На правах рукописи

**АНДРЕЕВ Дмитрий Александрович**

# РАЗРАБОТКА И ИССЛЕДОВАНИЕ РИСК-МОДЕЛЕЙ SYNflood-АТАК НА СЕРВЕРЫ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени кандидата технических наук



Воронеж – 2008

Работа выполнена в ГОУВПО «Воронежский государственный технический университет»

Научный руководитель — доктор технических наук, профессор Остапенко Александр Григорьевич

Официальные оппоненты: доктор технических наук, профессор Бугров Юрий Григорьевич;

кандидат технических наук Пархоменко Андрей Петрович

Ведущая организация — ОАО «Концерн «Созвездие» (г. Воронеж)

Защита состоится «25» декабря 2008 г. в $16^{00}$ часов в конференц-зале на заседании диссертационного совета Д 212.037.08 ГОУВПО «Воронежский государственный технический университет» по адресу: 394026, г. Воронеж, Московский просп., 14.

С диссертацией можно ознакомиться в научной библиотеке ГОУВПО «Воронежский государственный технический университет».

Автореферат разослан «24» ноября 2008 г.

Ученый секретарь диссертационного совета Батищев Р.В.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** В современном мире все большее внимание уделяется разработке общих формальных моделей оценки и управления информационными рисками различных классов систем. Эта задача актуальна и при построении вероятностных моделей атак на серверы, включая риск-анализ компьютерных систем и разработку алгоритмов управления их рисками.

Под атаками отказа в обслуживании (Denial of Service attack — DoS-attack) следует понимать сетевые атаки, приводящие к невозможности для легитимного пользователя сети получить доступ к ресурсам сервера.

Принципиальной особенностью DoS-атак является то, что такие атаки направлены на то, чтобы сделать сервер недоступным для нормальных пользователей. При атаке чаще всего используются обычные сетевые протоколы.

Особый класс DDoS-атак составляют так называемые распределенные атаки отказа в обслуживании (Distributed DoS — DDoS) — это тип атак DoS, при которых источниками атаки являются сразу несколько хостов. Обнаружение таких атак сильно затруднено, т. к. зачастую количество атакующих хостов очень велико и их состав постоянно меняется.

Задача предотвращения DoS-атак, исходя из вышесказанного, является достаточно сложной. Практически она решается только отбрасыванием части данных, идущих на сервер от пользователей, причем отбрасывание это должно происходить не на самом сервере, а до него. Такая схема имеет серьезные недостатки, поскольку необходима координация действий с провайдером из вышестоящей сети, что не всегда возможно. Кроме того, существует вероятность отбросить данные легитимного пользователя, не участвующего в атаке.

Риск-анализ в области обеспечения безопасности компьютерных систем выделяет качественные и количественные методы оценки рисков. Количественные методы оценки рисков в свою очередь можно разделить на статистические и аналитические. Статистические методы оценки рисков базируются на ряде фундаментальных понятий и предусматривают ряд процедур, зависящий от конкретной информационной системы, где проводится оценка риска и ее параметров. Аналитические методы оценки рисков зависят от вида информационных атак на систему, применительно к которой производятся оценочные операции.

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача — объективно идентифицировать и оценить наиболее значимые информационные риски, а также адекватность используемых средств контроля рисков для увеличения эффективности системы. Поэтому под термином «управление информационными рисками» обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков в соответствии с определенными ограничениями.

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Однако риски компьютерных систем в их аналитическом выражении до сих пор остаются «белым пятном» в теории информационной безопасности. Это касается, прежде всего, атак типа «отказ в обслуживании», в том числе наиболее распространенной их разновидности – SYNflood-атак. Отсюда вытекают объект, предмет, цель и задачи работы, ее актуальность.

Работа выполнена в соответствии с одним из основных научных направлений ГОУВПО «Воронежский государственный технический университет» «Перспективные радиоэлектронные и лазерные устройства, системы передачи, приема, обработки и защиты информации».

**Объектом исследования** является сервер, подвергающийся воздействию SYNflood-атак, направленных на отказ в обслуживании.

**Предметом исследования** является риск-анализ сервера, подвергающегося воздействию SYNflood-атак, направленных на отказ в обслуживании.

**Цель и задачи исследования.** Целью настоящей работы является построение и исследование риск-моделей SYNflood-атак на серверы компьютерных систем.

Для достижения указанной цели предполагается решить следующие задачи:

- разработать и исследовать вероятностную модель SYNflood-атак на сервер, направленных на отказ в обслуживании;
- получить аналитические выражения для расчета рисков и защищенности сервера, подвергающегося воздействию SYNflood-атак, определить функции их чувствительности;
- разработать алгоритм управления рисками сервера, подвергающегося SYN flood-атаке.

**Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации,** обеспечивается:

- корректным использованием методов теории вероятностей и математической статистики;
- сопоставлением результатов оценки рисков с известными аналогами;
- практической проверкой алгоритмов через компьютерное моделирование и в процессе внедрения.

**Методы исследования.** Для решения поставленных задач в работе используются методы теории вероятностей и математической статистики, теории автоматического управления, а также теории чувствительности.

