

критически важных информационных систем.
Модели, подходы, средства.

Динамический анализ защищенности критически важных информационных систем. Модели, подходы, средства.

Климовский А.А.

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

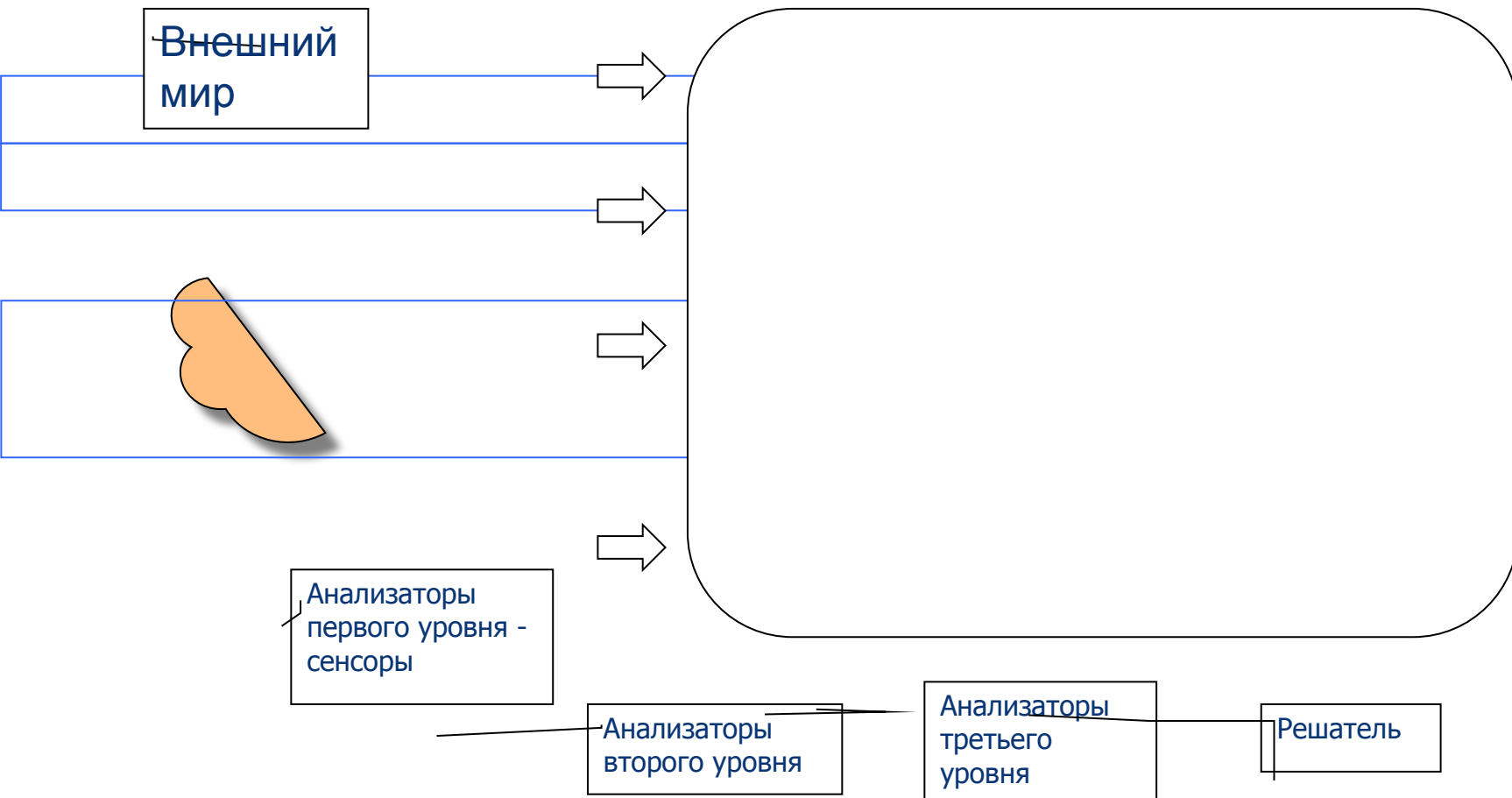
Содержание

- 1 Мониторинг защищенности КВИС
- 2 Математическая модель системы
- 3 Классификация атак
- 4 Направления дальнейшего развития

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 Σ - конечный алфавит.

