ТАКСОНОМИИ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ*

И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия В.О., д.39
ivkote@spiiras.nw.ru

УДК 681.3.06
И. В. *Котенко.* **Таксономии атак на компьютерные системы** // Труды СПИИРАН. Вып. 1, т. 2 — СПб: СПИИРАН, 2002.
Аннотация. *В статье представлен обзор таксономий атак на компьютерные системы. Проведен анализ следующих типов таксономий: списки терминов атак; списки категорий атак; категории результатов атак; эмпирические списки; матрицы уязвимостей; таксономии, базирующиеся на действиях; таксономии атак, основанные на их сигнатурах; таксономии дефектов и уязвимостей защиты; таксономии инцидентов.* — Библ. 25 назв.

UDC 681.3.06
I. V. Kotenko. **The taxonomies of the attacks on computer systems** // SPIIRAS Proceedings. Issue 1, v. 2. — SPb: SPIIRAS, 2002.
Abstract. *In the paper, a review of the taxonomies of the attacks on computer systems is presented. The analysis of the following types of the taxonomies are fulfilled: lists of attack terms; lists of attack categories; attack results categories; empirical lists of attack types; vulnerabilities matrices; action-based taxonomies; taxonomies based on the attack signatures; security flaws or vulnerabilities taxonomies; incident taxonomies.* — Bibl. 25 items.

1. Понятие таксономии атак на компьютерные системы. Требования к таксономиям атак

Под *атакой на компьютерную систему* будем понимать любое воздействие злоумышленника на компьютерную систему (КС) с целью нарушения информационной безопасности, заключающееся в поиске и использовании той или иной уязвимости [1]. *Таксономия атак на компьютерные системы* — это классификационная схема, которая структурирует знания о предметной области *атак на компьютерные системы* (АКС) и определяет отношения между элементами знаний.

В [17] сделано важное общее наблюдение: таксономия АКС не просто нейтральная структура для категоризации объектов. Она неявно описывает теорию предметной области АКС, определяет, какие объекты предметной области должны различаться и какие данные об этих объектах должны фиксироваться. Одна из основных целей создания любой таксономии атак состоит в том, чтобы предложить такие классификационные признаки, используя которые можно наиболее точно описать классифицируемые АКС.

Зачем нужно строить таксономию АКС? На этот вопрос можно привести несколько вариантов ответов:

(1) в целом, создание таксономий АКС позволяет осуществлять системное исследование вопросов защиты КС, в частности, структурировать статистические данные об атаках, выделять образцы типовых атак и делать выводы на основании собранных данных. Это приводит к систематизированному расширению знаний в области защиты информации и обеспечивает усиление защиты КС от возможных вторжений;

* Работа выполнена при финансовой поддержке РФФИ (проект № 01-01-00108)

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

(2) таксономии АКС необходимы при формировании сообщений об инцидентах. Таксономии могут использоваться в бюллетенях, выпускаемых различными группами анализа инцидентов, с целью предупреждения системных администраторов КС об обнаружении новых дефектов защиты;

(3) таксономии АКС важны для разработки компонентов систем защиты информации (например, подсистем обнаружения вторжений).

Аморосо выделил следующие *требования, которым должна удовлетворять таксономия АКС* [3]:

(1) *полнота* — таксономия должна охватывать все возможные АКС;

(2) *пригодность* — выбранная таксономия должна адекватно характеризовать АКС, любые ограничения используемой таксономии или целевой системы должны быть зафиксированы и проанализированы;

(3) *учет внутренних и внешних угроз* — в таксономии АКС атаки, реализуемые внутренними злоумышленниками, должны различаться от атак, которые инициируются извне системы.

Аморосо также выделил следующие *характеристики адекватных таксономий* [3]:

(1) *взаимоисключаемость* — отнесение объекта к одной категории исключает его сопоставление с другими категориями, потому что категории не пересекаются;

(2) *исчерпываемость* — взятые вместе категории охватывают все возможные варианты классификации объектов;

(3) *однозначность* (недвусмысленность) — ясность и точность таксономии, так что классификация имеет однозначный характер независимо от того, кто классифицирует;

(4) *повторяемость* — аналогичные объекты классифицируются одинаково независимо от того, кто классифицирует;

(5) *приемлемость* — классификация логична и интуитивна, вследствие чего категории могут быть принятыми повсеместно;

(6) *полезность* — таксономия может использоваться в различных приложениях.

Крсул переопределил эти желательные *(идеальные) свойства таксономии* [13]:

(1) категории в таксономии должны быть *взаимоисключающими* (каждый объект должен соответствовать самое большее одной категории) и совместно *исчерпывающими* (каждый образец должен соответствовать, по крайней мере, одной категории);

(2) каждая категория должна сопровождаться *ясными и однозначными* признаками (критериями) классификации, определяющими, какие объекты относятся к той или иной категории;

(3) таксономия должна быть понятна и полезна не только экспертам в области защиты информации, но также пользователям и администраторам с меньшими знаниями и опытом;

(4) терминология таксономии должна соответствовать терминологии, принятой в области защиты информации.

Однако таксономия является приближением к действительности (ее моделью) и поэтому удовлетворительная таксономия может иметь определенные недостатки. Данная особенность часто проявляется тогда, когда характеристики классифицируемых данных являются неточными и неопределенными, что, как правило, имеет место в типичной ситуации обработки конфиденциальной ин-

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

формации в распределенных КС. Тем не менее, классификация является важной и необходимой предпосылкой для систематических исследований.

