



# Операционные системы

---

Безопасность

# Правила безопасности

---

1. Защищающемуся приходится охраняться все слабые места, а нападающему достаточно выбрать одно
2. Защищающийся готовится отразить все известные атаки, а нападающий может придумать новые методики взлома
3. Оборону необходимо держать всегда, а удар возможен когда угодно
4. Защищающему приходится соблюдать все правила, а нападающему можно вести «игру не по правилам»

# Задачи безопасности

---

1. Конфиденциальность данных
2. Целостность данных
3. Работоспособность системы
4. Исключение постороннего доступа

# Категории злоумышленников

---

1. Праздное любопытство
2. Шпионаж внутри коллектива
3. Атаки с целью обогащения
4. Коммерческий или военный шпионаж

# Краткий список криптографических способов защиты информации

---

1. Шифрование с секретным ключом
2. Шифрование с открытым ключом
3. Односторонние функции
4. Цифровая подпись
5. Криптографический процессор

# Механизмы защиты

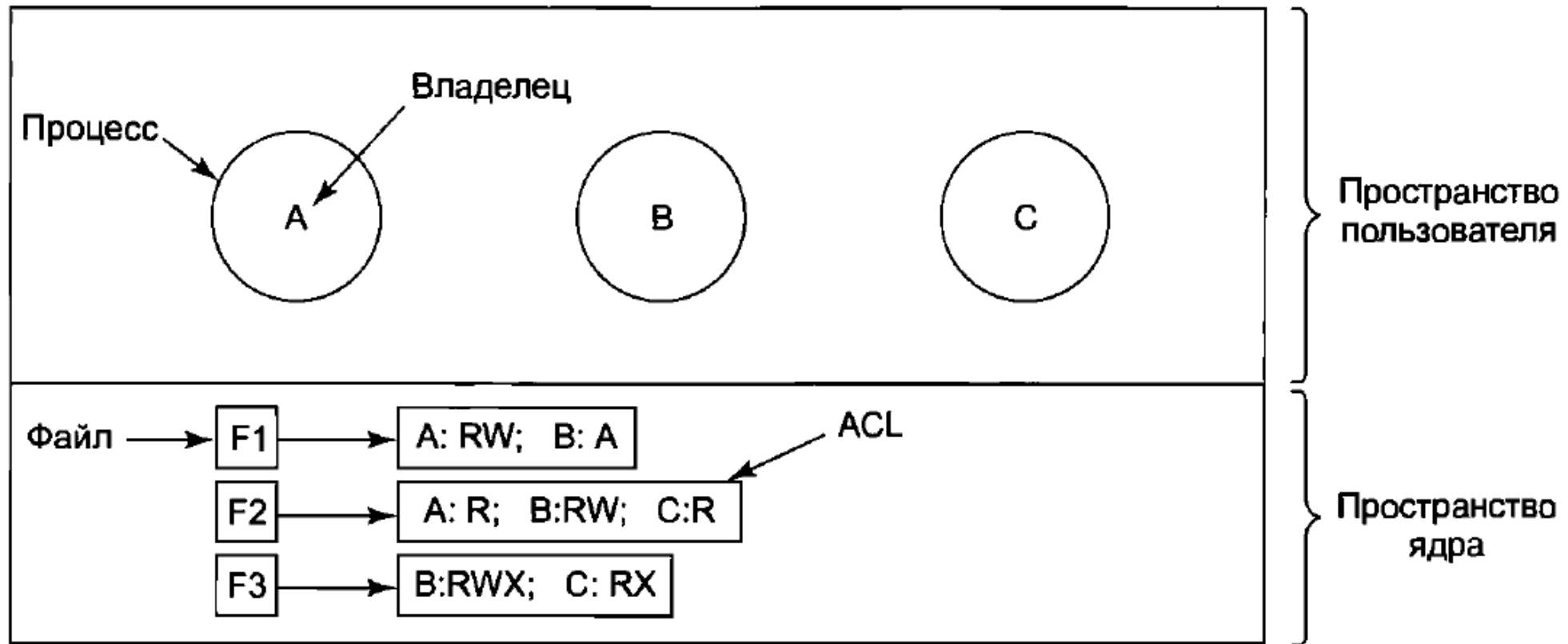
---

1. Домены защиты
2. Списки управления доступом
3. Перечень возможностей

