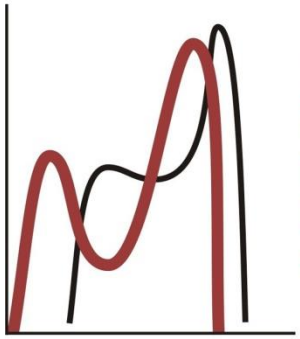


ИНСТИТУТ
МАТЕМАТИКИ
МЕХАНИКИ
КОМПЬЮТЕРНЫХ
НАУК

имени И.И. Воровича —

Архитектура компьютера и операционные системы

Лекция 23. Безопасность.

Андреева Евгения Михайловна
доцент кафедры информатики и вычислительного эксперимента

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

План лекции

- Планирование запросов подсистемы ввода вывода
- Основные вопросы безопасности
- Программные и системные угрозы (атаки)
- Защита систем (механизмы противодействия)
  - Аутентификация и авторизация
  - Обнаружение взлома
  - Шифрование
  - …

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Добор баллов

- 24 декабря по расписанию занятий– 7 группа
- 27 декабря по расписанию занятий– 8 и 9 группы
- 28 декабря в 9:50 вместо лекции будет дистанционный добор, можно сдать только лабораторные работы

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Планирование запросов

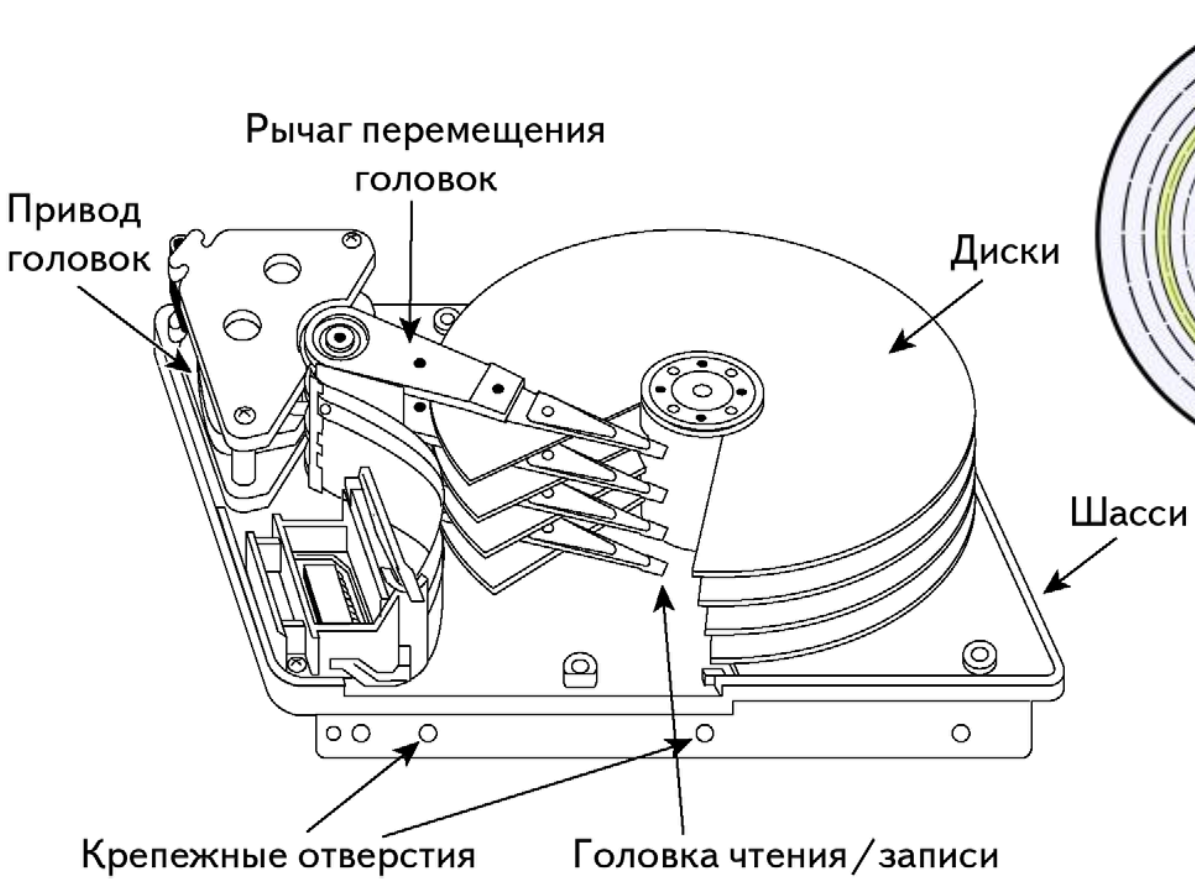
Для блокирующихся и асинхронных системных вызовов

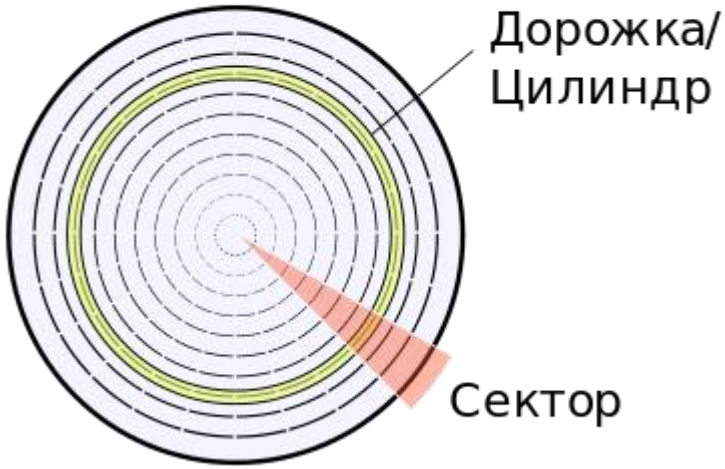
- При занятости устройства запрос ставится в очередь к данному устройству.
- После освобождения устройства необходимо принять решение: какой из запросов в очереди инициировать следующим – планирование запросов.