В данной статье проводится обзор и анализ существующих таксономий АКС. Рассматриваются следующие предложенные к настоящему времени типы таксономий: (1) списки терминов атак; (2) списки категорий атак; (3) категории результатов атак; (4) эмпирические списки; (5) матрицы уязвимостей; (5) таксономии, базирующиеся на действиях; (6) таксономии атак, основанные на их сигнатурах; (7) таксономии дефектов и уязвимостей защиты; (8) таксономии инцидентов.

2. Списки терминов атак, списки категорий атак и категории результатов атак

Наиболее широко используемые и простые таксономии атак представляются в виде *списков терминов с определениями*.

Пример такой таксономии — список, предложенный Коеном [6] (39 терминов):

Trojan horses	*Toll fraud networks*	*Fictitious people*	*Infrastructure observation*	*E-mail overflow*
Time bombs	*Get a job*	*Protection limit poking*	*Infrastructure interference*	*Human engineering*
Bribes	*Dumpster diving*	*Sympathetic vibration*	*Password guessing*	*Packet insertion*
Data diddling	*Computer viruses*	*Invalid values on calls*	*Van Eck bugging*	*Packet watching*
PBX bugging	*Shoulder surfing*	*Open microphone listening*	*Old disk information*	*Video viewing*
Backup theft	*Data aggregation*	*Use or condition bombs*	*Process bypassing*	*False update disks*
Input overflow	*Hang-up hooking*	*Call forwarding fakery*	*Illegal value insertion*	*E-mail spoofing*
Login spoofing	*Induced stress failures*	*Network services attacks*	*Combined attacks*	

Другой пример — список терминов, состоящий из 24 единиц [12]:

Wiretapping	*Dumpster diving*	*Eavesdropping on Emanations*	*Denial-of-service*	*Harassment*
Masquerading	*Software piracy*	*Unauthorized data copying*	*Degradation of service*	*Traffic analysis*
Trap doors	*Covert channels*	*Viruses and worms*	*Session hijacking*	*Timing attacks*
Tunneling	*Trojan horses*	*IP spoofing*	*Logic bombs*	*Data diddling*
Salamis	*Password sniffing*	*Excess privileges*	*Scanning*	

В [7] Коен расширил предложенный ранее список до 96 терминов. Некоторые из *наиболее часто используемых терминов* из этого списка имеют следующие определения:

- *Ошибки и упущения (Errors and omissions)* — ошибочные или опущенные записи, формируемые проектировщиками, программистами, администраторами и т.п. Забывание устранить (изменить) пароли по умолчанию, установка некорректной защиты и т.д.
- *“Троянский конь” (Trojan horse)* — компонент аппаратного или программного обеспечения, который имеет незаявленные, как правило, вредоносные эффекты.
- *Некорректное значение по вызову (Invalid value on call)* — передача некорректных значений на системные вызовы для останова функционирования операционной системы.

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- *Использование недокументированных или неизвестных функций (Undocumented or unknown function exploitations)* — то же самое, что и общеупотребительное значение.
- *Атака на доверие (Implied trust attack)* — программы неуместно доверяют другим программам.
- *Использование несовершенных демонов (Imperfect daemon exploits)* — атака несовершенной (дефектной) программы-демона.
- *Сдвиг данных (Data diddling)* — незаконная модификация данных, чтобы привести ("обманом") операционную систему к состоянию, позволяющему получить неправильные результаты.
- *Агрегация данных (Data aggregation)* — объединение отдельных данных для получения ценной информации.
- *Обход процесса (Process bypassing)* — обход некоторого процесса управления, который имеет неадекватные средства управления.
- *Переполнение "входа" (Input overflow)* — атака программы, которая не контролирует длину входных данных.
- *Вызванное ошибками неправильное функционирование (Error-induced misoperation)* — ошибки, вызванные атакой, приводят к некорректному функционированию системы.
- Подавление контроля *(Audit suppression)* — препятствование правильному функционированию средств аудита.
- Отказ, вызванный нажимом *(Induced stress failure)* — давление на систему, пока она не начинает совершать ошибки.
- Аппаратные и системные дефекты *(Hardware-system failure-flaw)* — используются известные аппаратные или системные дефекты.
- *Сетевая служба и протокол (Network service and protocol)* — используются характеристики сетевых служб.
- *Распределенные скоординированные атаки (Distributed coordinated attacks)* — атакующие распределены, используют для атаки системы промежуточного уровня и действуют согласовано.
- Атаки на межпроцессорное соединение *(Interprocess communication attacks)* — производится атака на каналы межпроцессорной связи.
- Условия гонок *(Race conditions)* — взаимозависимые последовательности событий прерваны другими событиями, которые разрушают критические зависимости.
- *Неподходящие умолчания (Inappropriate defaults)* — значения параметров по умолчанию "оставляют" систему открытой для атак.

Списки терминов, как правило, не удовлетворяют шести приведенным выше требованиям к таксономиям атак [3]. Как отмечено в [10, 11] термины в большинстве случаев не являются взаимоисключающими. Например, в приведенных списках встречаются термины *вирус* и *логическая бомба*, но вирус может содержать логическую бомбу, т.е. данные категории пересекаются.

На практике злоумышленники зачастую также используют множество методов реализации атак. Как результат, разработка полного списка методов реализации атак не обеспечит создание классификационной схемы, которая имеет взаимоисключающие категории (даже если индивидуальные термины являются взаимоисключающими), потому что реальные атаки должны быть классифицированы на множественные категории. Это обусловливает неоднозначность и трудноповторимость классификации.

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Более фундаментальная проблема состоит в том, что при разработке исчерпывающего списка, таксономия будет чрезмерно громоздкой и трудной для применения. Она также не позволит отобразить отношения между различными типами атак [10, 11].