Множество формул \mathcal{F} над алфавитом Σ (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 φ 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}_φ , задаваемый формулой φ :

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

Определение 4. Определим язык L_φ , задаваемый формулой φ :

- 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 $L_\varphi = \Sigma^* \setminus \tilde{L}_a$;
- если $\varphi_1, \varphi_2 \in \mathcal{F}$, тогда:

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

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

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

$$L_{\neg \varphi_1} = \Sigma^* \setminus \tilde{L}_{\varphi_1}.$$

Математическая модель анализатора

Определение. Запись вида:

$$a(p_1, \dots, p_{\nu(a)}) : - \varphi, \quad (*)$$

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

Определение. Последовательность правил преобразования

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

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

...

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

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:

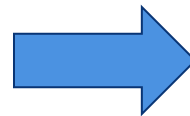
- *Четкость терминов*
- *Объективность*
- *Доступность/понятность*
- *Согласованность*

Подходы к решению

	Атакующий <u>не имеет</u> право запуска/использования программы/информации	Атакующий <u>имеет</u> право запуска/использования программы/информации
Атакующий <u>не имеет</u> доступ к компьютеру	<i>Категория А</i> Внешнее вторжение	-
Атакующий <u>имеет</u> доступ к компьютеру	<i>Категория В</i> Внутреннее вторжение	<i>Категория С</i> Злоупотребление полномочиями