# Домены защиты

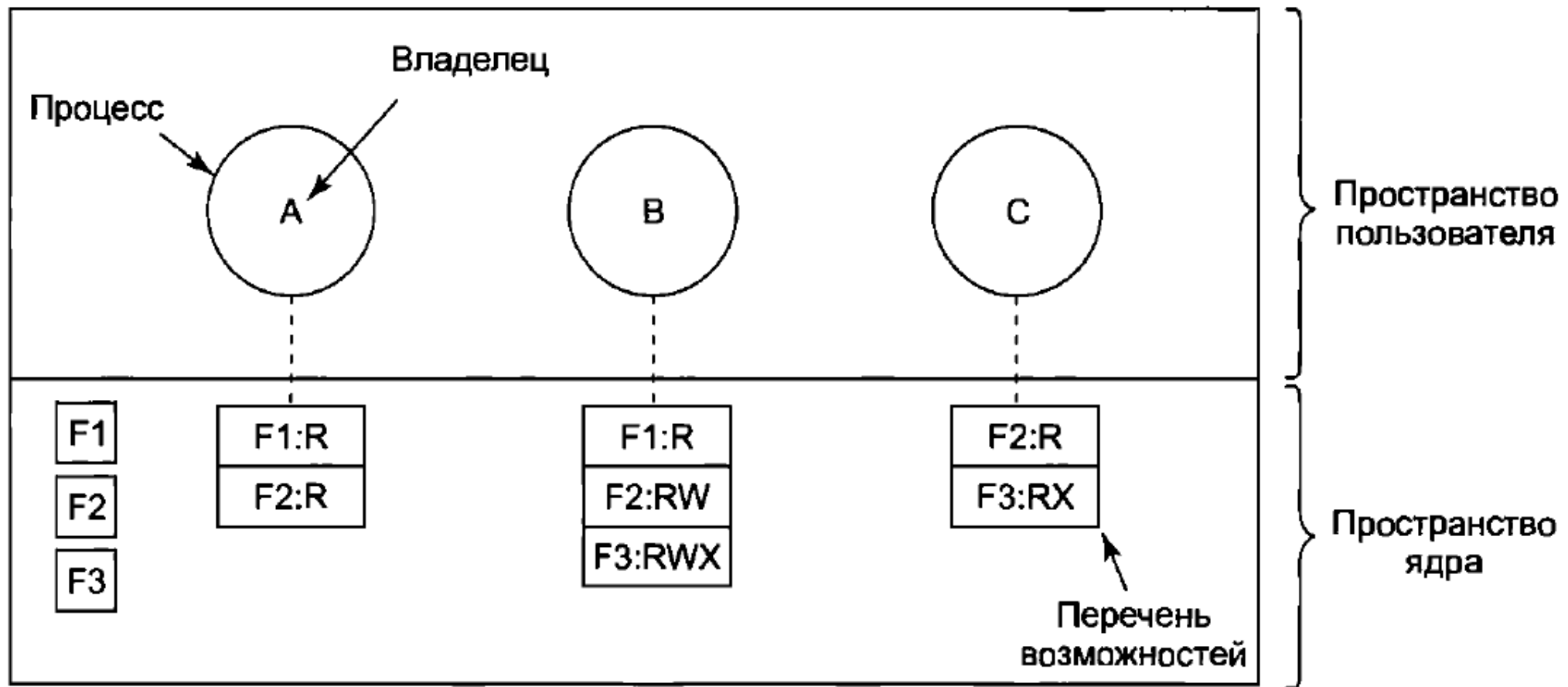
|   | Домен 1 |                  |        |                                |                  |                                | Плоттер 2 |         | Домен 2 |         |
|---|---------|------------------|--------|--------------------------------|------------------|--------------------------------|-----------|---------|---------|---------|
|   | Файл 1  | Файл 2           | Файл 3 | Файл 4                         | Файл 5           | Файл 6                         | Принтер 1 | Домен 1 | Домен 2 | Домен 3 |
| 1 | Чтение  | Чтение<br>Запись |        |                                |                  |                                |           |         | Enter   |         |
| 2 |         |                  | Чтение | Чтение<br>Запись<br>Исполнение | Чтение<br>Запись |                                | Запись    |         |         |         |
| 3 |         |                  |        |                                |                  | Чтение<br>Запись<br>Исполнение | Запись    | Запись  |         |         |

# Списки управления доступом (ACL)





# Перечень возможностей



# Многоуровневая защита

---

1. Модель Белла – Ла Падулы
2. Модель Биба

# Модель Белла – Ла Падулы

---

1. Простое свойство безопасности ( $k \rightarrow \text{read}(k), \text{read}(k-1) \dots$ )
2. Свойство  $*(k \rightarrow \text{write}(k), \text{write}(k+1) \dots)$

# Модель Биба

---

1. Простой принцип целостности ( $k \rightarrow \text{write}(k), \text{write}(k-1)$ )
2. Свойство целостности \* ( $k \rightarrow \text{read}(k), \text{read}(k+1), \dots$ )

# Соккрытие передачи информации

---

1. Тайный канал
2. Стеганография

# Аутентификация

---

1. Аутентификация с использованием паролей  
salt, одноразовые пароли
2. Аутентификация с использованием физического объекта
3. Аутентификация по биометрическим данным

# Существующие механизмы аутентификации

---

1. Базовая аутентификация
2. Аутентификация на основе хеша
3. Аутентификация на основе форм
4. Microsoft passport
5. OAuth
6. Kerberos
7. ...

# Атаки «изнутри»

---

1. Логические бомбы
2. Лазейки
3. Фальсификация входа в систему



# Атаки типа «отказ в обслуживании» (Denial of Service, DoS)

---

1. Атаки, вызывающие перегрузку процессора
2. Атаки, вызывающие нехватку памяти
3. Атаки, вызывающие нехватку ресурсов
4. Атаки, вызывающие снижение пропускной способности сети

# Дефекты кода. Переполнение буфера

---

1. Переполнение стека
2. Переполнение буфера
3. Ошибки индексации массива
4. Несовпадение размеров ANSI и Unicode
5. Переполнение целочисленных значений

# Дефекты кода. Инъекции программного кода

---

1. SQL
2. Acm
3. Bash, shell, cmd

# Дефекты кода. Данные и код размещают отдельно

---

1. Выносите строки для локализаций
2. Не размещать служебные строки в коде

# Проверка входных данных

---

1. Суть проблемы в излишнем доверии
2. Создание границы доверенной зоны и «контрольно-пропускных пунктов»
3. Проверка корректности данных
  - Регулярные выражение
  - Использование специализированных типов
  - Использование управляемого кода

# Вредоносное ПО

---

1. Троянский конь
2. Вирусы
3. Черви
4. Программы-шпионы
5. Руткиты

# Вирусы

---

1. Вирусы-компаньоны
2. Вирусы, заражающие исполняемые файлы
3. Резидентные вирусы
4. Вирусы, поражающие загрузочный сектор
5. Вирусы драйверов устройств
6. Макровирусы
7. Вирусы исходного кода

# Действия, предпринимаемые программой-шпионом

---

1. Изменение настроек браузера
2. Изменение стандартных программ пользователя
3. Генерация рекламы
4. Сбор информации



# Руткиты (скрытие присутствия)

---

1. Руткиты во встроенном ПО
2. Руткиты-гипервизоры
3. Руткиты в ядре
4. Руткиты в библиотеках
5. Руткиты в приложениях

# Средства защиты

---

1. Брандмауэры
2. Антивирусные технологии
  - Программы поиска вирусов  
Полиморфные вирусы
  - Программы проверки целостности файлов
  - Программы, контролирующие поведение
  - Контролирование на основе модели
3. Электронная подпись двоичных файлов
4. Песочницы