На правах рукописи

Сердюк Виктор Александрович

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ ИНФОРМАЦИОННЫХ АТАК

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2004

Работа выполнена в «МАТИ» - Российском Государственном Технологическом Университете им. К.Э. Циолковского на кафедре «Информационные технологии»

Научный руководитель – кандидат технических наук, доцент
Авдошин Сергей Михайлович

Официальные оппоненты: доктор технических наук, профессор, академик РАН
Левин Владимир Константинович

кандидат технических наук
Скородумов Борис Иванович

Ведущая организация – Федеральное Государственное Унитарное Предприятие
Научно-Исследовательский Институт «Восход»

Защита диссертации состоится «25» января 2005 г. в 14 часов на заседании диссертационного совета Д. 212.133.03 в Московском Государственном Институте Электроники и Математики по адресу: 109028 Москва, Б.Трехсвятительский пер., д. 1-3/12, стр. 8.

С диссертацией можно ознакомиться в библиотеке Московского Государственного Института Электроники и Математики

Автореферат разослан «__» декабря 2004 г.

Ученый секретарь
диссертационного совета Д. 212.133.03,
кандидат физико-математических наук, доцент Прокофьев И.В.

Общая характеристика работы

Актуальность работы. В настоящее время для обработки, хранения и передачи информации повсеместно используются автоматизированные системы (АС). АС являются одним из краеугольных камней, на основе которых построены бизнес-процессы предприятий различных форм собственности и назначений. Однако за последние несколько лет наметилась тенденция к увеличению числа информационных атак на ресурсы АС, реализация которых привела к значительным материальным потерям. Так, например, согласно данным координационного центра CERT (http://www.cert.org), в 2003 г. было зафиксировано 137529 информационных атак, что почти в два раза превышает аналогичный показатель 2002 г. и в десятки раз выше числа атак, реализованных в 1999 году.

Изложенное выше говорит о высокой актуальности и значимости работ, проводимых в области обеспечения безопасности АС. В этой связи необходимо констатировать, что методологическая база теории информационной безопасности, как нового научного направления, в настоящее время находится в стадии формирования, о чём говорят работы ведущих отечественных и зарубежных исследователей в этой области, таких как В. Галатенко, В. Герасименко, А. Грушо, П. Зегжда, Д. Деннинг, К. Лендвер, М. Ранум и др. Важно подчеркнуть, что значительное внимание эти учёные уделяют разработке формальных моделей разграничения доступа, защищённых операционных систем и криптографической защиты информации. В тоже самое время вопросы, касающиеся разработки математических моделей информационных атак, процесса их обнаружения и оценки риска, пока не находят должного внимания. Это обосновывает актуальность исследований, проводимых в области разработки формальных моделей информационных атак на АС, а также способов защиты от них.

Цель и задачи работы. Целью диссертационной работы является повышение эффективности защиты АС от информационных атак. Для достижения поставленной цели в работе решались следующие основные задачи:

1. Систематизация и анализ существующих типов информационных атак, а также средств защиты АС.
2. Сравнительный анализ существующих математических моделей защиты АС от информационных атак, включая модели атак, модели процесса обнаружения атак и модели процесса оценки рисков безопасности.
3. Разработка новой математической модели информационных атак на АС, модели процесса выявления атак, а также модели процесса оценки рисков информационной безопасности с учётом выявленных недостатков существующих моделей.
4. Разработка действующего прототипа системы обнаружения атак, реализующего созданную модель выявления атак.
5. Разработка структуры системы обнаружения атак, предназначенной для промышленной реализации.

Методы исследования. При решении поставленных задач использован математический аппарат теории графов, теории множеств, теории автоматов и теории вероятностей.

Научная новизна проведённых исследований и полученных в работе результатов заключается в следующем:

1. Разработана классификационная схема информационных атак, которая, в отличие от существующих классификаций, позволяет учитывать взаимосвязь уязвимостей, атак и их возможных последствий.
2. Разработана математическая модель информационных атак, которая может быть использована для представления разных типов атак в виде графовых структур. В отличие от существующих моделей информационных атак она является многофакторной, что позволяет учитывать три основных параметра атаки – уязвимость, метод реализации атаки и её возможные последствия.
3. Разработана поведенческая модель процесса выявления атак на основе конечных автоматных распознавателей, которая, в отличие от существующих моделей, позволяет более эффективно выявлять как известные, так и новые типы информационных атак. Модель также предусматривает возможность прослеживания процесса принятия решения о выявлении атаки в АС.
4. Разработана модель процесса оценки рисков информационной безопасности, которая базируется на созданной графовой модели атак. Модель позволяет вычислять значение риска путём определения уровня ущерба от атаки, а также вероятности её реализации. При этом в процессе оценки риска могут использоваться количественные и качественные шкалы.

Практическая значимость работы состоит в следующем:

1. Разработан программный прототип системы обнаружения атак, предназначенный для защиты Web-сервера Microsoft Internet Information Services. Прототип базируется на созданной математической модели процесса выявления атак.
2. Разработана структура системы обнаружения атак, предназначенная для промышленной реализации.
3. Создана методика разработки рекомендаций по повышению уровня защиты АС от информационных атак.

Полученные результаты могут быть использованы при создании средств защиты АС от информационных атак и оценки их эффективности.

