На правах рукописи

СВЕЧНИКОВ Лаврентий Александрович

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2010

Работа выполнена
на кафедре вычислительной техники и защиты информации
Уфимского государственного авиационного технического университета

Научный руководитель	д-р техн. наук, проф. Васильев Владимир Иванович
Официальные оппоненты	д-р техн. наук, проф. Миронов Валерий Викторович проф. каф. автоматизированных систем управления Уфимского государственного авиационного технического университета
	канд. техн. наук, доц. Цветов Виктор Петрович доц. кафедры безопасности информационных систем Самарского государственного университета
Ведущая организация	Башкирский государственный университет

Защита состоится «18» июня 2010 г. в 10 часов

на заседании диссертационного совета Д-212.288.07

Уфимского государственного авиационного технического университета по адресу: 450000, г. Уфа, ул. К.Маркса 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «___»_____2010 г.

Ученый секретарь
диссертационного совета,
д-р. техн. наук, проф. С.С. Валеев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В связи с увеличением объемов информации, циркулирующих в локальных вычислительных сетях (ЛВС) и расширением спектра задач, решаемых с помощью информационных систем (ИС), возникает проблема, связанная с ростом числа угроз и повышением уязвимости информационных ресурсов. Это обусловлено действием таких факторов, как:

- расширение спектра задач, решаемых ИС;
- повышение сложности алгоритмов обработки информации;
- увеличение объемов обрабатываемой информации;
- усложнение программных и аппаратных компонентов ЛВС, и соответственно – повышение вероятности наличия ошибок и уязвимостей;
- повышение агрессивности внешних источников данных (глобальных сетей);
- появление новых видов угроз.

Необходимо учитывать, что конкурентоспособность предприятий, размер получаемого ими дохода, их положение на рынке существенно зависят от корректности функционирования их информационной инфраструктуры, целостности основных информационных ресурсов, защищенности конфиденциальной информации от несанкционированного доступа. Исходя из этого, возрастают требования к системам защиты ЛВС, которые должны обеспечивать не только пассивное блокирование несанкционированного доступа к внутренним ресурсам сети предприятия из внешних сетей, но и осуществлять обнаружение успешных атак, анализировать причины возникновения угроз информационной безопасности и, по мере возможности, устранять их в автоматическом режиме.

Одним из основных качеств системы защиты информации ЛВС предприятия, удовлетворяющей перечисленным требованиям, является ее адаптивность, т.е. способность анализировать информацию, генерировать на ее основе знания и автоматически изменять конфигурацию системы для блокирования обнаруженных угроз информационной безопасности.

Анализ существующих подходов к реализации систем обнаружения атак показывает, что большинство программных продуктов, присутствующих в настоящее время на рынке, ориентируется на использование формальных описаний системной активности (сигнатур). Функции обнаружения и регистрации новых видов атак возлагаются в подобных системах на разработчика, выпускающего новые сигнатуры. Данный метод защиты является ненадежным, т.к. он ставит защищенность ИС в зависимость от действий внешнего неконтролируемого источника.

Несмотря на то, что разработка адаптивных систем защиты информации ведется уже достаточно длительное время, ни одно подобное решение не получило сколько нибудь широкого распространения в силу сложности и малоэффективности используемых алгоритмов, отсутствия в большинстве случаев

адекватных инструментов их развертывания и администрирования, а также – пользовательской документации.

Анализ работ, ведущихся в данной области, показывает, что указанная проблема требует дальнейшего изучения как с точки зрения построения адекватных математических моделей предметной области, так и реализации эффективных алгоритмов обнаружения атак и принятия решений, что подтверждает актуальность исследований в данной предметной области.

Объект исследований – система защиты информации корпоративной информационной системы.

Предмет исследований – алгоритмическое и программное обеспечение защиты информации.

Цель работы

Повышение эффективности обнаружения атак и принятия решений на основе оперативной оценки риска функционирования ИС с использованием динамических моделей на основе нечетких когнитивных карт.

Задачи исследования

Для достижения поставленной цели в работе были поставлены и решены следующие задачи:

1. Разработка системных моделей функционирования системы обнаружения атак на основе построения онтологии предметной области и использования SADT-методологии.
2. Синтез архитектуры системы обнаружения атак и алгоритмов принятия решений на основе динамической модели оценки рисков с использованием нечетких когнитивных карт.
3. Разработка алгоритма обучения нечеткой когнитивной карты на наборе эталонных сценариев.
4. Разработка исследовательского прототипа интеллектуальной системы обнаружения атак.
5. Анализ эффективности функционирования разработанной интеллектуальной системы обнаружения атак методом имитационного моделирования.

Методы исследования

В процессе исследования использовались методы системного анализа, теории вероятности, нечеткой логики, теории Марковских цепей и ветвящихся процессов, нечетких когнитивных карт, теории нейронных сетей, методы распознавания образов, математической статистики и информатики. Моделирование осуществлялось с использованием системного и прикладного программного обеспечения, разработанного автором.

Результаты, выносимые на защиту

1. Системные модели системы обнаружения атак на основе SADT-методологии.
2. Архитектура системы обнаружения атак, алгоритмы принятия решений на основе динамического моделирования с использованием нечетких когнитивных карт.
3. Алгоритм обучения нечеткой когнитивной карты на наборе эталонных сценариев.

