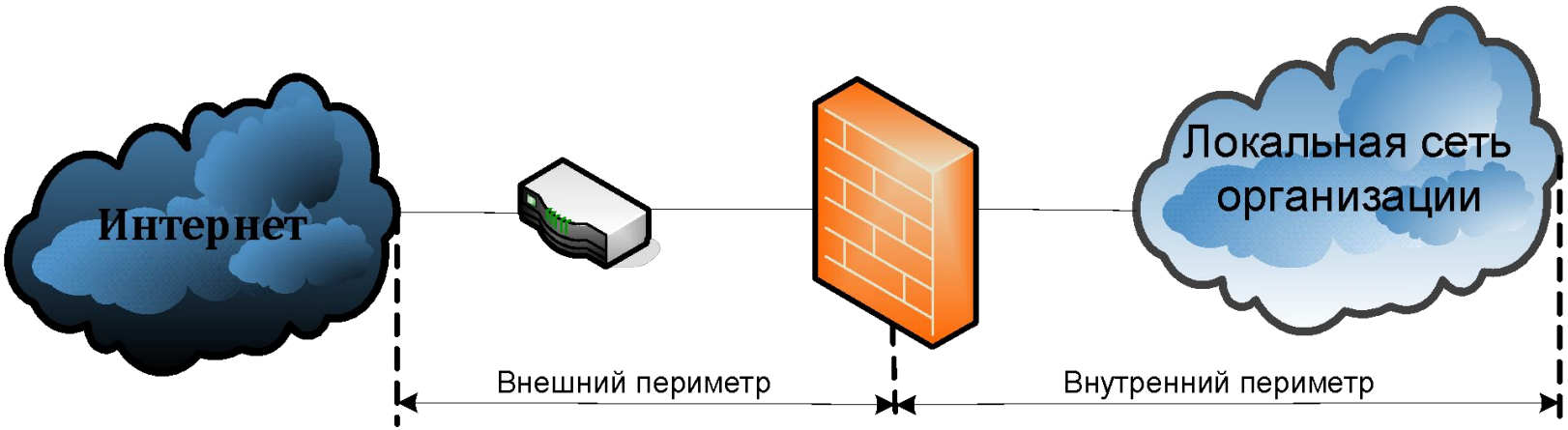
- общие положения
- политика управления паролями
- идентификация пользователей
- полномочия пользователей
- защита информационных ресурсов организации от компьютерных вирусов
- правила установки и контроля сетевых соединений
- правила политики безопасности по работе с системой электронной почты
- правила обеспечения безопасности информационных ресурсов
- обязанности пользователей по выполнению правил ПБ
- и т.д.

Жизненный цикл политики безопасности

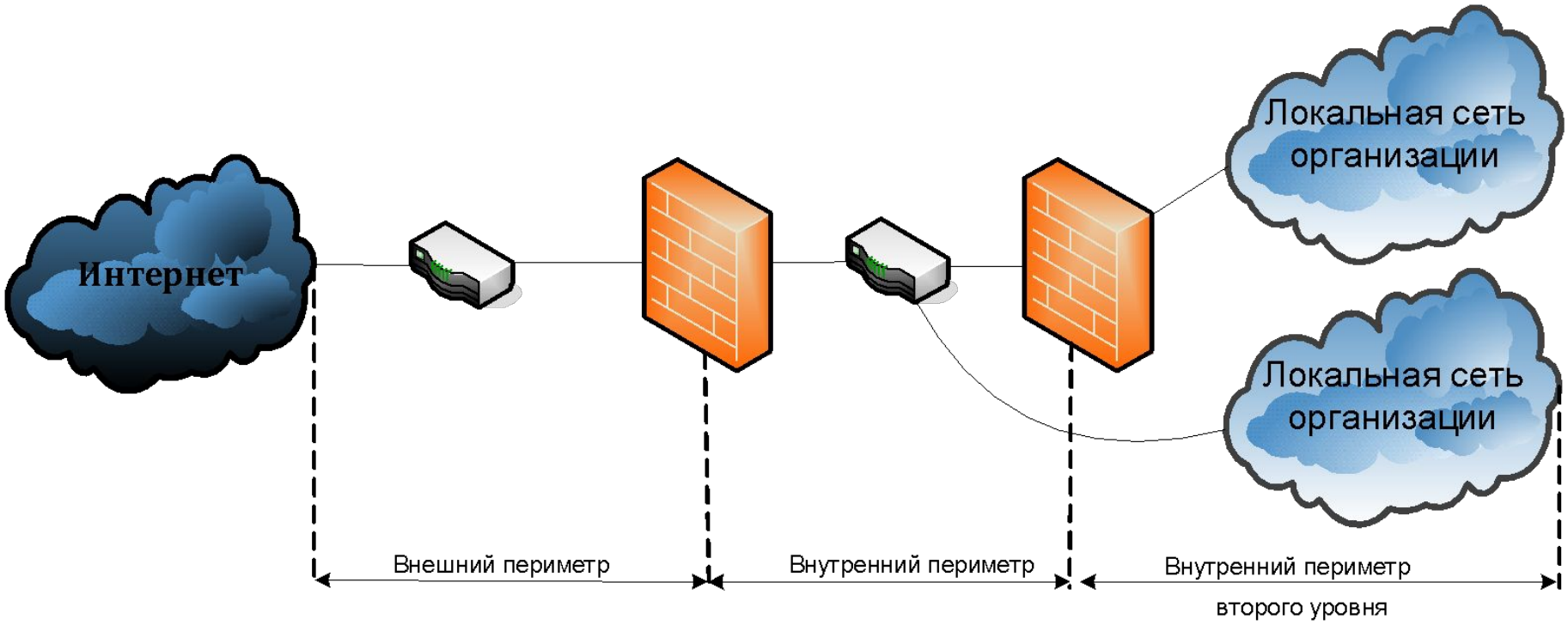
Сетевая политика безопасности

Типы сетевых периметров:

- Внешний
- Внутренний



Множество внутренних сетевых периметров



Эшелонированная оборона

Эшелонированная оборона (defense in depth) – это практическая стратегия достижения информационной гарантированности (information assurance) в сетевом оборудовании.

- Стрелы
- Ров
- Поднятый мост
- Узкий проход
- Внутренние ворота