Действия по планированию запросов могут быть частично или полностью делегированы драйверу устройства – функция strategy в интерфейсе драйвера

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК
имени И.И. Воровича

Строение жесткого диска





ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Параметры планирования

- Запрос полностью характеризуется:
  - типом операции
  - номером цилиндра
  - номером дорожки
  - номером сектора
- Параметр планирование – время, необходимое для выполнения запроса.
  - Время выполнения запроса = transfer time + positioning time
  - Positioning time = seek time + positioning latency

Единственным параметром запроса остается seek time – время пропорциональное разнице между номером цилиндра в запросе и номером текущего цилиндра

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Алгоритмы планирования запросов к жесткому диску

- Пусть
  - Диск имеет 100 цилиндров (от 0 до 99)
  - Очередь запросов: **23, 67, 55, 14, 31, 7, 84, 10**
  - Текущий цилиндр – **63**

- Алгоритм FCFS (First Come First Served)

  63 -> 23 -> 67 -> 55 -> 14 -> 31 -> 07 -> 84 -> 10

  Всего перемещение на 329 цилиндров

- Алгоритм SSTF (Short Seek Time First)

  63 -> 67 -> 55 -> 31 -> 23 -> 14 -> 10 -> 07 -> 84

  Всего перемещение на 141 цилиндр

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Алгоритмы планирования запросов к жесткому диску

- Пусть
  - Диск имеет 100 цилиндров (от 0 до 99)
  - Очередь запросов: **23, 67, 55, 14, 31, 7, 84, 10**
  - Текущий цилиндр – **63**

- Алгоритм SCAN

  63 -> 55 -> 31 -> 23 -> 14 -> 10 -> 07 -> 0 -> 67 -> 84

  Всего перемещение на 147 цилиндров
- Алгоритм LOOK

  63 -> 55 -> 31 -> 23 -> 14 -> 10 -> 07 -> 67 -> 84

  Всего перемещение на 133 цилиндра
- Алгоритм C-SCAN

  63 -> 55 -> 31 -> 23 -> 14 -> 10 -> 07 -> 0 -> 99 -> 84 -> 67
- Алгоритм C-LOOK

  63 -> 55 -> 31 -> 23 -> 14 -> 10 -> 07 -> 84 ->67

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Hi-Tech Crime Trends 2020/2021

- Угрозы в энергетическом секторе
  - Проводятся целенаправленные атаки с захватом контроля над всей сетью с целью заражения их инфраструктур программами-шифровальщиками.
- Угрозы в банковском секторе
  - Хищение информации о финансовых транзакциях VIP-клиентов и появление таких сведений в открытом доступе
- Угрозы в телекоммуникационном секторе
  - Логическая перегрузка сети
  - Угрозы на удаленке
- Угрозы в ретейле
  - К потерям для бизнеса могут привести атаки с помощью JS-сниффероов, атаки на POS-терминалы, credential stuffing и атаки с помощью шифровальщиков.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Безопасность

- Безопасность – одна из наиболее актуальных проблем в области ИТ:
  - повседневная деятельность и бизнес зависят от компьютерных технологий;
  - резко возросло число сетевых атак (киберпреступность).
- Основные "мишени" для атак - уязвимости в операционных системах и настройках сетей.
- Дефект, влияющий на безопасность операционной системы, называется уязвимостью.
- Вводимые данные, позволяющие воспользоваться дефектом, называются вредоносным кодом (exploit)

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Топ-20 продуктов с наибольшим количеством технических уязвимостей

Top 20 Products With the Most Technical Vulnerabilities Over Time

1999–2019		2019	
Debian Linux	3,067	Android	414
Android	2,563	Debian Linux	360
Linux kernel	2,357	Windows Server 2016	357
Mac OS X	2,212	Windows 10	357
Ubuntu	2,007	Windows Server 2019	351
Mozilla Firefox	1,873	Adobe Acrobat Reader DC	342
Google Chrome	1,858	Adobe Acrobat DC	342
iPhone iOS	1,655	cPanel	321
Windows Server 2008	1,421	Windows 7	250
Windows 7	1,283	Windows Server 2008	248
Adobe Acrobat Reader DC	1,182	Windows Server 2012	246
Adobe Acrobat DC	1,182	Windows 8.1	242
Windows 10	1,111	Windows RT 8.1	235
Adobe Flash Player	1,078	Ubuntu	190
Windows Server 2012	1,050	Fedora	184

Note: All products and vendors identified throughout the project were identified as such in the National Institute of Standards and Technology's National Vulnerability Database. We did not do any manual classification and are presenting the data as listed in the database.

SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S NATIONAL VULNERABILITY DATABASE

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Основные определения

- **Безопасность** (security) – состояние защищённости жизненно важных объектов, включает весь комплекс технических, административных, правовых и политических вопросов по обеспечению защиты.
- **Защитные механизмы** (protection mechanisms) - специфические средства операционной системы, используемые для защиты информации.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Защита в ОС

- безопасность отдельных компьютеров – защиту данных, хранящихся и обрабатывающихся компьютером, рассматриваемым как автономная система;
- сетевую безопасность – защиту данных при передаче по линиям связи и защиту от несанкционированного доступа в сеть.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Свойства безопасной системы

- Конфиденциальность(***Confidentiality***) – гарантия того, что информация будет доступна только авторизованным пользователям (легальным).
- Целостность и согласованность(***Integrity***) – гарантия сохранности данными правильных значений.
- Доступность(***Availability***) – постоянная готовность системы к обслуживанию авторизованных пользователей.