Достоверность полученных результатов подтверждается внутренней непротиворечивостью логики исследования, а также данными испытаний разработанного программного прототипа системы обнаружения атак.

Апробация работы. Основные теоретические и практические результаты работы обсуждались и получили одобрение на XX конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2002 г.), Второй и Четвёртой Международной научно-практической конференции «Моделирование. Теория, методы и средства» (Новочеркасск, 2002 и 2004 г.), Десятой юбилейной Международной студенческой школы-семинара «Новые информационные технологии» (Судак, 2002 г.), Второй всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты» (Сочи, 2003), Тринадцатой Международной научной конференции «Информатизация и информационная безопасность правоохранительных органов» (Москва, 2004 г.), а также на XXIX и XXX международных молодёжных научных конференциях «Гагаринские чтения» (Москва, 2003 и 2004 г.).

Основные положения и результаты диссертационной работы вошли в отчёты по научно-исследовательской работе по теме «Разработка предложений по технологии обеспечения информационной безопасности сети передачи данных дорожного уровня» (инвентарный номер 1872) и по специальной теме (инвентарные номера 14с, 15с, 82с и 83с), а также отражены в ряде работ, опубликованных в научно-технических журналах: "Информационные технологии", "Connect. Мир связи", "Сетевой журнал", "Системы безопасности и телекоммуникаций", "Ведомственные и корпоративные сети связи", "BYTE/Россия", "Сети и системы связи", "Informatica / Slovenia".

Публикации. По теме диссертации опубликовано 52 работы.

Основные положения, выносимые на защиту:

1. Классификация информационных атак, позволяющая учитывать взаимосвязь уязвимостей, атак и их возможных последствий.
2. Математическая модель информационных атак на АС, обеспечивающая возможность представления несанкционированных действий нарушителей в виде графовых структур.
3. Математическая модель процесса выявления атак, базирующаяся на конечных автоматных распознавателях и позволяющая эффективно выявлять известные и новые типы атак.
4. Математическая модель процесса оценки рисков безопасности, позволяющая вычислять значение риска с учетом уровня ущерба от атаки, а также вероятности её реализации.
5. Структурно-функциональная схема системы обнаружения атак, предназначенная для промышленной реализации.

Объём и структура работы. Диссертационная работа состоит из введения, четырёх глав, заключения и одного приложения. Основное содержание работы изложено на 171 странице, включая 74 рисунка, 34 таблицы и список литературы из 157 наименований.

Содержание работы

Во введении дана общая характеристика работы, сформулированы цель и задачи исследования, перечислены основные теоретические и практические результаты работы.

В первой главе рассмотрены базовые понятия информационной безопасности АС, приведено описание разработанной структурной модели АС, рассмотрена классификация информационных атак, а также дана характеристика функциональных возможностей существующих средств защиты АС.

В соответствии с целями проводимых исследований была разработана структурная модель АС как объекта защиты, которая представляет АС в виде совокупности взаимодействующих узлов. В качестве узлов могут выступать рабочие станции пользователей, серверы или коммуникационное оборудование. В разработанной модели каждый узел АС представлен тремя уровнями:

- уровнем аппаратного обеспечения. На этом уровне функционируют технические средства узла, такие как сетевые адаптеры, процессоры, микросхемы материнских плат и др.;
- уровнем общесистемного программного обеспечения, на котором функционирует операционная система узла и все её составные модули;
- уровнем прикладного программного обеспечения. На этом уровне функционирует программное обеспечение (ПО), обеспечивающее решение прикладных задач, для которых предназначена АС.

На каждом из узлов АС могут храниться и обрабатываться информационные ресурсы, доступ к которым может осуществляться посредством локального или сетевого взаимодействия. Локальное взаимодействие осуществляется при помощи элементов управления, непосредственно подключённых к узлам АС (например, консоли, клавиатуры, мыши и т.д.). Сетевое взаимодействие реализуется путём обмена с узлом информацией по каналам связи. Такая сетевая передача данных может быть представлена в виде семиуровневой модели взаимодействия открытых систем (ВОС), включающей в себя физический, канальный, сетевой, транспортный, сеансовый уровень, уровень представления, а также прикладной уровень. Помимо уровней модели ВОС, а также уровней аппаратного, общесистемного и прикладного ПО, в АС также присутствует уровень информационных ресурсов, на котором хранятся, обрабатываются и передаются данные. Типы и формат информационных ресурсов этого уровня определяются составом и конфигурацией используемого аппаратного и программного обеспечения АС.

Для проведения информационной атаки на АС нарушителю необходимо активизировать определённую уязвимость системы. Примерами уязвимостей АС могут являться: некорректная конфигурация сетевых служб АС, наличие ПО без установленных модулей обновления, использование нестойких к угадыванию паролей, отсутствие необходимых средств защиты информации и др. В

первой главе работы рассмотрена разработанная классификация информационных атак, в которой основным критерием классификации является этап жизненного цикла атаки, включающий четыре основные стадии:

1) *стадия рекогносцировки*. На этом этапе нарушитель осуществляет сбор информации об объекте атаки, на основе которой планируются дальнейшие стадии атаки;
2) *стадия вторжения в АС*. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех узлов АС, по отношению к которым совершается атака;
3) *стадия атакующего воздействия на АС*. Данный этап направлен на выполнение действий, направленных на нарушение конфиденциальности, целостности или доступности информации, в зависимости от тех целей, ради которых предпринималась атака;
4) *стадия дальнейшего развития атаки*. На этом этапе выполняются действия, направленные на продолжение атаки на ресурсы других узлов АС.