**Научная новизна результатов исследования.** В работе получены следующие основные результаты, характеризующиеся научной новизной:

- введена оригинальная характеристика ущерба при SYNflood-атаке, доказано, что эта характеристика подчиняется закону Пуассона;
- на основе выведенной характеристики впервые получены аналитические выражения для расчета рисков при единичной и распределенных SYNflood-атаках, а также - аналитические выражения для функций чувствительности риск-модели к изменению параметров атаки в отличие от аналогов позволяющие в данной проектной ситуации перейти от качественных к количественным оценкам риска;
- впервые предложены алгоритмы управления рисками для компьютерных систем, подвергающихся SYNflood-атакам.

**На защиту выносятся** следующие основные положения диссертационной работы:

- математическая модель процессов SYNflood-атак на серверы компьютерных систем, основанная на распределении Пуассона и предложенной характеристики ущерба;
- аналитические выражения для расчета рисков и защищенности атакуемых компьютерных систем на основе вероятностного распределения Пуассона;
- аналитические выражения функций чувствительности риска к изменению параметров атак заданного типа;
- алгоритмы управления рисками компьютерных систем, подвергающихся SYNflood-атакам.

**Практическая значимость работы** заключается в том, что разработанные модели и алгоритмы могут быть применены непосредственно при оценке рисков атак на серверы компьютерных систем их администраторами безопасности и аудиторскими компаниями при комплексной оценке эффективности защиты от информационных атак.

**Реализация результатов работы.** Работа выполнена в соответствии с одним из основных научных направлений ГОУВПО «Воронежский государственный технический университет» «Перспективные радиоэлектронные и лазерные устройства, системы передачи, приема, обработки и защиты информации». Ее результаты использованы в Межрегиональном центре «Инфозащита», а также внедрены в учебном процессе ГОУВПО «Воронежский государственный технический университет».

**Апробация работы.** Основные результаты диссертационной работы докладывались и обсуждались на следующих конференциях:

Региональной научно-практической конференции «Информационные аспекты безопасности систем» (Воронеж, 2007);

VI Всероссийской научно-практической конференции с международным участием «Современные информационные технологии в науке, образовании и практике». Секция «Вычислительные машины, комплексы и компьютерные сети» (Оренбург, 2007);

Межрегиональной научно-практической конференции «Информационные риски и безопасность» (Воронеж, 2007);

Региональной научно-практической конференции «Методы, системы и процессы обеспечения безопасности» (Воронеж, 2008);

Межрегиональной научно-практической конференции «Проблемы обеспечения безопасности систем» (Воронеж, 2008).

**Публикации.** По теме диссертации опубликовано 16 научных работ, в т.ч. 3 - в изданиях, рекомендованных ВАК РФ. В работах, опубликованных в соавторстве и приведенных в конце автореферата, лично соискателю принадлежат: [2] - предложена концепция риск-анализа атак рассматриваемого класса; [4] - предложен алгоритм управления защищенностью автоматизированной системы; [5] - предложено распределение Пуассона в качестве модели риск-анализа; [6] - выдвинута гипотеза о распределении рисков сетевых атак; [7] - предложена оценка отказа в обслуживании сервера сети; [8] - предложена методика риск-оценки ущерба атакуемых автоматизированных систем; [9] - адаптировано Пуасоновское распределение к задачам информационной безопасности; [11] - методически обоснован выбор закона распределения для риск-моделирования; [12] - получены выражения функции дифференциальной чувствительности для риск-модели пуассоновского типа; [13] - предложена оценка защищенности для Flood-атак; [16] - определена предметная область описания кибер-атак с помощью закона Пуассона.

**Структура и объем работы.** Диссертация состоит из введения, четырех глав, заключения и списка литературы, включающего 116 наименований. Основная часть работы изложена на 117 страницах и содержит 33 рисунка и 2 таблицы.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обоснована актуальность темы диссертации, сформулированы цель и задачи исследования, представлены основные научные результаты, выносимые на защиту, и описана их новизна.

**В первой главе** рассмотрены угрозы безопасности информации в компьютерных системах, предложена классификация DoS-атак; на основе анализа статистических данных рассмотрена статистическая характеристика для построения риск-модели, определено ее вероятностное распределение.

Эффективная защита компьютерной сети от атак в общем случае требует построения модели угроз, которая должна систематизировать информацию обо всех возможных атаках. Именно с ее помощью оценивается опасность деструктивных воздействий на информацию, а также разрабатываются мероприятия по противодействию угрозам применительно к конкретным атакам.

Признаком классификации DoS-атак может стать элемент системы, являющийся целью атаки: центральные процессоры; оперативная память (в ос-

новном, из-за утечек памяти в приложениях); запоминающие устройства (в основном, из-за низкой производительности жестких дисков; данный тип атак встречается очень редко, хотя и возможен); сетевое оборудование сервера; сетевое оборудование и системы безопасности, обеспечивающие работу сервера в сети (маршрутизаторы, коммутаторы и т. п.); операционная система и прикладные программы.

Чаще всего встречаются атаки на сетевое оборудование сервера, обусловленные асимметрией развития современных технологий.