4. Программная реализация исследовательского прототипа интеллектуальной системы обнаружения атак.

5. Результаты оценки эффективности функционирования интеллектуальной системы обнаружения атак.

Научная новизна диссертационной работы заключается в следующем:

1. Разработан комплекс системных моделей функционирования системы обнаружения атак на основе построения онтологии предметной области и использования SADT-методологии, которые позволяют выявить основные источники угроз, уязвимости и защищаемые ресурсы, сформулировать требования к архитектуре системы обнаружения атак.

2. Предложены архитектура системы обнаружения атак и алгоритмы распознавания атак, основанные на использовании динамических моделей информационной системы на базе нечетких когнитивных карт, что в отличие от существующих подходов на основе анализа базы сигнатур, позволяет повысить эффективность обнаружения атак, а также расширить сферу защищаемых ресурсов ИС за счет моделирования рисков в режиме реального времени.

3. Предложен алгоритм обучения нечеткой когнитивной карты на наборе эталонных данных, основанный на алгоритме обратного распространения ошибки, позволяющий существенно повысить точность распознавания и блокирования атак.

Практическая ценность

Практическая ценность данной работы заключается в следующем:

1. Предложенные системные модели и методы оценки риска функционирования ИС могут использоваться на ранних этапах разработки систем защиты информации для оценки их эффективности.

2. Разработанные алгоритмы обнаружения и подавления атак позволяют осуществлять защиту ИС в режиме реального времени.

3. Использование предложенной архитектуры интеллектуального модуля принятия решений позволяет увеличить эффективность систем обнаружения атак и снизить величину риска функционирования ИС.

Апробация работы

Основные положения, представленные в диссертационной работе, докладывались и обсуждались на следующих конференциях:

– Международной молодежной научно - технической конференции "Интеллектуальные системы обработки информации и управления", (г. Уфа 2003);

– VII и VIII международной научной конференции «Компьютерные, науки и информационные технологии» (CSIT’), (г. Уфа, 2005, г. Карслсруэ, Германия, 2006);

– VIII Международной научно-практической конференции "Информационная безопасность" (г. Таганрог, 2006);

- Региональной зимней школе – семинаре аспирантов и молодых ученых "Интеллектуальные системы обработки информации и управления", (г. Уфа, 2007);

– VII Всероссийском конкурсе студентов и аспирантов по информационной безопасности «SIBINFO-2007» (г. Томск, 2007);

– Всероссийской зимней школе-семинаре «Актуальные проблемы науки и техники» (г. Уфа, 2010).

Разработанный программный комплекс, реализующий исследовательский прототип интеллектуальной системы обнаружения атак, внедрен в проектном институте «РН-УфаНИПИНефть».

Результаты работы также внедрены в учебный процесс Уфимского государственного авиационного технического университета и используются на кафедре «Вычислительная техника и защита информации» при проведении лабораторных работ, выполнении курсовых и дипломных проектов для студентов специальности 090104.

Публикации

Результаты диссертационной работы отражены в 10 публикациях, в том числе в 3 научных статьях, из них 1 статья в издании из перечня ВАК РФ, а также в 6 материалах докладов международных и российских конференций, 1 свидетельстве об официальной регистрации программы.

Структура работы

Диссертация состоит из введения, четырех глав, заключения и списка литературы. Работа содержит 135 страниц машинописного текста, включая 31 рисунок и 27 таблиц. Список литературы включает 114 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении к диссертации дается краткая характеристика работы, сформулированы ее цели и задачи, обоснована актуальность исследований в данной предметной области, показана научная новизна и практическая ценность полученных результатов.

В первой главе выполнен анализ современного состояния предметной области, описаны задачи, решаемые с помощью автоматизированных информационных систем локальных вычислительных сетей (ИС ЛВС), перечислены основные подходы к их моделированию. Произведена классификация систем управления функционированием ИС ЛВС, выделен класс систем обнаружения атак (СОА), описаны его функции и основные возможности. На основе анализа существующих систем обнаружения атак, представленных в настоящее время на рынке и сформулированной системы критериев, показано, что функционал существующих систем обнаружения атак не позволяет им обеспечивать корректное обнаружение и блокирование неизвестных атак. Таким образом, исследования в данной предметной области являются актуальными и перспективными.

Во второй главе сформирован тезаурус терминов на основе которого построена онтология предметной области. На основе онтологии и использования SADT методологии разработан комплекс системных моделей системы обнаружения атак. Функциональная модель IDEF0 системы обнаружения атак состоит из функциональных блоков «собрать информацию», «обрабо-

тать информацию», «выявить атаку», «подавить атаку». Данные блоки отражают различные функции системы обнаружения атак и описывают процесс обнаружения и блокирования атак. Информационная модель IDEF1X представляет собой логическую модель базы данных и базы знаний системы обнаружения атак.