Ни один из разработанных списков терминов не был широко принят, частично потому что трудно согласиться с субъективными определениями терминов.

По этим причинам, списки терминов с определениями не являются приемлемыми таксономиями для классификации реальных атак.

Разновидностью одиночного списка терминов с определениями является *перечисление (список) категорий*.

Пример одного из наиболее содержательных списков категорий дан Чесвиком и Белловином в их книге о межсетевых экранах [5]. Они классифицируют атаки на семь следующих категорий.

1. *Захват паролей* (*Stealing passwords*) — методы, используемые для получения паролей других пользователей.

2. *Социальная инженерия* (*Social engineering*) — получение конфиденциальной информации путем искусных переговоров.

3. *Ошибки и черные ходы* (*Bugs and backdoors*) — использование систем, которые не соответствуют своим спецификациям, или замена программ скомпрометированными версиями.

4. *Ошибки аутентификации* (*Authentication failures*) — нарушение механизмов, используемых для аутентификации.

5. *Ошибки протоколов* (*Protocol failures*) — протоколы ненадлежащим образом разработаны или реализованы.

6. *Утечка информации* (*Information leakage*) — получение информации, которая необходима администраторам, для корректного функционирования сети, но также может использоваться злоумышленниками.

7. *Отказ в обслуживании* (*Denial of service*) — усилия, направленные на создание препятствий пользователям в использовании их систем.

Ранум выделил *восемь классов сетевых атак* [22]:

(1) *социальная инженерия* (*Social engineering*) — введение в заблуждение жертвы ради забавы и выгоды;

(2) *заимствование прав* (*Impersonation*) — захват прав доступа авторизованных пользователей;

(3) *использование* (*Exploits*) — использование дыр в программном обеспечении или операционных системах;

(4) *транзитивное доверие* (*Transitive trust*) — использование доверия между хостами (хост — хост) и сетями (сеть — сеть);

(5) *управляемые данными* (*Data driven*) — “троянцы”, лазейки (дыры), вирусы;

(6) *инфраструктура* (*Infrastructure*) — использование ошибок и особенностей сетевых протоколов или инфраструктуры сети;

(7) *отказ в обслуживании* (*Denial of service*) — препятствование использованию системы;

8) *волшебство* (*Magic*) — новые атаки, которые никто еще не фиксировал.

Списки категорий являются развитием списков терминов, поскольку они обладают некоторой структурой терминов, но этот тип таксономии страдает от большинства тех же самых проблем, что и большой список терминов.

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Другой разновидностью одиночного списка терминов является группирование всех атак в базовые *категории, описывающие результаты атак*.

В качестве примера можно привести категории, введенные Коэном [6]:

искажение (*corruption*),

утечка (*leakage*),

отказ (*denial*),

где *искажение* — неправомочная модификация информации, *утечка* — информация переносится туда, где она не должна быть, *отказ* — компьютерные или сетевые услуги не доступны для использования [6].

Рассел и Ганджеми [23] используют похожие категории, но определяют их, используя противоположные термины:

секретность (*secrecy*) и конфиденциальность (*confidentiality*);

точность (*accuracy*), целостность (*integrity*) и подлинность (*authenticity*);

доступность (*availability*).

За исключением атак, в результате которых только увеличиваются права атакующего по доступу к компьютеру или сети, или атак, при которых атакующие используют компьютерные или сетевые ресурсы без деградации обслуживания других пользователей — воровство ресурсов (*theft of resources*) [3], многие из индивидуальных атак могут быть однозначно связаны с одной из приведенных выше категорий.

Следует отметить, что сведение всех атак и инцидентов только к нескольким категориям представляет собой классификацию, имеющую лишь ограниченную практическую значимость [10, 11].

3. Эмпирические списки

Еще одним вариантом таксономий является *список категорий, базирующийся на классификации эмпирических данных*.

В ранней работе [16] Лаки предложил шесть категорий преодоления систем защиты КС. В этой работе отмечено, что предлагаемая классификация базируется на большом количестве примеров реальных вторжений, хотя не представлено соответствующих ссылок на имевшие место атаки.

Ньюман и Паркер разбили методы компьютерных злоупотреблений на девять классов (табл. 1).

Таблица 1. Методы компьютерных злоупотреблений

Класс	Описание
NP1. Внешнее злоупотребление	Нетехнологическое, физически отделяемое от КС и средств связи злоупотребление, например визуальный шпионаж
NP2. Злоупотребление аппаратным обеспечением	а) Пассивное, без (прямых) побочных эффектов б) Активное, с побочными эффектами
NP3. Маскарад	Заимствование прав, повторная передача данных, спуфинг и др. атаки
NP4. Инициирование последующего злоупотребления	Планирование и установка (приспосабливание) вредоносных программ
NP5. Обход средств контроля	Обход существующих средств контроля или несанкционированное получение полномочий
NP6. Активное злоупотребление ресурсами	Злоупотребление полномочиями для изменения системы или системных данных
NP7. Пассивное злоупотребление ресурсами	Злоупотребление полномочиями для чтения данных

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

NP8. Злоупотребление из-за бездействия	Отказ в своевременном предотвращении потенциальной проблемы или ошибка по недосмотру
NP9. Использование для реализации другого злоупотребления	Как средство для планирования злоупотребления

Они использовали данные о приблизительно 3,000 случаях. Эти данные собирались в течение 20 лет [19]. Авторы подчеркивают, что их классы не являются взаимоисключающими в том смысле, что для реальных компьютерных злоупотреблений часто используются методы, относящиеся к нескольким классам. Порядок перечисления этих классов — от “физического мира” (класс NP1) к аппаратным средствам (класс NP2), далее — к программному обеспечению (класс NP3 и выше) и от несанкционированного использования к неправильному применению полномочий.