Наиболее сложными с точки зрения обнаружения и анализа являются атаки типа flood. Это атака, при которой компьютерной системе или сетевому оборудованию посылается очень большое число запросов (обычно бессмысленных или некорректно сформированных), приводящих к ее недоступности. Сложность обнаружения связана с тем, что атакующий чаще всего создает нормальные запросы к системе, но из-за ограниченности ресурсов система не успевает обрабатывать их вместе с запросами нормальных пользователей.

При DoS и DDoS-атаках одним из важнейших факторов, позволяющих обнаружить как сам факт атаки, так и состав атакующих, являются так называемые аномалии сетевого трафика.

В данной работе рассматривается соотношение количества запросов на соединение и количества реально прошедших соединений за интервал времени.

Анализ статистических данных позволяет выдвинуть гипотезу о том, что рассматриваемый вид атак на серверы подчиняется закону распределения Пуассона.

В ходе доказательства выдвинутой гипотезы в работе получено аналитическое выражение для величины $X_n$, характеризующей активность сетевого обмена между сервером и клиентами

$$X = \left\langle X_n \middle| n = 0,1.. .,z \right\rangle = \left\langle \frac{\Delta_n}{F_a(n)} \middle| n = 0,1 \quad ,z \right\rangle = \left\langle \frac{NS_n - (NF_n + NR_n)}{F_a(n)} \middle| n = 0,1.. .,z \right\rangle,$$

где $\Delta_n$ – количество SYN-пакетов, не обработанных за n-й период;

$NS_n$ – количество SYN-пакетов, пришедших на сервер за n-й период;

$NF_n$, $NR_n$ – количество FYN и RST пакетов, отправленных за соответствующий период;

$F_a(n)$ – рекурсивная функция $F_a(n) = \alpha \ F(n-1) + (1-\alpha) \cdot (NF_n + NR_n)$;

α - значение, определяющее количество предыдущих периодов длительностью $t_0$, влияющих на значение функции в текущем периоде $0 \le \alpha \le .1$.

Критерий Пирсона позволяет доказать, что данная величина распределена по закону Пуассона со следующими характеристиками распределения:

$$M[U]=\sum_{k=1}^{n}\left(\frac{k}{n}\cdot\frac{\lambda^k e^{-\lambda}}{k!}\right)=\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!};\ D(U)=\frac{e^{-\lambda}}{n^2}\left(\sum_{k=2}^{n}\frac{\lambda^k}{(k-2)!}+\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}-e^{-\lambda}\left(\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)^2\right).$$

Начальные моменты:

$$\alpha_1=M(X)=\frac{e^{-\lambda}}{n}\left(\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right);\ \alpha_2=\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^2}{k!};\ \alpha_3=\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^3}{k!};\ \alpha_4=\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^4}{k!}.$$

Центральные моменты:

$$\mu_1=0;\ \mu_2=\frac{e^{-\lambda}}{n^2}\left(\sum_{k=2}^{n}\frac{\lambda^k}{(k-2)!}+\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}-e^{-\lambda}\left(\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)^2\right);$$

$$\mu_3=\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^3}{k!}-3\left(\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)\left(\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^2}{k!}\right)+2\left(\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)^3;$$

$$\mu_4=$$

$$=\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^4}{k!}-4\left(\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^3}{k!}\right)\left(\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)+6\left(\frac{e^{-\lambda}}{n^2}\sum_{k=1}^{n}\frac{\lambda^k k^2}{k!}\right)^3\left(\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right)^2-$$

$$-3\left(\frac{e^{-\lambda}}{n}\sum_{k=1}^{n}\frac{\lambda^k}{(k-1)!}\right),$$

где n – количество промежутков времени;

λ – параметр распределения Пуассона.

**Во второй главе** разработаны риск-модели систем, подвергающихся DoS-атаке и DDoS-атаке; на основе анализа построенных моделей получены выражения распределения вероятности ущерба, риска и защищенности систем.

Процессы обеспечения безопасности информации в значительной степени определяют многие факторы. Отсюда их модели могут быть стохастическими. Это сужает границы классификации и анализа, так как достаточно иметь в виду только четыре разновидности моделей: аналитические; имитационные; общие и частные.

В аналитических моделях структура моделируемых систем и процессы их функционирования представляются в виде формализовано записанной последовательности, то есть неявно. Характеристикам, полученным в результате аналитического моделирования, необходимо реальное подтверждение. Подтверждаются данные характеристики на практике, то есть статистика получается при функционировании реальных компьютерных систем.

В данной работе рассматриваются риск-модели систем, подвергающихся воздействию атак «отказ в обслуживании».

Основной целью риск-анализа является нахождение выражения риска для заданной системы. Причем система в каждый момент времени находится в состоянии вероятностной неопределенности: невозможно точно предсказать сле-

дующее событие, но можно вычислить вероятность каждого из возможных событий.

В простейших случаях множество будущих событий можно считать конечным и риск представляется вероятностным распределением на конечном пространстве элементарных событий. Элементарным событием (исходом) в данном контексте будем считать факт достижения ущербом системы определенного значения за некоторый интервал времени или после реализации некоторой угрозы.

Для DoS-атаки оценкой ущерба может являться соотношение количеств успешных и неуспешных запросов к серверу.

