# Таксономия кибератак и ее применение к задаче формирования сценариев их проведения

А. А. Климовский

## Введение

Постоянно увеличивающееся число компьютерных атак [1] приводит к необходимости создания организованных (или самоорганизующихся) структур, деятельность которых направлена на обеспечение актуальной информацией о найденных киберуязвимостях, на оперативное их устранение, на создание систем обнаружения вторжений (систем активного аудита) и на ряд других мер [2]. По этой причине недостатка в информации относительно последних уязвимостей и компьютерных атак не наблюдается. Однако зачастую (особенно это касается атак) такая информация очень разнородна, неструктурированна и мало пригодна для дальнейшего анализа. Как следствие, возникает необходимость в разработке модели и инструментария, позволяющих упорядочить и систематизировать накопленные знания, — создания таксономии.

Кроме содержательного и систематического описания компьютерных атак на практике таксономия атак нужна для их дальнейшего анализа с целью аккумулирования знаний при оценке рисков и создания моделей нарушителя с тем, чтобы проектировать критически важные системы, в частности, для выработки политики безопасности, а также для создания средств активного аудита [3].

## 1. Постановка задачи

Прежде чем перейти непосредственно к постановке задачи, определим понятие атака (для этого воспользуемся определением, данным в работе [4]):

*Атака — последовательность действий, предпринимаемых кем-либо для достижения несанкционированного результата, т. е. действий, направленных на нарушение правил функционирования системы, установленных ее владельцем.*

Субъект, совершающий эти действия, в нотации настоящей работы будет называться *атакующим*, а система, на которую производится атака — *объектом атаки.*

С формальной точки зрения задача классификации атак состоит в том, чтобы создать систему их категорирования, а именно, — выделить критерии, отличительные черты каждой из них и задать классификационную схему, как способ отнесения атаки к той или иной категории. При таком подходе возникает нечеткость терминологии. С тем чтобы не возникало разночтения между понятиями классификация, классификационная схема и рядом других, в дальнейшем будем использовать один термин — таксономия. Слово таксономия имеет греческое происхождение: ταξινομια (taxinomia) происходит от греческого taxis — order (порядок) и nomos — law (закон) [5], [6]. Строгое современное определение, которое используется в данной работе, можно найти в [7]: «*Таксономия — классификационная схема, которая разделяет совокупность знаний и определяет взаимосвязь частей».* Примером таксономии является известная таксономия растений и животных, предложенная шведским натуралистом Карлом Линнеем (Carolus Linnaeus) [8].

В настоящей работе будут описаны другие, менее известные таксономии, относящиеся непосредственно к классификации компьютерных атак. Автором выбрано несколько наиболее представительных таксономий, на примере которых показано развитие идей и подходов к решению рассматриваемой задачи.

Перед тем как перейти к их описанию, рассмотрим подходы к разработке/формулировке критериев оценки эффективности таксономии. Для того чтобы таксономия была пригодна для решения описанных ранее основных задач, она должна удовлетворять некоторым естественным и разумным требованиям.

Списки таких требований были изложены во многих работах по классификации атак ([4], [9]–[16]), ниже приведен объединенный список, полученный на основе анализа этих работ. Эти требования не являются абсолютно четкими, и в полной мере удовлетворить всем им сложно. Как будет показано ниже, на практике таксономия в большей мере является некоторым компромиссом между ними. Тем не менее, такие требования помогают указывать на достоинства и недостатки рассматриваемых таксономий, и этот факт является основной причиной, по которой их объединенный перечень приведен в данной работе.

- Взаимное исключение ([4], [9]–[11], [13], [14]).

Таксономия должна быть устроена таким образом, чтобы выбор одной категории исключал все остальные. Иными словами, категории таксономии, как атрибуты/идентификаторы множеств, состоящих из относящихся к ним атак, не пересекаются. Это требование необходимо, чтобы имело смысл понятие «класс атаки».

- Полнота ([9]–[14]).

Таксономия покрывает собой все возможные атаки и позволяет их классифицировать.

Вполне естественное требование того, чтобы таксономия покрывала всю область компьютерных атак, а не лишь какую-то ее часть.

Объединяя два этих требования, можно сказать, что категории классификации должны образовывать разбиение множества атак.

- Детерминированность ([9], [10], [14], [15]).

Необходимым условием является тот факт, что сама процедура (или классификационная схема), с помощью которой можно классифицировать атаки, должна быть четко определена.

- Четкость терминов (terms well defined) ([9], [10], [16]).

Все термины, используемые в таксономии должны быть четко определены и пояснены с тем, чтобы не возникало непонимания или разночтения в понимании того или иного термина.

- Объективность (objectivity) ([9], [13], [15]).

В таксономии должны рассматриваться только те сведения об атаке, которые могут быть получены исходя из свойств объекта в результате беспристрастного наблюдения.

- Применимость (useful) ([4], [9–14]).

Таксономия должна представлять собой систему, которую можно использовать для получения информации об поле исследования. Например, исходя из класса атаки, можно получить конструктивную информацию о ней самой.

- Понятность (comprehensible) ([9], [13], [14]).

Таксономия должна быть доступна для понимания отдельных лиц, не являющихся экспертами в области информационной безопасности.

- Недвусмысленность (unambigious) ([4], [9], [11]–[14]).

Каждая категория должна быть определена настолько четко, чтобы была однозначность в отношении того, к какой из категорий данная атака должна быть отнесена.

- Согласованность (conforming) ([9], [10], [13], [14]).

Терминология, используемая в таксономии, должна быть согласованна с общепринятой терминологией в области информационной безопасности.

- Повторяемость результатов (repeatable) ([4], [9]–[13], [15]).

Это требование означает, что при классификации одного и того же объекта двумя разными лицами должен получаться один и тот же результат.

Однако, как можно заметить, некоторые требования из перечисленного перечня пересекаются по смыслу, некоторые являются следствием других.

По этой причине представляется разумным такие требования совместить или, соответственно, удалить. Более того, требования по смыслу можно разделить на две группы: основные требования, как требования непосредственно к смыслу и структуре вводимых категорий, и второстепенные, относящиеся скорее к форме изложения таксономии. После внесения описанных изменений список требований примет следующий вид.

Основные требования: взаимное исключение, полнота, применимость, детерминированность, объективность, расширяемость.

Дополнительные требования: четкость терминов, доступность/понятность, согласованность.

Отметим, что к основным требованиям добавлено еще одно, новое требование — расширяемость (или возможность расширения). Это требование того, чтобы строение таксономии, во-первых, допускало возможность добавления новых категорий, а, во-вторых, чтобы они органично в нее встраивались, а именно — для их внесения требовались бы минимальные изменения основного каркаса таксономии. По мнению автора, оно является немаловажным требованием к таксономии в силу того, что информационно-телекоммуникационная сфера развивается очень динамично, постоянно появляются новые технологии, и, как следствие, новые способы и технические средства проведения атак. По этой причине невозможно разработать таксономию (достаточно детальную), которая бы не требовала доработок и изменений с течением времени.

## 2. Анализ существующих работ и возможные подходы

Существует несколько подходов к проблеме классификации кибератак. Традиционно атаки делят на категории в зависимости от эффекта, который они производят: нарушение конфиденциальности информации, нарушение целостности информации и отказ в обслуживании (нарушение доступности информации) [11], [18]. Основным недостатком такого деления является его слабая информативность (и, как следствие, применимость), так как по информации о классе атаки мы практически ничего не можем сказать о ее особенностях. Однако, разумеется, эффект атаки является важным ее свойством и этот параметр в том или ином виде используется во многих таксономиях ([4], [10], [13]).

Другим подходом к классификации является классификация уязвимостей аппаратного и программного обеспечения информационно-вычислительных и телекоммуникационных систем. Одной из первых работ в этом направлении является работа Атанасио, Маркштейна и Филлипса [19]. Частично деление по типу уязвимости было использовано Ховардом и Лонг-

стаффом в [4]. Далее этот подход получил продолжение, и в работе [20] развита уже достаточно подробная классификация уязвимостей. Однако этот подход является слишком узким и зачастую не отражает в должной мере характер атаки, поэтому применяется в основном лишь для специальных классов задач (например, при тестировании программного обеспечения).

Одним из возможных вариантов является деление исходя из начального доступа, которым обладает атакующий. Самый известный пример подобного подхода — это матрица Андерсона [17]. В своей работе Джеймс Андерсон (James P. Anderson) предложил положить в основу классификации возможность, либо невозможность доступа атакующего к компьютеру или к его компоненту. Таким образом, категория, к которой принадлежит атака, зависит от того, какими начальными привилегии обладал атакующий. Таким образом, можно составить следующую матрицу 2 × 2:

| | 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 |

Из приведенной таблицы можно заметить, что все атаки разбиваются на три категории, так как случай, когда атакующий не имеет доступа к компьютеру (такой доступ ему не разрешен доступ к компьютеру), однако при этом ему разрешено использовать хранящееся на компьютере данные и запускать программы, невозможен. Категория B подразделяется Андерсоном еще на 3 подкатегории, в зависимости от атакующего. Таким образом, полный список категорий имеет следующий вид.

A. Внешнее вторжение.
B. Внутреннее вторжение.
   i. Ложный пользователь (masquerader).
   ii. Легальный пользователь (legitimate user).
   iii. Скрытый пользователь (clandestine user).
C. Злоупотребление полномочиями.

Отличие между ложным пользователем, легальным пользователем и скрытым пользователем состоит в том, что ложный пользователь маскируется под легального пользователя и, например, с точки зрения системы, неотличим от него. Тайный же пользователь действует так, чтобы остаться незамеченным механизмами обнаружения или каким-либо образом избегает их.