В [3] Аморосо проинтерпретировал эти категории (с использованием примеров) и свел их к восьми следующим типам:

- внешняя кража информации (подглядывание за экраном компьютера);
- внешнее злоупотребление ресурсами (порча дисковода);
- маскарад (регистрация и воспроизведение передачи информации по сети);
- программы — вредители (установка злонамеренной программы);
- обход аутентификации или авторизации (раскрытие пароля);
- злоупотребление полномочиями (фальсификация записей);
- злоупотребление вследствие бездействия (преднамеренно плохое администрирование);
- косвенное злоупотребление (использование другой системы для создания злонамеренной программы).

Аморосо критикует указанный список следующим образом: недостаток этой таксономии атак заключается в том, что представленные восемь типов атак менее интуитивны и их труднее запомнить, чем три типа угроз при простой классификации угроз. Но, с другой стороны, так как более сложный список атак основывается на реальных случаях, трудно оспаривать его пригодность [3].

Другой пример эмпирического списка предложен в [18]. В данной работе представлены эмпирические категории как для методов реализации атак (табл.2), так и для их результатов (табл.3). Указанная таксономия является развитием таксономии, предложенной в [19].

Таблица 2. Таксономия атак: методы реализации атак

Категории		
NP5 Обход средств контроля	Атаки на пароли	Захват
		Подбор
	Спуфинг привилегированных программ	
	Использование слабой аутентификации	
NP6 Активное злоупотребление ресурсами	Использование произвольного разрешения записи	
	Исчерпание ресурсов	
NP7 Пассивное злоупотребление ресурсами	Ручной просмотр	
	Автоматический поиск	Использование индивидуальных средств
		Использование публично доступных средств

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Таблица 3. Таксономия атак: результаты атак

Категории		
Дискредитация	Раскрытие конфиденциальной информации	Раскрытие только пользовательской информации
		Раскрытие системной (и пользовательской) информации
	Несанкционированный доступ	Доступ с правами обычного пользователя
		Доступ с правами привилегированного пользователя
		Доступ с правами суперпользователя клиента
		Доступ с правами суперпользователя сервера
Отказ в обслуживании	Выборочный	Воздействует на одного пользователя
		Воздействует на группу пользователей
	Неизбирательный	Воздействует на всех пользователей системы
	Передаваемый	Воздействует на пользователей других систем
Ошибочный вывод	Выборочный	Воздействует на одного пользователя
		Воздействует на группу пользователей
	Неизбирательный	Воздействует на всех пользователей системы
	Передаваемый	Воздействует на пользователей других систем

Рассмотренные списки позволяют классифицировать большое количество реальных атак. При тщательной разработке эти списки могут иметь категории, удовлетворяющие четырем требуемым характеристикам: взаимоисключаемость, исчерпываемость, однозначность и повторяемость. Однако, только способности классифицировать все атаки по некоторым категориям явно недостаточно. Как отмечает Аморосо, так как список результатов не является логичным и интуитивно понятным, и не существует никакой дополнительной структуры, показывающей отношения категорий, то практическое использование любого эмпирического списка будет иметь ограниченный характер.

4. Матрицы уязвимостей

Перри и Валиш предложили классификационную схему, основанную на двух измерениях, отображающих уязвимости и потенциальных нарушителей. Она задает категоризацию инцидентов в виде *матрицы уязвимостей* (рис. 1). В ячейках матрицы задаются комбинации *потенциальных нарушителей* (операторов, программистов, служащих, обрабатывающих данные, внутренних пользователей, внешних пользователей и преступников) и *потенциальных эффектов* (физическое разрушение, разрушение информации, сдвиг данных, хищение услуг, просмотр и хищение информации) [3, 20].

Матрицы уязвимостей представляют собой по существу расширение списков категорий результатов атак. Используемые в матрицах два измерения, казалось бы, являются взаимоисключающими и возможно исчерпывающими категориями. К сожалению, термины внутри матрицы не представляются логичными или интуитивными. Между тем, взаимосвязь результатов атак и нарушителей является полезным подходом, который был использован Ховардом и Лонгстаффом [11] при разработке общего языка описания таксономии инцидентов, рассматриваемого ниже.

Возможно, наиболее развитый подход к построению таксономии атак на основе матриц уязвимостей был предложен Ландвером и др. в [17]. В этой работе была представлена таксономия дефектов защиты компьютерных систем

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

	Операторы	Программисты	Служащие, обрабатывающие данные	Внутренние пользователи	Внешние пользователи	Преступ
Физическое разрушение	*Короткие замыкания*					
Разрушение информации	*Стирание данных на диске*	*Злонамеренные программы*			*Злонамеренные программы*	*Через м*
Сдвиг данных		*Злонамеренные программы*	*Ложные записи данных*			
Хищение услуг		*Кража для использования*		*Несанкционированный доступ*	*Через модем*	
Просмотр	*Воровство носителей*			*Несанкционированный доступ*	*Через модем*	
Хищение информации				*Несанкционированный доступ*	*Через модем*	

Рис.1. Пример двумерной матрицы уязвимостей

(условий, которые могут приводить к отказу в обслуживании или несанкционированному доступу к данным [17]), основанная на трех измерениях:

(1) *происхождение* (как дефект защиты появляется в программе);

(2) *время введения* (в жизненном цикле программного или аппаратного обеспечения);

(3) *расположение* (в программном или аппаратном обеспечении).

