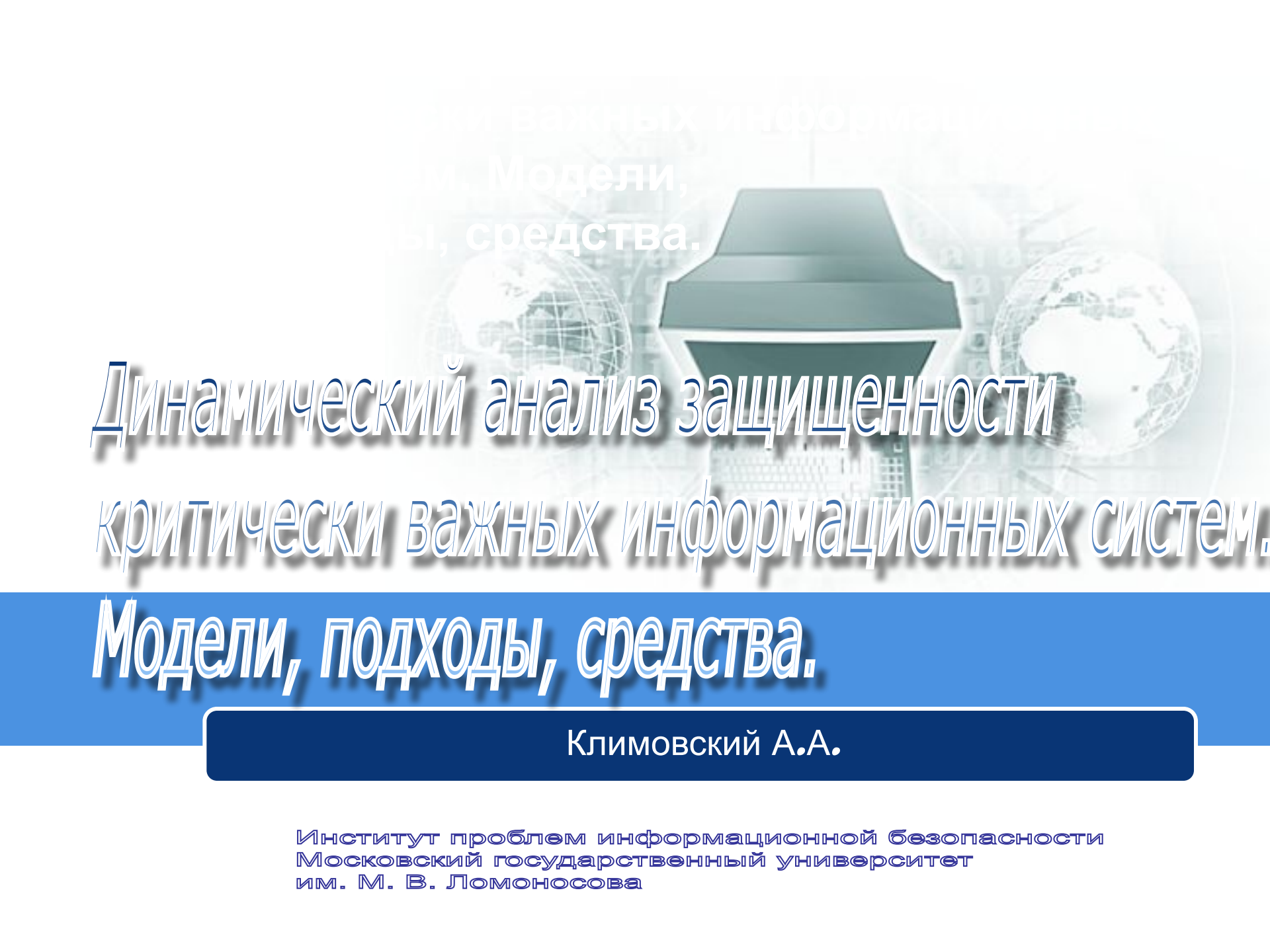


# Динамический анализ защищенности критически важных информационных систем.

## Модели, подходы, средства.

Климовский А.А.