Другими критериями классификации атак являются: этап жизненного цикла АС, на котором совершается атака; степень преднамеренности реализации атаки; уровень модели ВОС, к которому может быть отнесена атака; источник атаки; объект атаки; степень активности и распределённости атаки; тип активизируемой уязвимости, а также тип последствия, к которому может привести атака. В соответствии с разработанной классификацией в работе рассмотрены механизмы реализации различных типов информационных атак, включая атаки типа «buffer overflow» (переполнение буфера), «SQL injection» (модификация SQL-запроса), «format string» («форматирующая строка») и др.

Разработанная классификационная схема информационных атак на АС, в отличие от существующих классификаций, позволяет учитывать взаимосвязь уязвимостей, атак и их возможных последствий. Созданная классификация также даёт возможность определить, к какому уровню структурной модели АС относится атака.

На основе разработанной классификации средств защиты АС был проведён анализ функциональных возможностей средств криптографической защиты информации, средств разграничения доступа, средств анализа защищённости, средств обнаружения атак и средств антивирусной защиты.

Во второй главе приводятся результаты исследований следующих типов математических моделей защиты АС от информационных атак:

- моделей информационных атак, предназначенных для воспроизведения необходимых свойств и характеристик атак. Модели этого типа позволяют в лабораторных условиях провести исследование характеристик определённой атаки для того, чтобы установить, какие средства защиты могут использоваться для её нейтрализации;
- моделей процесса обнаружения информационных атак, позволяющих формально описать процесс выявления атаки на ресурсы АС;

- моделей оценки рисков информационной безопасности АС, которые позволяют определить эффективность применения всей системы обеспечения безопасности АС в целом.

Проведенные исследования существующих типов *моделей информационных атак* позволили констатировать, что созданные в настоящее время модели классифицируются по следующим базовым критериям: тип представления модели; возможность расширения модели; возможность учёта в модели последовательности действий, выполняемых нарушителем в процессе проведения информационной атаки; уровень детализации модели. Показано также, что для эффективного использования моделей атак в процессе исследования возможных действий злоумышленника по отношению к АС они должны иметь следующие основные свойства:

- универсальность – позволяет использовать модель для представления различных типов атак вне зависимости от источника, объекта и средства реализации атаки;
- расширяемость – обеспечивает возможность добавления в модель новых характеристик атаки. Это свойство позволяет пользователю изменять состав характеристик моделируемых атак в зависимости от среды АС, в которой они рассматриваются;
- формализуемость – свойство, которое указывает на возможность использования математического аппарата для описания параметров модели;
- простота – даёт возможность пользователю легко воспринимать структуру и способы реализации моделируемой атаки;
- многофакторность – позволяет учитывать три основных параметра моделируемой информационной атаки: уязвимость, активизируемая атакой, способ реализации атаки и её возможные последствия.

Результаты проведённых исследований показали, что наиболее перспективными представляются две модели, разработанные Б. Шнайером и Санкт-Петербургским институтом информатики и автоматизации РАН, поскольку они обладают наибольшим числом вышеперечисленных свойств. Однако ни одна из этих моделей не позволяет одновременно учесть три основных параметра атаки – уязвимость, активизируемую атакой, метод её реализации и возможные последствия. Другими словами, модели не обладают свойством многофакторности.

Анализ существующих *моделей процесса обнаружения информационных атак* показал, что для выявления информационных атак в АС могут быть использованы два основных класса моделей – сигнатурные и поведенческие. Сигнатурные модели описывают каждую атаку в виде специальной сигнатуры, примером которой может являться строка символов, семантическое выражение на специальном языке, формальная математическая модель и др. Алгоритм использования сигнатурных моделей заключается в поиске сигнатур атак в исходных данных, в качестве которых могут выступать журналы аудита, пакеты данных и др. В случае обнаружения искомой сигнатуры фиксируется факт ин-

формационной атаки, которая соответствует найденной сигнатуре. Поведенческие модели, в отличие от сигнатурных, базируются не на моделях информационных атак, а на моделях штатного процесса функционирования АС. Принцип использования поведенческих моделей заключается в обнаружении несоответствий между текущим режимом функционирования АС и режимом штатной работы системы, который описывается при помощи параметров модели. Любое такое несоответствие рассматривается в рамках поведенческой модели как информационная атака.

В результате проведённых исследований была разработана классификация существующих моделей процесса обнаружения атак по следующим базовым критериям: тип модели; вид представления модели; тип математического аппарата, заложенного в модель; зависимость от наличия формализованного описания обнаруживаемых атак или штатного процесса функционирования АС. В процессе проводимых исследований были выделены следующие критерии, по которым можно определить эффективность модели процесса обнаружения атак:

- возможность выявления атак, описание которых известно и заложено в параметры модели;
- возможность выявления новых атак, описание которых ещё неизвестно;
- возможность идентификации процесса вывода результатов применения модели, т.е. возможность точного определения причин, по которым было принято решение о выявлении атаки;
- расширяемость – свойство, обеспечивающее возможность внесения в модель дополнительных параметров, позволяющих обнаруживать новые типы атак;
- формализуемость – свойство, которое указывает на возможность использования математического аппарата при описании параметров модели;
- простота – свойство, позволяющее быстро и удобно настраивать параметры модели;
- масштабируемость – свойство, которое позволяет не замедлять процесс использования модели при увеличении количества её параметров, позволяющих обнаруживать новые типы атак.