Измерение *“происхождение”* показано на рис. 2.

<table>
<tr><td rowspan="8">Происхождение</td><td rowspan="5">Умышленные</td><td rowspan="3">Злонамеренные</td><td rowspan="2">“Троянский конь”</td><td>Не размножающиеся</td></tr>
<tr><td>Размножающиеся (вирус)</td></tr>
<tr><td colspan="2">Лазейка</td></tr>
<tr><td colspan="2">Логическая / временная бомба</td></tr>
<tr><td rowspan="2">Незлонамеренные</td><td rowspan="2">Скрытый канал</td><td>Памяти</td></tr>
<tr><td>Временной</td></tr>
<tr><td colspan="3">Другие</td></tr>
<tr><td rowspan="6">Неумышленные</td><td colspan="3">Ошибка проверки правильности (неполноты / противоречие)</td></tr>
<tr><td colspan="3">Ошибки определения (включая ошибки повторного использования объекта, остаточные ошибки, ошибки представления)</td></tr>
<tr><td colspan="3">Ошибки сериализации / совмещение имен</td></tr>
<tr><td colspan="3">Неадекватная идентификация / аутентификация</td></tr>
<tr><td colspan="3">Нарушение граничных условий (включая исчерпание ресурса и ошибки нарушения ограничений)</td></tr>
<tr><td colspan="3">Другие логические ошибки реализации</td></tr>
</table>

Рис.2. Таксономия дефектов безопасности: дефекты по происхождению

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Указанная таксономия включает множество терминов, таких как “троянский конь”, вирус, лазейка, логические и временные бомбы, для которых не имеется однозначно принятых определений. В результате, таксономия страдает от тех же самых проблем двусмысленности и отсутствия повторимости, присущих описанным ранее более простым таксономиям. Рассматриваемая таксономия также включает несколько дополнительных категорий, поэтому идентифицированные дефекты могут не представлять собой исчерпывающий список. Кроме того, в данном случае процедура классификации таксономии не является однозначной, если классифицируются реальные атаки, прежде всего, потому что реальные атаки могут быть классифицированы в несколько категорий.

Вероятно, что Ландвер и др. рекомендовали бы, чтобы классифицировались только отдельные части атак, так как атака может быть отнесена ко множеству категорий. Устранить эту проблему чрезвычайно трудно. При реализации атак в Internet используется множество различных методов.

Две дополнительных проблемы, связанные с рассматриваемой таксономией, заключаются в том, что ее основная логика не интуитивна, и таксономия может иметь лишь ограниченное использование для классификации реальных атак. Это следует из ограниченной логической взаимосвязи различных категорий. Из всего вышесказанного можно отметить, что данная таксономия представляет собой, прежде всего, сложный список, которому присущи недостатки списков, рассмотренных выше.

5. Таксономии, базирующиеся на действиях и сигнатурах атак

Столингс предложил простую *таксономию атак, основанную на действиях* [25]. Использованная им модель направлена на описание *угроз безопасности, проявляющихся при передаче информации*.

Столингс определяет четыре категории атак:

(1) *прерывание* (*Interruption*) — элемент системы разрушается или становится недоступным или неприменимым;

(2) *перехват* (*Interception*) — злоумышленник получает несанкционированный доступ к элементу системы;

(3) *модификация* (*Modification*) — злоумышленник не только получает несанкционированный доступ к элементу системы, но и оказывает на него влияние (портит, искажает);

(4) *подлог* (*Fabrication*) — злоумышленник вставляет поддельные (сфальсифицированные) объекты в систему [25].

Перехват рассматривается Столингсом как пассивная атака, а прерывание, модификация и подлог — как активные атаки. Эти четыре категории проиллюстрированы на рис. 3. Данная таксономия является упрощенной и, естественно, имеет ограниченную практическую значимость, однако следует заметить, что рассмотрение атак в виде последовательности указанных действий весьма плодотворно для построения более детальной таксономии.

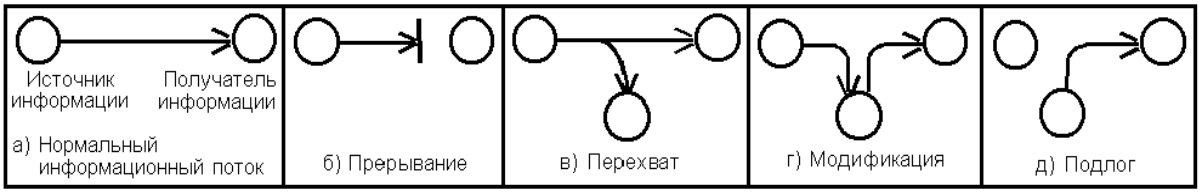

Рис.3. Модели атак Столингса

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В своей диссертации [15] Кумар выполнил *классификацию атак, основываясь на "сигнатурах" (образцах)*, фиксируемых в процессе реализации атак в записях аудита системы. Эта классификация предназначена для использования в системах обнаружения вторжения, использующих методы сопоставления с образцом. Однако данная классификация не учитывает атаки, которые не фиксируются в записях аудита, например, пассивное прослушивание трафика.

6. Таксономии дефектов и уязвимостей защиты

Некоторые авторы предлагают таксономии компьютерной безопасности, фокусирующиеся главным образом на дефектах и уязвимостях защиты, которые могут быть использованы в процессе реализации атак. Такие таксономии не анализируются в данном обзоре, если они не классифицируют также атаки.

В общем смысле дефекты защиты в компьютерных системах представляют собой определенные виды ошибок. *Бейзер* представил таксономию ошибок, построенную в соответствии с тем, на каком этапе процесса разработки программного обеспечения введена ошибка [4].