К примеру, если атакующий смог узнать пароль легального пользователя и воспользовался им для получения доступа, то он действовал как ложный пользователь. Если он подменил часть системных файлов для получения доступа, то он действовал как скрытый пользователь.

Прослеживая дальнейшее развитие подходов, можно заметить, что некоторые авторы в своих работах попытались не отталкиваться от каких-либо свойств и параметров атак, а составить общий список типов атак. Самая известная работа, представленная на этом направлении — это работа Ноймана и Паркера ([21]–[24]). Такие же в целом идеи были использованы Симоном Хансманом в работе [10], подробнее о которой будет изложено ниже. Бесспорным достоинством подхода, основанного на выделении списка типовых атак, является хорошее соответствие требованию применимости, так как в большинстве случаев тип атаки дает существенно больше информации нежели знание каких-либо ее свойств. Однако область применения такого подхода весьма ограничена в силу того, что при его использовании очень трудно удовлетворить первым двум очень немаловажным требованиям — полноте и взаимному исключению. В этой связи зачастую такие списки содержат сильно пересекающиеся категории атак, а вопрос об их полноте также остается открытым.

В работе Питера Ноймана и Дональда Паркера (Peter Neumann, Donald Parker) представлены 9 категорий техник вторжения (табл. 1). На их основе Нойман [22] разработал 26 типов атак, представленных в табл. 2.

В силу изложенных выше соображений наиболее перспективным является комбинированный подход, сочетающий себе в какой-то мере все вышеописанные методы. Примером такого подхода являются работы [4], [10], [13]. Однако следует заметить, что способы комбинирования могут быть различными.

**Таблица 1**

Категории техник вторжения

| | |
|---|---|
| 1 | Внешнее |
| 2 | Аппаратное |
| 3 | Маскировка |
| 4 | Вредоносные программы |
| 5 | Обход механизмов безопасности |
| 6 | Активное злоупотребление |
| 7 | Пассивное злоупотребление |
| 8 | Инертное злоупотребление (Inactive misuse) |
| 9 | Косвенное злоупотребление |

**Таблица 2**

Типы атак

| | |
|---|---|
| *Внешнее* | |
| Визуальное наблюдение | Наблюдение за клавиатурой или монитором |
| Обман | Обман операторов и пользователей |
| Извлечение мусора | Извлечение информации из виртуальных корзин |
| *Аппаратное* (hardware) | |
| Логическое восстановление | Извлечение информации с выброшенных или украденных носителей |
| Прослушивание | Перехват данных |
| Вмешательство | |
| Физическая атака | Разрушение или повреждение оборудования, источников питания |
| Физическое удаление | Изъятие оборудования и хранилищ данных |
| *Маскировка* | |
| Имитирование | Использование ложных идентификаторов |
| Узурпирование линий связи или хостов | |
| Атаки с подменой параметров | |
| Спутывание сетей | Маскировка физического месторасположения или маршрута |
| *Вредоносные программы* | *Создание возможности дальнейших злонамеренных действий* |
| Троянские кони | Внедрение вредоносного кода |
| Логические бомбы (Logic bombs) | Разновидность троянских коней |
| Черви | Овладение распределенными ресурсами |
| Вирусы | Прикрепление к программам и размножение |
| *Обход* | Обход механизмов безопасности |
| Эксплуатация уязвимостей | |
| Взлом паролей | |
| *Активное злоупотребление* | |
| Основной | |
| Инкрементальные атаки | Постепенная эскалация привилегий, медленное продвижение к цели |
| Отказ в обслуживании | Совершение массивных атак |
| *Пассивное злоупотребление* | |
| Обзор | Случайный или выборочный поиск |
| Сбор и вывод данных | Использование баз данных и анализ трафика |
| Скрытые каналы | Использование скрытых каналов или другие способы утечки информации |
| *Инертное злоупотребление* | |
| *Косвенное злоупотребление* | |

Первый способ состоит в том, чтобы разнести отдельно все анализируемые параметры и считать их независимыми. Такой подход был реализован в работа Хансмана, где автор использует так называемую концепцию «измерений», основная идея которой состоит в том, что свойства атаки расслаиваются на несколько независимых измерений, в каждом из которых есть свой список (или дерево) категорий.

В своей работе Симоном Хансманом (Simon Hansman, [10]) предложена таксономия сетевых и компьютерных атак, в основе которой лежит способ разделения параметров атаки на несколько измерений. Автором предложено четыре основных измерения и несколько вспомогательных.

- Первое измерение — это список типов атак (например, отказ в обслуживании).
- Второе измерение — это цель (целевой объект) атаки. Если у атаки несколько объектов нападения, то в этом измерении должно присутствовать несколько записей.
- Третье измерение — это уязвимости, используемые в процессе атаки. По словам автора, это измерение обычно содержит CVE-описания уязвимостей (Common Vulnerabilities an Exposures), причем если используется несколько уязвимостей, то в этом измерении присутствует несколько записей.
- Четвертое измерение — это, фактически, результат или цель атаки.

Опишем все эти измерения более подробно.

### Первое измерение

**Таблица 3**

| | | |
|---|---|---|
| Вирусы: | Инфицирующие файлы | |
| | Инфицирующие системные/загрузочные сектора | |
| | Макровирусы | |
| | | |
| Черви: | Использующие массовую рассылку | |
| | Распознающие состояние сети | |
| | | |
| Троянские программы: | Логические бомбы | |
| | | |
| Переполнение буфера: | Переполнение стека | |
| | Переполнение кучи | |

Окончание таблицы 3

| | | |
|---|---|---|
| Отказ в обслуживании: | Локальный (host based): | Исчерпание ресурсов |
| | | Вывод из строя |
| | Сетевой (network based): | TCP-флуд |
| | | UDP-флуд |
| | | ICMP-флуд |
| | Распределенные | |
| | | |
| Сетевые атаки: | Подмена пакетов | |
| | Перехват сессии | |
| | Беспроводные атаки: | Взлом криптоалгоритмов беспроводных сетей |
| | Атаки на веб-приложения: | Использование злоумышленных web-сценариев (Cross Site Scripting) |
| | | Подбор параметров |
| | | Использование некорректных cookies |
| | | Атаки на базы данных |
| | | Использование скрытых полей |
| | | |
| Физические атаки: | Простые | |
| | Энергетическое оружие: | HERF |
| | | LERF |
| | | EMP |
| | Van Eck | |
| | | |
| Атаки на пароли | Угадывание: | Атака методом грубой силы |
| | | Атака по словарю |
| | Использующие уязвимость в реализации | |
| | | |
| Атаки —сбор информации | Прослушивание | Прослушивание пакетов |
| | Выявление структуры сети | |
| | Сканирование | |

### Второе измерение

**Таблица 4**

| | | | | | |
|---|---|---|---|---|---|
| Аппаратное обеспечение: | Компьютер: | Жесткие диски | | | |
| | | ... | | | |
| | Сетевое оборудование: | Хаб | | | |
| | | Кабель | | | |
| | | ... | | | |
| | Периферийные устройства: | Монитор | | | |
| | | Клавиатура | | | |
| | | ... | | | |
| Программное обеспечение: | Операционная система: | Семейство Windows: | Windows XP | | |
| | | | Windows 2003 Server | | |
| | | | ... | | |
| | | Семейство Unix: | Linux: | 2,2 | |
| | | | | 2,4 | |
| | | | | ... | |
| | | | FreeBSD: | 4,8 | |
| | | | | 5,1 | |
| | | | | ... | |
| | | | ... | | |
| | | Семейство MacOS: | MacOS X: | 10,1 | |
| | | | | 10,2 | |
| | | | | ... | |
| | | | ... | | |
| | | ... | | | |
| | Приложение: | Серверное приложение: | База данных | | |
| | | | Почтовый сервер: | | |

Окончание таблицы 4

| | | | | | |
|---|---|---|---|---|---|
| | | | Веб-сервер: | IIS: | 4,0 |
| | | | | | 5,0 |
| | | | ... | | |
| | | Пользовательское приложение | Текстовый редактор: | MS Word | 2000 |
| | | | | | XP |
| | | | | | ... |
| | | | Почтовый клиент: | ... | |
| | | | ... | | |
| | | ... | | | |
| Сеть: | Протокол: | Транспортный уровень: | IP | | |
| | | | ... | | |
| | | Сетевой уровень: | TCP | | |
| | | | ... | | |
| | | ... | | | |

**Третье измерение**

Как уже было отмечено выше, третье измерение содержит в себе стандартные описания уязвимостей, используемых в атаке. В этой связи для него необходимость описания какой-либо общей схемы как для первых двух отпадает.

**Четвертое измерение**

Четвертое измерение служит для классификации атак, осуществляемых не только для достижения своей главной цели. Например, червь помимо своего прямого назначения — заражения компьютера, может служить для удаленного управления или уничтожения каких-то файлов. Четвертое измерение состоит из пяти категорий:

- непосредственная (номинальная) цель атаки;
- нарушение целостности информации;
- нарушение конфиденциальности информации;
- захват ресурсов;
- получение контроля над частью системы для дальнейшего использования.

**Другие измерения**

Другие измерения, как пишет Хансман, могут быть добавлены для улучшения и развития таксономии. В качестве вариантов дальнейшей детализации предлагаются следующие категории:

- ущерб, который описывает ущерб, нанесенный атакой;
- стоимость восстановления, которая описывает общую стоимость восстановления системы после атаки до первоначального состояния;
- распространение, которое описывает скорость и способ распространения атаки. Эта категория подходит больше всего для размножающихся атак наподобие вирусов и червей;
- способы защиты.

Второй способ основан на той же идее, однако является более гибким, так как подразумевает древовидную структуру категориальных классов с самого высокого уровня. Реализацию этого подхода можно найти в [13].

В своей работе Джеффри Андеркоффер и Джон Пинкстон (Jeffrey Undercoffer, John Pinkston) придерживаются структурного подхода к классификации. В графическом представлении (рис. 1) разработанная ими таксономия представляет собой дерево, корнем которого является вторжение. Ребра этого дерева имеют метки несущие смысловую нагрузку: например, из корня дерева выходят два ребра, означающие «осуществлено с помощью» и «имело результат». Несплошная стрелка выражает отношение «является подклассом» между вершинами, которые она соединяет и, для того чтобы излишне не нагружать рисунок, эта надпись опущена. Можно заметить, что применение таких способов хотя и дает более детальное описание атаки, однако не может отразить некоторые ее структурные особенности, сценарий атаки. Отмеченное обстоятельство является существенными недостатком, учитывая постоянное совершенствование современных систем защиты и, как следствие, тенденции к все более сложным и изощренными методам атак ([25]–[27]).

Третий способ — это комбинирование свойств с внесением структуры. Такой подход был применен в работе [4]. Основная его идея состоит в том, что вводится иерархия понятий: основным в данной работе считается понятие инцидент, в него включается понятие атака, а в понятие атака включается понятие действие. При этом инцидент может состоять из нескольких атак, а каждая атака из нескольких действий.

Джон Ховард и Томас Лонгстафф (John D. Howard, Thomas A. Longstaff) не только создали таксономию, но и разработали «Общий язык для инцидентов в области компьютерной безопасности». Как сказано во вступлении к [4], «Этот общий язык не является попыткой создания всеобъемлющего словаря терминов в области компьютерной безопасности. Вместо этого мы создали минимальный набор высокоуровневых терминов, вместе со структурой, отражающей их взаимосвязь (таксономией)».

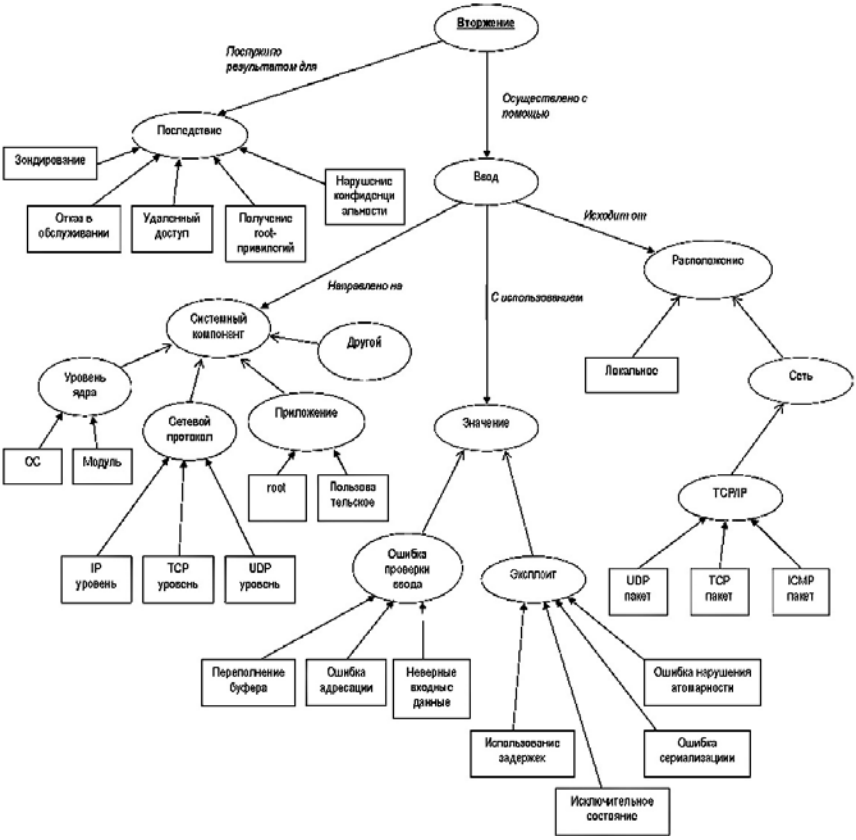


**Рис. 1.** Вторжение

Таксономия, разработанная этими авторами, представляет собой следующую диаграмму (рис. 2). Основным понятием в данной таксономии является понятие «инцидент», так как авторы разделяют два понятия — инцидент и атака. В понятие инцидент входит атакующий, атака и цель атаки. Под атакой понимаются те сущности, которые относятся непосредственно к процессу совершения атаки: инструмент, уязвимость, действие, целевой объект и несанкционированный результат. Инструмент — это средство, которое использовал атакующий при нападении. Совокупность действия и целевого объекта называется событием.

Предложенная авторами таксономия отличается от описанных выше тем, что в ней присутствуют структурные элементы: инцидент, атака, событие и заложена возможность комбинирования этих событий. Так в одном

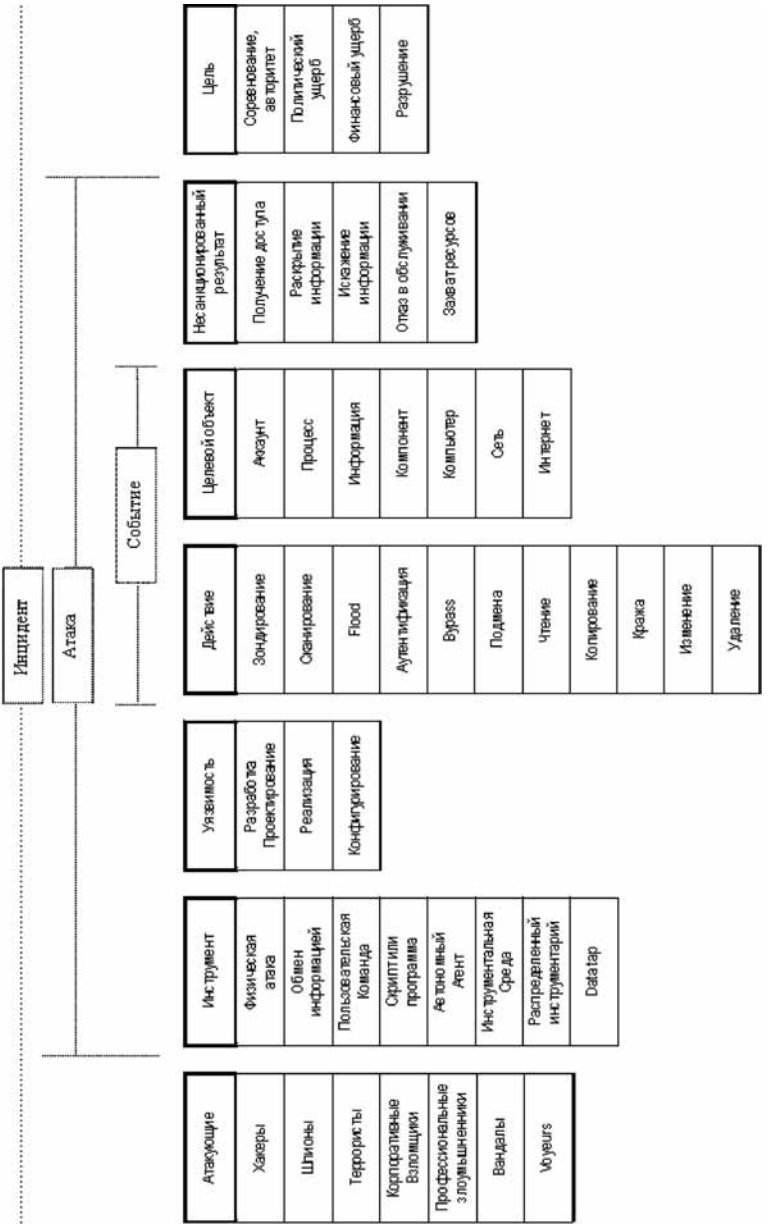


**Рис. 2.** Инцидент

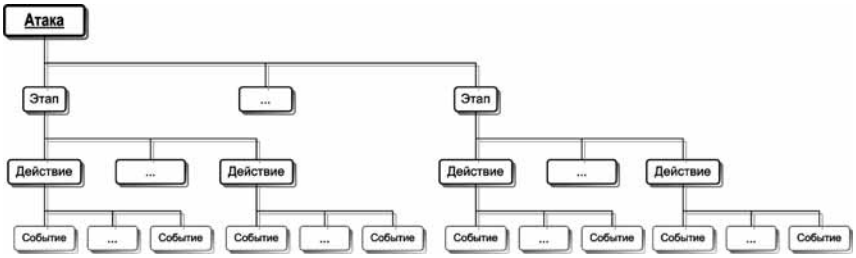


**Рис. 3.** Общая структура атаки

инциденте может быть вложена последовательность атак. Данное свойство в какой-то мере позволяет описывать неатомарные (многоходовые) составные атаки и учитывать их сценарий.

## 3. Предлагаемая таксономия

В предлагаемой автором таксономии развивается комбинированный подход к решению задачи классификации. Однако в отличие от предыдущих работ вводится иерархическая структура отношений с древовидным раскрытием категорий. Как самостоятельный отдельный объект вводится важное понятие «этап атаки», что позволяет, в отличие от предыдущий подходов, довольно естественным образом описывать многоэтапные атаки. На рис. 3 приведена общая схема атаки. Атака может состоять из нескольких этапов, этап, в свою очередь, из нескольких действий, действие — из нескольких событий. К примеру, взлом через pro-ftpd ([28], [29]) может являться частью одного из этапов атаки и состоит из четырех событий, которые могут совершаться в различном порядке.

Кроме вложенности в понятие более высокого уровня, каждое из этих четырех понятий раскрывается с помощью дерева подкатегорий, т. е. имеет свой собственный набор атрибутов.

### 3.1. *Атака*

Понятием самого верхнего уровня является *атака*. Это понятие имеет такие атрибуты, как глобальная цель/результат, свойства атаки, объект атаки и атакующий. Каждый из перечисленных атрибутов тоже имеет свои атрибуты и является поддеревом дерева атрибутов атаки. Важно отметить, что цель разделяется на две компоненты: информационную составляющую и социально значимую составляющую. Информационная составляющая отражает информационный аспект последствий

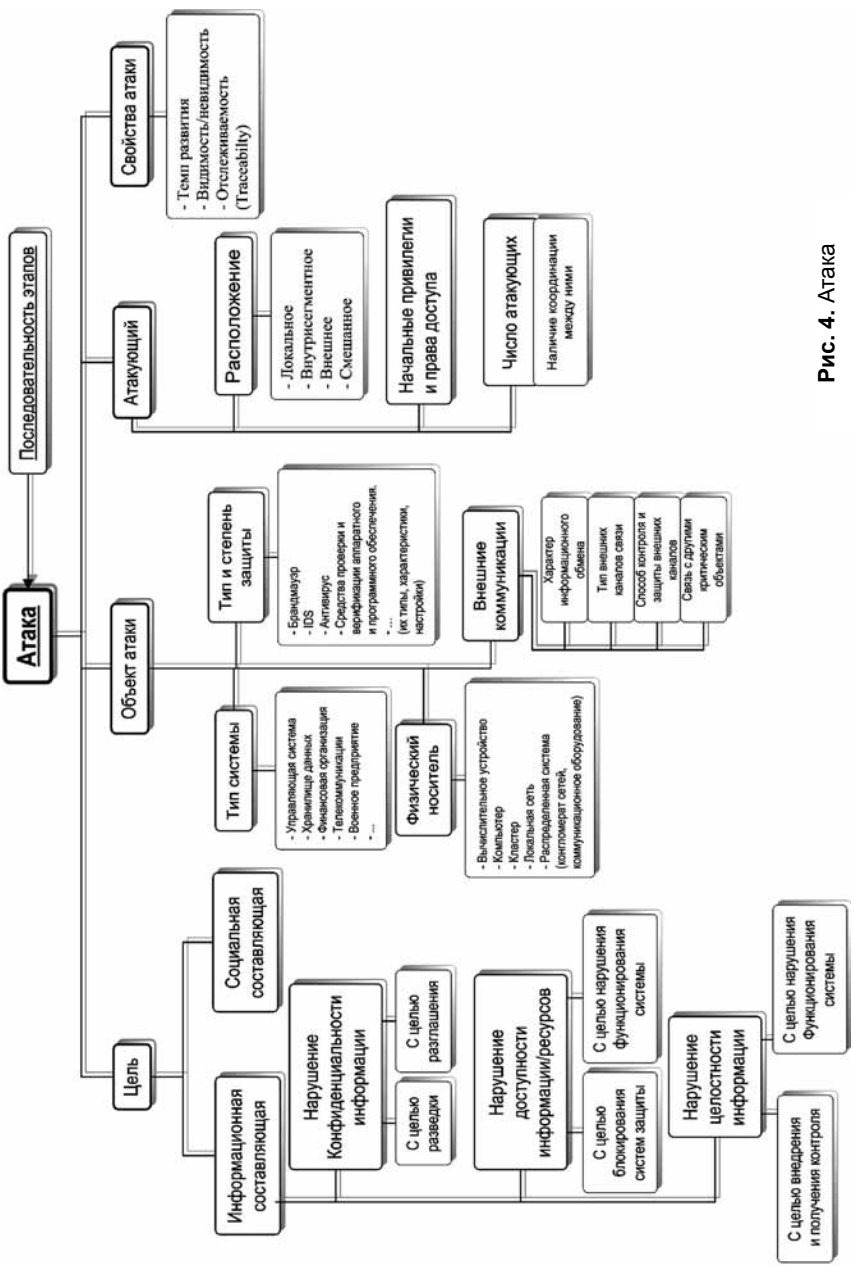
Атака
Последовательность этапов
Цель
Информационная составляющая
Социальная составляющая
Нарушение Конфиденциальности информации
С целью разглашения
С целью разведки
Нарушение доступности информации/ресурсов
С целью нарушения функционирования системы
С целью блокирования систем защиты
Нарушение целостности информации
С целью нарушения функционирования системы
С целью внедрения и получения контроля
Объект атаки
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 критическими объектами
Атакующий
Расположение
- Локальное
- Внутрисегментное
- Внешнее
- Смешанное
Начальные привилегии и права доступа
Число атакующих
Наличие координации между ними
Свойства атаки
- Темп развития
- Видимость/невидимость
- Отслеживаемость (Traceability)

**Рис. 4.** Атака

воздействия атаки на систему: нарушение конфиденциальности информации (которая подразделяется на нарушения конфиденциальности с целью разведки либо с целью разглашения), нарушение доступности информации/ресурсов системы (которая подразделяется на нарушения с целью блокирования системы защиты либо с целью нарушения функционирования самой системы) и нарушение целостности информации (с целью внедрения и получения контроля). Социально значимая составляющая, в отличие от информационной, отражает внеинформационные аспекты последствия атаки. Проиллюстрируем такие последствия на примере захвата компьютеров информационно-вычислительной среды атомной электростанции и проведение теракта с целью создания техногенной катастрофы путем выведения из строя реактора. В данном случае, информационной составляющей цели является захват компьютеров, а социально значимой — создание чрезвычайной ситуации посредством выведения из строя реактора.

Другим важным атрибутом является объект атаки, так как атаки на объекты разной функциональности и категорийности имеют, как правило, разный характер. Здесь выделяются такие свойства объекта атаки, как тип атакуемой системы, ее физический носитель (оборудование, которое формирует информационно-вычислительную среду системы), тип средств защиты, используемых в системе и степень защищенности (уровень жесткости правил безопасности) и внешние коммуникации системы.

Еще одним атрибутом атаки является атакующий. Основными свойствами, которые его характеризуют, являются расположение относительно системы, начальные привилегии и права доступа. Если атакующих несколько, то в этом случае возникает враждебная многоагентная система [30], [31], [35], поэтому становится крайне важным их число, наличие и характер координации между атакующими.

Из перечисленных свойств, пожалуй, наибольшее значение имеет расположение атакующего относительно объекта атаки. Атакующий может осуществлять атаку с того же компьютера, на котором находится информация, которая является его целью. Примером локальной атаки может быть повышение привилегий с помощью переполнения буфера в одной из программ, исполняющих часть операций в привилегированном режиме, и получения доступа к данным. Пример внутрисегментной атаки — это атака, когда атакующий начинает атаку с компьютера находящегося в одном сегменте сети, что позволяет ему использовать эксплоиты для сервисов, порты которых фильтруются извне межсетевым экраном и таким образом захватить компьютер-жертву. Внешняя атака — это атака, проводимая атакующим удаленно, например, атака суперкомпьютерного центра Сан-Диего, описанная в [32]. Очень хорошо и подробно методы реализации данного типа атак описаны и разобраны в [33]. Кроме отмеченных выше существует

и смешанный тип атак, которые обычно проводятся согласованно группой атакующих. Примером может служить атака, описанная в [35], проводимая двумя пользователями с помощью образования скрытого канала. Суть состоит в том, что один пользователь находится внутри сегмента сети и каким-либо образом получает доступ к необходимой информации и передает ее другому пользователю вовне с помощью скрытого канала. Атаку может проводить несколько атакующих из разных мест, в этом случае атака называется распределенной по атакующим (о чем говорит параметр «число атакующих»), простейший пример — DDoS-атака. Более подробную информацию о возможных типах таких атак можно найти в [36].

Последним атрибутом, представленным на диаграмме (рис. 4), является атрибут «свойства атаки». Для уменьшения риска быть обнаруженной атаки иногда длятся по нескольку месяцев, а других случаях, несколько секунд (чтобы, например, исключить возможность вмешательства администратора атакуемой системы). В силу этих обстоятельств темп развития атаки представляет собой немаловажное для классификации свойство атаки. Другие два свойства (упомянутые в [34]) — видимость и возможность проследить источник атаки. Видимость означает, что сценарий атаки разработан так, что предполагается, что во время проведения атака не будет обнаружена средствами обнаружения. Отслеживаемость означает, что после проведения атаки при проведении расследования существует возможность проследить источник атаки. Следует отметить, что эти два свойства сильно связаны друг с другом. Значение каждого из них зависит, в первую очередь, от поставленной злоумышленником цели, и они сильно влияют на выбор стратегии, используемой при атаке. Например, если задача злоумышленника незаметно проникнуть в систему и выкрасть конфиденциальную информацию, то при выборе стратегии он может вполне использовать сценарии, которые невидимы, однако прослеживаемы (к примеру, редактирование или стирание лог-файлов делает атаку существенно более заметной, но менее прослеживаемой).

### 3.2. *Этап*

Атака состоит из этапов, которые, в свою очередь, тоже имеют свои атрибуты. Понятие этап отражает (см. рис. 5) отдельную часть атаки, имеющую свою локальную цель. Приведем пример: одним из этапов атаки может быть этап-разведка — сканирование подсетей какой-нибудь атакуемой организации. Цель этого этапа — по возможности незаметно, не вызывая подозрений исследовать топологию и внутреннее устройство сетевого сегмента объекта атаки для нахождения слабых мест системы защиты и последующего вторжения. Для достижения этой цели существует значительное количество различных и довольно нетривиальных способов, подробнее о которых изложено в [33].

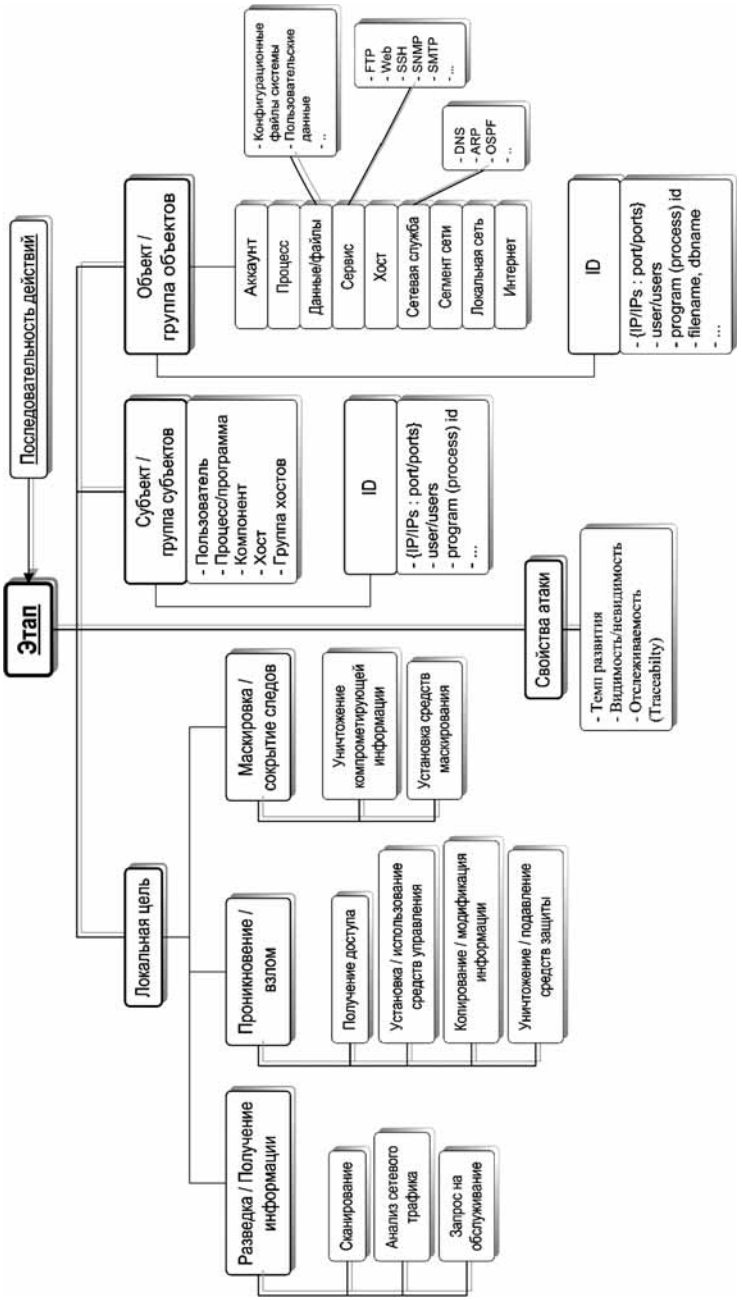
Этап
Последовательность действий
Субъект / группа субъектов
- Пользователь
- Процесс/программа
- Компонент
- Хост
- Группа хостов
ID
- {IP/IPs : port/ports}
- user/users
- program (process) id
- ...
Объект / группа объектов
Аккаунт
Процесс
Данные/файлы
Сервис
Хост
Сетевая служба
Сегмент сети
Локальная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

**Рис. 5.** Этап

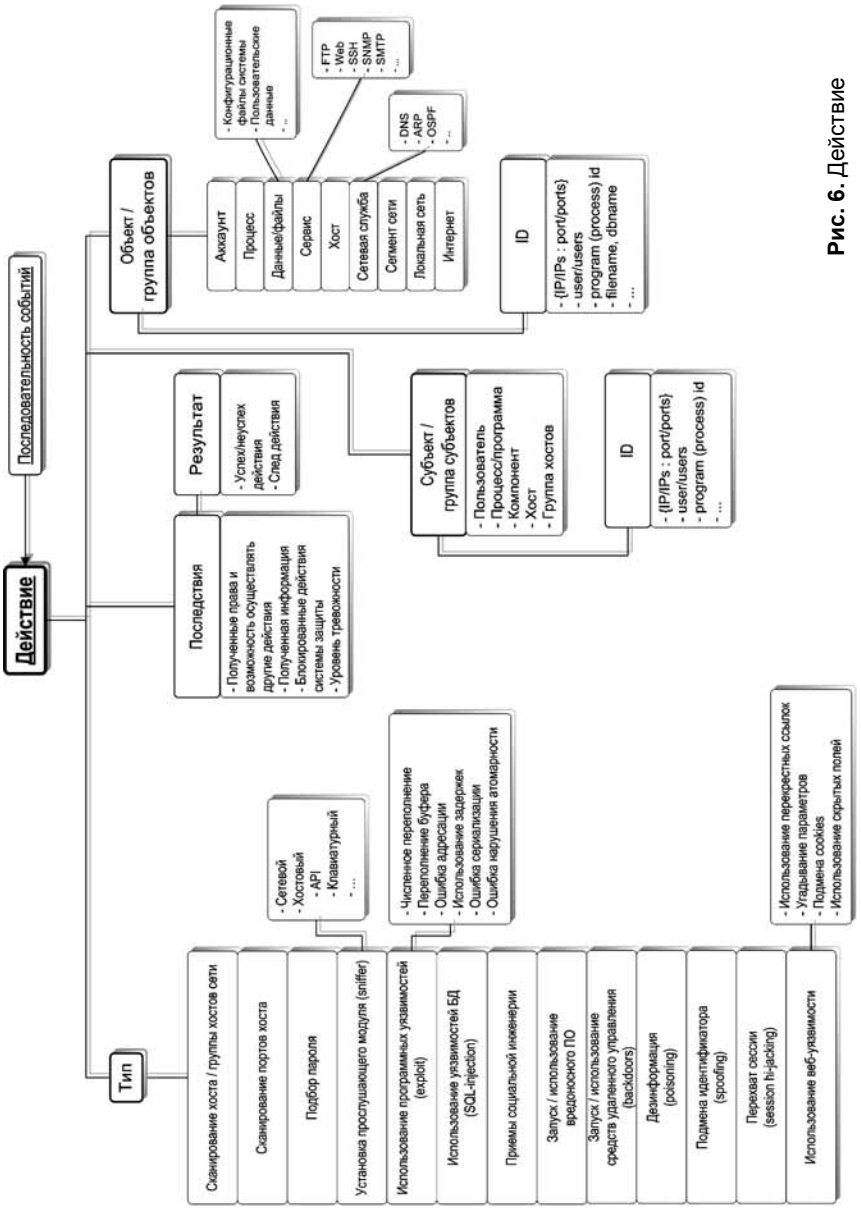


**Рис. 6.** Действие

### 3.3. *Действие*

Этап состоит из действий. Действие представляет собой, в некотором смысле, «атомарную» атаку (например, сканирование портов или использование программных уязвимостей). Действие тоже обладает атрибутами: тип действия, субъект, объект, последствия действия, результат. Фактически, оно является минимальными смысловым шагом атаки.

Рассмотрим атрибуты этого понятия (рис. 6). Атрибут «тип действия» описывает непосредственно само действие, происходящее на данном этапе атаки. Этот атрибут является наиболее важным и информативным. В некотором смысле, список возможных действий похож на перечень типовых атак ([4], [22], [24]). По этой причине ему тоже свойственно отсутствие полноты и, возможно, при применении таксономии на практике, представленный на рисунке список потребует расширения (в зависимости от специфики области применения). «Объект/группа объектов» — это то (программа, компьютер или сеть), на что данное действие направлено. «Субъект/группа субъектов» — это то, что производит данное действие. К примеру, если при взломе сети атакующему удалось захватить один из хостов сети (хост А), и дальше он производит сканирование портов другого хоста (назовем его В) от имени захваченного компьютера, то субъектом действия будет хост А, а объектом — хост В. Параметр «последствия» характеризует последствия действия, а именно, полученные атакующим права и привилегии в объекте атаки, информацию, к которой он получил доступ в результате этого действия и т. п. Этот параметр содержит также информацию об уровне тревожности данного действия (безусловно, уровень тревожности является весьма субъективной величиной и сильно зависит от предыстории и от окружения, в котором происходит действие, поэтому здесь имеется в виду некоторая априорная шкала оценок тревожности).

### 3.4. *Событие*

Заметим, что с точки зрения системы действие далеко не атомарно. Сканирование портов, например, это цепочка действий, которая может сильно варьироваться (например, [37], [38]). По этой причине, если настолько детально рассматривать атаку, то необходимо ввести еще один, самый нижний уровень абстракции — уровень событий (рис. 7).

Событием назовем минимальный (на заданном уровне детализации) шаг с точки зрения системы. Однако, вообще говоря, событие не входит в таксономию, так как в большинстве случаев это лишь усложняет понимание и увеличивает объем, однако не несет в себе какой-либо полезной информации. По этой причине вводить этот уровень рекомендуется лишь тогда, когда необходимо детальное описание (модель атаки), например, в случае дальнейшего формального анализа автоматизированными средствами.

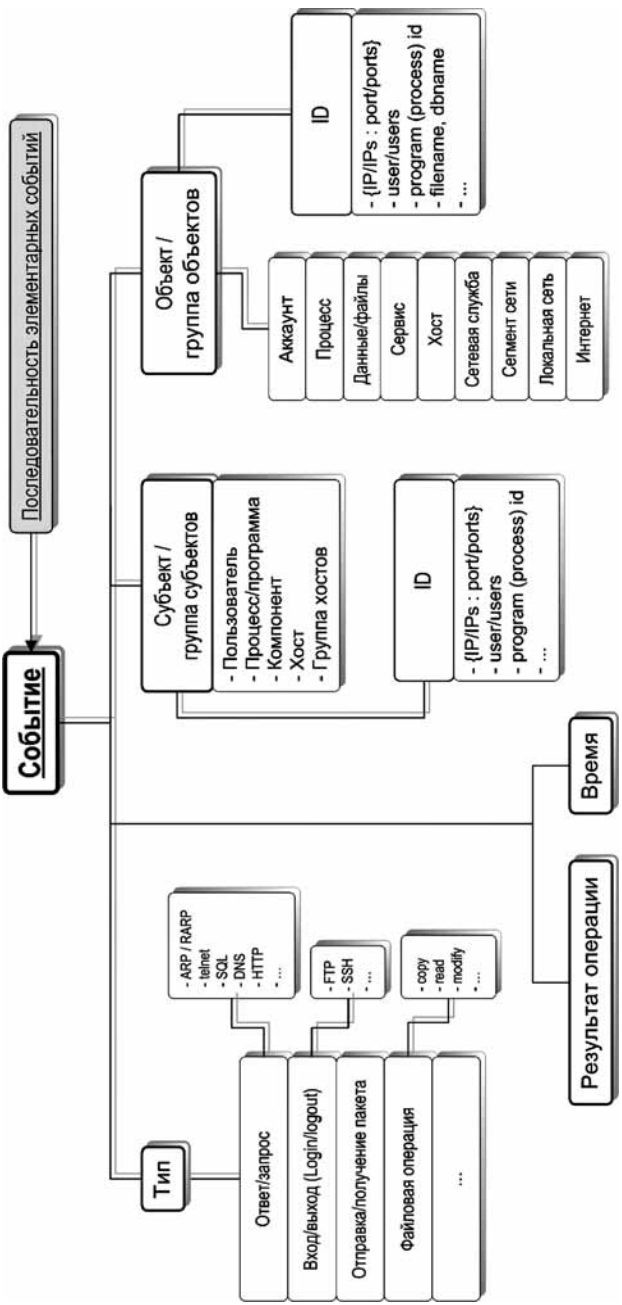


**Рис. 7.** Событие

# 4. Применение таксономии для моделирования многоэтапной распределенной кибертеррористической атаки на различных уровнях абстракции

В данной части работы будет предложен модельный пример информационной системы для управления критически важным объектом. Под критически важным объектом (КВО) будем понимать объект, частичная деградация или полное разрушение которого способно повлиять на национальную безопасность государства [39]. В контексте данной работы будем рассматривать только информационные аспекты функционирования КВО. Компоненты КВО, обеспечивающие такие аспекты будем называть критически важным информационным объектом (КВОИ). В разработанный пример включены параметры, отражающие основные аспекты устройства и архитектуры критически важных систем, имеющие значение при анализе защищенности таких объектов и рассмотрении возможных атак на КВОИ.

Далее будет показан способ описания с помощью построенной таксономии [41] атаки на рассматриваемый КВОИ. Для демонстрации изложенных выше описательных возможностей таксономии, в качестве примера выбран один из наиболее трудных для классификации типов атак, объединяющий многоэтапные распределенные кибератаки.

## 4.1. *Описание атакуемой системы (КВОИ)*

Рассмотрим схематичное описание модельного КВОИ, представленное на рис. 8.

Вся связь КВОИ с внешним миром осуществляется через внешний сервер. Почтовый и файловый сервер поддерживают работу информационной среды системы, главный сервер осуществляет контроль всей группы серверов. Серверы 1, 2, 3, 4 представляют собой сервера сегментов сети КВОИ (например, обслуживающие определенные отделы организации), троеточием обозначены рабочие станции соответствующего отдела. Прямоугольником обозначен атакующий, овалом — объект атаки. Цель атакующего нарушить функционирование третьего отдела КВОИ и получить доступ к секретной информации этого отдела.

## 4.2. *Подход к моделированию*

Для построения модели атак предлагается следующий подход [40]. На первом шаге необходимо построить модель системы в виде набора утверждений, фактически описывающих состояние и конфигурацию системы.

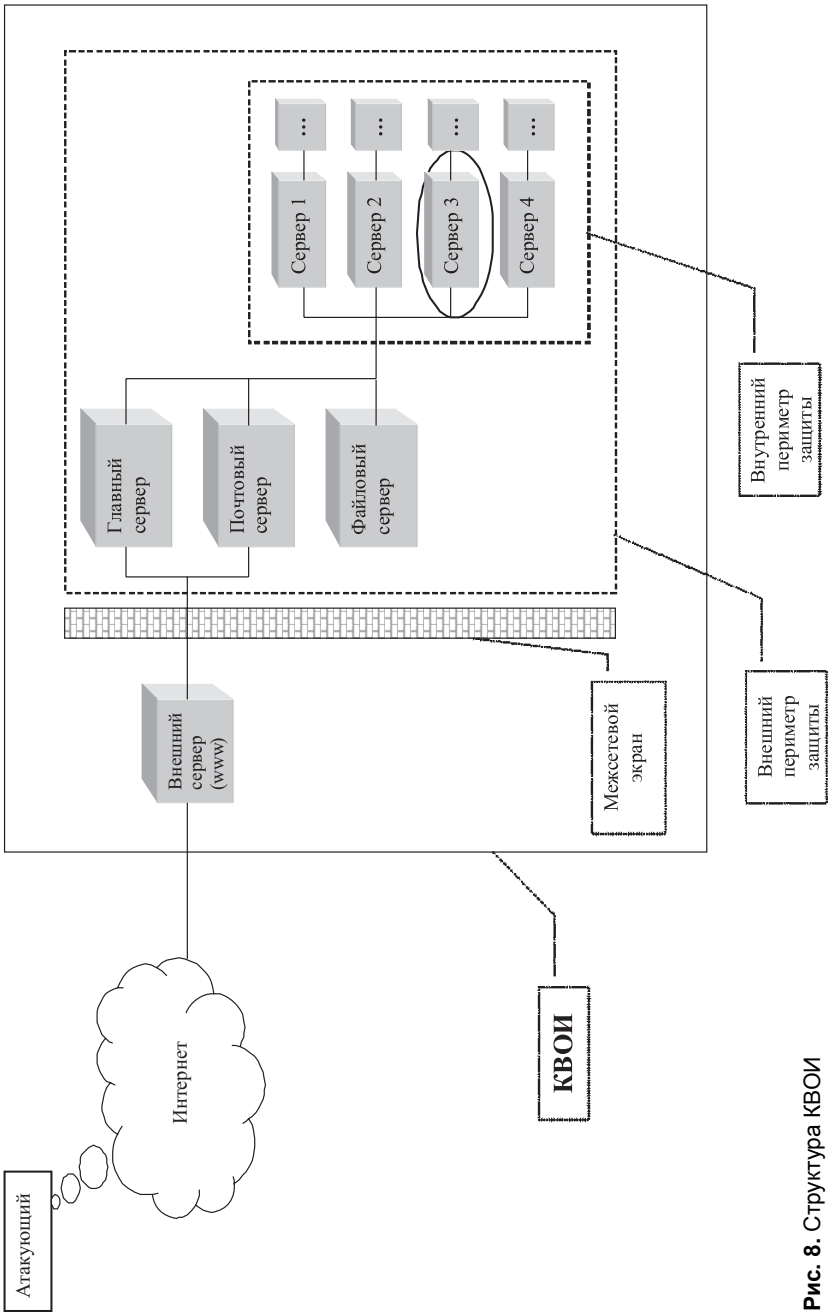


**Рис. 8.** Структура КВОИ

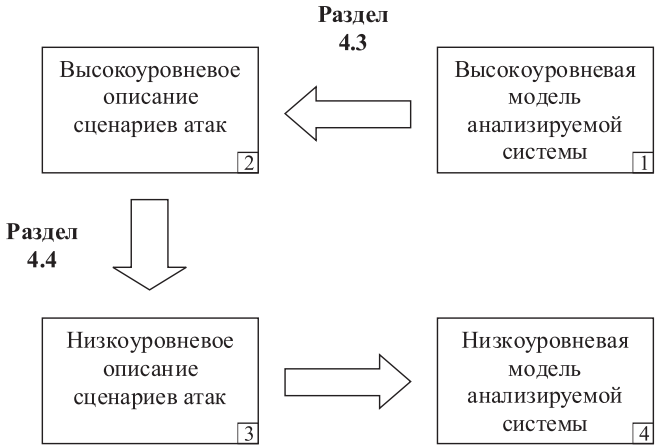


**Рис. 9.** Методика моделирования

Также необходимо идентифицировать свойства переходов в системе из одного состояния в другое (более подробно это будет изложено ниже).

На втором шаге определяется цель, которой атакующий хочет добиться при проведении атаки. Далее с помощью механизмов логического вывода на основании модели системы и построенных правил преобразования необходимо получить все возможные сценария развития атаки (последовательности действий), приводящих атакующего к поставленной цели. Таким образом получается описание сценария атаки на верхнем уровне (см. рис. 9).

На последнем шаге проводится трансляция высокоуровнего описания в низкоуровневое. Фактически происходит более детальное раскрытие каждого действия в той степени, в которой это необходимо в решаемой задаче для дальнейшего применения. Например, для задач имитационного моделирования необходимо свести высокоуровневые действия до степени детализации, в которой происходят события в используемой среде моделирования. Трансляция происходит с помощью библиотеки шаблонов действий, которая строится в зависимости от конкретной области применения.

### 4.3. *Получение сценария атаки на «верхнем» уровне* (1–2)

Как уже было написано, для получения сценария атаки на «верхнем» уровне необходимо построить высокоуровневую модель системы. С этой целью составим набор фактов для системы логического вывода вида:

- СуществуетХост(адрес)
- СуществуетСоединение(хост, хост)
- ЗапущенСервис(Хост, Порт, Сервис(имя_сервиса, версия, параметры))
- СуществуетУязвимость(сервис, уязвимость(характеристики уязвимости))
- РазрешеноСоединение(…)
- МонтированыДиректории(…)
- ЗапущенПроцесс(…)
- ИмеетДоступ(объект, субъект)
- ИмеетИнформациюО(объект, субъект)
- …

Выделим набор действий следующего вида:

- ИмеетИнформациюО(атакующий, объект = внешний сервер) & ИмеетИнформациюО(атакующий, уязвимость) & СуществуетХост(адрес) & СуществуетУязвимость(уязвимость) → ИмеетДоступ(атакующий, внешний сервер, привилегии(…))
- ИмеетДоступ(атакующий, главный сервер, привилегии = root) → ЗапущенПроцесс(описание процесса)
- …

Далее, задав начальные условия для данной системы, мы можем получить сценарии возможных атак.

Ниже приведен пример одного из таких сценариев. Отметим, что данный сценарий был получен «вручную», однако очевидно, что при подборе надлежащего набора действий и соответствующего начального состояния системы получить такой сценарий автоматически не представляет труда. Для лучшего восприятия приведено описание не в виде сплошной последовательности, а адаптированное с помощью предложенной таксономии структурное описание в виде последовательности этапов.

1. Получение информации о внешнем сервере.
   1.1. Сканирование портов.
   1.2. Поиск уязвимых сценариев сервера.
2. Взлом внешнего сервера.
   2.1. Использование найденной веб-уязвимости и получение непривилегированного доступа.
   2.2. Использование shell-кода.
   2.3. Использование эксплойта и получение root-привилегий.
3. Маскировка и закрепление на внешнем сервере.
   3.1. Создание suid-shell.
   3.2. Маскировка средств удаленного управления (backdoor).

3.3. Маскировка suid-shell.
3.4. Сокрытие следов, редактирование лог-файлов ОС.

4. Получение информации о главном сервере.
   4.1. Просмотр системных лог-файлов и файлов истории набранных команд.
   4.2. Сканирование портов главного сервера.
5. Взлом главного сервера.
   5.1. Использование эксплойта mysqld и получение непривилегированного доступа.
   5.2. Получение пароля MySQL.
   5.3. Получение root привилегий (совпадение паролей).
6. Закрепление и дальнейшее продвижение в системе.
   6.1. Установка слушающего модуля (keylogger).
7. Выход из системы.
   7.1. Logout.
   7.2. Закрытие соединений.
   7.3. Деактивация средств удаленного управления.
8. Вход в систему (через некоторое время).
   8.1. Активация соединения средств удаленного управления.
   8.2. Запуск suid-shell.
   8.3. Логин к главному серверу.
   8.4. Просмотр лог-файлов слушающего модуля и получение root паролей к почтовому и файловому серверу.
9. Взлом файлового сервера.
   9.1. Логин к файловому серверу.
10. Получение информации о сервере 3.
    10.1. Просмотр почтовой информации.
11. Дальнейшее продвижение.
    11.1. Модификация бинарных файлов.
    11.2. Установка агента для связи с троянской программой на главном сервере.
    11.3. Установка агента для удаленного управления на внешнем сервере.
12. Выход из системы.
    12.1. Logout.
    12.2. Закрытие соединений.
    12.3. Деактивация средств удаленного управления.
13. Действия пользователя (спустя некоторое время).
    13.1. Запуск модифицированных бинарных файлов на сервере 2.

13.2. Запуск модифицированных бинарных файлов на сервере 1.
13.3. Запуск модифицированных бинарных файлов на сервере 3 и активация троянского коня.

14. Действия злоумышленных программ-агентов.
14.1. Подключение к агенту на главном сервере.
14.2. Отправка секретной информации агенту на главном сервере.
14.3. Переход программы-агента на сервере 3 в режим ожидания команд.
14.4. Передача информации агентом на главном сервере агенту на внешнем сервере.
14.5. Переход программы-агента главного сервера в режим ожидания команд.
14.6. Подключение агента внешнего сервера к серверу атакующего.
14.7. Передача информации агента внешнего сервера серверу атакующего.
14.8. Переход программы-агента на внешнем сервере в режим ожидания команд.

15. Управление системой злоумышленником.
15.1. Получение секретной информации.
15.2. Передача агенту внешнего сервера команды самоуничтожения агентам внешнего сервера, главного сервера, сервера 3, команды нарушить функционирование объекта агенту сервера 3.

16. Действие агентов.
16.1. Передача команд агентом внешнего сервера агенту главного сервера.
16.2. Выполнение команды самоуничтожения агентом внешнего сервера.
16.3. Передача команд агентом главного сервера агенту сервера 3.
16.4. Выполнение команды самоуничтожения агентом главного сервера.
16.5. Выполнение команды нарушения функционирования объекта программой-агентом сервера 3.
16.6. Выполнение команды самоуничтожения агентом сервера 3.

### 4.4. *Реализация абстрактного сценария на нижнем уровне* (3–4)

1. Получение информации о внешнем сервере.
1.1. Сканирование портов.
1.1.1. Сканирование порта №..
1.1.2. …

1.2. Поиск уязвимых сценариев.
1.2.1. Обращение к сценарию …
1.2.2. …

2. Взлом внешнего сервера.
2.1. Использование найденной веб-уязвимости и получение непривилегированного доступа.
2.1.1. Обращение к уязвимому сценарию с подстроенным параметром.
2.2. Использование shell-кода.
2.2.1. Загрузка shell-кода (reversing backdoor).
2.2.2. Установка shell-кода.
2.3. Использование эксплойта и получение root-привилегий.
2.3.1. Загрузка текста эксплойта.
2.3.2. Сборка эксплойта.
2.3.3. Запуск эксплойта.

3. Маскировка и закрепление на внешнем сервере.
3.1. Создание suid-shell.
3.1.1. Создание бинарного файла — оболочки для запуска эксплойта.
3.2. Маскировка средств удаленного управления.
3.2.1. Копирование в системную папку.
3.2.2. Переименование под системный бинарник.
3.2.3. Изменение времени создания.
3.3. Маскировка suid-shell.
3.3.1. Копирование в системную папку.
3.3.2. Переименование под системный бинарник.
3.3.3. Изменение времени создания.
3.4. Редактирование лог-файлов.
3.4.1. Модификация файлов из папки /var/logs.

4. Получение информации о главном сервере.
4.1. Просмотр системных лог-файлов и истории набранных команд
4.1.1. Чтение /var/logs/ и /.bash_history.
4.2. Сканирование портов главного сервера.
4.2.1. Сканирование порта №…
4.2.2. …

5. Взлом главного сервера.
5.1. Использование эксплойта mysqld и получение непривилегированного доступа.

5.1.1. Загрузка эксплойта.
5.1.2. Запуск эксплойта.
5.2. Получение пароля MySQL.
5.2.1. Получение хеш-значения.
5.2.2. Расшифровка хеш-значения (bruteforce).
5.3. Получение root привилегий.
5.3.1. Запуск псевдотерминала.
5.3.2. Выполнение su с паролем MySQL.
6. Закрепление и дальнейшее продвижение в системе.
6.1. Установка прослушивающего модуля.
6.1.1. Установка ядерного модуля keylogger.
7. Выход из системы.
7.1. Logout.
7.2. Закрытие соединений.
7.3. Деактивация средств удаленного управления.
8. Вход в систему.
8.1. Активация соединения со средством удаленного управления.
8.2. Запуск suid-shell.
8.3. Логин к главному серверу.
8.4. Просмотр логов прослушивающего модуля и получение root паролей к почтовому и файловому серверу.
9. Взлом файлового сервера.
9.1. Логин к файловому серверу.
9.1.1. Ssh_login(fileserver, root).
10. Получение информации о сервере 3.
10.1. Просмотр почтовой информации.
10.1.1. Логин к почтовому серверу.
10.1.2. Просмотр заголовков и тел писем.
11. Дальнейшее продвижение.
11.1. Модификация бинарных файлов.
11.1.1. Загрузка модифицированных версий.
11.1.2. Замена файлов.
11.2. Установка агента для связи с программой-агентом на главном сервере.
11.2.1. Загрузка агента.
11.2.2. Установка агента.
11.3. Установка агента для удаленного управления на внешнем сервере.
11.3.1. Загрузка агента.
11.3.2. Установка агента.

12. Выход из системы.
    12.1. Logout.
    12.2. Закрытие соединений.
    12.3. Деактивация средства удаленного управления.
13. Действия пользователя.
    13.1. Запуск модифицированных бинарных файлов на сервере 2.
    13.2. Запуск модифицированных бинарных файлов на сервере 1.
    13.3. Запуск модифицированных бинарных файлов на сервере 3 и активация программы-агента.
14. Действия агентов.
    14.1. Подключение к агенту на главном сервере.
    14.2. Отправка секретной информации агенту на главном сервере.
    14.3. Переход в режим ожидания команд.
    14.4. Передача информации агентом на главном сервере агенту на внешнем сервере.
    14.5. Переход агента главного сервера в режим ожидания команд.
    14.6. Подключение агента внешнего сервера к серверу атакующего.
    14.7. Передача информации агента внешнего сервера серверу атакующего.
    14.8. Переход в режим ожидания команд.
15. Управление системой злоумышленником.
    15.1. Получение информации.
    15.2. Передача агенту внешнего сервера команды самоуничтожения агентам внешнего сервера, главного сервера и команды сервера 3 команду нарушить функционирование объекта.
16. Действие агентов.
    16.1. Передача команд агентом внешнего сервера агенту главного сервера.
    16.2. Выполнение команды самоуничтожения агентом внешнего сервера.
    16.3. Передача команд агентом главного сервера агенту сервера 3.
    16.4. Выполнение команды самоуничтожения агентом главного сервера.
    16.5. Выполнение команды нарушения функционирования объекта.
    16.6. Выполнение команды самоуничтожения агентом сервера 3.

Далее, для трансляции низкоуровневого сценария в конечную реализацию для системы низкоуровневого моделирования проводим замену всех событий и действий (если действие атомарно и не разбито на события) на их специализированное представление в терминах языка низкоуровневой системы, составляем из них последовательность, накладываем ее на некоторую «типичную» последовательность функционирования системы и запускаем модель.

## Заключение

В работе рассмотрены существующие подходы к решению задачи классификации компьютерных атак. Во введении обоснована актуальность решаемой задачи, рассмотрены возможные области применения таксономии. Сформулирован ряд требований, которым должна удовлетворять таксономия атак для того, чтобы ее было удобно применять на практике.

Описаны некоторые известные подходы к созданию таксономии компьютерных атак, проведен анализ достоинств и недостатков каждого из таких подходов, соответствие предъявляемым к ним требованиям. На основании результатов такого анализа предложен подход к решению поставленной задачи. Описана общая схема таксономии и способы устранения основных недостатков предыдущих подходов. Далее детально изложены все составляющие таксономии: атака, этап, действие, событие и приведены диаграммы каждой из них с пояснением используемых терминов. Предложена методика формирования сценариев возможных атак с учетом модели атакуемой системы, показан пример возможного результата применения данной методики.

Задача классификации и моделирования атак является начальным этапом решения более сложного и объемного класса задач, связанных с анализом защищенности сложных критически важных объектов. Как уже было отмечено, КВО характеризуются тем, что их работоспособность прямо или косвенно влияет на национальную безопасность, как отдельных регионов, так и государства в целом. По этой причине необходим строгий контроль и всесторонний анализ их состояния не только в процессе эксплуатации, но и на этапе проектирования и разработки. Первым шагом для разработки средств проведения подобного перманентного анализа является структурирование знаний о кибератаках и создание методик и средств для их моделирования.

Следующим этапом является создание средств более детального описания и построения модели проектируемого КВО, учитывающую как структурные, так и функциональные аспекты КВО. Важно отметить, что такая модель должна быть тесно «привязана» к возможным угрозам данного КВО, включать в себя информацию для анализа потенциально осуществимых атак на КВО (в соответствии с описанной в данной работе методикой) и обеспечивать возможность оценки рисков при его эксплуатации.

## Литература

1. CERT/CC Statistics 1988–2005 (www.cert.org/stats/cert_stats.html).
2. *Васенин В. А.* Проблемы математического, алгоритмического и программного обеспечения компьютерной безопасности в Интернет / Материалы конференции «Математика и безопасность информационных технологий-2003». М., 2003. С. 111–142.

3. *Васенин В. А.*, *Галатенко А. В.*, *Корнеев В. В.*, *Макаров А. А.* Математическое и программное обеспечение активного аудита больших распределенных систем / Материалы конференции «МаБИТ-2004». М., 2004. С. 99–117.
4. *John D. Howard*, *Thomas A. Longstaff* A common language for computer security incidents». Sandia Report. Sandia National Laboratories. 1998.
5. Wikipedia, free internet encyclopedia.
6. Большая советская энциклопедия. Советская энциклопедия, 1969–1978.
7. The IEEE standard dictionary of electrical and electronics terms. Sixth edition. John Radatz. editor. Institute of Electrical and Electronics Engineers. New York, 1996
8. *Carolus Linnaeus* Systema Naturae per Regna Tria Naturae, Secundum Classes, Ordines, Genera, Species, cum Characteribus, Differentis, Synonymis, Locis. n/a, editio duodecima, reformata edition, 1766. Tomus I, Regnum Animale, 1766; Tomus II, Regnum Vegetabile, 1767; Tomus III, Regnum Lapideum, 1768.
9. *Daniel L. Lough* A taxonomy of computer attacks with applications to wireless networks. Ph. D. dissertation. 2001.
10. *Simon Hansman* A taxonomy of network and computer attacks methodologies. University of Canterbury. New Zealand, November 2003.
11. *Edward Amoroso* Fundamentals of Computer Security Technology, P T R Prentice Hall, New Jersey, 1994.
12. *John D. Howard* An analysis of security incidents on the internet 1989–1995, PhD thesis, Carnegie Mellon University, 1997.
13. *Jeffrey Undercoffer*, *John Pinkston* Modeling computer attacks: a target-centric ontology for intrusion detection. University of Maryland Baltimore Country.
14. *Ulf Lindqvist*, *Erland Jonsson* How to systematically classify computer security intrusions. Chalmers University of Technology, Sweden, 1997.
15. *Ivan Victor Krsul* Software vulnerability analysis. PhD thesis, Purdue University, 1998.
16. *Matt Bishop*, *David Bailey* A critical analysis of vulnerability taxonomies. University of California, Davis, September 1996.
17. *James P. Anderson* Computer security threat monitoring and surveillance. Technical Report Contract 79F296400, Washington, April 1980.
18. *Васенин В. А.*, *Галатенко А. В.* Математические модели распределенных компьютерных систем / Материалы конференции «МаБИТ-2004». М., 2004. С. 91–98.
19. *Attanasio C. R.*, *Markstein P. W.*, *Phillips R. J.* Penetrating an operating system: a study of VM/370 integrity. IBM System Journal, 15(1), 1976. P. 102–116.
20. *Giri Vijayaraghavan*, *Cem Kaner* Bug Taxonomies. STAR EAST 2003, Orlando, FL, May-2003.
21. *Peter Neumann*, *Donald Parker* A summary of computer misuse techniques, In 12th National Computer Security Conference, 1989.
22. *Peter G. Neumann* Computer-Related Risks. ACM Press / Addison Wesley, 1995.
23. *Donald B. Parker* COMPUTER CRIME Criminal Justice Resource Manual. U.S. Department of Justice National Institute of Justice Office of Justice Programs, August 1989.

24. *Donald B. Parker* Computer Security Reference Book. chapter 34, Computer Crime. CRC Press, K.M. Jackson and J. Hruskh, U.S. AssociateEditor Donn B. Parker, Boca Raton, Florida, 1992. P. 437–476.
25. *Грушо А. А.*, *Тимонина Е. Е.* Роль скрытых каналов при построении защиты в распределенных компьютерных системах / Материалы конференции «Математика и безопасность информационных технологий-2003». М., 2003. С. 276–283.
26. *Галатенко А. В.*, *Наумов А. А.*, *Слепухин А. Ф.* Реализация системы управления доступом к информации в виде встраиваемых модулей аутентификации / Материалы конференции «Математика и безопасность информационных технологий-2003». М., 2003. С. 237–240.
27. *Бетелин В. Б.*, *Галатенко В. А.*, *Годунов А. Н.*, *Грюнталь А. И.* Обеспечение информационной безопасности систем на программной платформе ос2000 / Материалы конференции «Математика и безопасность информационных технологий-2003». М., 2003. С. 254–267.
28. *Shai Rubin*, *Somesh Jha*, *Barton P. Miller* Language-based generationand evaluation of NIDS signatures. University of Wisconsin.
29. Beyond Security Inc. ProFTPD ASCII file remote root exploit. (www.securiteam.com/exploits).
30. *Грушо А. А.*, *Тимонина Е. Е.* Враждебные многоагентные системы / Материалы конференции «МаБИТ-2004». М., 2004. С. 249–256.
31. *Городецкий В.*, *Котенко И.*, *Карсаев О.* Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning. 2003.
32. *Медведовский И. Д.*, *Семьянов П. В.*, *Платонов В. В.* Атака через Internet. М., 1997.
33. *Roelof Temmingh* Breaking into computer networks from the Internet. 2001.
34. *Ariel Futoransky*, *Luciano Notarfrancesco*, *Gerardo Richarte*, *Carlos Sarraute* Building Computer Network Attacks. CoreLabs, Core Security Technologies, 2003
35. *Sviatoslav Bryanov*, *Murtuza Jadiwala* Representation and analysis of coordinated attacks.
36. *Jelena Mirkovic*, *Peter Reiher* A taxonomy of DDoS Attack and DDoS defense mechanisms. 2002.
37. *Arpit Aggarwal*, *Ranveer Kunal* A Comparison of Various Port Scanning Techniques. Indian Institute of Information Technology, Allahabad, India.
38. Examining port scan methods — Analysing Audible Techniques. Synnergy Networks, 2001.
39. *Васенин В. А.* Научные проблемы противодействия кибертерроризму / Материалы конференции «МаБИТ-2005». М., 2005. С. 49–64.
40. *Большаков М. В.* К вопросу о создании комплекса имитационного моделирования составных компьютерных атак / Материалы конференции «МаБИТ-2005». М., 2005. С. 414–424.
41. *Климовский А. А.* К анализу подходов классификации компьютерных атак / Материалы конференции «МаБИТ-2005». М., 2005. С. 368–391.