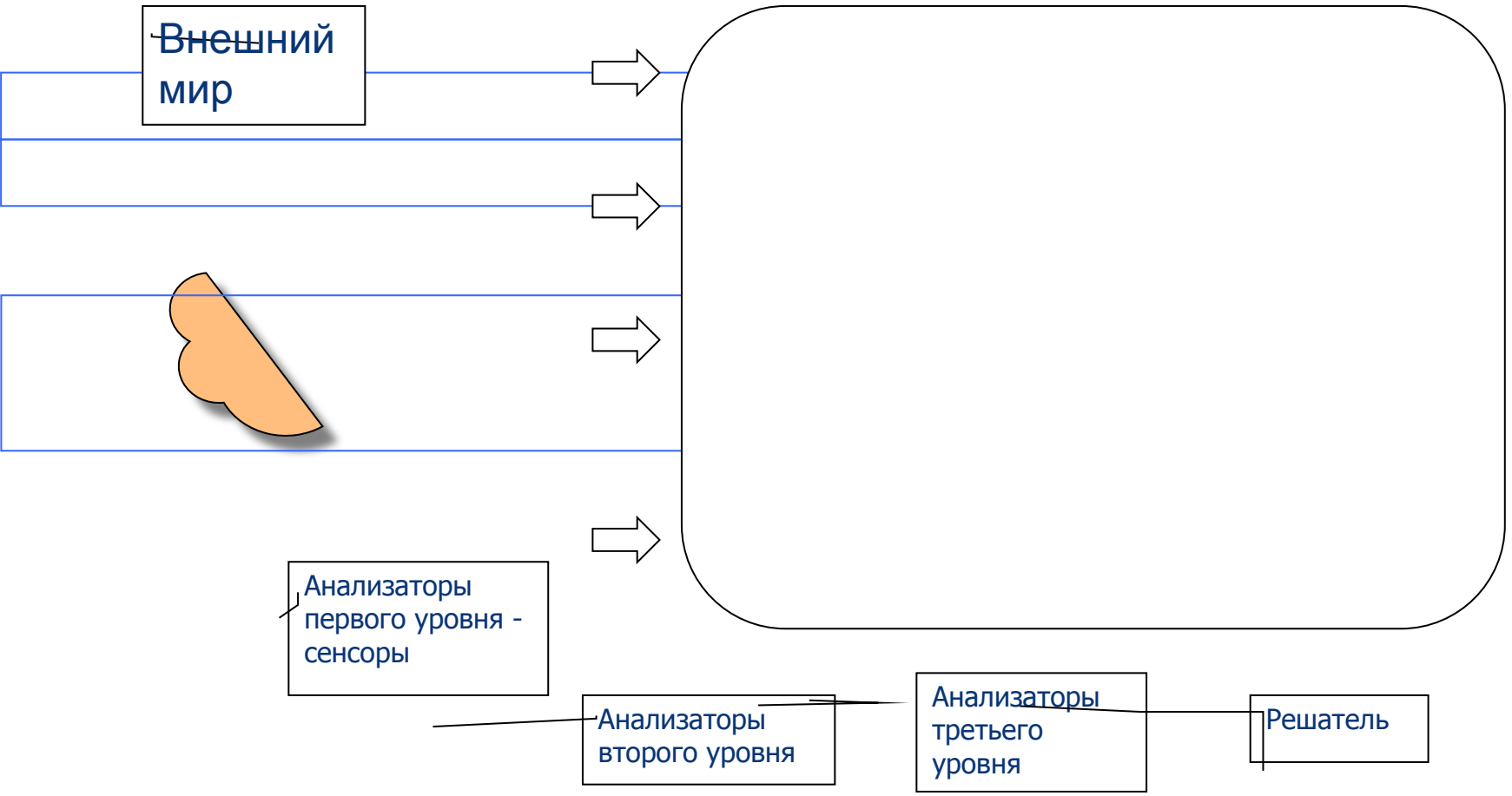
Институт проблем информационной безопасности
Московский государственный университет
им. М. В. Ломоносова

# Содержание

# Система мониторинга защищенности КВИС

- Цели и предназначение
- Методика формирования индикаторов защищенности КВИС
  - Определение функциональности системы, выделение регламентов функционирования
  - Анализ на основе регламентов и схемы программно-аппаратной реализации событий риска, угроз их возникновения и оценка возможного ущерба.
  - Анализ сценариев, приводящим к потере функциональности системы в целом, либо каких-то ее компонент
  - Разработка методов выявления нежелательного поведения системы и вычисления индикаторов защищенности

# Модель системы



# Определение языка

**Определение 1.** Пусть $\Sigma$ - конечный алфавит.

*Множество формул* $\mathcal{F}$ над алфавитом $\Sigma$ (будем обозначать $\mathcal{F}(\Sigma)$) определим следующим образом:

1. $a \in \Sigma \Rightarrow a \in \mathcal{F}$
2. $\varphi, \psi \in \mathcal{F} \Rightarrow \varphi \wedge \psi, \varphi \vee \psi, \bar{\varphi} \in \mathcal{F}$
3. $\varphi, \psi \in \mathcal{F} \Rightarrow \varphi \cdot \psi \in \mathcal{F}$

**Определение 2.** Введем понятие истинности формулы $\varphi$ на строке $u$ ($\varphi \models u, \varphi \in \mathcal{F}, u \in \Sigma^*$):

1. $a \models u \Leftrightarrow a$ входит в $u$
2. $a \cdot b \models u \Leftrightarrow ab$ входит в $u$
3. $\bar{\varphi} \models u \Leftrightarrow \varphi \not\models u$
4. $\varphi \wedge \psi \models u \Leftrightarrow \varphi \models u$ и $\psi \models u$
5. $\varphi \vee \psi \models u \Leftrightarrow \varphi \models u$ или $\psi \models u$

# Определение языка

**Определение 3.** Определим $\sim$-язык $\tilde{L}_\varphi$, задаваемый формулой $\varphi$:

$$\tilde{L}_\varphi := \{u : \varphi \models u\}$$

**Определение 4.** Определим язык $L_\varphi$, задаваемый формулой $\varphi$:

- если $\varphi = a$, где $a \in \Sigma$, то $L_\varphi = \{a\}$;
- если $\varphi = a \cdot b$, где $a, b \in \Sigma$, то $L_\varphi = \{ab\}$;
- если $\varphi = \bar{a}$, где $a \in \Sigma$, то $L_\varphi = \Sigma^* \backslash \tilde{L}_a$;
- если $\varphi_1, \varphi_2 \in \mathcal{F}$, тогда:

$$L_{\varphi_1 \cdot \varphi_2} = \{uv : u \in L_{\varphi_1},\, v \in L_{\varphi_2}\};$$

$$L_{\varphi_1 \vee \varphi_2} = \{uv : u \in L_{\varphi_1},\, v \in L_{\varphi_2} \cup \{\epsilon\}\} \cup \{uv : u \in L_{\varphi_2},\, v \in L_{\varphi_1} \cup \{\epsilon\}\};$$

$$L_{\varphi_1 \wedge \varphi_2} = \{uv : u \in L_{\varphi_1},\, v \in L_{\varphi_2}\} \cup \{uv : u \in L_{\varphi_2},\, v \in L_{\varphi_1}\};$$

$$L_{\neg\varphi_1} = \Sigma^* \backslash \widetilde{L}_{\varphi_1}.$$

# Математическая модель анализатора

**Определение.** Запись вида:

$$a(p_1, ..., p_{\nu(a)}) \ :- \varphi, \qquad (*)$$

где $a \in \Sigma$, $p_i \in D, \varphi \in \mathcal{F}(E)$ будем называть *правилом преобразования*

**Определение.** Последовательность правил преобразования

$$a_1(p_{1,1}, ..., p_{1,\nu(a_1)}) \ :- \varphi_1;$$

$$a_2(p_{2,1}, ..., p_{2,\nu(a_2)}) \ :- \varphi_2;$$

$$...$$

$$a_m(p_{m,1}, ..., p_{m,\nu(a_m)}) \ :- \varphi_m.$$

будем называть *программой*.