Определим риск как сочетание ущерба от атаки и вероятности этого ущерба. Тогда риск в n-й промежуток времени можно представить следующим образом:

$$Risk(n,\lambda) = X_n \cdot \frac{\lambda^{X_n} e^{-\lambda}}{X_n!} = \frac{\lambda^{X_n} e^{-\lambda}}{(X_n - 1)!}.$$

Абсолютная защищенность будет равна:

$$E_{абс}(n,\lambda) = 1 - Risk(n,\lambda) = 1 - \frac{\lambda^{X_n} e^{-\lambda}}{(X_n - 1)!},$$

а относительная защищенность:

$$E_{отн}(\lambda) = \frac{\sum_{n=1}^{z} E_{абс}(n,\lambda)}{\sum_{n=1}^{z} Risk(n,\lambda)} = \frac{\sum_{n=1}^{z}\left(1 - \frac{\lambda^{X_n} e^{-\lambda}}{(X_n - 1)!}\right)}{\sum_{n=1}^{z} \frac{\lambda^{X_n} e^{-\lambda}}{(X_n - 1)!}} = \frac{\sum_{n=1}^{z} (X_n - 1)!}{\sum_{n=1}^{z} \lambda^{X_n} e^{-\lambda}} - 1.$$

В результате проведенного анализа получены следующие характеристики распределения риска:

$$M(Risk) = e^{-2\lambda} \cdot \sum_{k=1}^{z} \frac{U_k \lambda^{2U_k}}{(U_k!)^2}; \; D(Risk) = e^{-3\lambda}\left(\sum_{k=1}^{z} \frac{U_k^2 \lambda^{U_k}}{(U_k!)^3} - e^{-\lambda} \cdot \left(\sum_{k=1}^{z} \frac{U_k \lambda^{2U_k}}{(U_k!)^2}\right)^2\right),$$

$$\sigma(Risk) = e^{-\lambda}\sqrt{e^{-\lambda}\left(\sum_{k=1}^{z} \frac{U_k^2 \lambda^{U_k}}{(U_k!)^3} - e^{-\lambda} \cdot \left(\sum_{k=1}^{z} \frac{U_k \lambda^{2U_k}}{(U_k!)^2}\right)^2\right)}$$

Получены также выражения для начальных и центральных моментов случайной величины.

Коэффициенты асимметрии и эксцесса рассчитываются соответственно:

$$A_s = \frac{\mu_3}{\sigma^3} = \frac{\alpha_3 - 3\alpha_2\alpha_1 + 2\alpha_1^3}{\sigma^3}; \quad A_e = \frac{\mu_4}{\sigma^4} = \frac{\alpha_4 - 4\alpha_3\alpha_1 + 6\alpha_2\alpha_1^2 - 3\alpha_1^4}{\sigma^4}.$$

Энтропия риска определена следующим образом

$$H(Risk) = \sum_{k=1}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \log_2\left(\frac{\lambda^k e^{-\lambda}}{k!}\right)$$

Далее рассмотрена компьютерная система, подвергающаяся распределенной DoS-атаке (DDoS) в течение z интервалов времени длительностью $t_0$ 1<n<z. Пусть в течение интервала времени z' <z система перестала отвечать на запросы легитимных пользователей, т. е. фактически вышла из строя.

Из анализа построенной графовой модели атаки показано, что DDoS-атака может быть разделена на (s-1) обычных DoS-атак типа flood. Соответственно, в течение интервала времени z' успешной может считаться только одна DoS-атака (та, при которой сервер перестал быть доступен). Следовательно, атаки становятся зависимыми несовместными событиями.

Риск, абсолютная и относительная защищенность в этом случае определены как:

$$Risk(n,\lambda,s)=U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right),\ E_{абс}(n,\lambda,s)=1-U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right),$$

$$E_{отн}(\lambda,s)=\frac{\sum_{n=1}^{z}\left(1-U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right)\right)}{\sum_{n=1}^{z}U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right)}.$$

По аналогии математическое ожидание и дисперсия риска выражены следующим образом:

$$M(Risk)=\sum_{m=1}^{z}U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right)^2;$$

$$D(Risk)=\sum_{n=1}^{z}U^2{}_n\left(\frac{(s-1)\lambda^{U_n}e^{-2\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right)^3-\left(\sum_{n=1}^{z}U_n\left(\frac{(s-1)\lambda^{U_n}e^{-\lambda}}{U_n!}-\left(\frac{\lambda^{U_n}e^{-\lambda}}{U_n!}\right)^{s-1}\right)^2\right)^2$$

Рассмотренные понятия и найденные характеристики являются необходимой математической базой для оценки рисков и защищенности в компьютерных системах.

**В третьей главе** на основании анализа полученных риск-моделей при различных параметрах DoS-атак найдены аналитические выражения коэффициентов чувствительности и функций чувствительности. Приведены примеры расчета функций чувствительности для заданных параметров.

Анализ чувствительности связан с изучением влияния изменения модели (в данном случае риска) на изменение какого-либо параметра.

Полученная в данной работе модель позволяет найти для сервера, подвергающегося SYNflood-атаке, чувствительность риска $Risk(n,\lambda,s)$ к воздействию таких величин, как $\lambda$ (интенсивность атаки) и $s$ (количество атакующих).