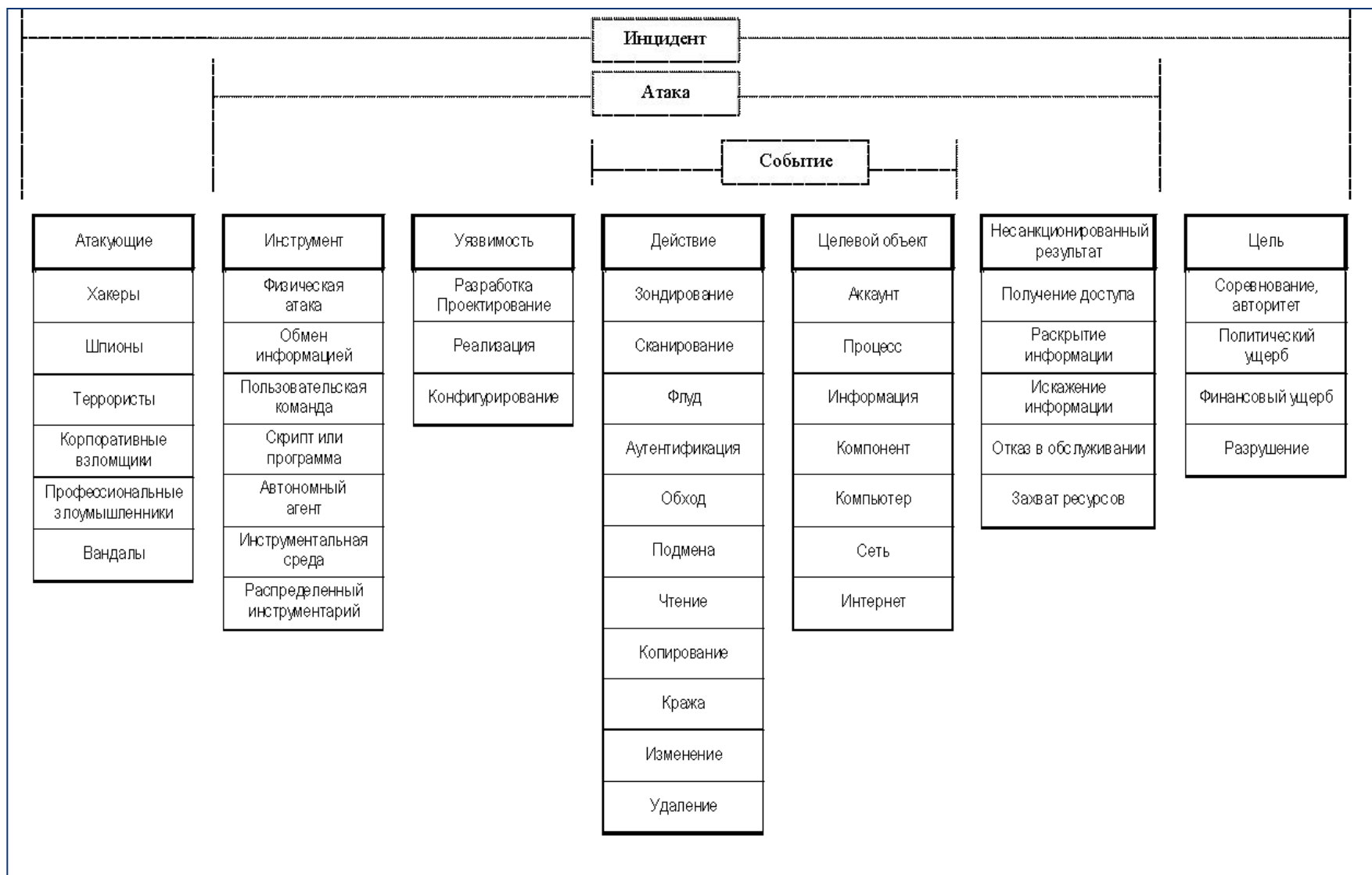
Нойман и Паркер

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.