# Классификация компьютерных атак

- Атака – это последовательность действий предпринимаемых кем-либо для достижения несанкционированного результата, то есть действий, направленных на нарушение правил функционирования системы, установленных ее владельцем.

*«A common language for computer security incidents», John D. Howard, Thomas A. Longstaff, Sandia Report, Sandia National Laboratories.*

# Понятие таксономии

- Таксономия – это классификационная схема, которая разделяет совокупность знаний и определяет взаимосвязь частей.

*«The IEEE standard dictionary of electrical and electronics terms»*

# Задача классификации

- Создание связующего звена между классификацией критических объектов, возможными угрозами критическим объектам и оценкой рисков угроз
- Создание на основе классификации подходов к моделированию атак и применение полученных результатов для разработки моделей нарушителя
- Разработка методов выявления атак для средств активного аудита

# Требования к классификации

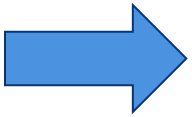
- Основные требования:
  - *Взаимное исключение*
  - *Полнота*
  - *Применимость*
  - *Детерминированность*
  - *Расширяемость*
- Второстепенные требования:
  - *Четкость терминов*
  - *Объективность*
  - *Доступность/понятность*
  - *Согласованность*

# Подходы к решению

| | Атакующий не имеет право запуска/использования программы/информации | Атакующий имеет право запуска/использования программы/информации |
|---|---|---|
| Атакующий не имеет доступ к компьютеру | *Категория A*<br>Внешнее вторжение | - |
| Атакующий имеет доступ к компьютеру | *Категория B*<br>Внутреннее вторжение | *Категория C*<br>Злоупотребление полномочиями |

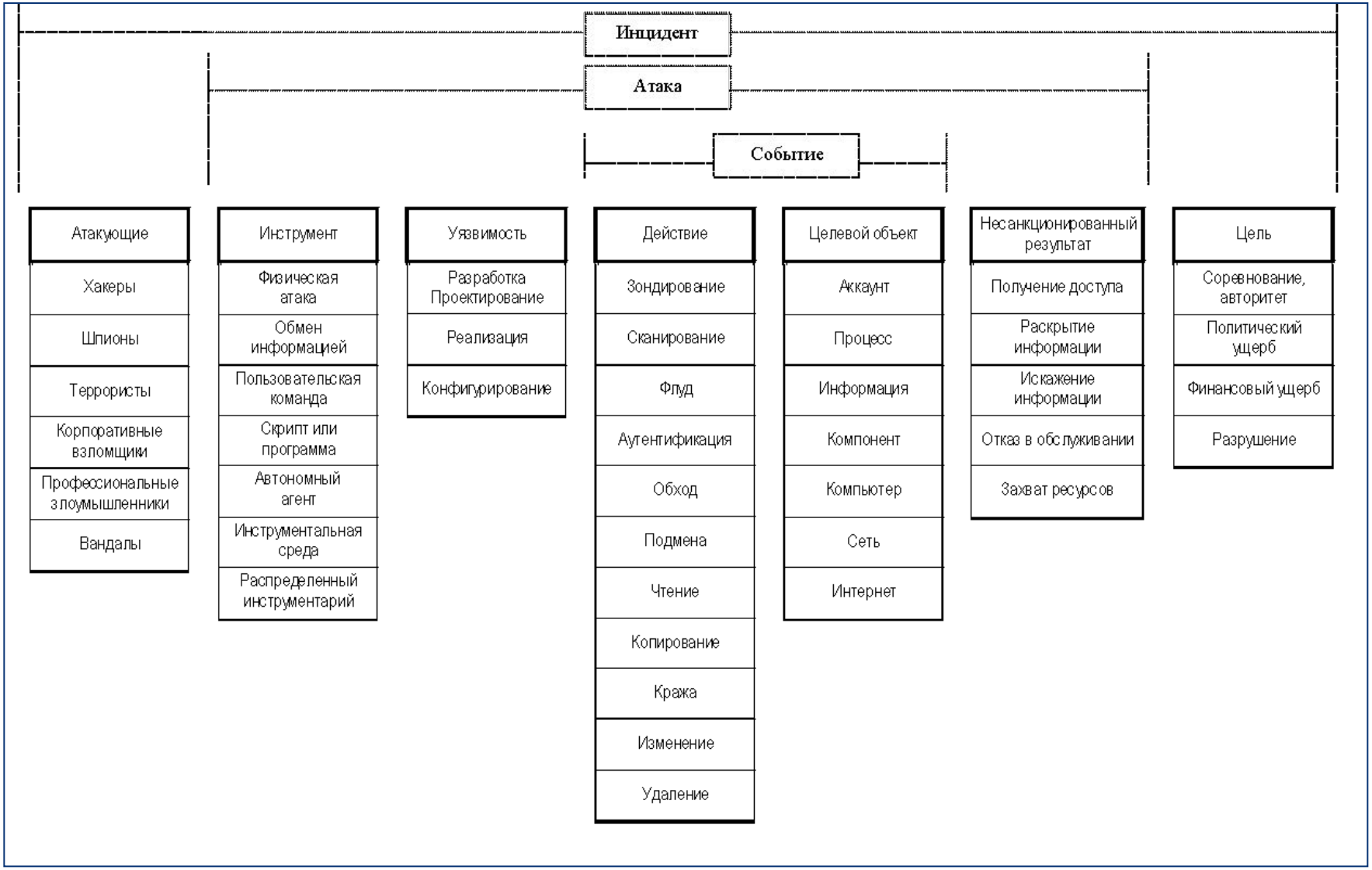
# Нойман и Паркер

| |
|---|
| Внешнее |
| Аппаратное |
| Маскировка |
| Вредоносные программы |
| Обход механизмов безопасности |
| Активное злоупотребление |
| Пассивное злоупотребление |
| Косвенное злоупотребление |



26 типов атак

# Ховард и Лонгстафф



# Хансман

- *Первое измерение*

  Список типов атак.