Результаты анализа сигнатурных моделей процесса обнаружения атак показывают, что на момент проводимых исследований наибольшей эффективностью обладала модель контекстного поиска информации, основанная на специализированных языках. Однако, принимая во внимание тот факт, что сигнатурные модели выявления атак не позволяют обнаруживать новые типы атак, использовать их целесообразно совместно с поведенческими моделями. В тоже время полученные результаты показывают, что рассмотренные в работе поведенческие модели процесса обнаружения атак не способны эффективно выявлять новые типы атак.

Анализ существующих *моделей процесса оценки рисков безопасности* показал, что эти модели могут быть сгруппированы в два основных класса: 1) модели, предназначенные для оценки рисков путём определения степени со-

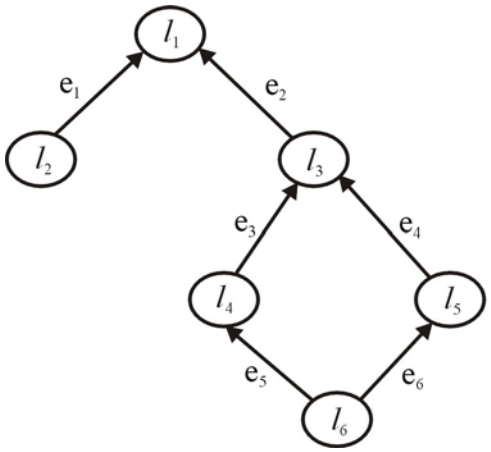
ответствия текущего уровня защиты АС заданному множеству требований безопасности; 2) модели, предназначенные для оценки рисков посредством определения вероятности проведения атак и уровня ущерба от них. В результате проведенных работ показано, что модели оценки рисков первого типа, могут быть использованы для эффективной проверки организационных мер защиты, применяемых в АС. Однако для оценки эффективности применяемых технических средств защиты целесообразнее использовать модели второго типа, позволяющие учитывать вероятность атаки и уровень ущерба. Тем не менее, результаты проведённых исследований показали, что эти модели имеют ряд следующих недостатков: отсутствие формализации, невозможность оценки риска сценариев атак, состоящих из нескольких этапов, а также высокая сложность настройки параметров моделей.

В третьей главе представлены результаты исследований по созданию новых математических моделей защиты АС от информационных атак. В процессе разработки моделей были учтены недостатки существующих типов моделей, рассмотренных во второй главе диссертационной работы.

Разработанная в процессе проведения исследований *математическая модель информационной атаки* базируется на следующих трёх основных множествах: V – множество уязвимостей АС, A – множество методов реализации атак и C – множество последствий атак. Для описания взаимосвязи между элементами множеств A, V и C определено тернарное отношение W на множестве $U = A \times V \times C$. Принадлежность элемента (a,v,c) отношению W, где $a \in A, v \in V, c \in C$, интерпретируется следующим образом: «Информационная атака, реализуемая нарушителем методом a путём активизации уязвимости v, и приводящая к последствию c».

Созданная математическая модель атаки представлена в виде графа $G=(L,E)$, где L – множество вершин графа, а $E \subset L^2$ - множество дуг графа. Для графа G определено отношение $T \in \{E \times W\}$, которое каждой дуге из множества E ставит в соответствие один или более элементов отношения W. Использование отношения T позволяет интерпретировать каждую дугу графа G как один из этапов моделируемой информационной атаки. При этом в отношении T одной дуге $e \in E$ может соответствовать одновременно несколько элементов множества W только при условии, что эти элементы обозначают атаки, приводящие к одним и тем же последствиям. В каждую вершину графа G может входить одновременно несколько дуг только при условии, что в отношении T каждой такой дуге соответствуют элементы множества W, описывающие атаки, которые приводят к одинаковым последствиям. Таким образом, вершины графа G могут объединять различные этапы атаки, приводящие к идентичным последствиям.

На рис. 1 показан пример графа G, описывающего произвольную информационную атаку, а также отношение T, которое определяет этапы атаки, моделируемые при помощи дуг графа G.



T = {(e1,(a1, v2, c1)),
(e2,(a2, v2, c1)),
(e3,(a1, v3, c4)),
(e4,(a3, v3, c4)),
(e5,(a2, v4, c2)),
(e6,(a2, v5, c3)) }

Рис. 1. Пример взвешенного графа G, описывающего произвольную атаку

Граф G, изображённый на рис. 1, представляет собой модель информационной атаки, успешная реализация которой приводит к последствию $c_1 \in C$. Структура графа G позволяет определить все возможные сценарии действий нарушителя в моделируемой атаке. Формально сценарии проведения атаки представлены множеством возможных путей в графе G - Gp, где каждый путь $gp \in Gp$ представляет собой последовательность дуг $(e_{p_1}, e_{p_2}, ..., e_{p_n})$ вида $e_{p_k} = (l_i, l_j),\ l_i, l_j \in L$, при этом конечная вершина дуги e_{p_k} одновременно является начальной вершиной дуги $e_{p_{k+1}}$. В качестве начальной вершины пути могут выступать такие вершины $l \in L$ графа G, полустепень захода которых равна 0. Конечной же вершиной пути может являться только такая вершина l, полустепень исхода которой равна 0.