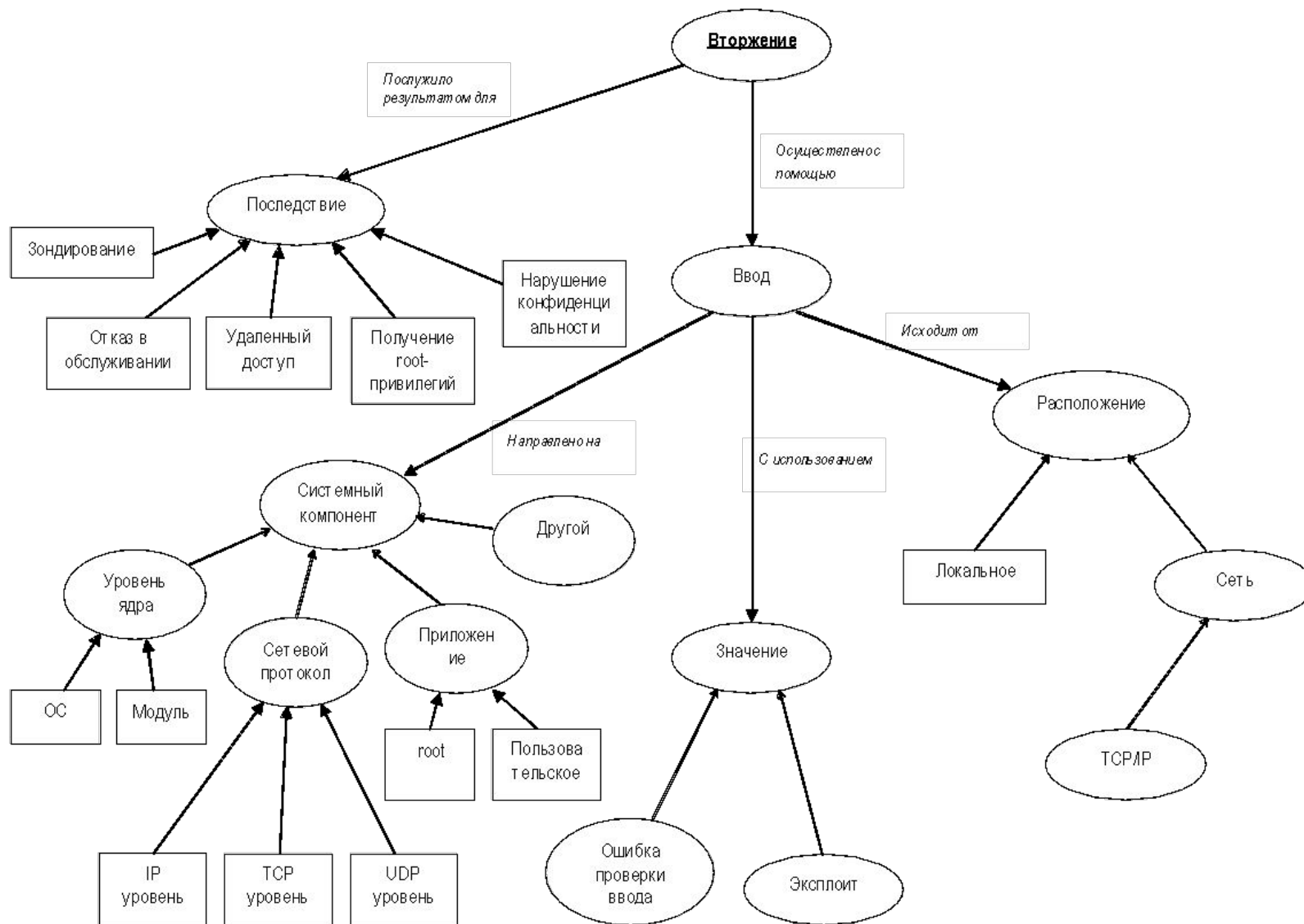
- *Третье измерение*

Список уязвимостей, используемых в процессе атаки.