Коэффициент чувствительности показывает, насколько изменится величина риска *Risk(n,λ,s)* при изменении одного из параметров $x_i$ данной величины, то есть фактически является «скоростью» изменения величины риска *Risk(n,λ,s)*, в точке x при $\Delta x_i \to 0$ относительно параметра $x_i$. Расчет коэффициентов чувствительности по всем параметрам $x_i$ позволяет определить именно тот параметр $x_m$, к изменению которого наиболее чувствительна величина риска (коэффициент чувствительности для параметра $x_m$ будет максимальным). Нахождение параметра $x_m$ повышает эффективность процесса минимизации величины риска, так как по найденному параметру $x_m$ риск минимизируется в первую очередь, что обеспечивает значительное снижение его величины уже на первом шаге алгоритма оптимизации.

Чувствительность риска *Risk(n,λ,s)* по параметру $\lambda$ для единичной DoS-атаки определена в следующем виде:

$$S_{\lambda}^{Risk} = \frac{U_n \cdot \lambda^{U_n-1} \cdot e^{-\lambda} - \lambda^{U_n} \cdot e^{-\lambda}}{(U_n-1)!} = \frac{\lambda^{U_n-1} \cdot e^{-\lambda} \cdot (U_n-\lambda)}{(U_n-1)!},$$

где $U_n$ – значение ущерба.

Из коэффициентов относительной чувствительности можно построить функцию чувствительности величины *Risk*. Функция чувствительности позволяет определить «интервалы монотонности» коэффициентов чувствительности и произвести минимизацию величины риска не только для отдельного значения ущерба, но и для всего диапазона ущербов в целом.

Относительная чувствительность риска *Risk(n,λ)* для единичной DoS-атаки аналитически выражена так:

$$S^{Risk} = \frac{\lambda^{U_n-1} \cdot e^{-\lambda} \cdot (U_n-\lambda)}{(U_n-1)!} \cdot \frac{(U_n-1)!}{\lambda^{U_n-1} \cdot e^{-\lambda}}$$

Отсюда матрица чувствительности для риска при одиночной DoS-атаке имеет вид:

$$S^{Risk}=[(U_n-\lambda)\lambda].$$

Аналогично определены коэффициенты чувствительности и функцию чувствительности для DDoS-атаки. Коэффициенты чувствительности и матрица чувствительности для сервера во время работы при DDoS-атаке аналитически выглядят следующим образом:

$$S_{\lambda}^{Risk} = \frac{U_n \cdot (s-1) \cdot (U_n-\lambda) \cdot \lambda^{U_n-1} \cdot e^{-\lambda}}{U_n!} \cdot \left(1 - \left(\frac{\lambda^{U_n} \cdot e^{-\lambda}}{U_n!}\right)^{s-2}\right),$$

$$S_{\lambda}^{Risk} = \frac{(U_n!)^{s-2} \cdot (s-1) \cdot (U_n-\lambda) - (\lambda^{U_n} \cdot e^{-\lambda})^{s-2}}{(s-1)\ (U_n!)^{s-2} - (\lambda^{U_n} \cdot e^{-\lambda})^{s-2}};$$

$$S_{\lambda}^{Risk} = \frac{U_n \cdot \lambda^{U_n} \cdot e^{-\lambda}}{U_n!} \cdot \left(1 - \left(\frac{\lambda^{U_n} \cdot e^{-\lambda}}{U_n!}\right)^{s-2} \cdot (U_n \cdot \ln(\lambda) - \ln(U_n!) - \lambda)\right),$$

$$\dot{S}_s^{Risk} = \frac{S\left((s-1)\cdot(U_n!)^{s-2} - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}\right)}{(U_n!)^{s-2}(U_n\cdot\ln(\lambda) - \ln(U_n!) - \lambda)\left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}};$$

$$S^{Risk} = \begin{bmatrix} \dfrac{(U_n!)^{s-2}\cdot(s-1)\cdot(U_n-\lambda) - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}}{(s-1)\cdot(U_n!)^{s-2} - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}} & \lambda \\ \dfrac{S\left((s-1)\cdot(U_n!)^{s-2} - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}\right)}{(U_n!)^{s-2}(U_n\cdot\ln(\lambda) - \ln(U_n!) - \lambda)\left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}} & S \end{bmatrix}$$

Аналогично для промежутка времени, когда сервер выходит из строя:

$$S_\lambda^{Risk} = \frac{U_n\cdot(s-1)\cdot\lambda^{2U_n-2}\cdot e^{-\lambda}\cdot(U_n-\lambda)\cdot\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}}{(U_n!)^s};$$

$$\dot{S}_\lambda^{Risk} = \frac{(s-1)\cdot(U_n-\lambda)\cdot\lambda^{U_n-1}}{U_n! - \lambda^{U_n}\cdot e^{-\lambda}};$$

$$S_s^{Risk} = \frac{U_n\cdot\lambda^{U_n}\cdot e^{-\lambda}\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right)^{s-1}}{(U_n!)^s}\cdot\left(\ln\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right) - \ln(U_n!)\right);$$

$$\dot{S}_s^{Risk} = s\cdot\left(\ln\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right) - \ln(U_n!)\right);$$

$$S^{Risk} = \begin{bmatrix} \dfrac{(s-1)\cdot(U_n-\lambda)\cdot\lambda^{U_n-1}}{U_n! - \lambda^{U_n}\cdot e^{-\lambda}} & \lambda \\ s\cdot\left(\ln\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right) - \ln(U_n!)\right) & S \end{bmatrix}$$

Построенные на основе полученных выражений графики позволяют получить динамические риск-модели при изменении параметров DoS-атак.