Множество путей Gp для графа, изображённого на рис. 1, имеет следующий вид: $Gp = \{\{(l_2,\ l_1)\},\ \{(l_6,\ l_4),\ (l_4,\ l_3),\ (l_3,\ l_1)\},\ \{(l_6,\ l_5),\ (l_5,\ l_3),\ (l_3,\ l_1)\}\}$. Таким образом, к последствию $c_1 \in C$ может привести один из трёх следующих сценариев реализации атаки:

1) реализация атаки методом $a_1 \in A$, активизирующим уязвимость $v_2 \in V$, приводящим к последствию $c_1 \in C$ ($gp_1 = (e_1),\ (e_1, (a_1, v_2, c_1)) \in T$);
2) реализация атак при помощи методов $a_2, a_1, a_2 \in A$, активизирующих уязвимости $v_4, v_3, v_2 \in V$ и приводящих к последствиям $c_2, c_4, c_1 \in C$, соответственно ($gp_2 = (e_5, e_3, e_2)$, $\{(e_5, (a_2, v_4, c_2)), (e_3, (a_1, v_3, c_4)),\ (e_2, (a_2, v_2, c_1))\} \in T$);
3) реализация атак при помощи методов $a_2, a_3, a_2 \in A$, активизирующих уязвимости $v_5, v_3, v_2 \in V$ и приводящих к последствиям $c_3, c_4, c_1 \in C$, соответственно ($gp_3 = (e_6, e_4, e_2), \{(e_6, (a_2, v_5, c_3)), (e_4, (a_3, v_3, c_4)),\ (e_2, (a_2, v_2, c_1))\} \in T$).

В диссертационной работе продемонстрировано практическое использование разработанной модели на примере создания графов информационных атак на ресурсы Web-портала, подключенного к сети Интернет.

Разработанная математическая модель информационной атаки обладает свойством универсальности, поскольку может быть использована для представ-

ления разных типов атак, и является расширяемой за счёт возможности добавления новых параметров в модель атаки. Модель предусматривает возможность как текстового, так и графического изображения в виде графа. Модель может быть представлена в формализованном виде при помощи математического аппарата теории графов. В отличие от существующих моделей информационных атак она характеризуется многофакторностью, что позволяет учитывать три основных параметра атаки – уязвимость, метод реализации атаки и её возможные последствия. Наличие всех этих свойств позволяет сделать вывод о том, что использование разработанной модели позволяет более продуктивно исследовать особенности моделируемых информационных атак и, следовательно, более эффективно выбирать средства защиты от этих атак.

Созданная *поведенческая модель процесса обнаружения атак* обеспечивает возможность обнаружения атак путём выявления сетевых запросов, которые нарушают штатный протокол сетевого взаимодействия между узлами АС. Ниже приведены примеры таких сетевых запросов, обнаружение которых в АС может являться признаком проведения информационных атак:

- запросы, синтаксис и семантика которых не соответствует стандартам RFC, описывающим протоколы сетевого взаимодействия между узлами АС;
- запросы к несуществующим информационным ресурсам АС;
- запросы, обработка которых не поддерживается ПО АС;
- запросы, длина которых превышает заданные ограничения.

Разработанная модель базируется на автоматном языке L, который описывает штатный протокол сетевого взаимодействия узлов АС. Язык L состоит из цепочек, каждая из которых соответствует штатному сетевому запросу, который может быть корректно обработан общесистемным и прикладным ПО АС и не представляет угрозы для безопасности системы. При этом язык L задаётся при помощи конечного автомата-распознавателя следующего вида - $A =< S, X, Y, s_0, \delta, \lambda, F, s_a >$, где:

- S - множество состояний;
- X - множество входных символов;
- Y - множество семантических операторов, выполняющих функции анализа данных, поступающих на вход автомата;
- $s_0 \in S$ - начальное состояние автомата;
- $\delta : S \times X \to S$ - функция переходов;
- $\lambda : S \times X \to Y$ - функция определения семантического оператора, который выполняется при анализе очередного входного символа;
- $F \subseteq S$ - множество заключительных состояний, в которые переходит автомат при корректном распознавании цепочки языка L;
- $s_a \in S$ - заключительное состояние, в которое переходит автомат в том случае, если ему на вход поступает цепочка символов, не являющаяся элементом языка L.

На вход конечному автомату, задающему язык L, подаётся для анализа цепочка символов, которая соответствует сетевому запросу, поступающему к защищаемому узлу АС. Если в результате обработки входной цепочки символов автомат переходит в одно из своих заключительных состояний F, то это означает, что анализируемый сетевой запрос не представляет угрозы для АС и не используется для проведения информационной атаки. В противном случае, если автомат перейдёт в состояние s_a или в результате выполнения одного из своих семантических операторов будет остановлена работа автомата, то это будет означать факт выявления сетевой атаки в АС.