- *Второе измерение*

  Цель (целевой объект) атаки.

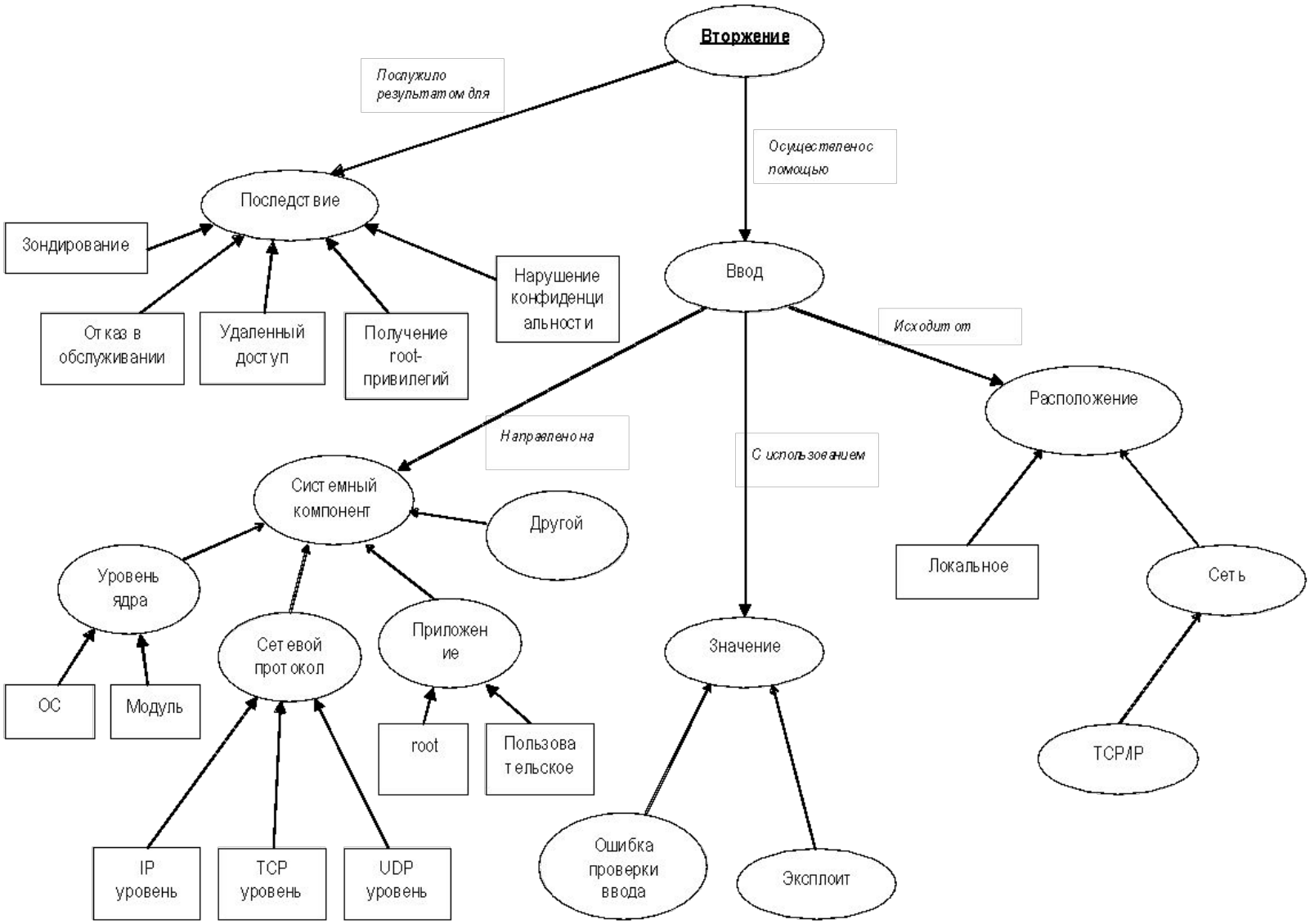
- *Третье измерение*

  Список уязвимостей, используемых в процессе атаки.