В течение DDoS-атаки уравнение движения риска будет иметь вид:

$$\Delta Risk(n,\lambda,s) = \frac{(s-1)\cdot(U_n-\lambda)\cdot\lambda^{U_n-1}}{U_n! - \lambda^{U_n}\cdot e^{-\lambda}}\cdot\Delta\lambda + \left(\ln\left(U_n! - \lambda^{U_n}\cdot e^{-\lambda}\right) - \ln(U_n!)\right)s\cdot\Delta s$$

Для интервала времени, в который сервер выходит из строя, уравнение движения:

$$\Delta Risk(n,\lambda,s) = \frac{(U_n!)^{s-2}\cdot(s-1)\cdot(U_n-\lambda) - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}}{(s-1)\cdot(U_n!)^{s-2} - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}}\cdot\Delta\lambda + \frac{S\left((s-1)\cdot(U_n!)^{s-2} - \left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}\right)}{(U_n!)^{s-2}(U_n\cdot\ln(\lambda) - \ln(U_n!) - \lambda)\left(\lambda^{U_n}\cdot e^{-\lambda}\right)^{s-2}}\cdot\Delta s$$

Полученные уравнения движения риска и его параметров позволяют отследить всю полноту движения показателей качества системы, определить скорость и другие динамические величины при изменении параметров исследуемого распределения (атаки).

**В четвертой главе** проводится обоснование критериев качества управления рисками; выполняется постановка задачи оптимального управления рисками; определяются оптимальные стратегии управления; на основе введенных ограничений на процесс управления разрабатывается алгоритм управления риском, основанный на оптимальных стратегиях.

Смысл понятия "качество управления риском" интуитивно ясен и в целом отражает уровень совершенства процессов управления. Вместе с тем примени-

тельно к управленческим задачам категория "качество" нуждается в анализе не только для раскрытия сущности этой категории, но и в целях четкой структуризации и формировании конкретных путей повышения качества управления.

Эффективность управления оценивается на основе критериев, показателей качества. Критерий качества представляет показатель, характеризующий качественные свойства управленческой деятельности и позволяющий сформировать суждение о ее качестве.

Существуют три группы критериев, позволяющих судить о качестве управления риском. 1) Целевые критерии. Это критерии актуальности, значимости, весомости конечных результатов работы, реальности, надежности получения ожидаемых результатов. 2) Критерии качества методов и организации управленческих работ. Сложность применения целевых критериев, характеризующих результативность управления, обусловлена неочевидностью получения желаемых итогов в процессе выработки управленческих решений и осуществления управления. По содержанию данные критерии делятся на три группы: критерии, характеризующие методическое совершенство работ; критерии, характеризующие технологическое совершенство; критерии, характеризующие организационное совершенство. 3) Критерии качества ресурсного обеспечения работ. Показатели, характеризующие ресурсное обеспечение, представляют косвенные оценки качества управленческих работ, однако они играют немаловажную роль в выработке суждений о качественном уровне этих работ.

С учетом вышеизложенного, в качестве критериев качества управления рисками можно использовать следующие показатели:

- эффективность управления риском:

$$Э_{УР} = \frac{Risk_{ДУ} - Risk_{ПУ}}{\text{Затраты на управление}},$$

где $Risk_{ДУ}$ - риск до применения алгоритма управления,

$Risk_{ПУ}$ - риск после применения алгоритма управления;

- экономическая эффективность управления риском:

$$\text{Эффективность} = \frac{\text{Прибыль от управления риском}}{\text{Затраты на управление}};$$

- уровень риска.

Полученные критерии качества позволяют учесть как результат управления - уровень риска, так и выбрать наиболее эффективный с точки зрения расходования материальных ресурсов способ управления.

Применение математического аппарата теории оптимального управления к рискам, описанным с помощью уравнений чувствительности, позволяет вскрыть математическую сущность процесса управления рисками.

Компьютерная система в общем виде – это конечномерная непрерывная система, зависящая от параметра. Наиболее общее математическое описание данного класса систем дают системы обыкновенных дифференциальных уравнений, в которых независимой переменной является время $t$. Состояние системы в каждый момент времени определяется несколькими величинами $x_1, x_2, \ldots, x_n$.

Имеется два вида ограничений на выбор способа управления. Ограничением первого вида являются законы природы, в соответствии с которыми происходит движение управляемой системы. Второй вид ограничений вызван ограниченностью ресурсов, используемых при управлении, или иных величин, которые в силу физических особенностей той или иной системы не могут или не должны превосходить некоторых пределов.