Поведенческая модель, основанная на конечноавтоматных распознавателях, рассмотрена на примере модели процесса выявления сетевых атак на Web-серверы, взаимодействие с которыми осуществляется по протоколу HTTP. Для обнаружения таких атак на основе созданной модели был разработан конечный автомат A_{HTTP}. Автомат A_{HTTP} распознаёт язык L_{HTTP}, состоящий из цепочек, определяющих все возможные типы штатных HTTP-запросов, которые могут быть корректно обработаны защищаемым Web-сервером. Структура конечного автомата A_{HTTP}, выполняющего функции обработки входных цепочек символов, включает в себя следующие пять составных блоков (рис. 2):

- блок распознавания и анализа типа метода формирования HTTP-запроса;
- блок распознавания и анализа идентификатора ресурса HTTP-запроса;
- блок распознавания и анализа параметров доступа к ресурсу Web-сервера;
- блок распознавания и анализа версии HTTP-протокола;
- блок распознавания и анализа заголовков HTTP-запроса.

Рис. 2. Структура конечного автомата A_{HTTP}

Принцип работы конечного автомата A_{HTTP} заключается в выявлении потенциально опасных HTTP-запросов, структура и содержимое которых нарушает штатный протокол сетевого взаимодействия с Web-сервером, заданный при помощи языка L_{HTTP}.

Созданная поведенческая модель процесса выявления атак, в отличие от существующих, позволяет выявлять как известные, так и новые атаки, функционируя при этом в режиме «белого ящика» и обеспечивая возможность полностью прослеживать процесс принятия решения о выявлении атаки в АС. Разработанная модель может быть задана в формализованном виде на основе аппарата теории графов. Модель обнаружения атак расширяема, что даёт возможность добавлять новые параметры, необходимые для выявления информационных атак. С учетом этих свойств можно утверждать, что разработанная поведенческая модель позволяет более эффективно обнаруживать атаки в АС в сравнении с аналогичными моделями, рассмотренными во второй главе диссертационной работы.

Разработанная *модель процесса оценки рисков информационной безопасности АС* разделяет процесс проведения оценки на следующие основные этапы:

1) этап формирования множества, элементами которого являются защищаемые информационные ресурсы АС;
2) этап формирования множества, элементами которого является программное и аппаратное обеспечение, используемое для обработки, хранения или передачи защищаемых информационных ресурсов АС;
3) этап определения информационных потоков доступа пользователей АС к защищаемым ресурсам АС;
4) этап формирования множества, элементами которого являются средства защиты АС;
5) этап оценки возможного ущерба в случае нарушения конфиденциальности, целостности или доступности защищаемых ресурсов;
6) этап оценки вероятности проведения атак на защищаемые информационные ресурсы;
7) этап расчета значения рисков информационной безопасности.

Все этапы процесса оценки рисков выполняются рабочей группой, состоящей из экспертов в области информационной безопасности, при участии представителей организации-владельца АС.

На первых четырёх этапах формируются множества защищаемых информационных ресурсов, средств защиты, программного и аппаратного обеспечения, а также множество пользователей и их прав доступа к информации. После этого определяется логическая взаимосвязь между этими множествами, которая схематично изображена на рис. 3.