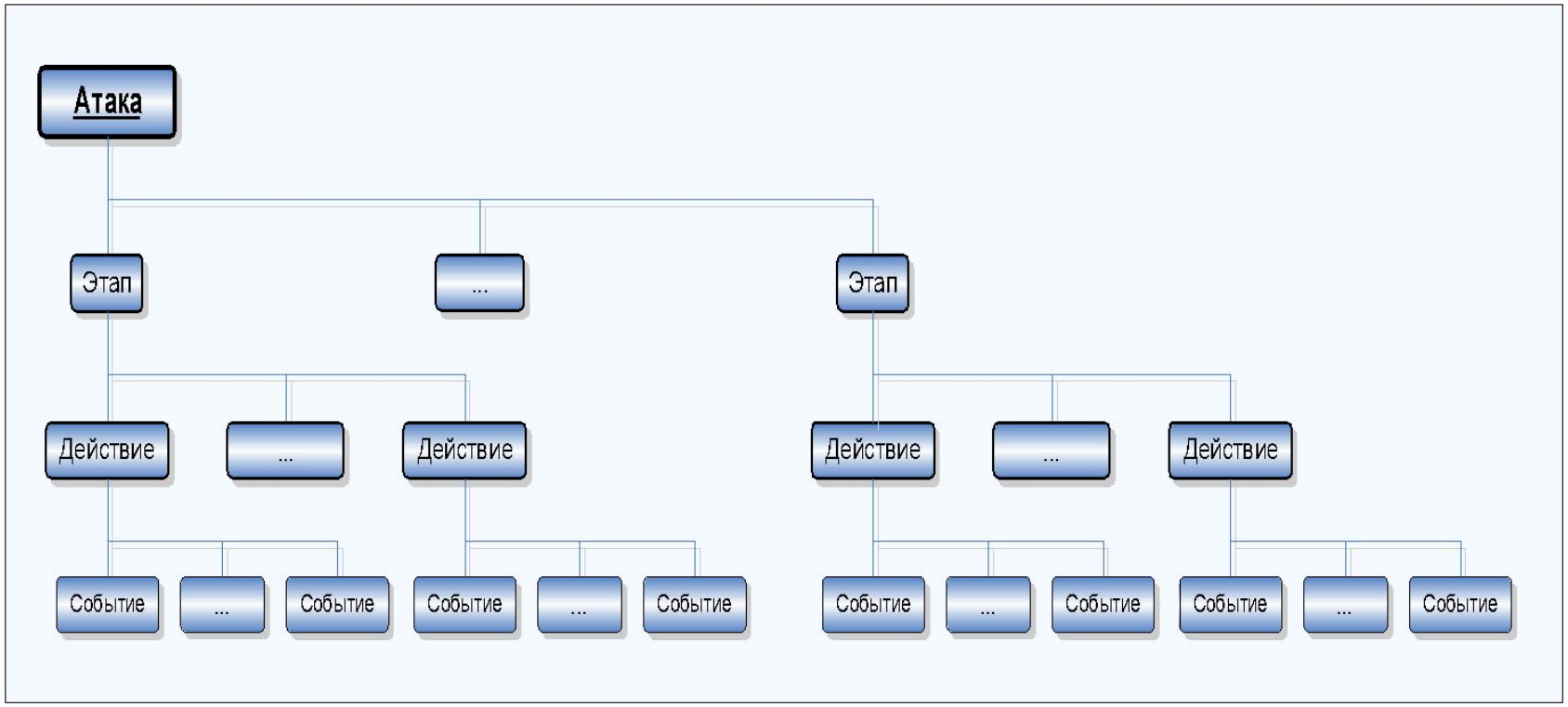
- *Четвертое измерение*

  Результат или цель атаки.