В связи с тем, что информационные системы являются сложными гетерогенными комплексами, функционирование которых не может быть описано в детерминированном виде, моделирование многих аспектов функционирования подобных систем обычно связано с использованием знаний экспертов, описанных в нечеткой форме. Для того чтобы учесть подобные аспекты ИС, в работе предлагается использовать динамическую модель ИС на основе нечетких когнитивных карт (НКК). Данный подход основан на выделении совокупности основных факторов (концептов), обозначающих различные понятия моделируемой предметной области и построении на их основе ориентированного графа, отображающего взаимосвязи между концептами (рис. 1).

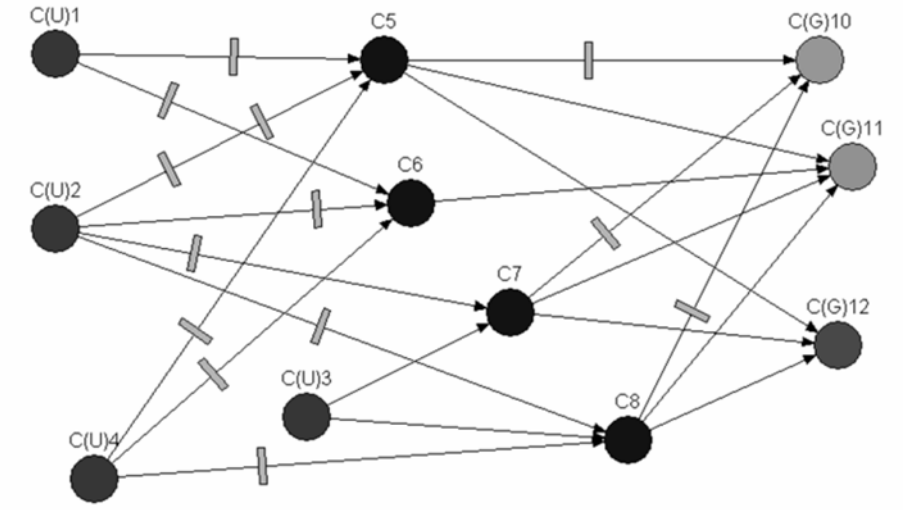

Рисунок 1 – Нечеткая когнитивная карта

Каждому i-му концепту нечеткой когнитивной карты ставится в соответствие переменная состояния X_i и вес w_{ij}, характеризующий влияние i-го концепта на j-й концепт. Величина веса w_{ij} лежит в пределах [0;1] и характеризует степень значимости (влияния) соответствующего концепта. Переменные состояния концептов модели динамически изменяются во времени в соответствии с формулой:

$$X_i(k+1) = f(X_i(k) + \sum_{\substack{j=1 \\ j \neq i}}^{n} w_{ij} X_j(k)), \tag{1}$$

где $X_i(k)$ – переменная состояния i-го концепта в момент времени k; w_{ij} – вес связи между концептами i и j; $f(x)$ – нелинейная функция следующего вида:

$$f(x) = \frac{1}{1+e^{-\lambda x}}, \tag{2}$$

где значение коэффициента λ подбирается эмпирически в ходе численного эксперимента.

Для использования НКК с целью оценки риска функционирования ИС выделяются 4 группы концептов, обозначающих различные факторы поведения ИС:

1) дестабилизирующие факторы (ДФ) – отображают совокупность факторов, негативно влияющих на ИС;

2) промежуточные факторы (ПФ) – совокупность объектов, групп объектов либо параметров, описывающих состояние ИС;

3) целевые факторы (ЦФ) – описывают различные негативные последствия (ущерб), возникающие в результате воздействия ДФ на ИС;

4) управляющие факторы (УФ) – моделируют управляющие и защитные механизмы ИС.

Для определения влияния i-го ДФ на j-й ЦФ рассчитывается величина полного эффекта T_{ij}, которая находится по следующей формуле:

$$T_{ij} = \max_{\ell} \left\{ T_{ij}^{l} \right\} \tag{3}$$

где T_{ij} - минимальный вес связи ℓ-го пути между вершинами (концептами) i и j нечеткой когнитивной карты.

Оценка совокупного влияния всех ДФ на определенный (j-й) ЦФ описывается величиной полного (комплексного) эффекта:

$$T_j = \max_{1 \le i \le k} (T_{ij}) \tag{4}$$

где k – число ДФ.

Для оценки полного риска функционирования ИС можно воспользоваться формулой

$$R = \sum_{j=1}^{N} T_j \, r_j v_j \,, \tag{5}$$

где N – общее число ЦФ модели; r_i – величина возможного ущерба от реализации j-го ЦФ; v_i – значимость j-го ЦФ.

Динамическая модель системы обнаружения атак была построена с использованием нечетких когнитивных карт, что позволяет не только отслеживать процессы, протекающие в ИС при реализации различных видов атак, но и определять величины рисков, а также индивидуальный и суммарный эффекты от внедрения различных средств защиты. Для построения модели ИС предлагается использовать следующую методологию:

1. Формирование списка угроз и оценка вероятности их реализации. На данном этапе группа экспертов формирует список угроз, воздействующих на моделируемый компонент ИС и оценивает вероятность их реализации. Оценка может осуществляться как на основе статистической базы инцидентов по каждой атаке, так и с использованием методов нечеткой логики. Полученные значения вероятностей переводятся в проценты и представляют собой начальные состояния ДФ-концептов НКК.
2. Формирование списка промежуточных факторов и вычисление их начальных значений. Эксперты анализируют компоненты моделируемой ИС и на их основе составляют список ПФ-концептов, в качестве которых могут рассматриваться как реальные компоненты ИС, так и неко-

торые их характеристики, отображающие корректность ее функционирования.