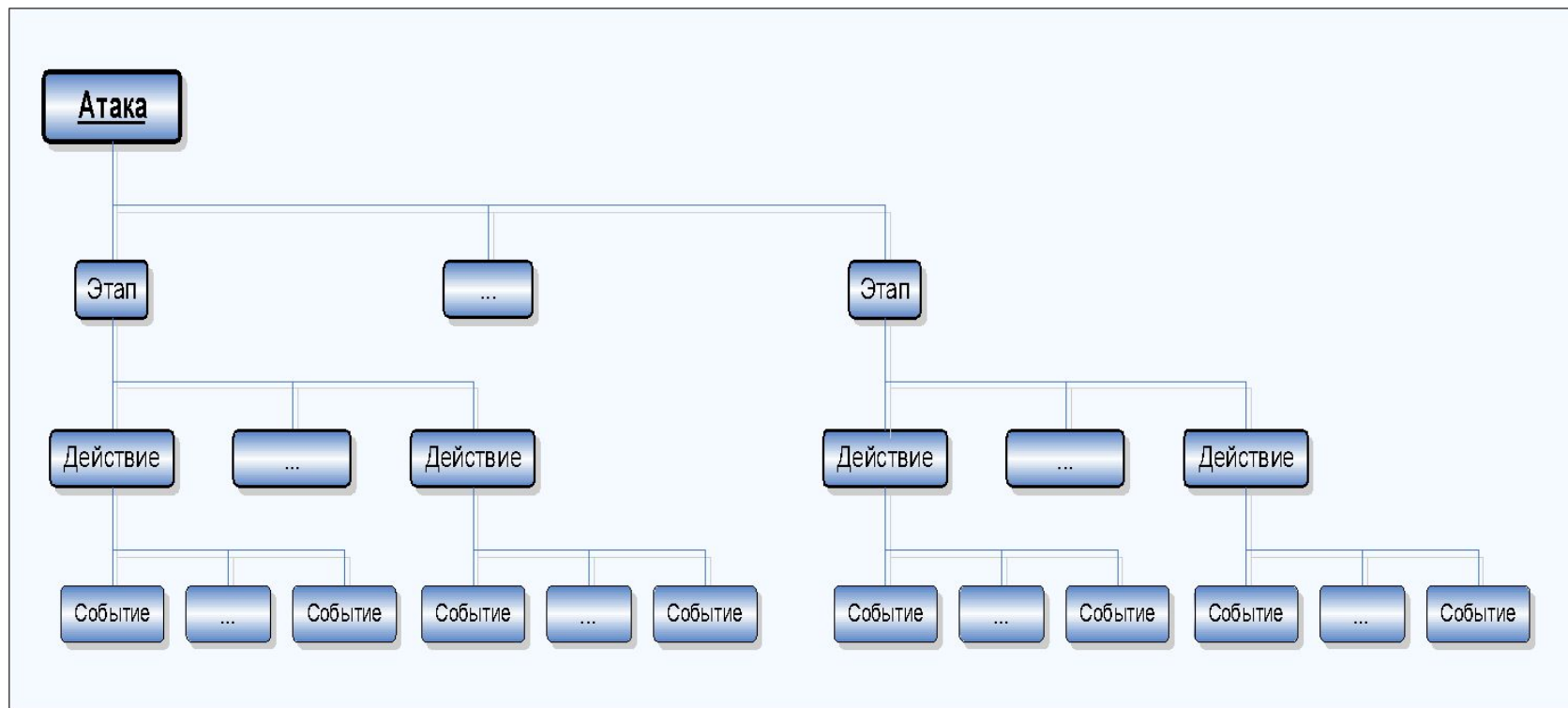
- *Четвертое измерение*

Результат или цель атаки.