В качестве ограничения первого рода выступает уравнение движения риска. В качестве ограничений второго рода выступают критерии качества управления риском: $Risk \to min$; экономическая эффективность $E \geq 0$; интенсивность атаки $\lambda \in [0,4]$.

С помощью одношаговой задачи принятия решения проведена оптимизация риска по параметру $\lambda$ — интенсивность атаки для модели единичной DoS-атаки, разработанной ранее. Целевая функция для данной задачи имеет вид:

$$q = q(\lambda, t) = \frac{(\lambda t)^{U_n} e^{-\lambda t}}{(U_n - 1)!}.$$

Из построенной модели DDoS-атаки следует, что целевая функция системы будет зависеть от следующих параметров:
$\lambda$- интенсивность каждой из DoS-атак в рамках DDoS; $s$-количество атакующих.

Для этого случая будут существовать 2 целевые функции:
— в течение DoS-атаки до выхода системы из строя:

$$q(\lambda, s) = U\left(\frac{(s-1)\lambda^U e^{-\lambda}}{U!} - \left(\frac{\lambda^U e^{-\lambda}}{U!}\right)^{s-1}\right);$$

— в промежуток времени, когда система выходит из строя:

$$q(\lambda, s) = \frac{\lambda^U e^{-\lambda}}{(U-1)!}\left(1 - \frac{\lambda^U e^{-\lambda}}{U!}\right)^{s-1}.$$

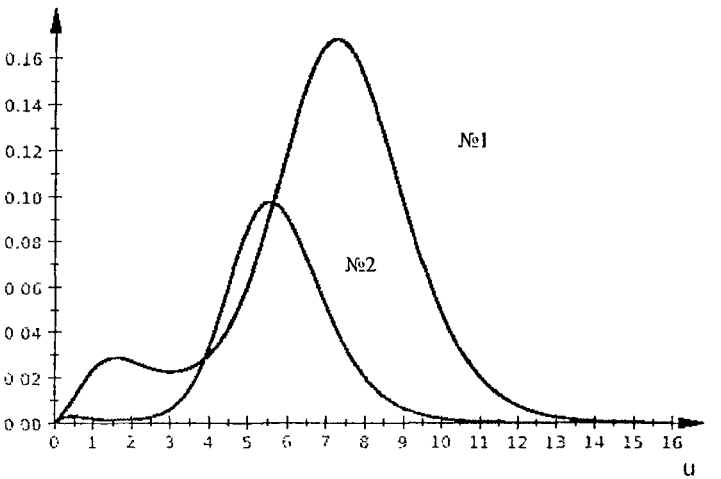
Для выбора наиболее подходящей стратегии управления необходимо определить существует ли зависимость между угрозами. Соответственно необходимо отнести исследуемое множество к одному из двух классов: множества независимых угроз; множество зависимых угроз. На практике чаще используются стратегии, считающие угрозы безопасности условно независимыми. Рассмотрим основные стратегии для множества независимых угроз: учет и ограничение рисков; устранение рисков (уклонение от рисков); устранение уязвимостей; игнорирование рисков; страхование рисков.

В качестве алгоритма минимизации риска предложено использовать численный алгоритм Нелдера-Мида, также известный как симплекс-алгоритм. Суть алгоритма состоит в последовательном перемещении и деформировании симплекса вокруг точки экстремума. На вход алгоритма подается функция $f_i(x^{(1)},\ldots,x^{(n)})$, для которой необходимо найти минимум; коэффициент отражения $\alpha>0$; коэффициент сжатия $\beta>0$; коэффициент растяжения $\gamma>0$; точность $\varepsilon>0$.

На подготовительном этапе выбирается $n+1$ точка $x_i=( x_i^{(1)},...,x_i^{(n)})$. Эти точки должны образовывать симплекс в $n$-мерном пространстве. Далее алгоритм повторяется до достижения нужной точности $\varepsilon$.

В качестве примера можно привести следующий график (рисунок), иллюстрирующий управление риском при решении задачи его минимизации.

На рисунке кривой №1 обозначен график зависимости риска от ущерба при DDoS-атаке (в промежуток времени, когда система выходит из строя) с параметрами $\lambda=4$ и $s=21$. Кривой №2 обозначен график после минимизации (предложенные алгоритмом параметры $\lambda=2,4$, $s=16$).




Пример минимизации риска с помощью алгоритма Нелдера-Мида

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработана и исследована математическая модель процесса SYNflood-атаки, направленной на отказ в обслуживании компьютерной системы. Данное исследовачие проводилось с учетом того, что компьютерная система представляет собой сложный объект, поэтому процесс атаки рассматривался с использованием распределения вероятностей Пуассона, что позволило учесть большинство особенностей такой системы, в частности:

- предметная область исследования определена как SYNflood-атаки на сервер, направленные на отказ в обслуживании;
- рассмотрена статистика сетевых пакетов при работе сервера в нормальных условиях и во время SYNflood-атаки;
- предложена характеристика активности сетевого обмена атакуемого сервера и доказано, что она распределена по Пуассону.

2. Получены аналитические выражения для расчета рисков и защищенности компьютерных систем, находящихся под воздействием SYNflood-атаки, направленной на отказ в обслуживании. Для этого было проведено исследование вероятностной природы информационных рисков для одиночных и распределенных атак, направленных на отказ в обслуживании, на основе данного исследования были найдены аналитические выражения для расчета рисков, как произведение величины ущерба на вероятность возникновения данного ущерба.