3. Формирование списка целевых факторов. Составляется список возможных последствий реализации атак на ИС, эксперты оценивают величину ущерба для каждого фактора, а также ранжируют их по степени важности.
4. Описание функций принадлежности и нечетких переменных, используемых для задания весов и связей между концептами НКК.
5. Построение графа НКК. Эксперты строят граф НКК с учетом выбранных семантических связей между концептами модели.
6. Формирование списка контрмер. Эксперты формируют список контрмер, используемых для блокирования атак. Для каждой контрмеры оценивается степень ее влияния на каждую атаку, а также стоимость внедрения данной контрмеры.
7. Формирование базы правил. Эксперты формируют нечеткую базу правил, которая позволяет вычислять реальную величину влияния контрмеры на риск реализации угрозы путем нечеткого логического вывода.
8. Выбор рациональных контрмер с учетом величин полного эффекта, риска и предотвращенных потерь вследствие использования выбранных средств защиты.

В качестве примера построения модели атаки на ИС рассмотрим угрозу внедрения модуля реализации вредоносного кода (rootkit) на локальный компьютер корпоративной сети ИС. Моделирование осуществлялось с помощью разработанного в рамках данной работы исследовательского прототипа системы обнаружения атак. Схема реализации подобной угрозы показана на рисунке 2.

В качестве основных угроз при реализации данного сценария атаки выступают:

1) перехват пользовательских паролей путем внедрения промежуточного драйвера в стек драйверов ввода-вывода;
2) модификация структур ядра с целью маскировки присутствия шпионского модуля и контроля функционирования системы;
3) кража либо повреждение пользовательских данных;
4) анализ сетевой активности пользователя с целью получения персональных данных;
5) несанкционированное использование сетевого канала (рассылка спама, DoS атаки и т.п.).

Рассматриваемые дестабилизирующие факторы оказывают непосредственное влияние на следующие компоненты вектора состояний системы X:

1) корректность функционирования системного ПО – в силу модификаций внутренних структур ядра операционной системы возможно нарушение ее работоспособности (некорректное поведение, перезагрузки, критические сбои);
2) конфиденциальность пользовательской информации;
3) целостность пользовательской и системной информации;

4) доступность информации.

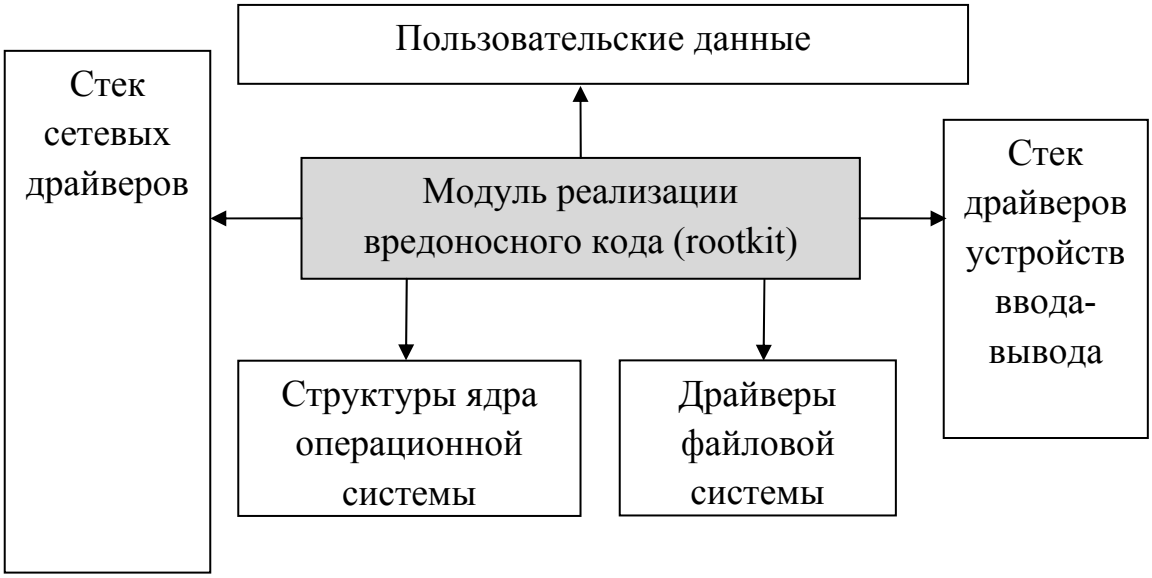

Рисунок 2 – Схема реализации угрозы внедрения rootkit

Влияние дестабилизирующих факторов на ПФ-концепты может привести к реализации следующих факторов риска:

1) потеря данных;
2) моральный ущерб (в результате утраты важных данных, нарушения работоспособности компонентов ИС, противозаконных действий совершенных модулем реализации вредоносного кода и т.п.);
3) простой оборудования в результате нарушения работоспособности компонентов ИС.