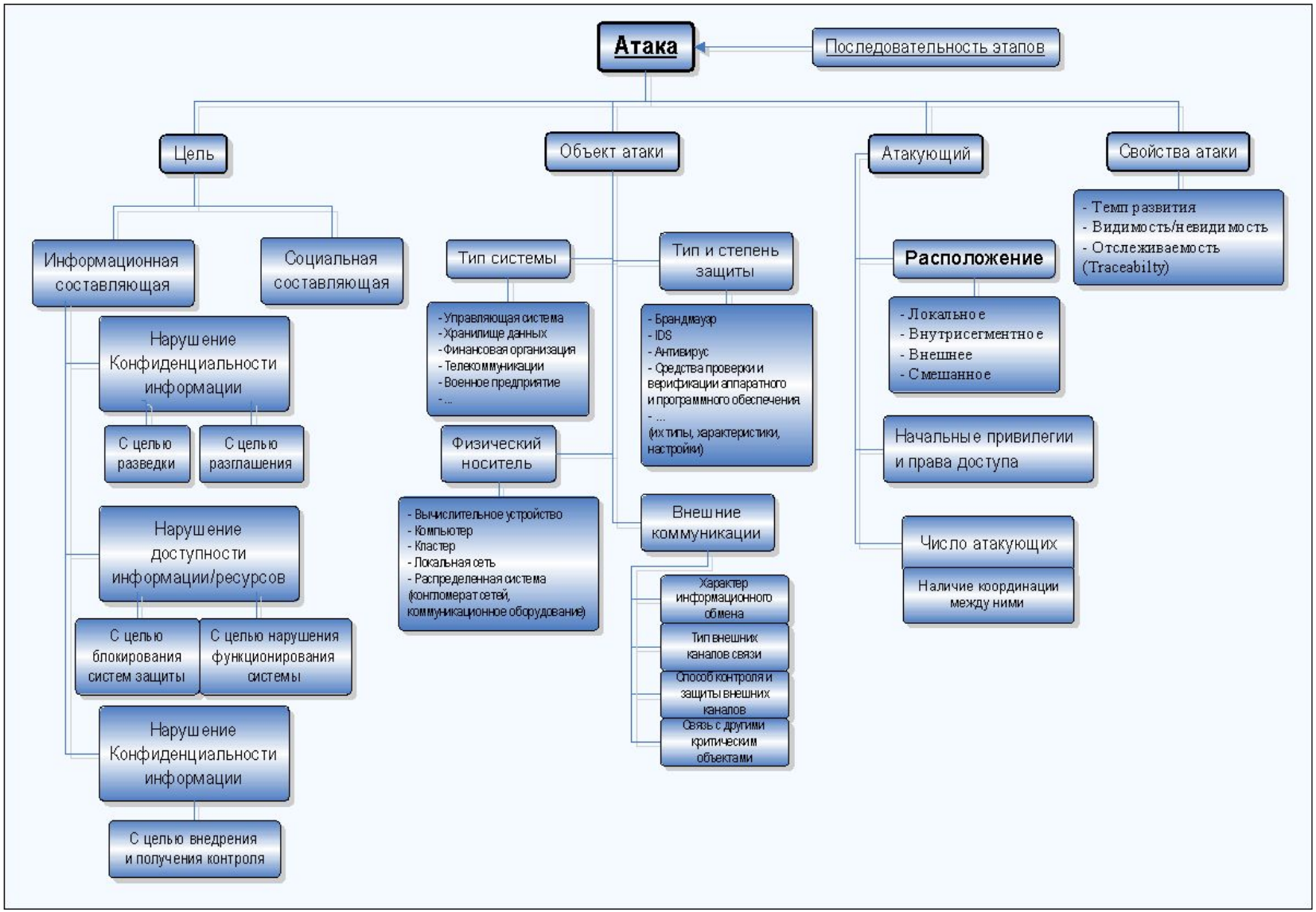
# Андеркоффер и Пинкстон



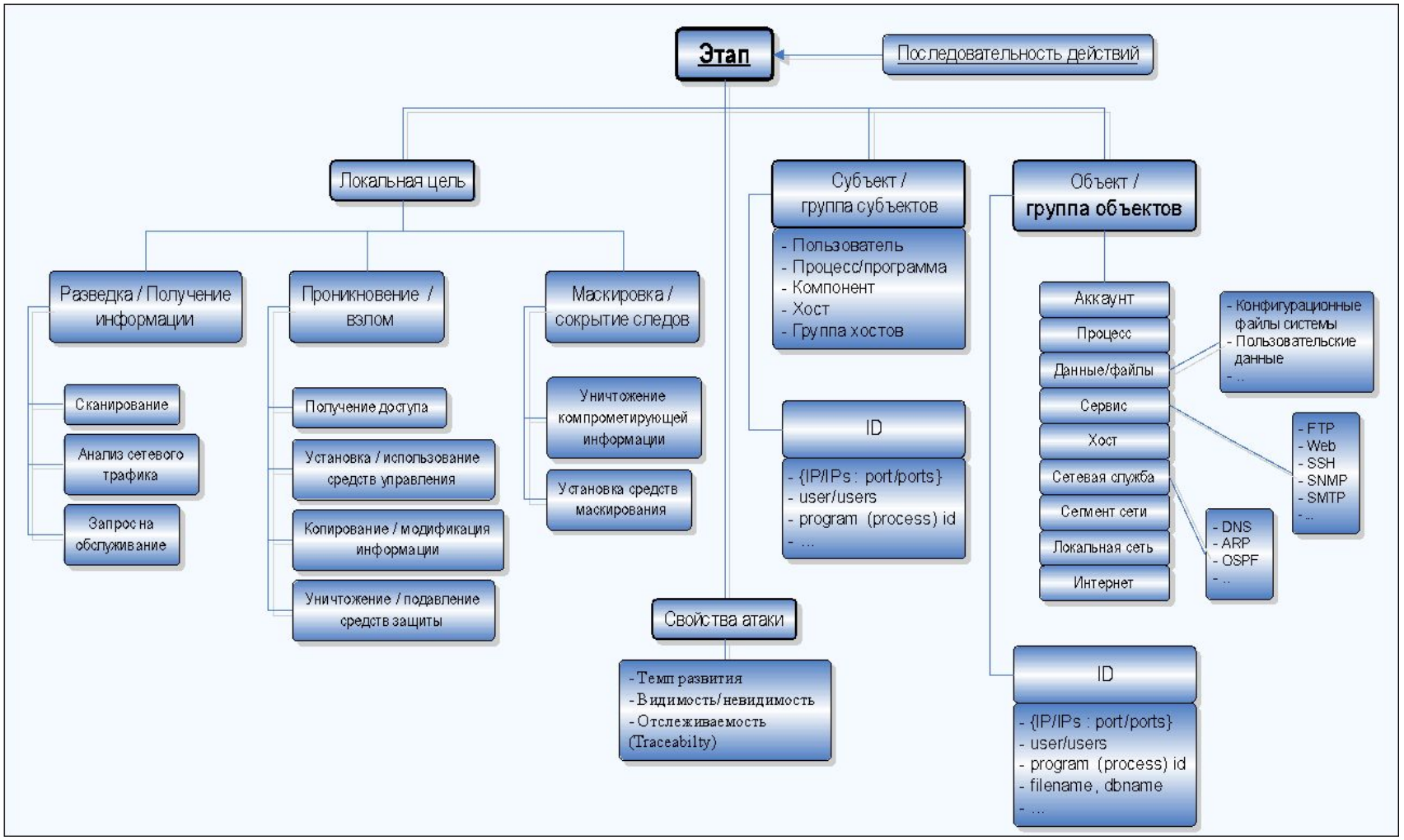
# Предлагаемая классификация



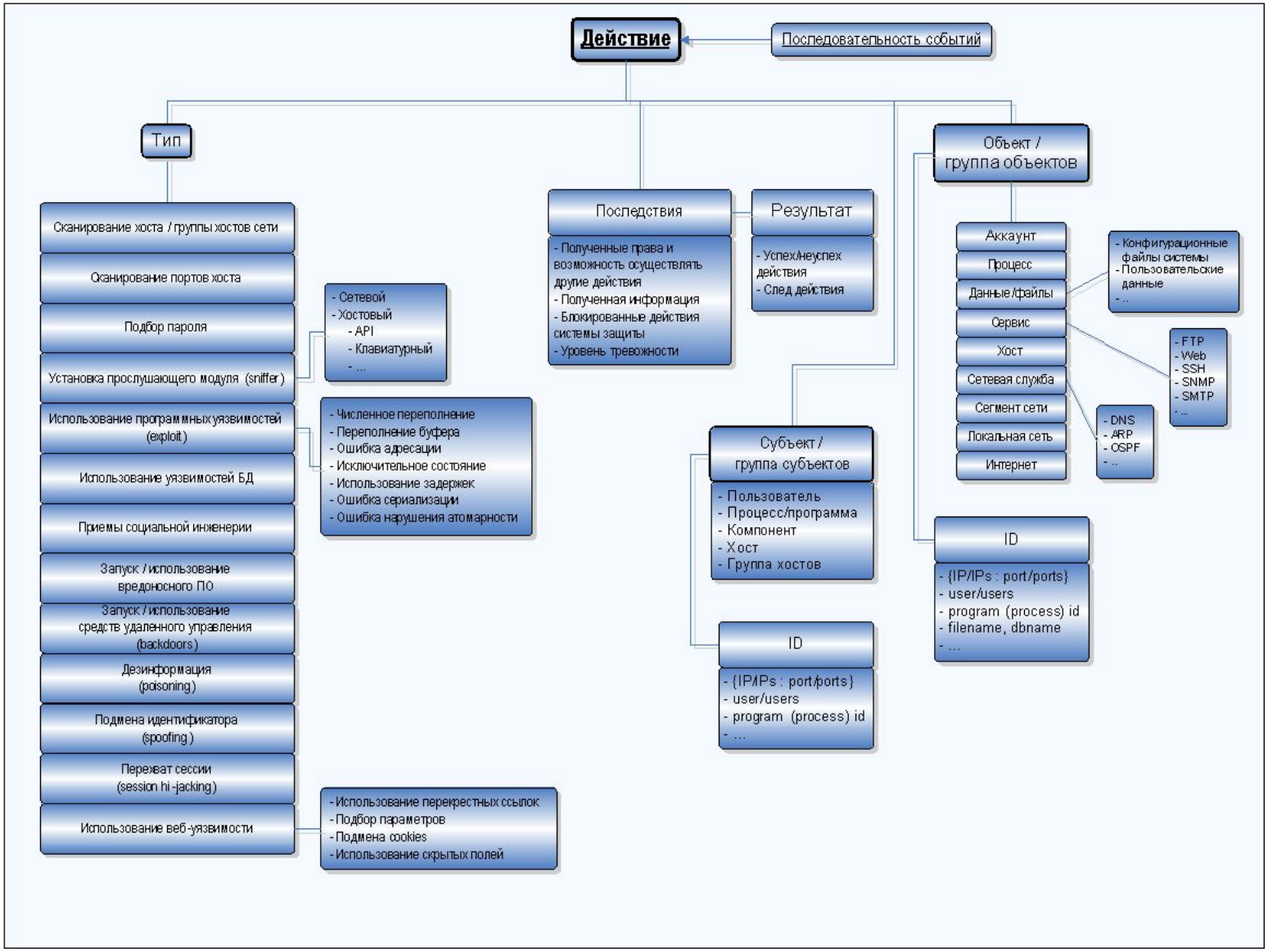
# Атака


Атака
Последовательность этапов
Цель
Объект атаки
Атакующий
Свойства атаки
Информационная составляющая
Социальная составляющая
Нарушение Конфиденциальности информации
С целью разведки
С целью разглашения
Нарушение доступности информации/ресурсов
С целью блокирования систем защиты
С целью нарушения функционирования системы
Нарушение Конфиденциальности информации
С целью внедрения и получения контроля
Тип системы
- Управляющая система
- Хранилище данных
- Финансовая организация
- Телекоммуникации
- Военное предприятие
- ...
Физический носитель
- Вычислительное устройство
- Компьютер
- Кластер
- Локальная сеть
- Распределенная система (конгломерат сетей, коммуникационное оборудование)
Тип и степень защиты
- Брандмауэр
- IDS
- Антивирус
- Средства проверки и верификации аппаратного и программного обеспечения
- ...
(их типы, характеристики, настройки)
Внешние коммуникации
Характер информационного обмена
Тип внешних каналов связи
Способ контроля и защиты внешних каналов
Связь с другими критическим объектами
Расположение
- Локальное
- Внутрисегментное
- Внешнее
- Смешанное
Начальные привилегии и права доступа
Число атакующих
Наличие координации между ними
- Темп развития
- Видимость/невидимость
- Отслеживаемость (Traceabilty)

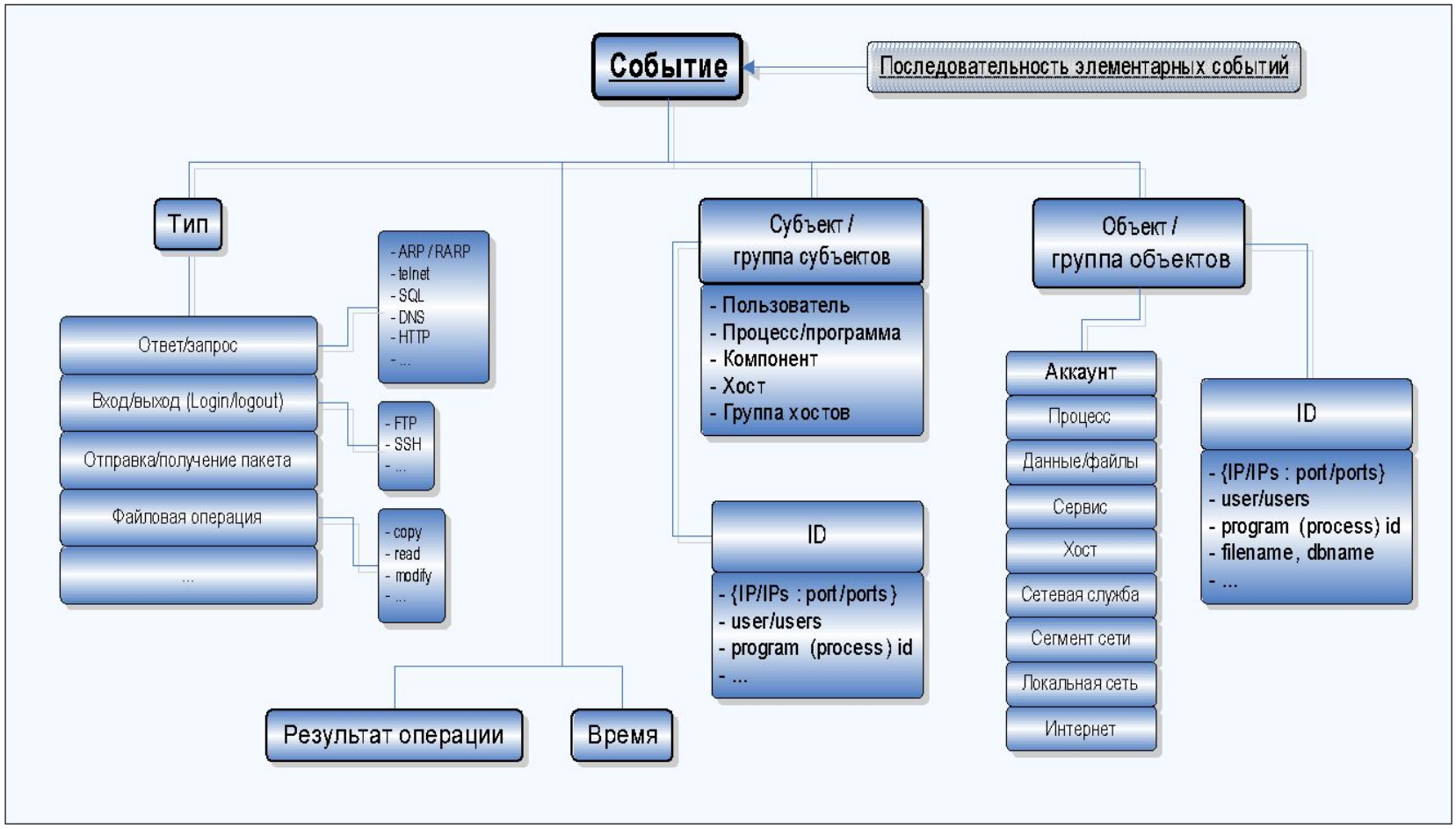
# Этап


Этап
Последовательность действий
Локальная цель
Субъект / группа субъектов
Объект / группа объектов
Разведка / Получение информации
Проникновение / взлом
Маскировка / сокрытие следов
- Пользователь
- Процесс/программа
- Компонент
- Хост
- Группа хостов
Аккаунт
Процесс
Данные/файлы
Сервис
Хост
Сетевая служба
Сегмент сети
Локальная сеть
Интернет
- Конфигурационные файлы системы
- Пользовательские данные
- ..
- FTP
- Web
- SSH
- SNMP
- SMTP
- ...
- DNS
- ARP
- OSPF
- ..
Сканирование
Анализ сетевого трафика
Запрос на обслуживание
Получение доступа
Установка / использование средств управления
Копирование / модификация информации
Уничтожение / подавление средств защиты
Уничтожение компрометирующей информации
Установка средств маскирования
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- ...
Свойства атаки
- Темп развития
- Видимость/невидимость
- Отслеживаемость (Traceabilty)
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- filename, dbname
- ...

# Действие


Действие
Последовательность событий
Тип
Сканирование хоста / группы хостов сети
Сканирование портов хоста
Подбор пароля
Установка прослушающего модуля (sniffer)
- Сетевой
- Хостовый
- API
- Клавиатурный
- ...
Использование программных уязвимостей (exploit)
- Численное переполнение
- Переполнение буфера
- Ошибка адресации
- Исключительное состояние
- Использование задержек
- Ошибка сериализации
- Ошибка нарушения атомарности
Использование уязвимостей БД
Приемы социальной инженерии
Запуск / использование вредоносного ПО
Запуск / использование средств удаленного управления (backdoors)
Дезинформация (poisoning)
Подмена идентификатора (spoofing)
Перехват сессии (session hi-jacking)
Использование веб-уязвимости
- Использование перекрестных ссылок
- Подбор параметров
- Подмена cookies
- Использование скрытых полей
Последствия
- Полученные права и возможность осуществлять другие действия
- Полученная информация
- Блокированные действия системы защиты
- Уровень тревожности
Результат
- Успех/неуспех действия
- След действия
Субъект / группа субъектов
- Пользователь
- Процесс/программа
- Компонент
- Хост
- Группа хостов
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- ...
Объект / группа объектов
Аккаунт
Процесс
Данные/файлы
Сервис
Хост
Сетевая служба
Сегмент сети
Локальная сеть
Интернет
- Конфигурационные файлы системы
- Пользовательские данные
- ...
- FTP
- Web
- SSH
- SNMP
- SMTP
- ...
- DNS
- ARP
- OSPF
- ..
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- filename, dbname
- ...

# Событие


Событие
Последовательность элементарных событий
Тип
Ответ/запрос
Вход/выход (Login/logout)
Отправка/получение пакета
Файловая операция
...
- ARP / RARP
- telnet
- SQL
- DNS
- HTTP
- ...
- FTP
- SSH
- ...
- copy
- read
- modify
- ...
Субъект / группа субъектов
- Пользователь
- Процесс/программа
- Компонент
- Хост
- Группа хостов
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- ...
Объект / группа объектов
Аккаунт
Процесс
Данные/файлы
Сервис
Хост
Сетевая служба
Сегмент сети
Локальная сеть
Интернет
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- filename, dbname
- ...
Результат операции
Время

# Перспективы

- Дальнейшее развитие классификации
  - Учет корреляции действий атакующего
  - Учет ответных действий системы защиты
- Создание связующего звена между критическими информационными системами, угрозами и атаками, объединение их в общую таксономию
- Применение полученных результатов для генерации сценариев атак и создание системы тестирования
- Разработка методов выявления атак для средств активного аудита
- Исследование и доработка математической модели, методов формирования индикаторов защищенности
  - Устойчивость захвату/компрометации отдельных частей
  - Вопросы дискретного управления
  - Исследование надежности

# Спасибо за внимание!