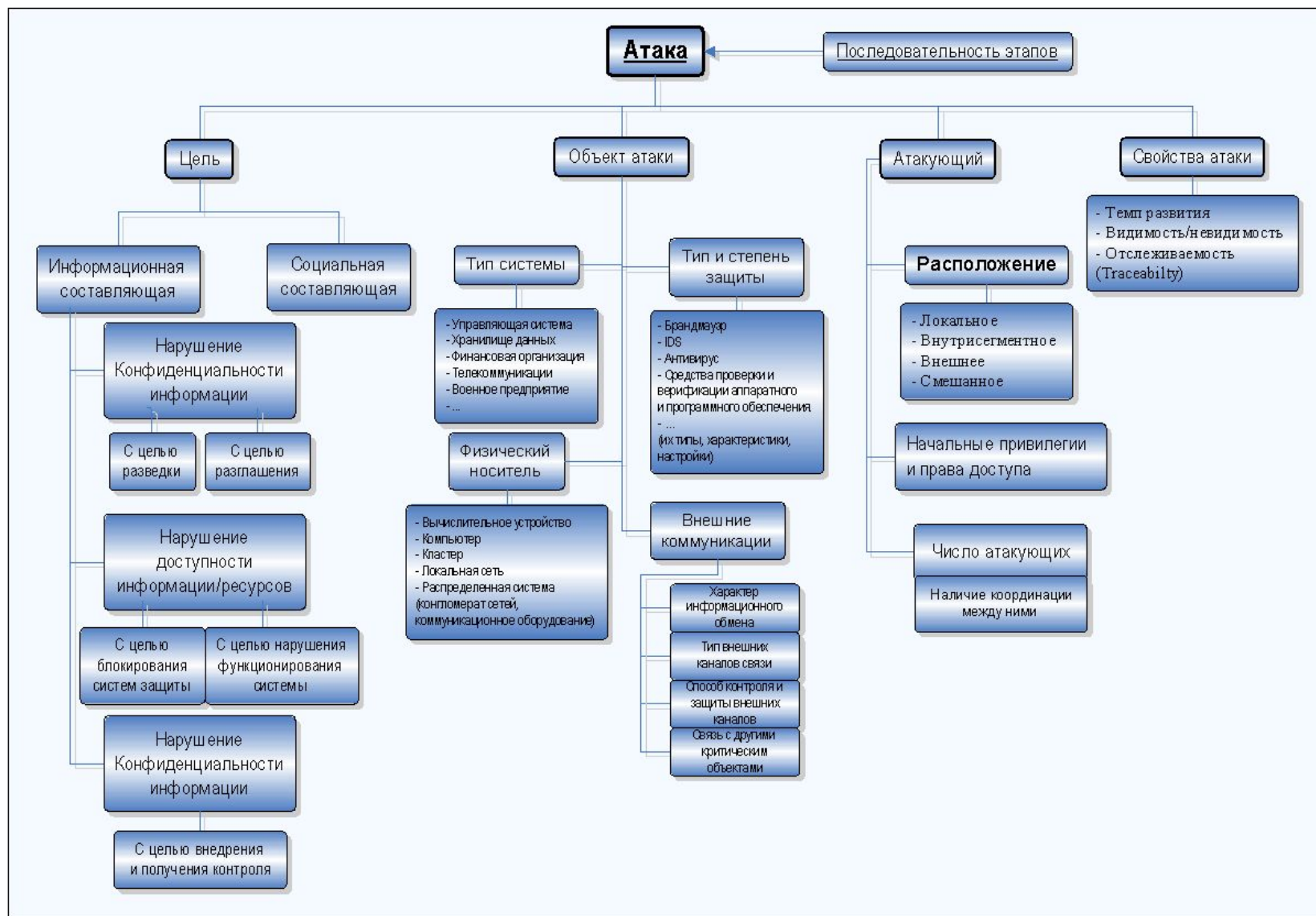
Андеркоффер и Пинкстон



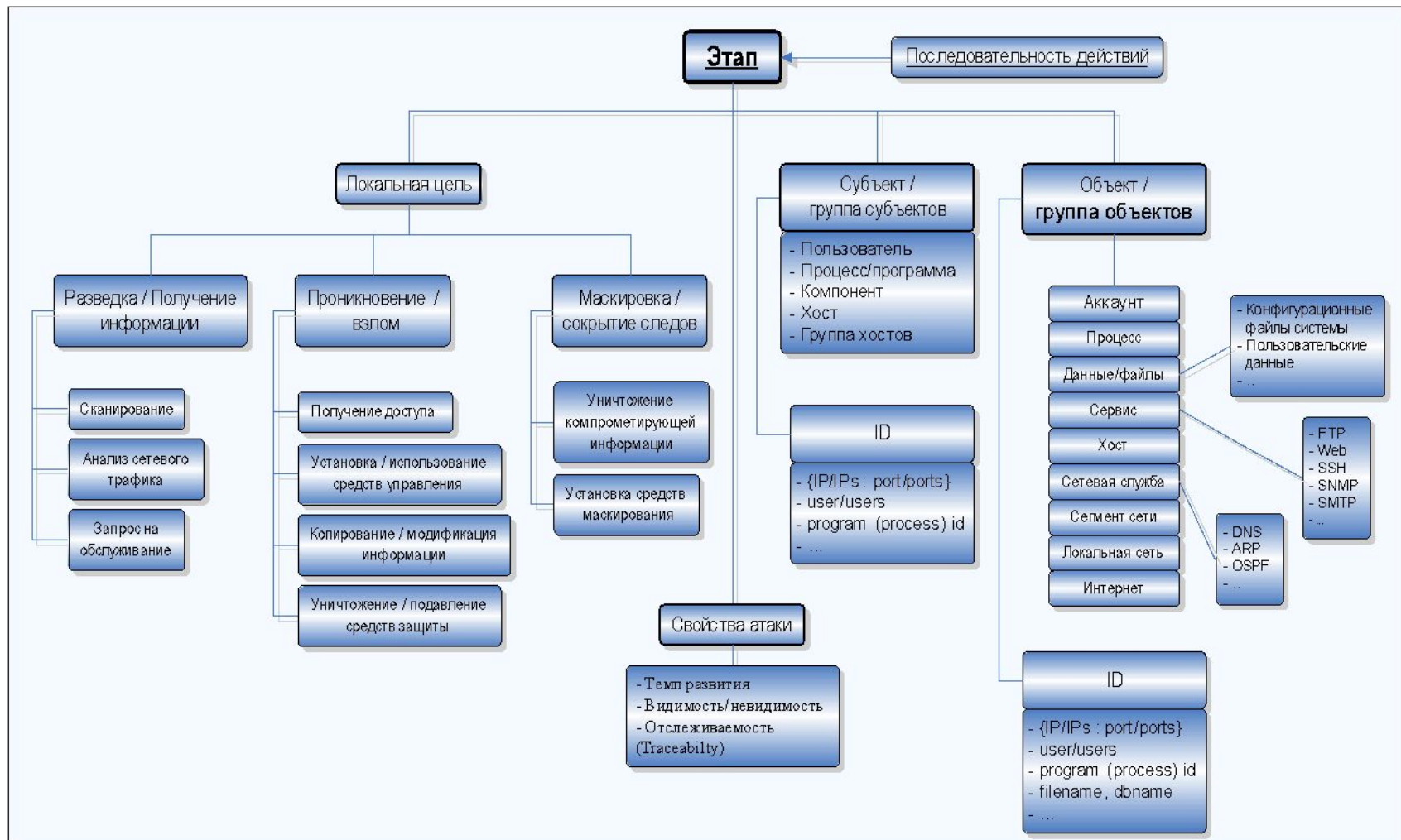