В своей классической статье Зальтцер и Шредер определили восемь принципов проектирования механизмов защиты, одним из которых является хорошо известный принцип наименьших привилегий [24].

На основе этих принципов, используя UNIX как пример "небезопасной операционной системы", Хоган классифицировал дефекты защиты в автономных и распределенных системах [9]. Эта классификация отражает главным образом причины наличия дефектов в системе.

Основываясь на 49 случаях, в которых дефекты безопасности операционной системы UNIX привели к вторжениям, Аслам разработал таксономию дефектов безопасности в UNIX, а также создал проект базы данных об уязвимостях [2]. Аслам предложил критерии выбора, которые позволяют провести однозначную классификацию исследованных 49 случаев. При этом использовались атрибуты только дефектов программного обеспечения.

Работа Аслама содержит классификационную схему, которая позволяет выполнить группирование уязвимостей. Эта классификация позднее была уточнена Крсулом.

Расширением классификационной схемы, предложенной в [2], является классификационная схема уязвимостей Додсона [8]. В ней классы определяют обобщенные дефекты программ. Каждый класс состоит из 20-ти местного кортежа единиц и нулей. Каждый элемент в 20-местном кортеже показывает, утвердительный или отрицательный ответ был получен на один из вопросов, перечисленных ниже (единицы соответствуют положительным ответам, а нули — отрицательным).

1. Ошибка случилась, когда процесс пытался читать или записывать за пределами границы действительного адреса?

2. Ошибка возникла, когда был исчерпан системный ресурс?

3. Ошибка явилась результатом переполнения структуры данных статического размера?

4. Ошибка произошла, когда субъект вызвал операцию на объекте за пределами его области доступа?

5. Ошибка явилась результатом чтения или записи файла или устройства за пределами области доступа субъекта?

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

6. Ошибка случилась, когда объект получил входные данные от неавторизованного субъекта?

7. Ошибка явилась результатом неправильной или неполной аутентификации субъекта?

8. Ошибка имела место вследствие того, что программа не смогла произвести корректный синтаксический разбор входных данных?

9. Ошибка случилась, когда некоторый модуль принимал посторонние входные поля?

10. Ошибка произошла, когда модуль не обрабатывал отсутствующие входные поля?

11. Ошибка случилась из-за ошибки корреляции со значением поля?

12. Ошибка произошла, потому что система не смогла обработать исключительное условие, сгенерированное модулем, устройством, или полученное при вводе данных пользователем?

13. Ошибка возникла в течение временного интервала между двумя операциями?

14. Ошибка вызвана неадекватной или несоответствующей сериализацией операций?

15. Ошибка произошла вследствие взаимодействия в определенной среде между функционально корректными модулями?

16. Ошибка возникает, только когда программа выполняется на определенной машине, имеющей специфическую конфигурацию?

17. Ошибка произошла, потому что операционная среда отличается от той среды, для которой было разработано программное обеспечение?

18. Ошибка случилась, потому что системная утилита была установлена с неправильными параметрами установки?

19. Ошибка произошла при использовании системной утилиты, которая была установлена в неправильном месте?

20. Ошибка имела место, потому что для некоторой утилиты были неправильно установлены правила доступа, что привело к нарушению политики безопасности?

В [13] Крсул представил большой обзор таксономий уязвимостей. Рассмотрим некоторые из этих таксономий.

Таксономия уязвимостей по категориям программного обеспечения (ПО) идентифицирует компонент информационной системы, который имеет уязвимость: общее ПО; утилиты; ПО регистрации; ПО электронной почты; сетевое ПО; программное обеспечение криптографической защиты.

Таксономия уязвимостей по последствиям определяет влияние уязвимости на характер последствий атаки. Этот признак используется для определения как прямого, так и косвенного влияния. *Прямое влияние* приводит к непосредственному воздействию на объект атаки после использования уязвимости. *Косвенное влияние* сказывается опосредованно.

Таксономия уязвимостей по воздействию задает степень сложности реализации атак, использующих ту или другую уязвимость, вне зависимости от того, существует ли сценарий или инструментальное средство для использования уязвимости:

- атака, использующая некоторую уязвимость, представляет собой простую последовательность команд или инструкций;
- для использования уязвимости требуется большое количество команд или инструкций;

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- атака, использующая некоторую уязвимость, требует выбора времени реализации и синхронизации действий. В общем случае необходим сценарий, который выполняется несколько раз и может приводить к замедлению функционирования системы.

В [21] описана классификация угроз, которые обусловлены различными уязвимостями. Она представляет собой классификацию враждебных действий, которые может предпринять злоумышленник:

- *угрозы доступности и пригодности* (уничтожать, повреждать или заражать; отказывать, отсрочивать или задерживать использование доступа);
- *угрозы целостности и подлинности* (вводить, использовать или выводить ложные данные; модифицировать, заменять или переупорядочивать; неправильно интерпретировать; отвергать, отказываться; неправильно использовать или терпеть неудачу в правильном использовании);
- *угрозы конфиденциальности и собственности* (осуществлять доступ; раскрывать; подсматривать; копировать; воровать);
- *воздействие других угроз* (подвергать опасности воздействия других угроз).

7. Таксономии инцидентов. Язык описания инцидентов

Ховард [10] предложил выполнять классификацию компьютерных и сетевых атак с помощью *таксономии инцидентов*, которая определяет процесс, “связывающий” атакующих с конечными целями атак. Взаимосвязь между атакующими и целями атак устанавливается в виде следующей последовательности:

Атакующие $\Rightarrow$ *Средства* $\Rightarrow$ *Доступ* $\Rightarrow$ *Результаты* $\Rightarrow$ *Цели.*

Данная классификация может быть представлена в виде классификационного дерева, имеющего множество уровней, на каждом из которых должен осуществляться выбор одного из нескольких значений.