3. Найдены аналитические выражения функций чувствительности риска к изменению параметров безопасности компьютерных систем, подвергающихся SYNflood-атакам, направленным на отказ в обслуживании. В результате найдены аналитические выражения функций чувствительности риска к изменению параметров безопасности является ключевым моментом в процессе построения риск-модели и последующим нахождением формулы движения риска. С помощью полученной формулы движения риска можно проанализировать влияние параметров вероятностного распределения на функцию риска, а также возможно произвести минимизацию величины риска не только для отдельного значения ущерба, но и для всего диапазона ущербов в целом.

4. На основе аналитических выражений функций чувствительности величины риска разработаны алгоритмы управления рисками в компьютерных системах, подвергающихся SYNflood-атакам, направленным на отказ в обслуживании. Проведено соответствующее математическое моделирование данной проектной ситуации, исходя из того, что:

- в качестве критериев качества управления рисками предлагается использовать: экономическую эффективность управления риском и уровень риска;
- в качестве ограничения первого рода на процесс управления предложено уравнение движения риска;
- в качестве ограничений второго рода на процесс управления рассматриваются критерии качества управления риском;
- предложен алгоритм минимизации риска, с помощью которого проиллюстрирован метод расчета желаемых параметров атаки для сдвига максимума риска в сторону малых значений ущерба.

**Основные результаты диссертации опубликованы в следующих работах:**

**Публикации в изданиях, рекомендованных ВАК РФ**

1. Андреев Д.А. Атакуемые компьютерные системы и распределение Пуассонна // Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2008. Т. 11. Ч.2. С. 318.

2. Андреев Д.А., Пичугин А.К. Концепция управления рисками информационных атак на основе распределения Пуассона// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2008. Т. 11. Ч.3. С. 407-412.

3. Андреев Д.А. Относительная чувствительность к изменению параметров риск-модели// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2008. Т. 11.Ч.1. С. 148-149.

**Статьи и материалы конференций**

4. Андрев Д.А., Филиппов Ю.Е. Автоматизированные системы при значительном количестве атак и малых значениях вероятности успеха атаки: статистический риск-анализ и управление защищенностью // Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 343.

5. Анализ рисков применительно к автоматизированным системам с заданным количеством пораженных объектов/ Д.А. Андреев, А.В. Чулюков, Р.В. Батищев, А.С. Афанасьева // Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 347.

6. Андреев Д.А., Батищев А.В., Радько Н.М. Сетевые атаки автоматизированных систем: статистический риск-анализ и управление защищенностью // Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 358.

7. Андреев Д.А., Фурсов Д.М., Радько Н.М. Оценка отказоустойчивости узлов автоматизированных систем и доступности информации: статистический риск-анализ и управление защищенностью// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 359.

8. Андреев Д.А., Паршин А.Ю. Автоматизированные системы при непреднамеренных внешних воздействиях: статистический риск-анализ и управление защищенностью// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 360.

9. Андреев Д.А., Остапенко А.Г. Пуассоновское распределение в задачах обеспечения безопасности автоматизированных систем// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Вып.2. С. 367.

10. Андреев Д.А., Остапенко А.Г., Филиппов Ю.Е. К вопросу о принятии решения при управлении рисками// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Т. 10.Ч.3. С. 469.

11. Андреев Д.А., Щербаков В.Б., Филиппов Ю.Е. Выбор вероятностного закона распределения информационных атак на автоматизированные системы при построении вероятностной модели в заданных условиях// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Т. 10.Ч.3. С. 481.

12. Андреев Д.А., Филиппов Ю.Е. Дифференциальная чувствительность параметров риск-модели// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Т. 10.Ч.3. С. 491-495.

13. Андреев Д.А., Щербаков В.Б., Филиппов Ю.Е. Измерение рисков при значительном количестве атак и малых значениях вероятности успеха// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Т. 10.Ч.3. С. 499-503.

14. Андреев Д.А. Риски информационных систем при массовых кибератаках// Информация и безопасность: регион. науч.-техн. журнал. Воронеж. 2007. Т. 10.Ч.4. С. 618.

15. Андреев Д.А. Специфика управления рисками информационных систем при обилии малоуспешных кибер-атак//Современные информационные технологии в науке, образовании и практике: материалы VI Всерос. науч.-практ. конф. с междунар. участием. Секция «Вычислительные машины, комплексы и компьютерные сети». Оренбург, 2007. С. 197-199.

16. Андреев Д.А., Фролов С.Ю. Предметная область описания информационных конфликтов компьютерных систем с помощью распределения Пуассона//Информационные риски и безопасность: сб. науч. тр. Межрегион. науч.-практ. конф. Воронежского отделения Российской инженерной академии. Воронеж, 2007. С.47-51.

Подписано в печать 21.11.2008.
Формат 60x84/16. Бумага для множительных аппаратов.
Усл. печ. л. 1,0. Тираж 85 экз. Заказ № 605

ГОУВПО «Воронежский государственный технический университет»
394026 Воронеж, Московский просп., 14