Предлагаемая классификация



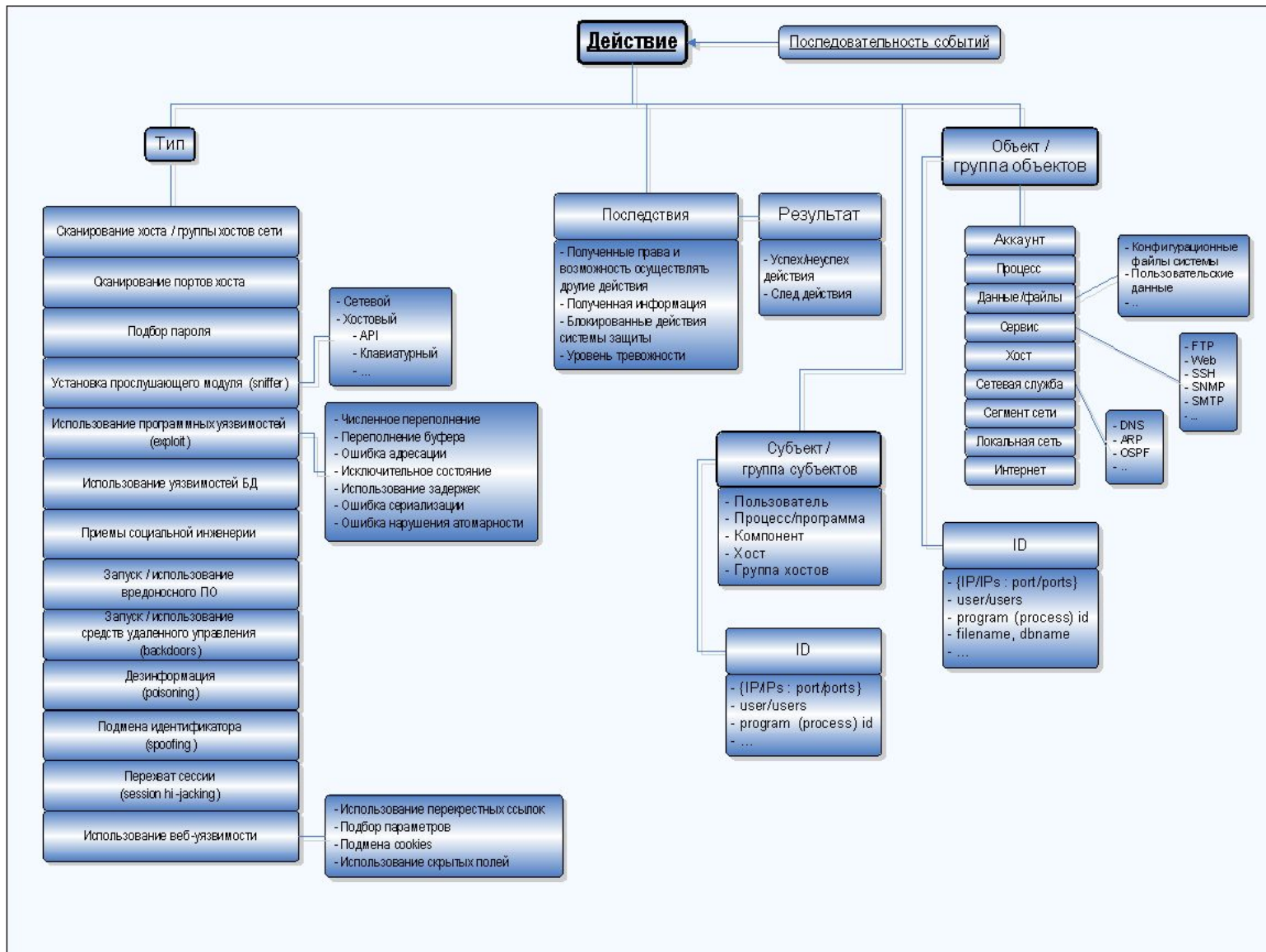
Атака



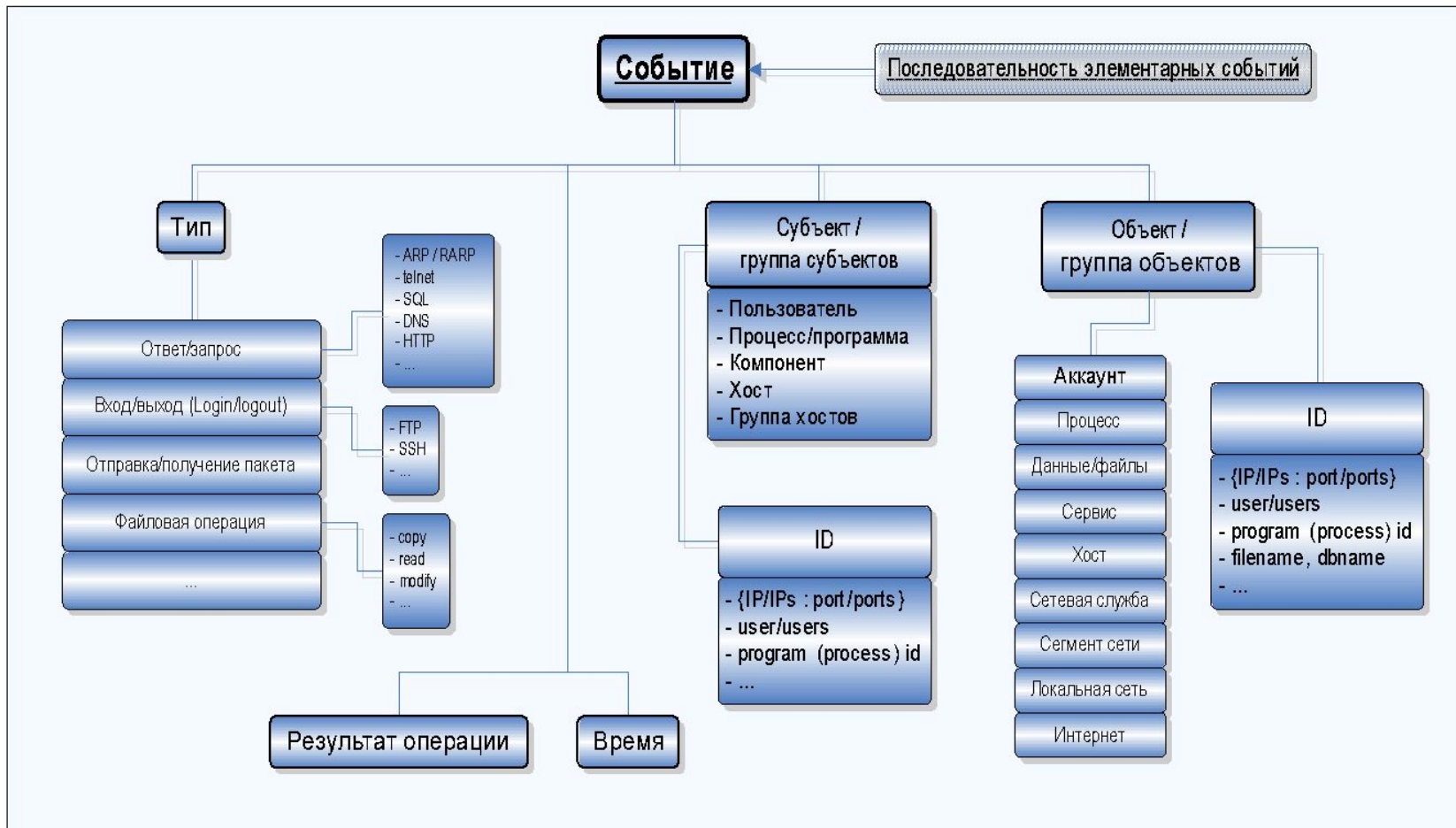
Этап



Действие



Событие



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!