- В совокупности эти три ключевых принципа информационной безопасности именуются триадой CIA

- Аутентификация и авторизация – способность системы проверять идентичность пользователя и соответствие выделенных ему прав

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Основные уязвимости

- процессор ЭВМ(Spectre, Meltdown);
- BIOS, контроллеры внешних устройств, интерфейсов и пр.;
- программное обеспечение ОС;
- прикладное ПО, включая программы защиты;
- ПО аппаратных сетевых устройств и систем аутентификации;
- сетевые протоколы и их программные реализации.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Угрозы безопасности. Классификация

- Угроза – любое действие, направленное на нарушение конфиденциальности, целостности и/или доступности информации, а также нелегальное использование ресурсов системы.
- Неумышленные угрозы - ошибочные действия сотрудников, последствия ненадежной работы аппаратных и программных средств и ОС
- Умышленные угрозы:
  - пассивные - чтение данных, мониторинг системы;
  - активные - нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств системы.
- Реализованная угроза называется **атакой**.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

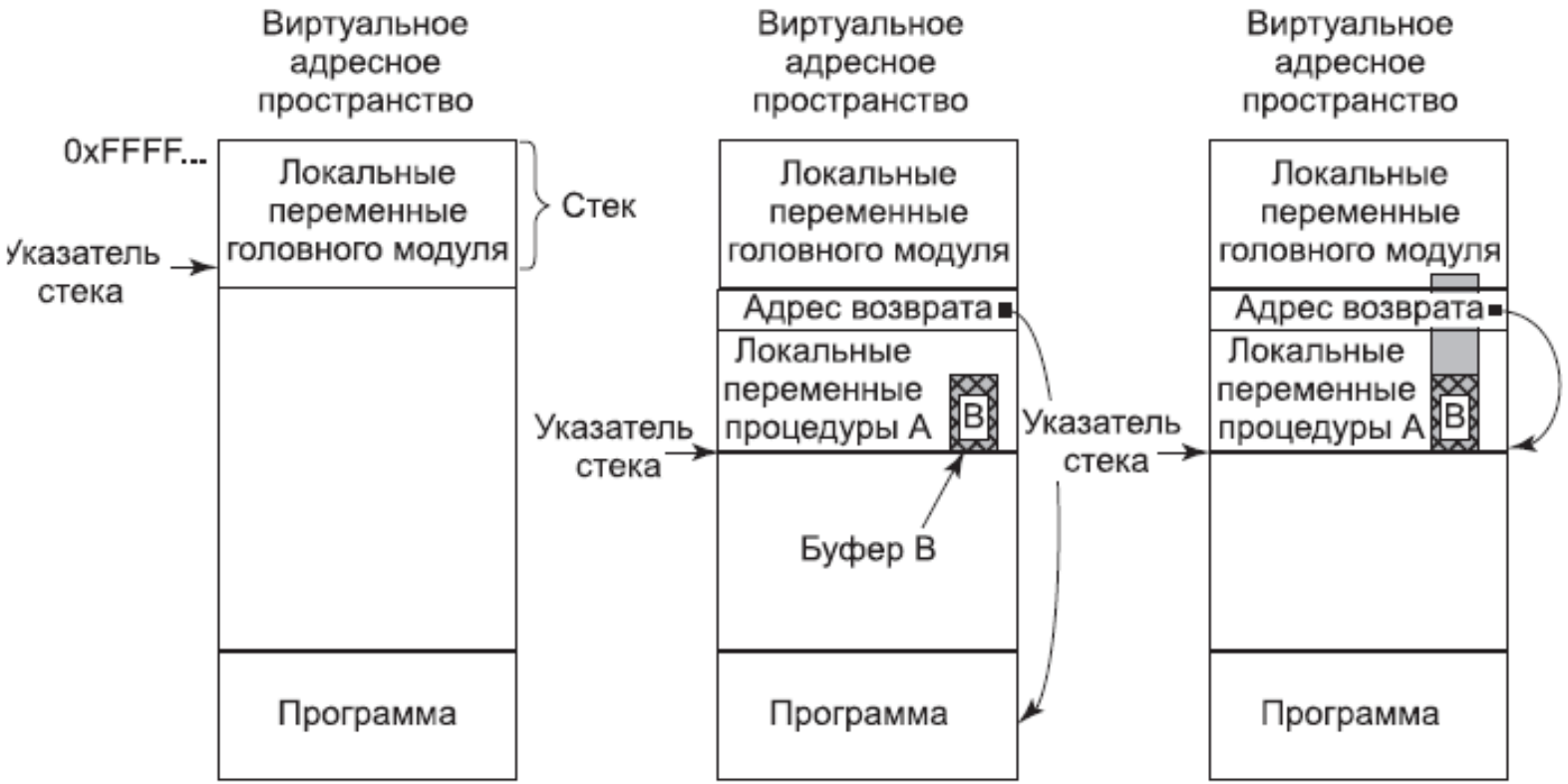
Взлом ПО(пример)

Переполнение буфера

```
void A()
{
        char B[128]; /* буфер 128 байт */
        printf ("Type log message:");
        gets (B); /* чтение сообщения */
        writeLog (B); /* вывод строки */
}
```

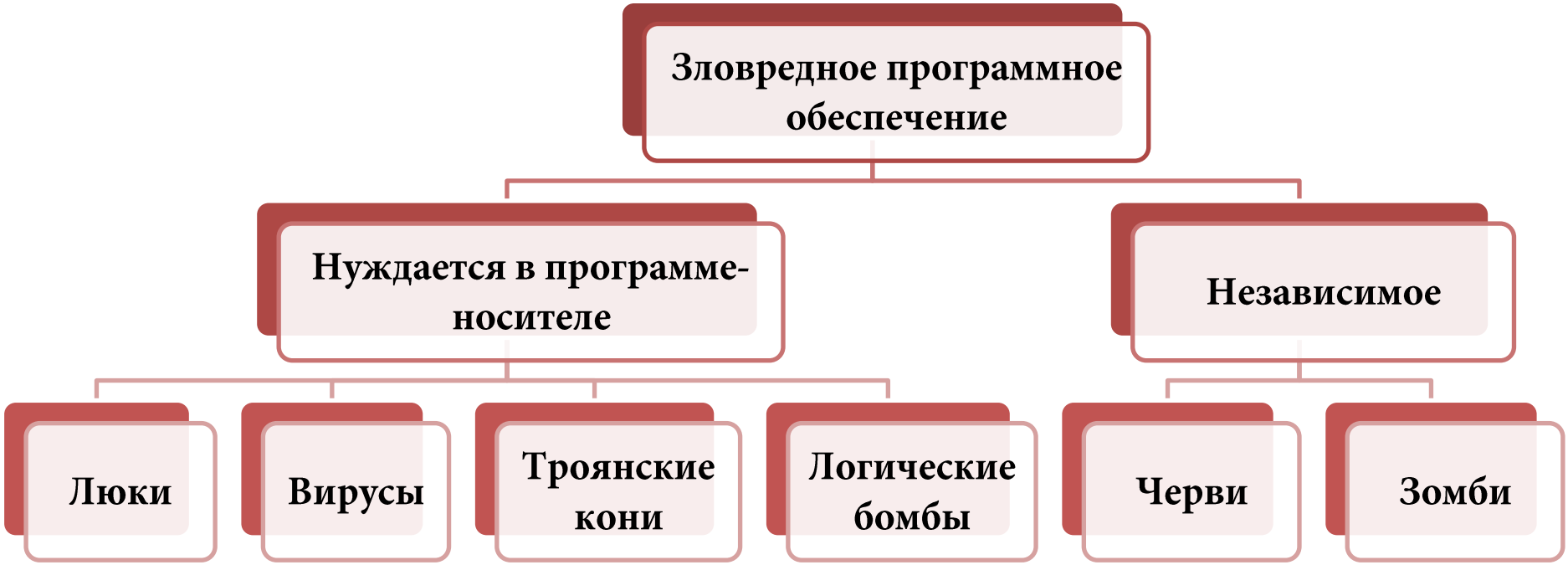
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Переполнение буфера



ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Атаки на систему снаружи



ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Типы сетевых атак

- **Phishing** (password harvesting fishing) – попытка украсть login и пароль пользователя, номер его банковского счета, PIN-код и т.д.
- **Pharming** – перенаправление на злонамеренный Web-сайт (обычно с целью phishing)
- **Tampering with data** – злонамеренное искажение или порча данных
- **Spoofing** – “подделка” под определенного пользователя (применение login, пароля и полномочий)
- **Elevation of privilege** – попытка расширить полномочия (до системного администратора) с целью злонамеренных действий

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Степени надежности информационных систем

- В **оранжевой книге** Министерства обороны США определяется четыре уровня безопасности – D, C, B и A
- По мере перехода от уровня D до A к надежности систем предъявляются все более жесткие требования
- Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3)
- Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее защита должна удовлетворять оговоренным требованиям.
- Сегодня на смену оранжевой книге пришел стандарт **Common Criteria**

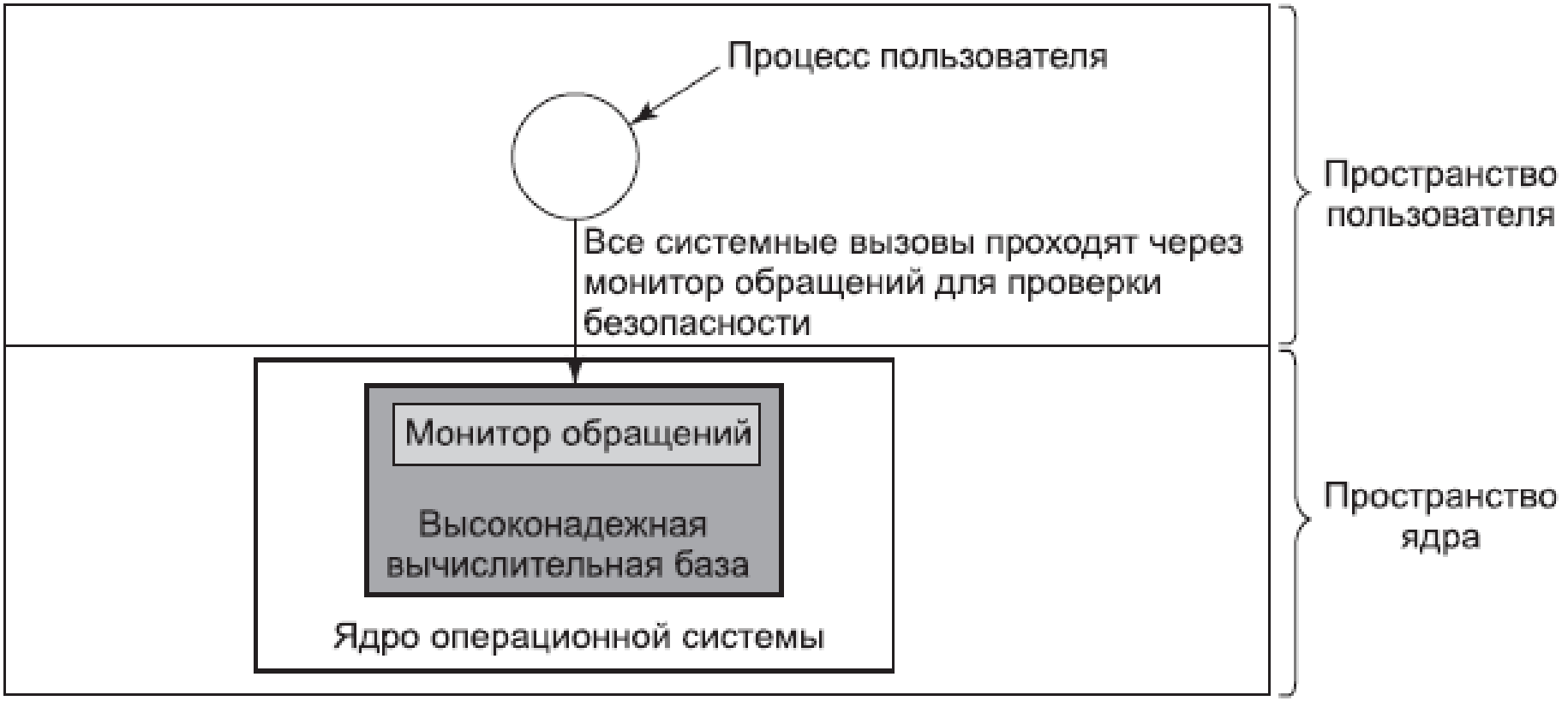
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Базовые принципы безопасности

- Минимальный уровень привилегий на доступ к данным.
- Использование средств, обеспечивающих максимальную защиту при атаке (полная блокировка входа в сеть и др.).
- Единый пропускной путь – весь трафик через один узел сети (firewall).
- Баланс возможного ущерба от угрозы и затрат на ее предотвращение.
- Внутренняя сеть предприятия и политика доступа к сети предприятия и к службам Интернет.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Защита с помощью монитора



ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Аутентификация

- **Аутентификация** (authentication) – идентификация пользователей при входе в систему
- Аутентификация базируется на одном или более из трех пунктов:
  - то, чем пользователь владеет (ключ или магнитная карта);
  - то, что пользователь знает (пароль);
  - биохарактеристики (отпечатки пальцев, подпись, голос).

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Уязвимость паролей

- Попытка применить пароли стандартных учетных записей (Guest, Demo).
- Настойчивый перебор всех коротких паролей.
- Перебор слов из «справочника» паролей.
- Сбор информации о пользователях (полные имена, имена супругов и детей, хобби пользователей).
- Использование в качестве вероятного пароля дат рождения, номеров комнат, номеров различных удостоверений и т. д.
- Использование в качестве вероятного пароля номеров автомобилей.
- Обход ограничений доступа с помощью троянских коней.
- Перехват сообщений, которыми обмениваются удаленный пользователь и узел системы.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Защита пользовательских паролей

- Одностороннее (необратимое) шифрование. Пароль используется для генерации ключа для функции шифрования.
- Контроль доступа к файлу с паролями. Доступ ограничен одной учетной записью или малым числом учетных записей (администраторы).

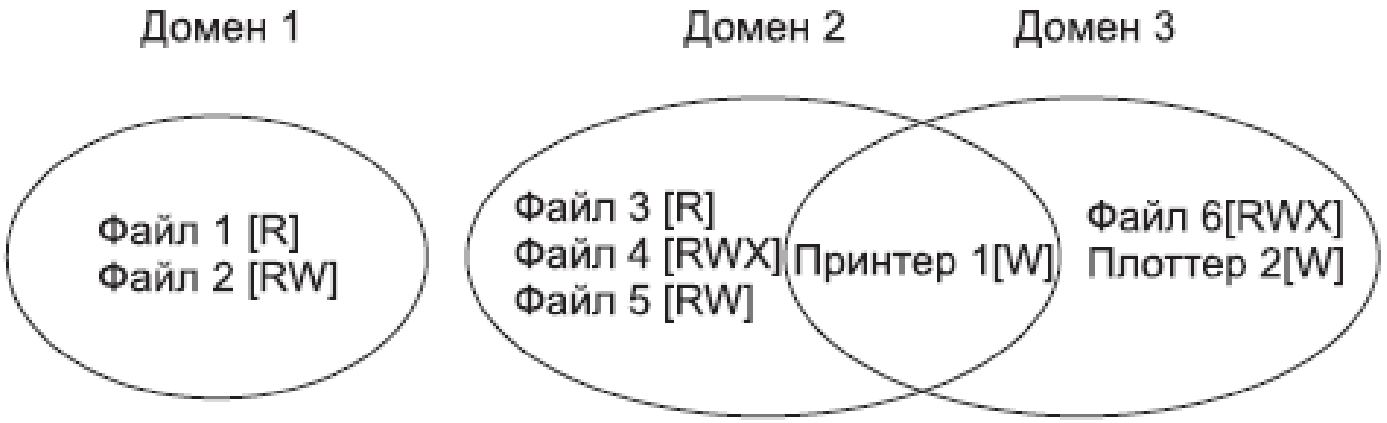
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Авторизация

- Цель подсистемы авторизации – предоставить каждому легальному пользователю те виды доступа и к тем ресурсам, которые были для него определены администратором системы.

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

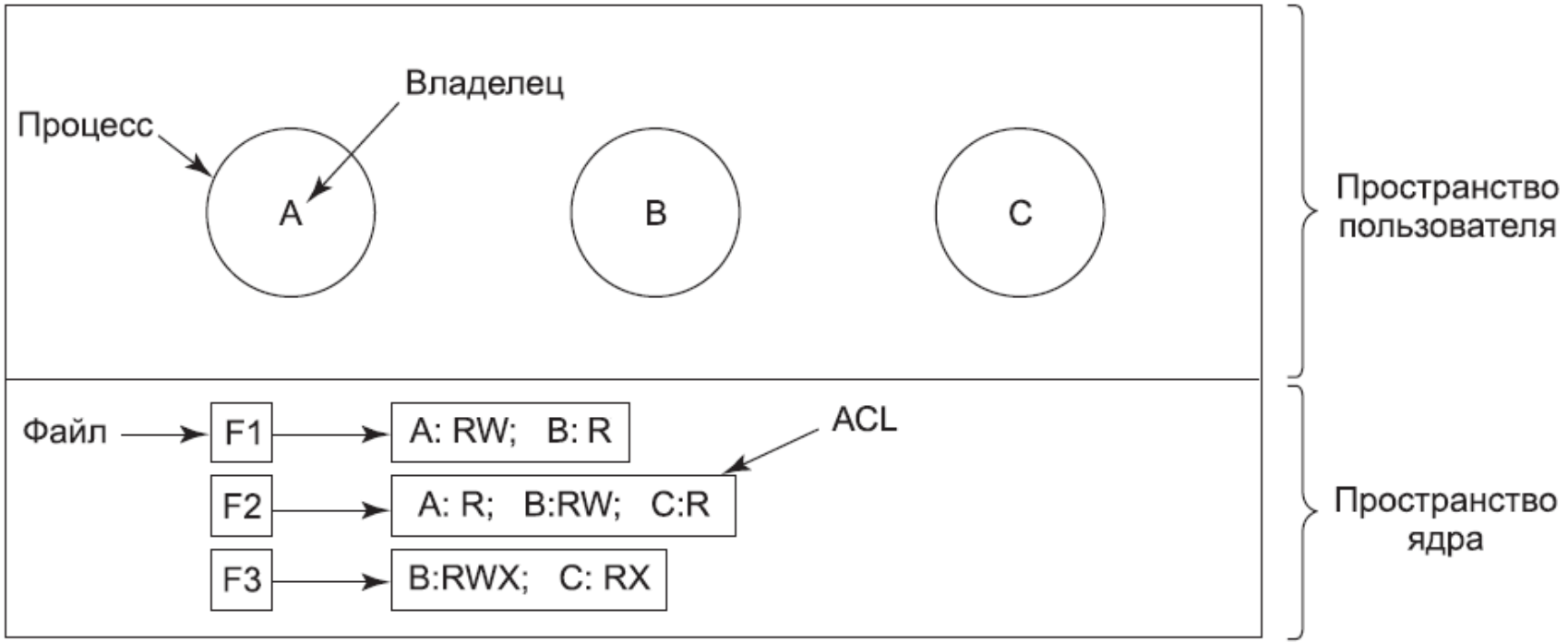
Управление доступом



Объект

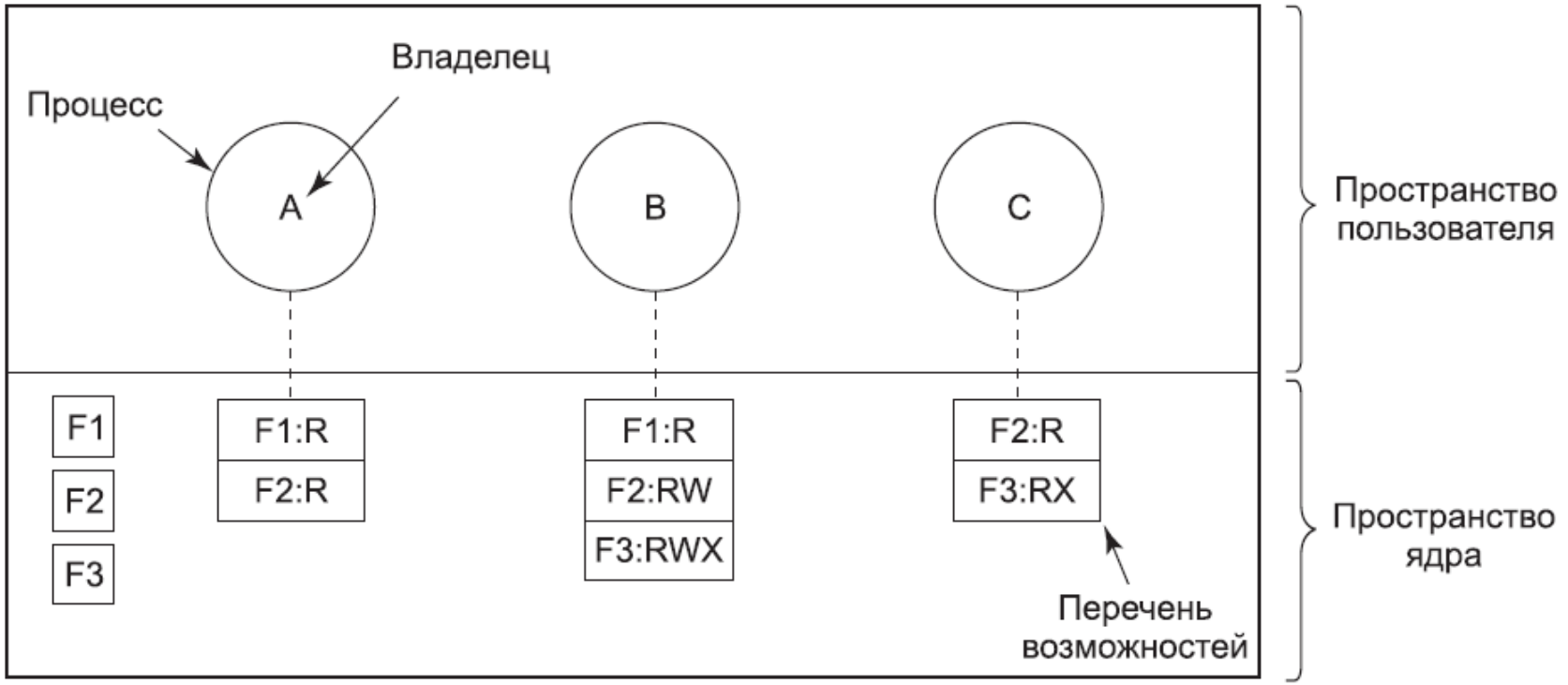
Домен	Файл 1	Файл 2	Файл 3	Файл 4	Файл 5	Файл 6	Принтер 1	Плоттер 2
1	Чтение	Чтение Запись						
2			Чтение	Чтение Запись Исполнение	Чтение Запись		Запись	
3						Чтение Запись Исполнение	Запись	Запись

Списки управления доступом



ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Перечень возможностей



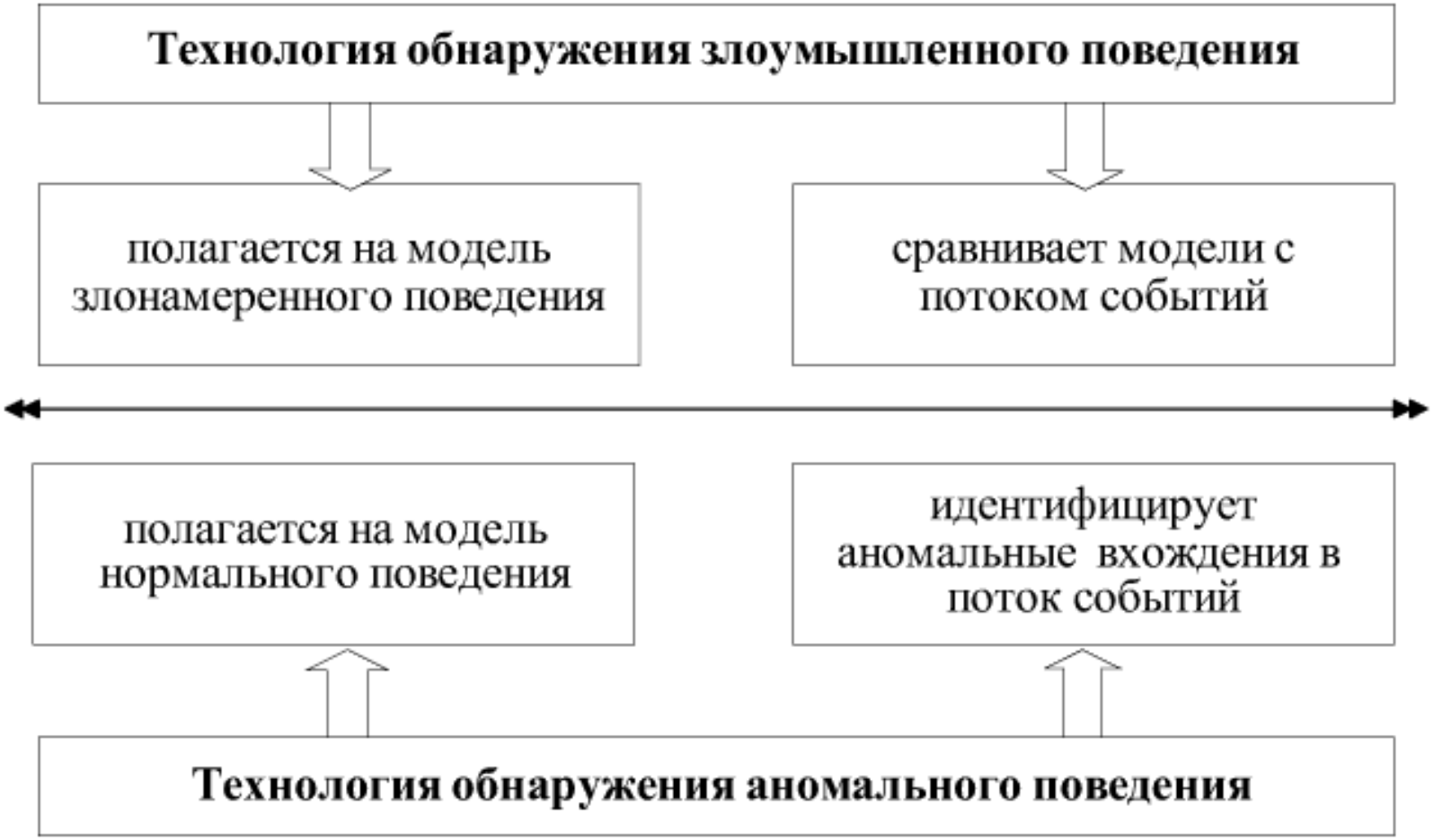
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Выявление вторжений

- Быстрое обнаружение вторжения позволяет идентифицировать и изгнать взломщика прежде, чем он причинит вред.
- Обнаружение вторжений позволяет собирать информацию о методах вторжения, которую можно использовать для повышения надежности средств защиты.
- Эффективная система обнаружения вторжений служит сдерживающим средством, предотвращающим вторжения.

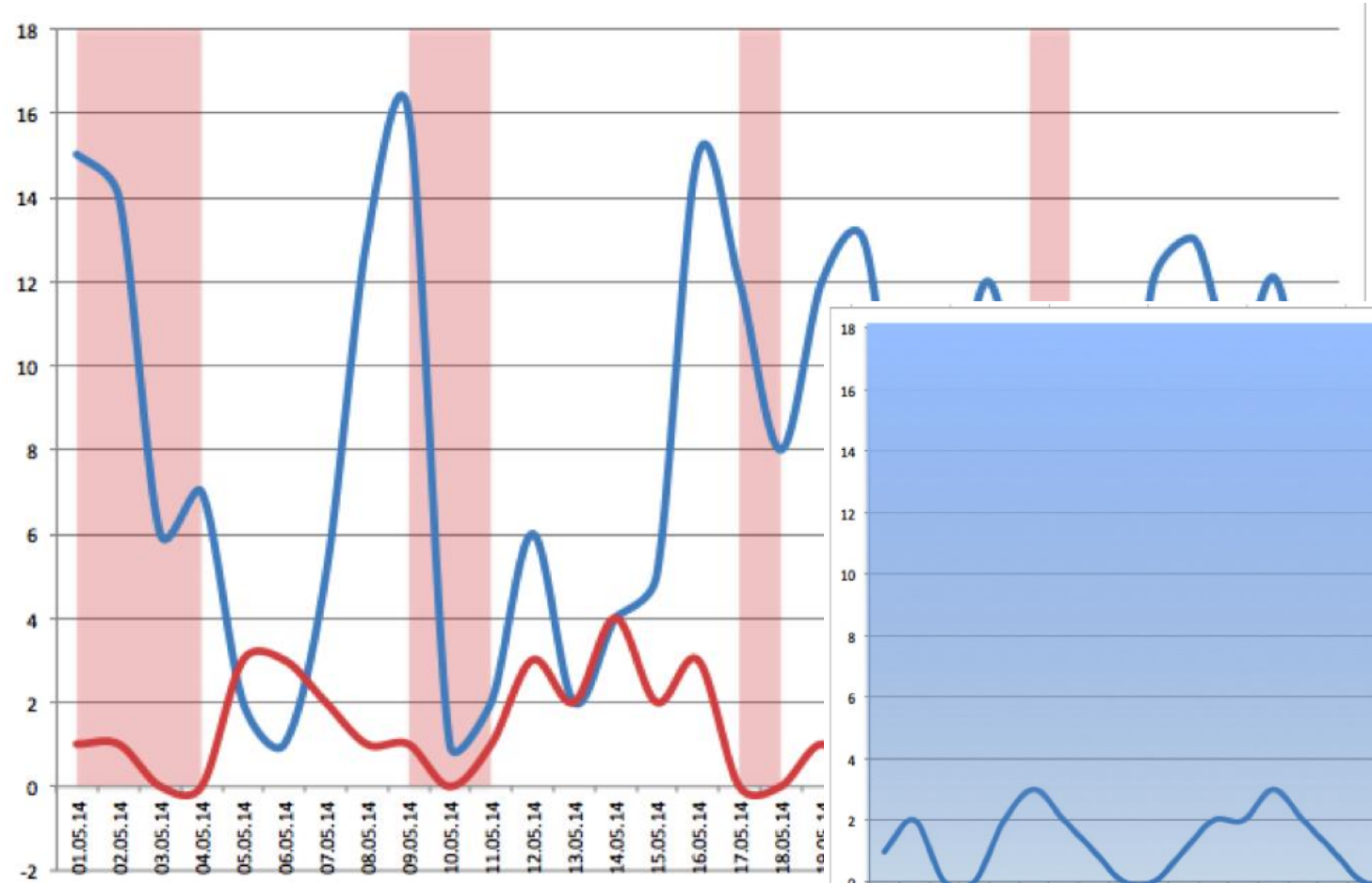
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

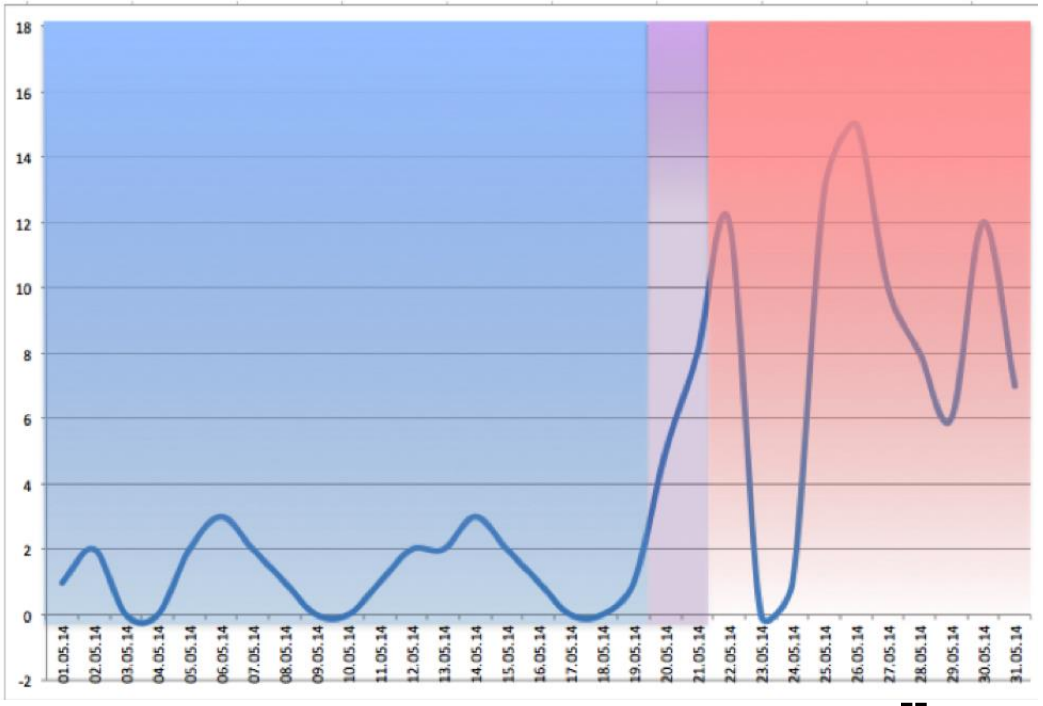
Подходы к выявлению вторжений



ИНСТИТУТ
МАТЕМАТИКИ
МЕХАНИКИ
КОМПЬЮТЕРНЫХ
НАУК
имени И.И. Воровича

«Почерк» взломщика





ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Борьба с атаками

- Проверка на подозрительные примеры активности.
- Ведение журнала аудита (audit log)
  - вход или выход из системы;
  - операции с файлами (открыть, закрыть, переименовать, удалить);
  - обращение к удаленной системе;
  - смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).
- Периодическое сканирование системы на предмет "дыр" в системе безопасности.

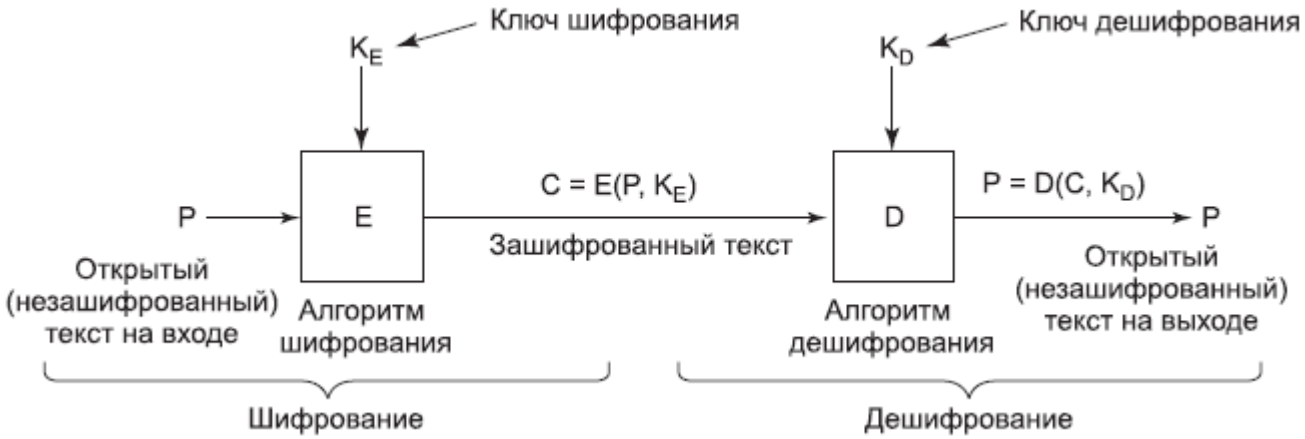
ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Периодические проверки

- Короткие или простые для угадывания пароли
- Несанкционированные программы, «изучающие» другие имена пользователей
- Неавторизованные программы в системных директориях
- Неожиданно долгие по времени процессы
- Нелогичная защита как пользовательских, так и системных директорий и файлов. Примером нелогичной защиты может быть файл, который запрещено читать его автору, но в который разрешено записывать информацию постороннему пользователю;
- Изменения в системных программах, обнаруженные при помощи контрольных сумм.

Шифрование

- Шифрование с секретным ключом
- Шифрование с открытым ключом



- Односторонние функции (криптографические хэш-функции)
- Цифровые подписи

ИНСТИТУТ МАТЕМАТИКИ МЕХАНИКИ КОМПЬЮТЕРНЫХ НАУК имени И.И. Воровича

Домашнее задание

- Читать книгу Таненбаум Э., Бос Х. Современные операционные системы, стр. 659-776.
- Информационная безопасность в компании