Позднее в [11] Ховард и Лонгстафф предложили *язык описания инцидентов*. В этой работе разработанная ранее таксономия инцидентов была скорректирована (рис. 4).

Эта таксономия показывает отношения событий, атак и инцидентов. Она предполагает, что достижение целей атаки может предотвращаться посредством создания препятствий атакующим в выполнении любой законченной цепочки, состоящей из семи элементов, выделенных на рис. 4.

Создание препятствий может осуществляться, например, по следующим направлением:

- изучение пользователей, которые могут являться потенциальными *атакующими*;
- периодическое обследование системы на наличие инструментальных *средств* атаки;
- исправление обнаруженных *уязвимостей* системы;
- усиление механизмов управления доступом для предотвращения *действий* атакующего по доступу к *объектам воздействий* (например, учетным записям);

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- шифрование файлов для предотвращения одного из *результатов* несанкционированных действий — раскрытия информации;
- реализация общественных образовательных программ для предотвращения достижения *целей* атакующих.

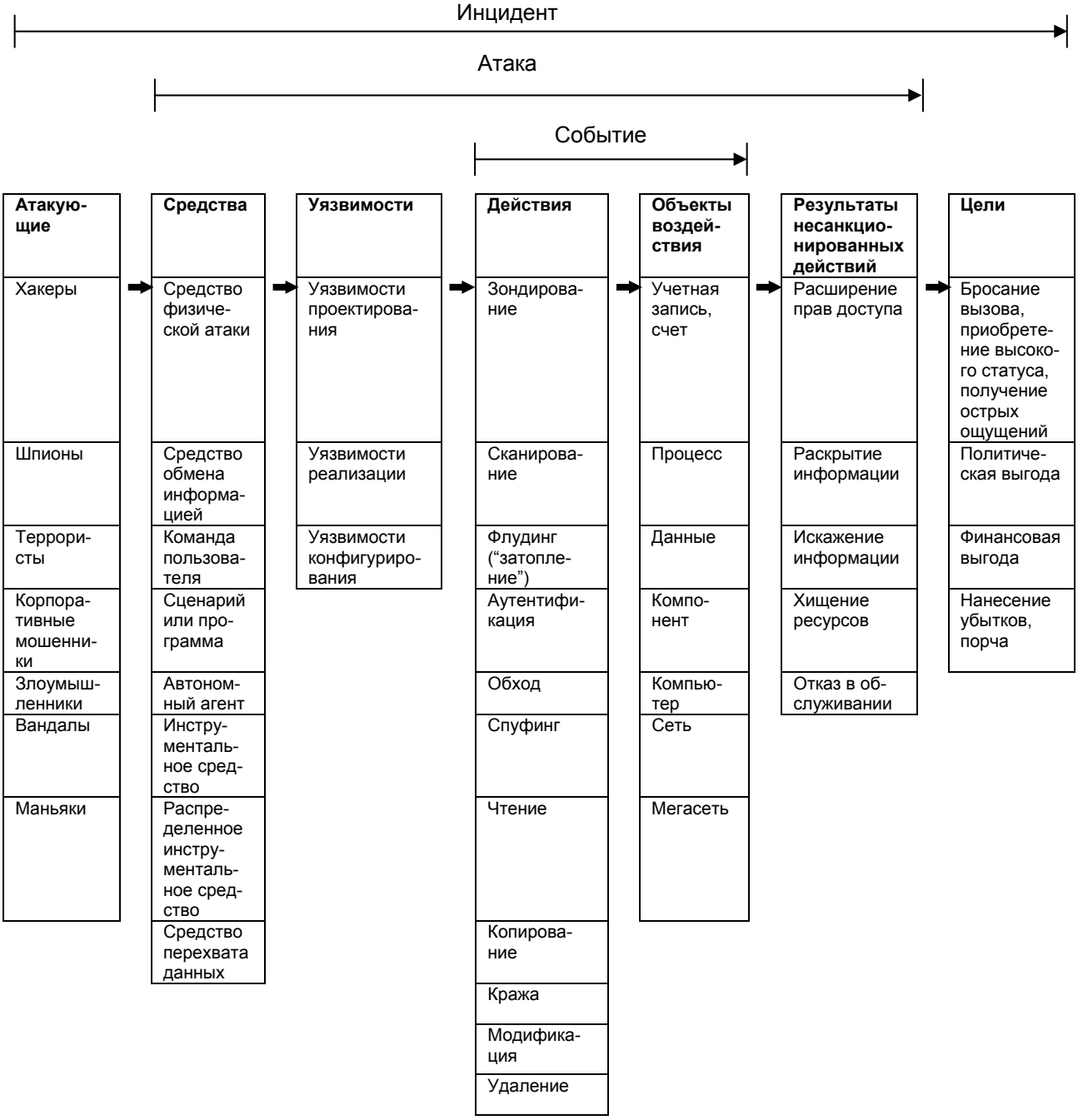

Рис.4. Таксономия атак на компьютерные системы и сети

В предложенном языке описания инцидентов Ховард и Лонгстафф выделили три *основных высокоуровневых понятия* (инцидент, атака и событие). Эти понятия определены на основании семи групп *базовых низкоуровневых понятий* (атакующие, средства, уязвимости, действия, объекты воздействий, результаты несанкционированных действий и цели) [11]. Приведем определения некоторых базовых понятий, введенных в языке описания инцидентов. Под *ин-*