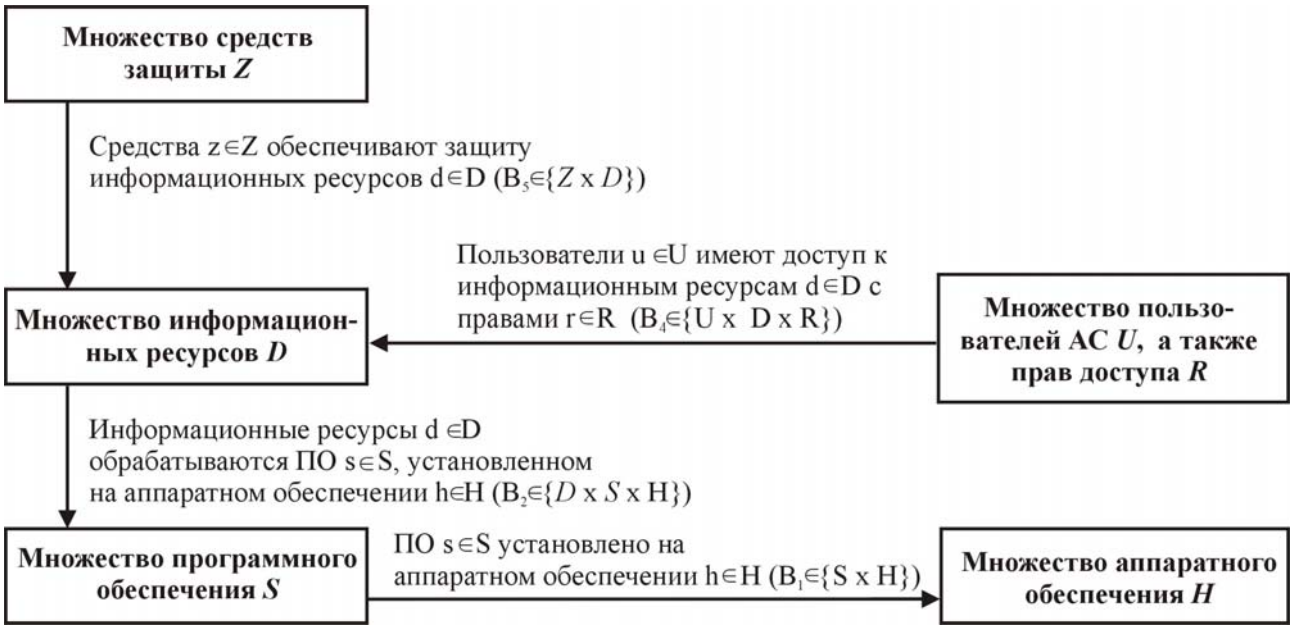


Рис. 3. Схема взаимосвязи между элементами множеств D, S, H и Z

Пятый этап оценки рисков предполагает оценку ущерба, который может быть нанесён в случае успешной атаки на защищаемые информационные ресурсы АС. Оценка ущерба проводится по отношению к трём возможным последствиям атаки – нарушению конфиденциальности, целостности или доступности информационного ресурса АС. На шестом этапе оценки рисков определяется вероятность того, что в случае проведения атак на защищаемые ресурсы будут успешно преодолены все средства защиты, используемые в АС. В этих целях для каждого информационного ресурса разрабатываются графовые модели возможных атак, направленных на нарушение конфиденциальности, целостности или доступности ресурса. На основе этих графовых моделей рассчитывается вероятность проведения информационной атаки при помощи метода экспертных оценок. На седьмом этапе оценки рисков вычисляется значение риска на основе ранее определённого уровня ущерба и вероятности атак. Для каждого защищаемого информационного ресурса вычисляются три значения риска – риск нарушения конфиденциальности, целостности и доступности ресурсов АС.

Проиллюстрированы особенности применения разработанной модели на примере оценки рисков информационной безопасности Web-портала. На базе модели оценки рисков создана методика разработки рекомендаций по повышению уровня защиты АС от информационных атак.

Разработанная модель оценки рисков информационной безопасности базируется на графовой модели атак, что позволяет описать её в терминах математического аппарата теории графов, а также обеспечить возможность текстового и графического представления модели. Модель позволяет вычислить значение риска путём определения уровня ущерба от атаки, а также вероятности её реализации. При этом в процессе оценки риска могут использоваться количественные и качественные шкалы. Созданная модель оценки учитывает три воз-

можных последствия атак: нарушение конфиденциальности, целостности и доступности информации. Модель позволяет также вычислять значение риска безопасности для сложных сценариев атак, состоящих из нескольких этапов реализации. Таким образом, обладая этими свойствами, разработанная модель позволяет проводить оценку рисков информационной безопасности более эффективно в сравнении с аналогичными моделями, рассмотренными во второй главе диссертационной работы.

В четвёртой главе приведено описание прототипа системы обнаружения атак (СОА), разработанного на основе созданной поведенческой модели выявления атак. Прототип СОА был реализован в виде активного ISAPI-фильтра, предназначенного для выявления и блокирования атак на Web-сервер Microsoft Internet Information Services. Общая структура разработанного прототипа СОА, реализующего поведенческую модель выявления атак, изображена на рис. 4.

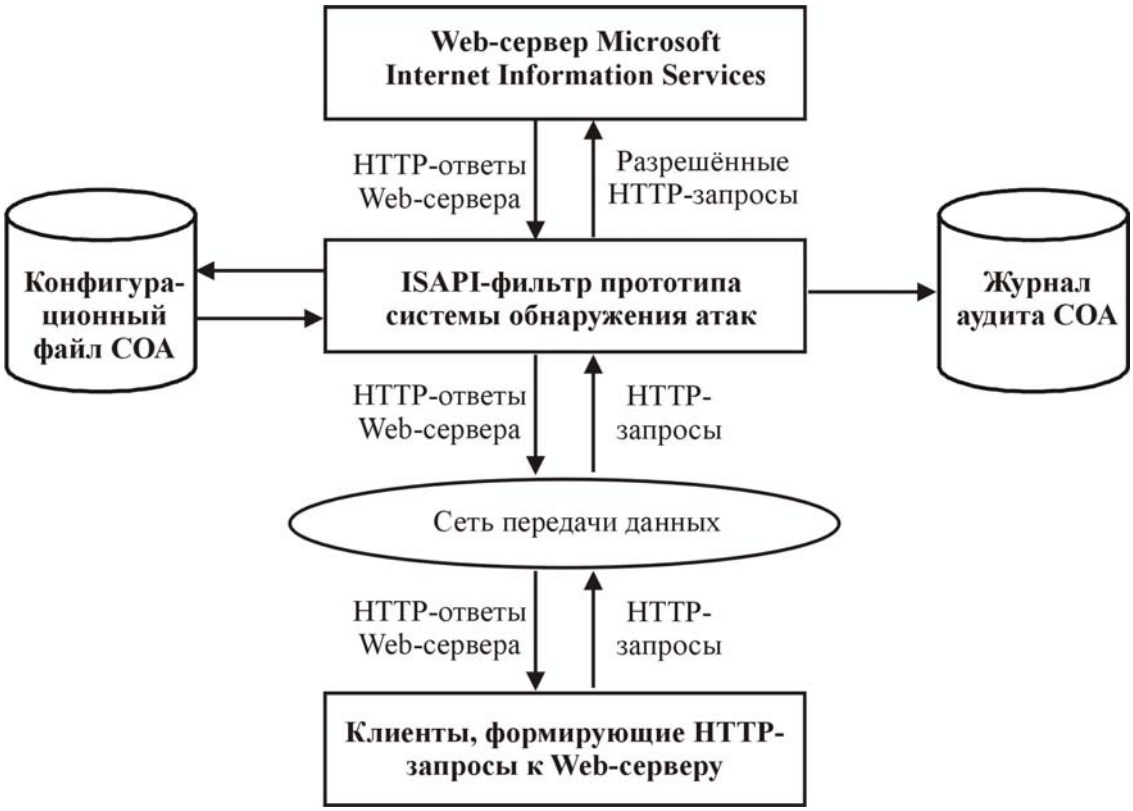


Рис. 4. Структура прототипа системы обнаружения атак

Проведённые испытания прототипа СОА позволили установить следующее: прототип позволяет эффективно выявлять и блокировать как известные, так и новые типы атак; прототип не снижает производительности работы защищаемого им Web-сервера; конфигурационный файл прототипа позволяет гибко настраивать систему на выявление новых классов атак.

В четвёртой главе приводится также описание структуры промышленного варианта СОА, который должен включать в себя следующие компоненты:

- сетевые датчики, предназначенные для обнаружения атак в рамках того сегмента АС, где они установлены;
- хостовые датчики, устанавливаемые на серверы АС и обеспечивающие защиту определённых сетевых сервисов системы;
- модули-агенты, выполняющие функции управления датчиками, а также обеспечения передачи данных между датчиками и модулем координации;
- модуль координации, выполняющий функции маршрутизации информации, передаваемой между компонентами СОА;
- информационный фонд, который выполняет функции централизованного хранения конфигурационной информации, а также результатов работы СОА;
- модуль реагирования на информационные атаки;
- консоль администратора, предназначенная для централизованного управления компонентами СОА.

В заключении приведены основные результаты, полученные в процессе проводимых исследований.

Приложение содержит копию документа, подтверждающего внедрение результатов диссертационной работы.

В работе получены следующие основные результаты:

1) Разработана классификация информационных атак, учитывающая взаимосвязь уязвимостей, атак и их возможных последствий.
2) Разработана математическая модель информационных атак, которая может быть использована для представления разных типов атак в виде графовых структур.
3) Разработана поведенческая модель процесса выявления информационных атак, позволяющая эффективно выявлять известные и новые типы атак.
4) Разработана математическая модель процесса оценки рисков безопасности, которая позволяет вычислять значение риска посредством определения уровня ущерба от атаки, а также вероятности её реализации.
5) Разработан прототип системы обнаружения атак на основе созданной поведенческой модели процесса выявления атак.
6) Разработана структурно-функциональная схема СОА, предназначенная для промышленной реализации.

Основные результаты диссертационной работы изложены в 52 научных трудах. Ниже приведены основные из них:

1. Сердюк В.А. Технологии несанкционированных воздействий на Интернет //Приложение к журналу «Информационные технологии». 2001. №5. с. 1-24.
2. Сердюк В.А. Новое в технологиях обнаружения атак на информационную сферу сетей связи. //Ведомственные корпоративные сети связи. 2001. №4. с. 19-28.
3. Сердюк В.А. Математическая модель оценки уровня защищённости сетей передачи данных //Тезисы II Международной научно-практической конференции «Моделирование. Теория, методы и средства». Новочеркасск. 2002. с. 31-34.
4. Сердюк В.А. Классификация угроз информационной безопасности сетей связи, их уязвимостей и атак нарушителя //Информационные технологии. 2002. №9. с. 7-12.
5. Avdoshin Sergey, Serdiouk Victor. Some approaches to information security of communication networks. // Slovenia. Informatica. 2002. №26. с. 1-10.
6. Сердюк В.А. Перспективы развития новых технологий обнаружения информационных атак //Системы безопасности связи и телекоммуникаций. 2002. №5. с. 82-84.
7. Сердюк В.А. Предотвращение информационных атак //Сетевой журнал. 2003. №2. с. 62-67.
8. Сердюк В.А. Сбор данных системами обнаружения атак //BYTE/Россия. 2003. №2 (54). с. 74-78.
9. Сердюк В.А. Защищённость информационной сферы глобальных сетей передачи данных //Приложение к журналу «Информационные технологии». 2003. №3. с. 1-24.
10. Сердюк В.А. Математическая модель поведенческого метода обнаружения информационных атак //Тезисы Международной молодёжной научной конференции «XXIX Гагаринские чтения». Москва. МАТИ. 2003. n. 5, с. 5 – 6.
11. Сердюк В.А. Математическая модель поведенческого метода обнаружения атак, базирующаяся на конечных автоматных распознавателях // Тезисы IV Международной научно-практической конференции «Моделирование. Теория, методы и средства». Новочеркасск. 2004. с. 8-13.
12. Сердюк В.А. Анализ современных тенденций построения моделей информационных атак. //Информационные технологии. 2004. №5. с. 20-26.