Для противодействия влиянию дестабилизирующих факторов на концепты НКК анализируется набор следующий набор контрмер:

1) внедрение эффективной политики безопасности;
2) установка межсетевого экрана (МСЭ);
3) установка антивируса;
4) установка системы обнаружения атак;
5) шифрование данных;
6) внедрение системы резервного копирования информации.

В третьей главе описана процедура имитационного моделирования атак на информационную систему.

Имитационное моделирование осуществлялось с целью проверки степени адекватности предложенной математической модели операционной среды, реальной обстановке. Процесс моделирования сводился к исследованию реакции различных компонентов прототипа системы обнаружения атак на всевозможные возмущающие факторы, воздействующие на защищаемый объект. В ходе первой стадии тестирования осуществлялся набор атак, а также возможных действий, имеющих признаки атаки, однако являющихся легальными. Анализ реакции системы выполняется путем измерения величин дес-

табилизирующих факторов и рисков в модулях принятия решения локальных рабочих станций и сетевых сервисов.

Вторая стадия тестирования заключалась в проверке способности системы к подавлению атак. В ходе нее сопоставлялись величины рисков до и после реакции системы на обнаруженную атаку, вычислялись величины ошибок первого и второго рода при принятии решений об классификации активности как атаки.

Входные данные (уровни угроз) поступают с сенсоров системы обнаружения атак и генерируются на основе следующей информации:

- D1 – информация о вредоносной активности пользователей, формируется на основе вычисления степени отклонения текущих действий пользователя от его шаблонного поведения;
- D2 – степень вредоносности потока инструкций;
- D3 – степень подозрительности действий модуля.
- D2 – степень вредоносности потока инструкций;
- D3 – степень подозрительности действий модуля.

Помимо этого, на вход системы поступает средний коэффициент загрузки (R1), вычисляемый на основе следующих данных:

- загрузка центрального процессора;
- коэффициент занятости физической памяти;
- коэффициент использования физической памяти;
- скорость использования оперативной памяти.

Для оценки поведения модели был сформирован набор экспериментов, каждый из которых заключался в запуске определенного набора программ, причем часть из них являлась вредоносными, а часть представляла собой различные утилиты сторонних разработчиков. Атака считалась зарегистрированной моделью, если уровень риска превышал значение 0,6. Список произведенных экспериментов приведен в таблице 1.

Таблица 1 - Список экспериментов

Номер	Является атакой	Описание
1	Да	Внедрение rootkit ядра SSDT
2	Нет	Использование утилиты regmon
3	Да	Внедрение rootkit ядра KOM
4	Да	Использование dll-injection
5	Да	Модификация IAT
6	Да	Использование keylogger ядра

В ходе первого эксперимента проверялась способность модели выявлять

атаки, основанные на внедрении rootkit уровня ядра операционной системы, осуществляющего перехват вызовов функций системного API за счет модификации таблицы дескрипторов системных сервисов (SSDT).

Данный эксперимент позволяет проверить возможность распознавать внедрение модуля rootkit, реализованного в виде драйвера ядра и использующего модификацию таблицы дескрипторов системных сервисов для скрытия своего присутствия. Для выполнения эксперимента использовался специально разработанный для этой цели программный модуль, что гарантировало невозможность его распознавания системами антивирусной защиты. Графики зависимостей уровней угроз и риска от времени показаны на рис. 3.

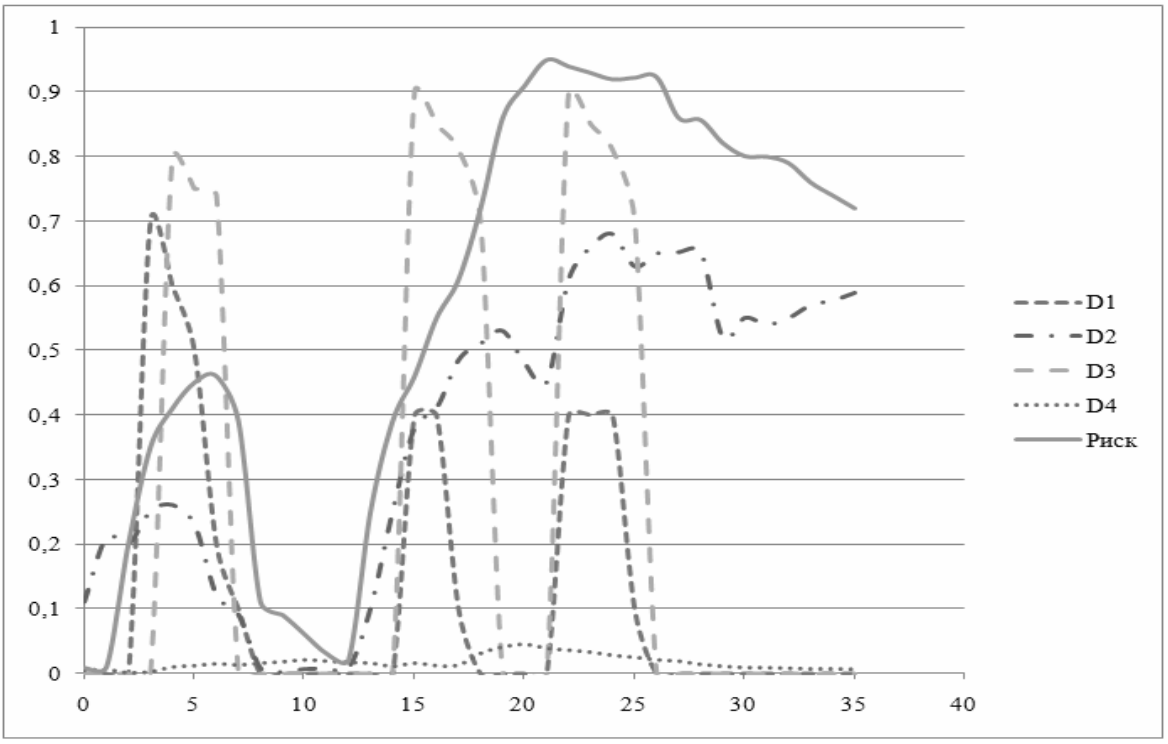

Рисунок 3 – Изменение уровней угроз и риска в ИС

На первом шаге эксперимента выполнялась загрузка программой-носителем шпионского модуля (такты 2-7). На графике наблюдается резкое увеличение уровня угрозы D1, т.к. ручная загрузка драйверов ядра не является регулярным действием пользователя и не соответствует его профилю поведения. Модель также регистрирует наличие подозрительной активности модуля D3, связанной с использованием функций SCM программой – носителем. Высокий уровень угрозы, регистрируемый сенсорами D1 и D3, приводит к повышению величины риска функционирования системы, который, однако, не превышает величины порогового значения регистрации атаки, т.к. подобная ситуация, вообще говоря, является штатной.

На втором шаге эксперимента выполнялось изменение значений нескольких векторов таблицы SSDT по команде программы-носителя (такты 14-18). На графике наблюдается увеличение уровня угрозы D1, связанное с использованием функций IOCTL программой-носителем (прямая коммуникация с

драйверами ядра также не входит в текущий шаблон поведения). Также наблюдается резкое увеличение уровня угрозы D3, вызванное тем, что сенсор обнаружил в таблице дескрипторов указатели на модули, принадлежащие адресному пространству шпионского драйвера, что является крайне нетипичным поведением для системных модулей. Наблюдается также повышение уровня угрозы D2 получаемого на основе анализа потока инструкций загруженных модулей. Эти события приводят к увеличению уровня риска и регистрации атаки на 17-м такте.

На третьем шаге эксперимента измененялось возвращаемое значения системной функции *ZwQuerySystemInformation* для того, чтобы скрыть процесс программы-носителя (такты 20-27). Вновь наблюдается увеличение уровня угрозы D1, связанное с коммуникацией программы-носителя с драйвером. Повышение уровня угрозы D3 связано с тем, что сенсор обнаружил искажение результатов вызова системной функции. Уровень риска на данном шаге эксперимента превысил 0,9, и на 35-м такте атака была заблокирована путем восстановления таблицы дескрипторов, выгрузки шпионского драйвера и завершения процесса программы – носителя.

Для оценки корректности распознавания различных атак в работе выполняется оценка величины ошибок первого и второго рода, с использованием результатов проведенных экспериментов в качестве базовых эталонов при формировании тестирующих выборок. Моделирование атак осуществлялось на виртуальной машине *VMware Workstation* для обеспечения нормированной среды при каждом эксперименте, использовались шпионские модули, находящиеся в открытом доступе и обладающие исходными кодами. Тестирование каждого шпионского модуля производилось по 100 раз, результаты усреднялись для исключения влияния ПО виртуализации.

Полученные в ходе эксперимента результаты объясняются двумя причинами: завышенным значением порога регистрации атак и высоким уровнем неопределенности экспертных знаний модели. В первом случае решение ищется путем внедрения в систему принятия решений гибкой системы сигнатурного анализа, что позволяет избавиться от жесткого порога активации модели. Во втором случае решение возможно за счет дополнительного обучения весов связей нечеткой когнитивной карты на сформированной обучающей выборке.

Предлагаемая модель на основе нечеткой когнитивной карты может быть представлена в виде нейронной сети, где концепты карты выполняют функции сумматоров, а нормирующая функция представляет собой функцию активации. Если воспользоваться данным представлением НКК, то возможно снизить уровень избыточной неопределенности, путем обучения НКК на заданной обучающей. Суть работы данного алгоритма сводится к уменьшению величины рассогласования между результатом моделирования и значением эталона. Для уменьшения величины ошибок первого и второго рода в диссертации использовался алгоритм обратного распространения ошибки (*Back Propagation*). Формирование обучающей выборки производилось на основе набора различных шпионских модулей, а также всевозможных системных

утилит, активно использующих работу с системным реестром, службами операционной системы и позволяющих модернизировать внутренние объекты ядра операционной системы (*regmon, filemon, gflags* и т.п.).

Таблица 2 Величины ошибок 1-го и 2-го рода после обучения

Тип атаки	Количество модулей	Ошибка 1-го рода	Ошибка 2-го рода	Описание
1	25	0	0	SSDT rootkit
2	16	0	0,063	Системная утилита
3	10	0	0	KOM rootkit
4	30	0,067	0	Dll injection
5	26	0,038	0	Модификация IAT
6	8	0	0	Keylogger

После обучения НКК было произведено повторное имитационное моделирование и, вычислены значения ошибок первого и второго рода. Результаты численного эксперимента представлены в таблице 2.

Результаты, представленные в таблице 2, демонстрируют эффективность предложенных алгоритмов обучения НКК для устранения неопределенности базы экспертных знаний, лежащих в основе построения НКК. Использование данных методов позволяет существенно повысить точность распознавания атак компонентами системы обнаружения атак, дополнительно снижая величину риска функционирования ИС. Существенным недостатком данной методики является невозможность ее использования для «калибрования» базы нечетких правил, лежащей в основе методики вычисления степени взаимного влияния концептов.

В четвертой главе рассмотрена задача реализации исследовательского прототипа системы обнаружения атак. В силу гетерогенности структуры и свойств объектов ЛВС, охват ИС разнородным ПО сбора данных и формирование единого потока информации для анализа вредоносной активности может потребовать ресурсы, сопоставимые или даже превосходящие затраты на организацию ИС в целом, поэтому целесообразно распределить вычислительную нагрузку между сетью агентов-сенсоров и иерархическим деревом агентов принятия решений. В основе предложенной в работе архитектуры системы обнаружения атак лежит наделение каждого агента базовой функциональностью системы в целом, т.е. способностью к анализу и принятию решений в рамках жестко поставленной задачи (анализ сетевого трафика хоста, анализ активности системных процессов и т.п.). Таким образом, каж-

дый сенсор системы обнаружения атак представляет собой систему обнаружения атак в миниатюре, способную к автономному функционированию при потере связи с модулями принятия решений более высоких уровней.

Модули, входящие в СОА, можно разбить по функциональному назначению на два основных класса:

1) базовые модули системы;
2) модули системы обнаружения атак (СОА).

Базовые модули обеспечивают интеграцию и взаимодействие компонент системы друг с другом, позволяют изменять конфигурацию системы обнаружения атак и взаимодействовать с ПО блокирования вторжений. Модули СОА позволяют отслеживать и блокировать атаки в реальном времени. В основе функционирования данной подсистемы лежит метод анализа сигнатур активности.

Центральным компонентом системы, объединяющим все остальные модули в единое целое, является глобальная база знаний (ГБЗ), содержащая информацию о всех известных системе видах атак, методах противодействия вторжениям, архив событий системы, а также конфигурацию всех компонентов системы обнаружения атак. Для обеспечения требуемого уровня надежности и отказоустойчивости, в качестве ГБЗ возможно использование современной клиент-серверной реляционной СУБД, обладающей возможностями кластеризации и прозрачной репликации данных.

Основным инструментом настройки и управления системы обнаружения атак является консоль администратора, представляющая собой комплекс программных средств, обеспечивающий настройку модулей системы, вывод информации об обнаруженных атаках и предоставляющий возможность классификации администратором активности, не распознанной модулями системы обнаружения атак. Подключение консоли администратора к ГБЗ осуществляется через унифицированный интерфейс *ISysManage*, реализуемый каждым компонентом системы. Данный подход позволяет осуществлять настройку отдельных компонент системы на более низком уровне, что позволяет разделять задачи администрирования СОА между несколькими пользователями ИС.

Сенсоры системы обнаружения атак образуют нижний уровень сети сбора и анализа данных. После обработки сенсором, информация поступает в модули анализа и принятия решений более высоких уровней через универсальный интерфейс «Анализатор - Решатель». Данный подход позволяет строить иерархическое дерево из модулей анализа и сенсоров, причем для каждого узла дерева нижележащее поддерево будет представляться как единый сенсор.

Модуль реакции представляет собой промежуточный интерфейс между системы обнаружения атак и средствами блокирования вторжений сторонних производителей. Данный компонент обеспечивает интеграцию системы обнаружения атак в общую систему защиты ИС и позволяет ей гибко изменять политику безопасности в зависимости от внешних условий.

Каждый сенсор представляет собой набор блоков сбора данных ($S_1 \ldots S_n$), блоков первичной реакции ($R_1 \ldots R_n$), а также содержит блок первичного анализа данных. Данный модуль осуществляет первичный анализ потока данных активности объектов КИС и формирует на его основе совокупность первичных сигнатур. Совокупность первичных сигнатур содержит описание активности, отмеченной сенсором, и полный перечень операций, выполненных субъектом активности (последовательность вызова системных функций, цепочки пакетов TCP/IP и т.п.).

В случае если определенная активность классифицируется сенсором как атака, осуществляется формирование вторичной сигнатуры, представляющей собой формализованное описание атаки. Данная сигнатура поступает на вход модуля анализа данных, который формирует целостную картину распространения атаки в информационной системе. Архитектура разрабатываемой системы обнаружения атак позволяет организовывать модули анализа в виде иерархического дерева, формируя тем самым несколько каскадов обработки информации, что позволяет гибко масштабировать систему обнаружения атак в зависимости от размеров и структурной организации ИС. Помимо формирования вторичной сигнатуры, сенсор осуществляет поиск в локальной базе прецедентов информации о методах блокирования обнаруженной атаки.

Если данная информация присутствует, блок первичного анализа осуществляет активацию соответствующего блока первичной реакции и, по изменению данных с блоков сбора информации, определяет степень эффективности подавления атаки. В случае, если методы локального подавления оказываются неэффективными либо локальная база не содержит информации о методах блокирования данной атаки, инициируется запрос глобального модуля принятия решений, который может выполнить дополнительную настройку систем защиты предприятия, блокировать источник атаки либо выдать запрос в консоль администратора.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработан комплекс системных моделей системы обнаружения атак на информационную систему на основе построения онтологии предметной области и использования SADT-методологии, которые позволили выявить основные процессы, лежащие в основе функционирования системы обнаружения атак, выявить ее составные компоненты, их взаимосвязи и сформулировать требования к реализации системы, исходя из современных требований к обеспечению защищенности ИС.
2. Предложена архитектура и алгоритмы интеллектуальной системы обнаружения атак, основанной на основе построения динамической модели ИС с использованием нечетких когнитивных карт, что позволяет повысить эффективность системы обнаружения атак за счет прогнозирования и управления рисками ИС в режиме реального времени.
3. Предложен алгоритм обучения нечеткой когнитивной карты на наборе эталонных сценариев с использованием алгоритма обратного распростране-

ния ошибки, что позволяет уменьшить неоднозначность экспертных данных и существенно сократить число ошибок распознавания атак первого и второго рода.

4. Разработан исследовательский прототип системы обнаружения атак на основе нечетких когнитивных карт, реализующий предложенные алгоритмы обнаружения атак на основе моделирования рисков ИС в режиме реального времени.

5. Тестирование разработанного прототипа системы обнаружения атак подтвердило высокую эффективность используемого подхода при обнаружении атак на компоненты ИС. В частности, в проведенных экспериментах разработанный прототип системы обнаружения атак позволяет распознать и блокировать до 97 % атак на защищаемые компоненты ИС, при этом ошибка второго рода не превышает 6 %.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Комплексный подход к построению интеллектуальной системы обнаружения атак / Васильев В. И., Свечников Л. А., Кашаев Т. Р. // Системы управления и информационные технологии, Воронеж, №2, 2007. – С. 76-82.

В других изданиях

2. Проблема построения защищенных Internet-серверов / Свечников Л.А., Кашаев Т.Р. // Интеллектуальные системы управления и обработки информации: Материалы Всероссийской молодежной науч.-технич. конференции. Уфа: УГАТУ, 2003. – С. 9.

3. Использование AD для разработки защищенных приложений / Свечников Л.А., Кашаев Т.Р., Кустов Г.А. // Интеллектуальные системы управления и обработки информации: Материалы Всероссийской молодежной науч.-технич. конференции. Уфа: УГАТУ, 2003. – С. 21.

4. Структура интеллектуальной распределенной системы обнаружения атак / Васильев В.И., Свечников Л.А., Калабухов М.С. // Компьютерные науки и информационные технологии: Труды 7-й Международной конференции (CSIT’2005), Т. 2, Уфа: Изд-во УГАТУ, 2005. – С. 200-206 (на англ. языке).

5. Архитектура распределенной системы обнаружения атак / Васильев В.И., Свечников Л.А., // Информационная безопасность: Материалы 8-й международной научно-практической конференции. Часть 1 – Таганрог: Изд-во ТРТУ, 2006. – С. 180-184.

6. Архитектура распределенной системы обнаружения атак / Свечников Л.А. // Компьютерные науки и информационные технологии: Труды 8-й Международной конференции (CSIT’2006), г. Карлсруэ, Германия, Уфа: Изд-во УГАТУ, 2006. – Том 2, С. 177-179 (на англ. языке).

7. Подход к реализации нейросетевого сенсора интеллектуальной системы обнаружения атак / Васильев В.И., Свечников Л.А. // Вычислительная техника и новые информационные технологии. Межвузовский научный сборник, Уфа: Изд-во УГАТУ,2006. №6 – С. 161-166.

8. Моделирование и оптимизация системы обнаружения атак в локальных вычислительных сетях/ Свечников Л.А. // Интеллектуальные системы обработки информации и управления: Сборник статей 2-й региональной зимней школы-семинара аспирантов и молодых ученых, г. Уфа: Издательство «Технология», 2007 – Том 1, С. 175-178.

9. Подход к моделированию атак на автоматизированную информационную систему / Свечников Л.А. // Интеллектуальные системы обработки информации и управления: Сборник статей 2-й региональной зимней школы-семинара аспирантов и молодых ученых, г. Уфа: Издательство «Технология», 2010. – Том 1, С. 178-183.

10. Васильев В.И., Свечников Л.А. Свид. об офиц. рег. программы для ЭВМ №2008611106. Модуль обнаружения, анализа и подавления атак. М.: Роспатент, 2008. Зарег. 29.08.2008.

Диссертант Свечников Л.А.

СВЕЧНИКОВ Лаврентий Александрович

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати 13.05.2010. Формат 60×84 1/16.
Бумага офсетная. Печать плоская. Гарнитура Times New Roman Cyr.
Усл. печ. л. 1,0. Усл. кр.-отт. 1,0. Уч.-изд. л. 0,9.
Тираж 100 экз. Заказ № 224.

ГОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К. Маркса, 12