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

цидентом понимается группа атак, которые отличаются типами атакующих, типами атак, достигаемыми целями, местом и временем их реализации. *Атака* определяется как последовательность шагов (несанкционированных действий), предпринимаемых атакующим для достижения несанкционированных результатов. *Событие* — это действие, направленное на объект воздействия, имеющее целью изменение его состояния. *Зондирование* — доступ к объекту воздействия для определения его характеристик. *Сканирование* — последовательный доступ к множеству объектов воздействия для выявления объектов, имеющих специфические характеристики. *Флудинг* — неоднократный доступ к объекту воздействия с целью перегрузки его пропускной способности. *Обход* — уклонение от некоторого процесса путем использования альтернативного метода доступа к объекту воздействия. *Спуфинг* — подмена при сетевом соединении субъекта доступа другим субъектом.

8. Заключение

В статье представлен обзор наиболее известных таксономий атак на компьютерные системы, составленный на основе зарубежных работ. Данный обзор не претендует на полноту и в силу ограничений на объем статьи выполнен в краткой форме. Наиболее развитой из рассмотренных таксономией является таксономия инцидентов Ховарда и Лонгстаффа, но и она не удовлетворяет всем представленным требованиям к таксономиям атак на компьютерные системы. Заслуживает внимания представленный общий язык описания инцидентов безопасности. Он может послужить базисом для построения более развитых языков представления атак. В настоящее время в рамках работ по созданию системы моделирования атак на компьютерные сети автором статьи разрабатывается таксономия атак, обеспечивающая выполнение большинства рассмотренных требований.

Литература

[1] Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. Учебное пособие / Под ред. *И.В.Котенко*. — СПб: ВУС, 2000.

[2] *Aslam T.* A taxonomy of security faults in the Unix operating system. Master's thesis. — Purdue University, West Lafayette, Indiana, USA. 1995.

[3] *Amoroso E. G.* Fundamentals of Computer Security Technology. — Prentice-Hall PTR, Upper Saddle River, NJ. 1994.

[4] *Beizer B.* Software Testing Techniques. — Van Nostrand Rein-hold. 1990.

[5] *Cheswick W. R., Bellovin S. M.* Firewalls and Internet Security: Repelling the Wily Hacker. — Addison-Wesley Publishing Company, Reading, MA. 1994.

[6] *Cohen F. B.* Protection and Security on the Information Superhighway. — John Wiley & Sons, New York. 1995.

[7] *Cohen F. B.* Information System Attacks: A Preliminary Classification Scheme // Computers and Security, Vol. 16, No. 1, 1997.

[8] *Dodson J.* Specification and Classification of Generic Security Flaws for the Tester's Assistant Library. M.S. thesis. — University of California at Davis. 1996.

[9] *Hogan C. B.* Protection imperfect: The security of some computing environments // Operating Systems Review, Vol. 22, No. 3, 1988.

[10] *Howard J. D.* An Analysis of Security Incidents on the Internet, *1989 — 1995*, Ph.D. Dissertation. — Carnegie Mellon University, Pittsburgh, PA. 1997.

[11] *Howard J. D., Longstaff T. A.* A Common Language for Computer Security Incidents, SANDIA REPORT, SAND98-8667. October 1998.

[12] *Icove D., Seger K., Vonstorch W.* Computer Crime: A Crimefighter's Handbook. — O'Reilly & Associates, Inc., Sebastopol, CA. 1995.
[13] *Krsul I. V.* Software Vulnerability Analysis, Ph.D. Dissertation. — Purdue University, Lafayette, IN, May, 1998.
[14] *Kumar S., Spafford E. H.* An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR 94 013. The COAST Project. — Purdue University. West Lafayette. 1994.
[15] *Kumar S.* Classification and Detection of Computer Intrusions. PhD thesis. — Purdue University, West Lafayette, Indiana, USA, 1995.
[16] *Lackey R. D.* Penetration of computer systems an overview // Honeywell Computer Journal, Vol. 8, No. 2, 1974.
[17] *Landwehr C. E., Bull A. R., McDermott J. P., Choi W. S.* A Taxonomy of Computer Security Flaws // ACM Computing Surveys, Vol. 26, No. 3, 1994.
[18] *Lindqvist U., Jonsson E.* How to Systematically Classify Computer Security Intrusions // Proceedings of the 1997 IEEE Symposium on Security and Privacy. — IEEE Computer Society Press, Los Alamitos, CA, May, 1997.
[19] *Neumann P., Parker D.* A Summary of Computer Misuse Techniques // Proceedings of the 12th National Computer Security Conference, 1989.
[20] *Perry T., Wallich P.* Can Computer Crime Be Stopped? // IEEE Spectrum, Vol. 21, No. 5, 1984.
[21] *Power R.* Current And Future Danger: A CSI Primer of Computer Crime & Information Warfare // CSI Bulletin. 1996.
[22] *Ranum M.* A Taxonomy of Internet Attacks. Web Security Sourcebook. — John Wiley & Sons. 1997.
[23] *Russell D., Gangemi G. T.* Computer Security Basics. — O'Reilly & Associates, Inc., Sebastopol, CA. 1991.
[24] *Saltzer J. H., Schroeder M. D.* The protection of information in computer systems // Proceedings of the IEEE, Vol. 63, No. 9, 1975.
[25] *Stallings W.* Network and Internetwork Security Principles and Practice. — Prentice Hall, Englewood Cliffs, NJ. 1995.

Труды СПИИРАН. 2002. Вып. 1. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru