На правах рукописи

КАШАЕВ Тимур Рустамович

АЛГОРИТМЫ АКТИВНОГО АУДИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

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

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Уфа 2008

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**

канд. техн. наук, доцент **Набатов Александр Нурович**

Ведущая организация — **ООО «Башпромавтоматика»**

Защита диссертации состоится «17» октября в 10:00 на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете по адресу: 450000, Уфа, ул. К.Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан « » сентября 2008 г.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Обеспечение безопасности информации в современном бизнесе является одной из ключевых задач. Развитие компьютерных сетей и их объединение в глобальную сеть Интернет привело к росту числа преступлений, связанных с нарушением основополагающих принципов информационной безопасности: доступности, целостности и конфиденциальности информации. Несмотря на развитие средств защиты, таких как брандмауэры, количество вторжений в информационные системы компаний возрастает с каждым годом. Увеличение числа атак на ресурсы локальных вычислительных сетей (ЛВС) приводит к необходимости применения средств защиты не только на рубеже «Интернет/Интранет», но и внутри самой ЛВС. Согласно статистическим отчетам аудиторской компании *Deloitte & Touche*, в 2007 г. внутренним атакам подвергались более 38% опрошенных компаний. Для обнаружения атак внутри сетей используются различные классы инструментальных средств, такие как системы обнаружения атак, системы предотвращения атак, сканеры уязвимостей, комплексные системы управления безопасностью. Однако использование этих средств сегодня ограничено рядом факторов:

- высокая стоимость и сложность их развертывания и поддержки;
- низкая эффективность функционирования при наличии неизвестных атак;
- высокая нагрузка на компоненты ЛВС.

В настоящее время исследования в области защиты объектов ЛВС ведутся в направлении разработки средств «активного аудита» (САА), которые позволяют решить часть этих проблем за счет использования технологий интеллектуального анализа данных, модульности и многоагентного подхода. Вместе с тем, многие вопросы при построении этих систем, связанные с эффективностью применения новых методов и технологий и их реализацией в режиме реального времени, остаются открытыми и не до конца исследованными, поэтому тема диссертации, посвященная разработке интеллектуальных систем активного аудита информационных систем с использованием одного из перспективных направлений - искусственных иммунных систем, является актуальной.

Объект исследования – информационная система локальной вычислительной сети.

Предмет исследования – математическое, алгоритмическое и программное обеспечение САА.

Цель работы

Целью диссертационной работы является повышение эффективности процессов аудита безопасности информационной системы (ИС) на основе разработки алгоритмов и программного обеспечения интеллектуальной системы активного аудита с использованием технологий искусственных иммунных систем.

Задачи исследования

Для достижения поставленной цели в диссертационной работе решаются следующие задачи:

1. Разработка комплекса системных моделей системы активного аудита.
2. Разработка алгоритмов активного аудита ИС на основе технологии искусственных иммунных систем.
3. Оценка эффективности предложенных алгоритмов активного аудита ИС на основе технологий искусственных иммунных систем.
4. Реализация исследовательского прототипа интеллектуальной системы активного аудита ИС с использованием механизмов искусственных иммунных систем.

Методы исследования

В работе использовались методы теории принятия решений, математической статистики, системного анализа, теории распознавания образов, теории нейронных сетей и нечеткой логики, искусственных иммунных систем, теории информационной безопасности.

Научная новизна

Научная новизна работы заключается в следующем:

1. Разработан комплекс системных моделей системы активного аудита ИС с применением SADT-методологии, позволивших выделить основные бизнес-процессы, лежащие в основе её функционирования, и сформулировать требования к реализации системы, исходя из современных требований к обеспечению защищенности ИС.
2. Разработаны алгоритмы активного аудита ИС, основанные на применении технологий искусственных иммунных систем, повышающие эффективность обнаружения атак за счёт отказа от использования конечного множества сигнатур известных атак и перехода к использованию более общего принципа распознавания «свой - чужой».
3. Предложен модифицированный алгоритм генерации детекторов системы обнаружения атак, основанный на использовании генетического алгоритма, позволяющий сократить сроки обучения и повысить

эффективность функционирования системы активного аудита на основе механизмов искусственной иммунной системы.

Практическая ценность

Предложенные алгоритмы построения интеллектуальной системы обнаружения атак позволяют повысить эффективность обнаружения атак, в том числе обнаружения неизвестных атак, т. е. атак, для которых не существует эталонной сигнатуры, до 85%, при этом в проведенных экспериментах ошибка второго рода не превысила 6%.

Исследовательский прототип интеллектуальной системы активного аудита ИС зарегистрирован в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам (№2008611107 от 29 февраля 2008г.). Разработанный прототип интеллектуальной системы активного аудита ИС может быть интегрирован в существующую инфраструктуру систем управления информационной безопасностью ИС, в том числе в гетерогенных ЛВС.

Основные результаты диссертационной работы внедрены в РНТИК «Баштехинформ», а также в учебный процесс Уфимского государственного авиационного технического университета.

Результаты, выносимые на защиту

1. Функциональная, информационная и динамическая модели системы активного аудита ИС.
2. Алгоритмы обнаружения атак в ИС на основе технологий искусственных иммунных систем.
3. Результаты экспериментальных исследований эффективности предложенных алгоритмов построения интеллектуальной системы активного аудита ИС.
4. Исследовательский прототип интеллектуальной системы активного аудита ИС с использованием технологий искусственных иммунных систем.

Апробация работы

Основные научные и практические результаты диссертационной работы докладывались и обсуждались на:

- Всероссийской молодежной научно-технической конференции «Интеллектуальные системы управления и обработки информации», г.Уфа, 2003 г.
- Научно-практической конференции студентов и молодых ученых с международным участием «Вопросы теоретической и практической медицины», Уфа, 2004.

- 7 и 8 Международных научных конференциях «Компьютерные науки и информационные технологии» (CSIT), Уфа, 2005; Карлсруэ, Германия, 2006.
- 2 Региональной зимней школе-семинаре аспирантов и молодых ученых "Интеллектуальные системы обработки информации и управления", Уфа, 2007.
- 3 Всероссийской зимней школе – семинаре аспирантов и молодых ученых, Уфа, 2008.

Публикации

Результаты диссертационной работы отражены в 13 публикациях, в том числе в 7 научных статьях, из них 1 статья в издании из перечня ВАК РФ, а также в 6 материалах докладов международных и российских конференций.

Структура работы

Диссертация состоит из введения, четырех глав, заключения, приложений и библиографического списка. Работа содержит 130 страниц машинописного текста, включая 40 рисунков и 17 таблиц. Библиографический список включает 105 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность исследований в области построения систем активного аудита информационных систем (ИС). Формулируются цель работы и задачи исследований, научная новизна и практическая ценность выносимых на защиту результатов.

В первой главе проводится анализ существующих подходов к решению задачи обнаружения внутренних атак в информационной системе.

На основе проведенного анализа сделан вывод о том, что существующие прототипы систем обнаружения внутренних атак обладают рядом недостатков, не позволяющих широко использовать их в корпоративных сетях. Это обусловлено, прежде всего, сложностью их реализации, включающей в себя:

- выбор методики сбора данных об информационной системе;
- выбор метода обнаружения внутренних атак;
- обработку полученных данных;
- выбор способа противодействия атаке;
- распределение нагрузки на компоненты информационной системы.

Традиционные методы обнаружения атак, такие, как сигнатурный метод или метод обнаружения аномалий, не позволяют достичь оптимальных характеристик обнаружения внутренних атак. Нейросетевые методы

обнаружения атак в принципе позволяют достичь приемлемых характеристик, однако обладают такими недостатками, как трудность выбора параметров и структуры нейронных сетей, ресурсоёмкий характер обучения нейронной сети, сложность дообучения и переобучения нейронной сети.

Поэтому возникает необходимость в выборе и применении метода, который позволил бы избежать указанных выше недостатков при допустимом уровне надёжности обнаружения внутренних атак. Анализ показал, что достаточно перспективным для этих целей является построение систем активного аудита на основе технологий искусственных иммунных систем. Этот подход обладает рядом преимуществ по сравнению с другими методами, обеспечивая:

- высокую скорость работы;
- сравнительно простой алгоритм обучения;
- низкую ресурсоёмкость.

В данной работе под «активным аудитом» понимается непрерывный системный процесс проверки ИС на соответствие декларируемым целям политики безопасности, организации обработки данных, норм эксплуатации средств вычислительной техники, а также автоматического реагирования на выявленные отклонения. Таким образом, «система активного аудита» сочетает в себе как элементы традиционных систем аудита (сканеров безопасности), так и элементы систем обнаружения и предотвращения вторжений.

В заключении главы формулируются цели и задачи исследования.

Во второй главе проводится анализ субъектов и объектов ИС на основе SADT-методологии, позволяющей представить основные процессы в ИС и её компонентах в графическом, удобном для понимания виде. Разработаны функциональная, информационная и динамическая модели системы активного аудита. Функциональная модель IDEF0 системы активного аудита состоит из блоков «собрать информацию», «обработать информацию», «выявить нарушение политики безопасности» и «реагировать на нарушение». Данные блоки отражают различные функции системы активного аудита, включая функции сбора информации, обнаружения атак и выработки реакции на атаку. Функциональный состав каждого из блоков раскрывается в соответствующих функциональных диаграммах.

Поскольку состояние защищенности ИС зависит от совокупности происходящих в этой сети событий, её функционирование описывается с помощью нечеткой сети Петри. Для этого определяется множество состояний ИС

$$S = \{S_1, S_2, S_3, S_4, S_5\}, \quad (1)$$

где S_1 – состояние нормального функционирования ИС;

S_2 – состояние атаки на ИС, при котором злоумышленник воздействует на ИС с целью нарушения её нормального функционирования;

S_3 – состояние нарушения конфиденциальности ресурсов ИС;

S_4 – состояние нарушения целостности ресурсов ИС;

S_5 – состояние нарушения доступности ресурсов ИС.

Определяется множество событий в ИС

$$K = \{K_1, \ldots, K_6\}, \quad (2)$$

где K_1 – событие появления злоумышленника;

K_2 - множество событий, приводящих к нарушению конфиденциальности;

K_3 – множество событий, приводящих к нарушению целостности;

K_4 – множество событий, приводящих к нарушению доступности;

K_5 – множество событий срабатывания средств защиты ИС;

K_6 – множество событий восстановления ИС после атаки.

Множество событий в ИС представляет собой объединение множеств указанных выше событий в ИС, т.е.:

$$K = K_1 \cup K_2 \cup K_3 \cup K_4 \cup K_5 \cup K_6. \quad (3)$$

Нечеткая сеть Петри (НСП), описывающая поведение ИС, представляется в виде:

$$C_f = (N, f, \lambda, m_0), \quad (4)$$

где N – структура НСП, $N = (P, T, I, O)$;

$f = \{f_1, \ldots, f_u\}$ – вектор значений функции принадлежности нечеткого срабатывания переходов, $f_j \in [0, 1]$, $j = 1, \ldots, u$;

$\lambda = (\lambda_1, \ldots, \lambda_u)$ – вектор значений порогов срабатывания переходов, $\lambda_j \in [0,1]$, $j = 1, \ldots, u$;

m_0 – вектор начальной маркировки, $m_i^0 \in [0, 1]$, $i = 1, \ldots, n$.

Структура НСП $N = (P, T, I, O)$ при этом аналогична структуре традиционных сетей Петри и может быть представлена следующими элементами (рис. 1):

$P = \{p_1, \ldots, p_n\}$ – множество позиций НСП;

$T = \{t_1, t_2, \ldots, t_u\}$ – множество переходов НСП, $u \in N$;

I – входная функция переходов, I: $P \times T \rightarrow \{0, 1\}$;

O – выходная функция переходов, O: $T \times P \rightarrow \{0, 1\}$.

В работе формулируется база правил нечеткого логического вывода, определяющих условия срабатывания переходов НСП. Каждому предикату из составленных правил сопоставляется определенная позиция НСП. Каждой позиции $P = \{p_1, \ldots, p_n\}$ сопоставляются элементы множеств S и K:

$$P = \{S_1, K_1, S_2, K_2, K_3, K_4, K_5, S_3, S_4, S_5, K_6\}.$$

Определяется вектор начальной маркировки:

$$m_0 = (m^0_1, m^0_2, m^0_3, m^0_4, m^0_5, m^0_6, m^0_7, m^0_8, m^0_9, m^0_{10}, m^0_{11}).$$

Здесь m^0_i (i = 1, 3, 8, 9, 10) – значения функций принадлежности наличия маркеров в позициях $S_{1...5}$, т.е. значения функций принадлежности определяющих различные состояния ИС; m^0_2 – значение функции принадлежности наличия маркера в позиции K_1, т.е. фактически вероятность появления злоумышленника в ИС; m^0_j (j = 4, 5, 6) – значения функций принадлежности наличия маркеров в позициях K_2, K_3, K_4, т.е. значения функций принадлежности возникновения событий, приводящих к нарушению конфиденциальности, целостности и доступности информации в ИС; m^0_7 – значение функции принадлежности наличия маркера в позиции K_5, т.е. фактически вероятность корректной реакции на атаку средств активного аудита; m^0_{11} – значение функции принадлежности наличия маркера в позиции K_6, т.е. вероятность правильной реакции средств восстановления после атаки.

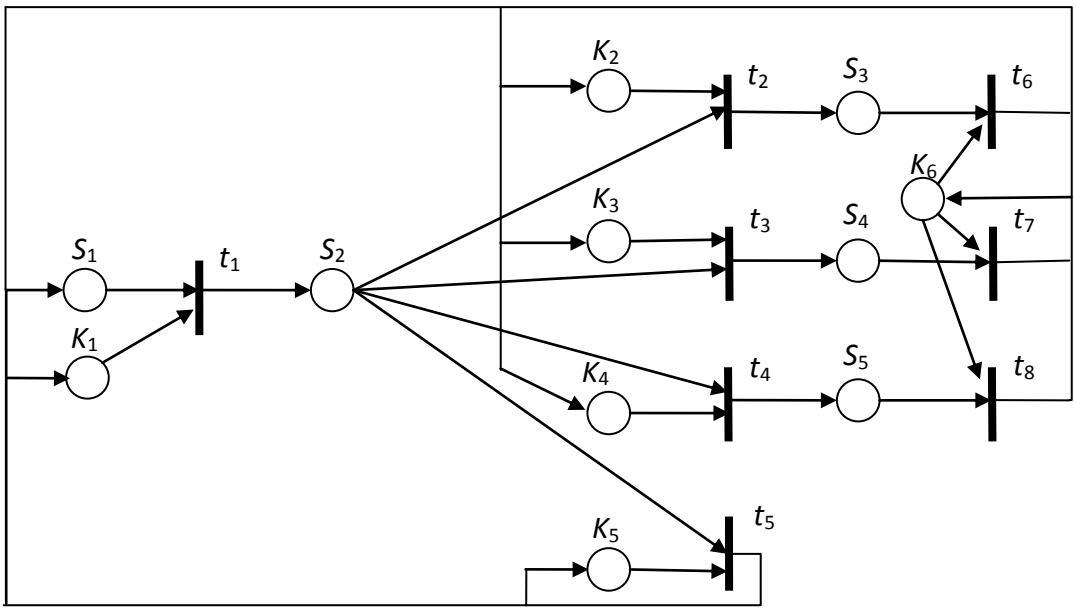

Рисунок 1 - Структура нечеткой сети Петри

В работе приняты следующие значения функций принадлежности: $m^0_1 = 1$, $m^0_{3,8,9,10} = 0$, $m^0_{4,5,6} = 1$, $f_{1\text{-}8} = 1$.

Динамика изменения маркировок НСП определяется следующими правилами:

1) *правило определения текущей маркировки.* Любое состояние НСП определяется вектором m, компоненты которого интерпретируются как

значения функции принадлежности наличия одного маркера в соответствующих позициях НСП;

2) *правило активности перехода*. Переход $t_k \in T$ НСП является активным, если выполнено условие:

$$\min_{(i\in\{1,2,\dots n\})\wedge(I(p_i,t_k)>0)} \{m_i\} \geq \lambda_k; \qquad (5)$$

3) *правило нечеткого срабатывания перехода*. Если переход $t_k \in T$ НСП является активным, то нечеткое срабатывание приводит к новой маркировке m^v, компоненты вектора которой определяются следующим образом:

$$m_i^v = 0, \quad (\forall p_i \in P) \wedge (I(p_i,t_k) > 0), \qquad (6)$$

$$m_j^v = \max\{m_j, \min_{i\in\{1,2,\dots n\})\wedge(I(p_i,t_k)>0)}\{m_i, f_k\}\}, \quad (\forall p_i \in P) \wedge (I(p_i,t_k) > 0)$$

Отмечается, что при начальной маркировке переход t_1 является активным при

$$m^0{}_2 \geq \lambda_1, \qquad (7)$$

т.е. в случае, если вероятность появления злоумышленника будет больше порога срабатывания перехода t_1. Далее производится анализ следующих переходов в информационной системе. Если условие (7) выполняется, тогда нечеткое срабатывание перехода t_1 приведет к новой маркировке m_1. При этом $m^1{}_1 = m^1{}_2 = 0$, поскольку позиции S_1 и K_1 являются входными для перехода. Для позиции S_2 : $m^1{}_3 = max\ \{0, min\ \{m^0{}_2, 1\}\}$, т.е. $m^1{}_3 = m^0{}_2 \geq \lambda_1$. Все остальные позиции остаются без изменений. Поскольку $m^1{}_{4,5,6} = 1$, то переходы t_2, t_3 и t_4 будут активными при выполнении условий $m^1{}_3 > \lambda_2$, $m^1{}_3 > \lambda_3$, $m^1{}_3 > \lambda_4$. Переход t_5 будет активным при выполнении условия: $min\ \{m^1{}_3, m^1{}_7\} > \lambda_5$ или

$$min\ \{m^0{}_2, m^0{}_7\} > \lambda_5. \qquad (8)$$

Анализ выражений (7) и (8) показал, что безопасная работа ИС достигается:

а) повышением значения коэффициента λ_1, что достигается корректной настройкой правил политики безопасности ИС;

б) уменьшением значения коэффициента λ_5, который представляет собой порог чувствительности системы активного аудита. Кроме того, необходимо добиваться увеличения коэффициента $m^1{}_7$.

Предложена структура системы активного аудита (рис. 2), которая включает в себя *набор сенсоров* для анализа и обработки информации о функционировании информационной системы и действиях пользователя, *базу данных*, в которой хранится полученная информация, *блок анализа и*

обработки данных для потоковой обработки поступающих данных и выработки управляющих воздействий на информационную систему, *блок реагирования*, воздействующий на информационную систему, *консоль администратора, журнал работы системы активного аудита.*

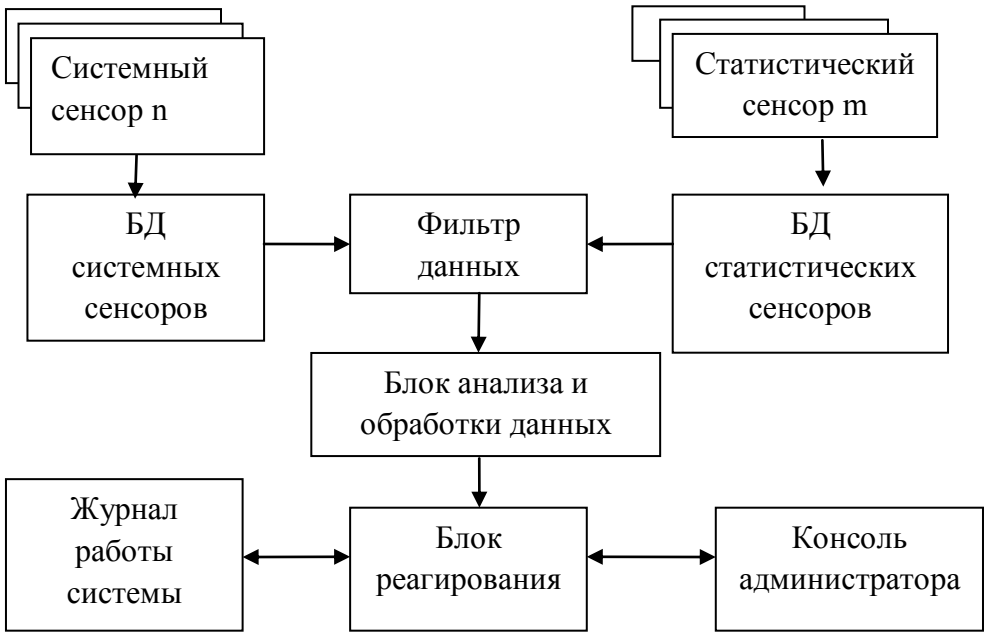

Рисунок 2 - Структура системы активного аудита

Системные сенсоры предназначены для анализа параметров системы и действий пользователя, а также выдачи предупреждений для обработки в блоке анализа и обработки данных о заранее заданных событиях, например, о попытках перебора паролей, монтирования носителей, входе/выходе пользователя из системы и т.д. *Статистические сенсоры* анализируют поведение каждого пользователя системы. При этом для каждого пользователя создаются отдельные профили, в которые заносятся информация о типичном поведении пользователя, собираемая в течение определенного интервала времени. *Фильтр данных* предназначен для удаления из очереди повторяющихся предупреждений для ускорения работы системы.

В третьей главе рассматривается метод построения системы активного аудита информационной системы на основе технологий искусственных иммунных систем.

Отмечается, что для повышения эффективности обработки входных сигналов необходимо:

1) обеспечить надёжное хранение поступающей информации до её обработки системой активного аудита;

2) обеспечить быструю обработку сигналов сенсоров с целью обнаружения атак системой активного аудита и принятия решения по предотвращению атаки;

3) обеспечить безопасное хранение необходимой информации в целях сохранения истории атак и обновления профилей пользователей.

Поведение информационной системы обычно характеризуется дискретными временными рядами наблюдений. При этом проблему обнаружения атак можно сформулировать как задачу «разладки», т.е. задачу выявления недопустимых отклонений в характеристиках системы.

Существует несколько методов анализа недопустимых отклонений, включающих в себя: сигнатурный метод и применение нейронных сетей. Однако данные методы не позволяют достичь оптимальных характеристик обнаружения внутренних атак. Нейросетевые методы обнаружения в принципе позволяют достичь приемлемых характеристик, но обладают такими существенными недостатками, как сложность выбора параметров и структуры нейронных сетей, ресурсоёмкий характер обучения нейронной сети, сложность дообучения / переобучения нейронной сети. Анализ показал, что достаточно перспективным является построение систем обнаружения атак на основе технологий искусственных иммунных систем. Этот метод обладает рядом преимуществ по сравнению с другими методами, обеспечивая высокую скорость работы, сравнительно простой алгоритм обучения, низкую ресурсоёмкость.

Особенностью иммунной системы живых организмов является способность отличать собственные клетки от любых чужеродных клеток и молекул, что дает основание использовать данный подход для построения интеллектуальной системы обнаружения атак в классе искусственных иммунных систем. Распознавание в иммунной системе живого организма основано на выработке т.н. *T*-клеток, выполняющих роль шаблонов чужеродных клеток. При построении искусственной иммунной системы данный процесс обобщается и выглядит следующим образом:

1. Определяются нормальные шаблоны активности системы (множество *S*) в виде строк равной длины *l*, составленных из букв конечного алфавита (рис. 3).

2. Генерируется набор детекторов *R*, каждый из которых не совпадает ни с одной из строк из нормального шаблона активности. При этом кандидат в детекторы считается совпадающим с нормальным шаблоном в том и только

том случае, когда совпадают символы в *r* одинаковых позициях. Величина *r* подбирается в соответствии с решаемой задачей.

3. Данные контролируются путем сопоставления детекторов с поведением системы. Любое совпадение на данном шаге означает изменение в работе системы (аномалию).

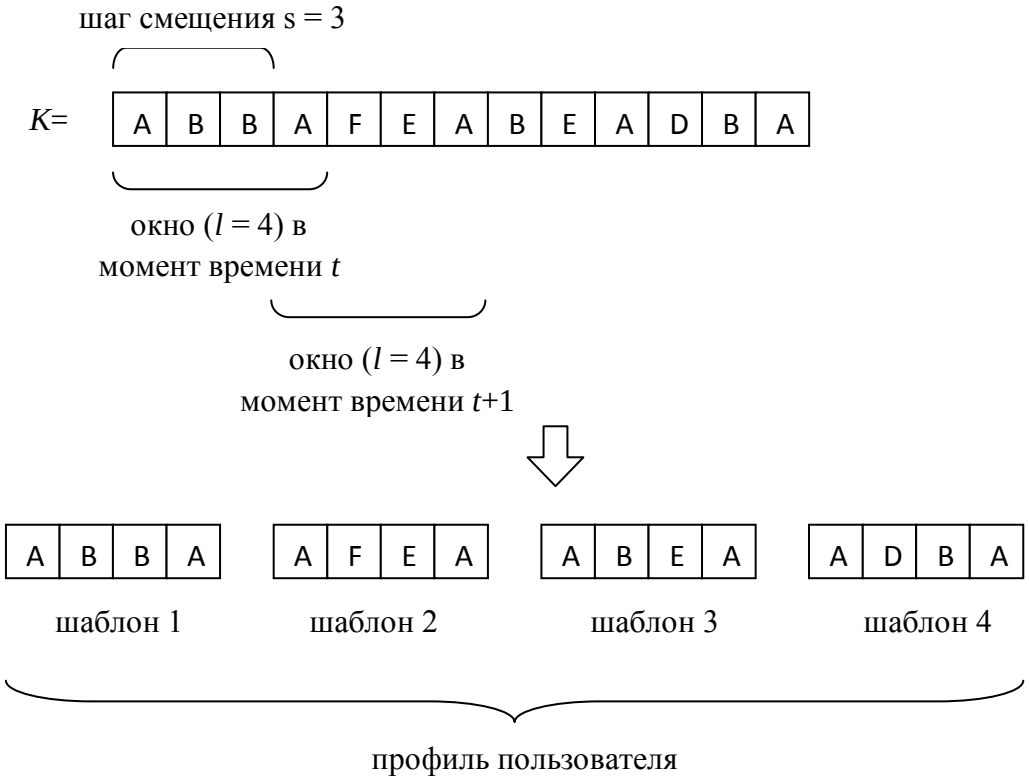

Рисунок 3 – Обработка входных данных для алгоритма отрицательного отбора (построение нормальных шаблонов активности)

Отмечается, что в известном варианте алгоритма отрицательного отбора детекторы генерировались случайным образом, а затем сравнивались с нормальными шаблонами активности для обнаружения совпадения. Для повышения эффективности процесса обработки входных сигналов, в работе предложен модифицированный алгоритм генерации детекторов, основанный на использовании генетического алгоритма.

В работе решена задача определения необходимого числа детекторов. Для этого использовались следующие исходные данные:

N_{R0} – число детекторов, сформированных алгоритмом генерации;

N_R – число детекторов, оставшихся после удаления детекторов, совпадающих с нормальными шаблонами активности;

N_S – число нормальных шаблонов активности;

P_m – вероятность совпадения двух случайных строк;

$f = (1 - P_m)^{N_S}$ – вероятность того, что случайная строка не совпадет с одним из N_s нормальных шаблонов активности;

P_f – вероятность того, что оставшиеся N_R детекторов не смогут обнаружить атаку.

Отмечается, что если величина P_m достаточно мала, а N_S – достаточно велико, то можно f и P_f аппроксимировать следующим образом:

$$f = (1 - P_m)^{N_S} \approx e^{-PmNs}; P_f = (1 - P_m)^{N_R} \approx e^{-P_m N_R}, \quad (9)$$

откуда, с учетом зависимости

$$N_R = N_{R0} * f = \frac{-\ln P_f}{P_m}, \quad (10)$$

вытекает выражение N_{R0}:

$$N_{R0} = \frac{-\ln P_f}{P_m * (1 - P_m)^{N_S}}. \quad (11)$$

Формула (11) позволяет определить число детекторов N_{R0}, которое необходимо сгенерировать с помощью генетического алгоритма как функцию вероятности обнаружения атаки (1 – P_f), числа нормальных шаблонов активности N_s и вероятности совпадения двух строк P_m.

Результаты тестирования эффективности искусственной иммунной системы с генерацией детекторов с помощью генетического алгоритма подтверждают преимущества использования предложенного модифицированного алгоритма генерации детекторов.

В четвертой главе обсуждаются результаты практической реализации исследовательского прототипа системы активного аудита. В качестве базовой платформы для реализации системы выбрана ОС Microsoft Windows и технология .NET, которая обладает такими преимуществами, как возможность взаимодействия служб и программ, написанных на разных языках программирования, гибкость, высокая скорость работы.

Исследуется задача выбора системы хранения информации о пользователях системы активного аудита, профилях и настройках. Учитывая, что наибольшее распространение на российском рынке в настоящее время получили СУБД MySQL и Microsoft SQL, произведено сравнительное тестирование этих систем СУБД, которое показало преимущества использования Microsoft SQL 2005 в качестве СУБД для хранения базы знаний разрабатываемой системы активного аудита.

В работе представлен пример реализации сенсора системы активного аудита безопасности, отмечается удобство использования интерфейса Windows Management Interface (WMI) для сбора информации об информационной системе.

В работе выполнена сравнительная оценка эффективности системы аудита на основе искусственных иммунных систем и системы на основе нейронных сетей, а также получена зависимость эффективности обнаружения атак от параметров искусственной иммунной системы (рис. 4, 5).

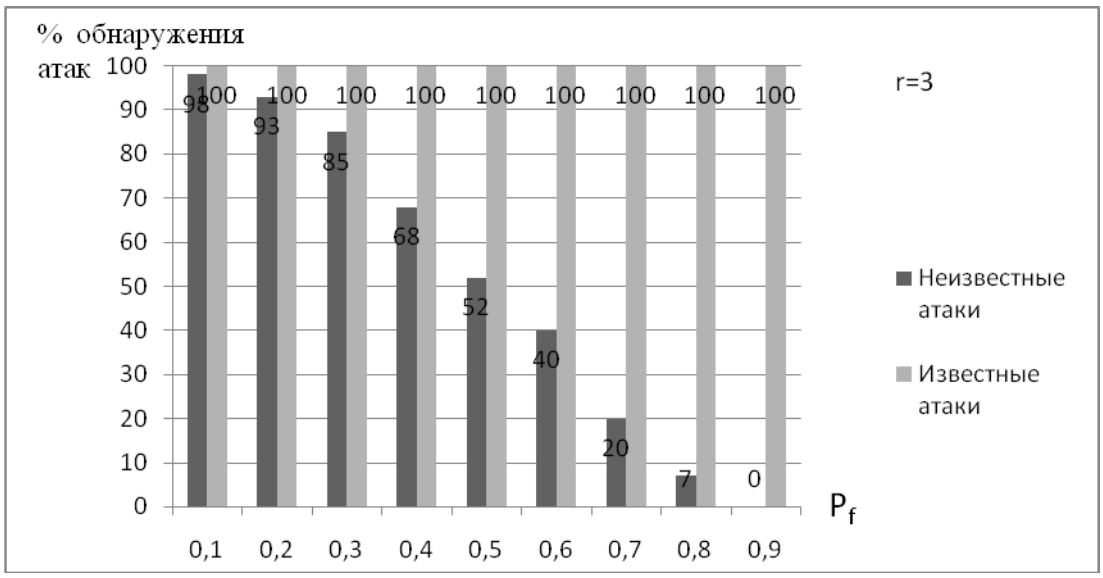

Рисунок 4 – Зависимость эффективности обнаружения атак от параметра P_f

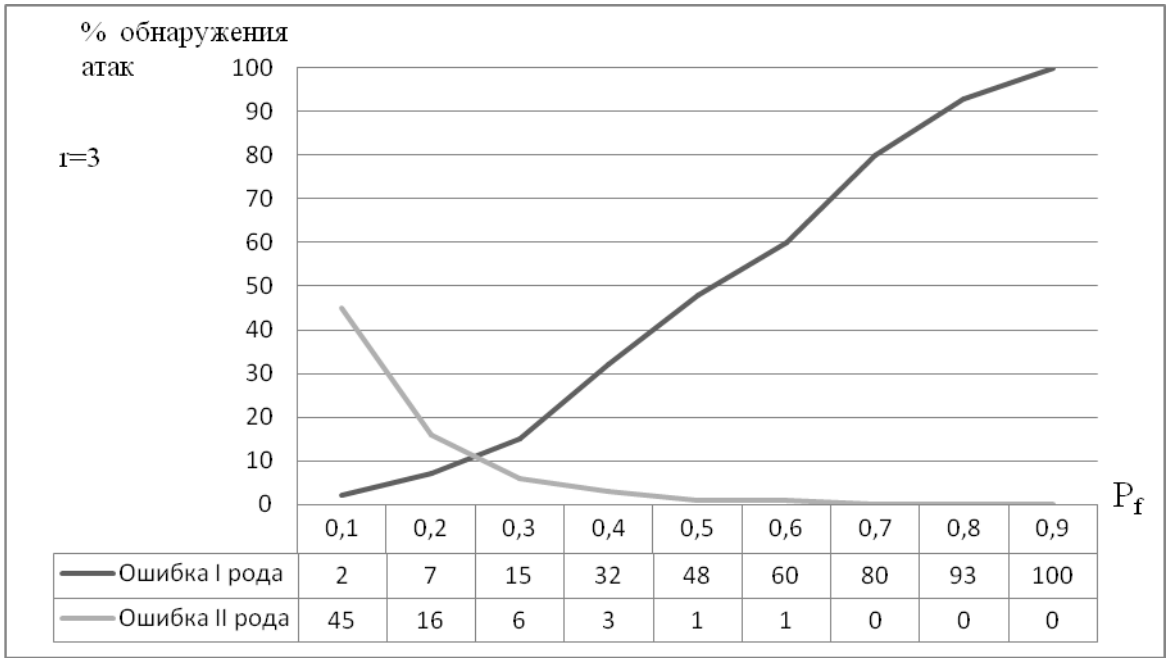

Рисунок 5 – Зависимость ошибок I и II рода при обнаружения атак от параметра P_f

Из графиков следует, что по мере роста параметра P_f ошибка первого рода возрастает, а ошибка второго рода уменьшается. Иначе говоря, при снижении качества процесса обнаружения атак (что вызвано уменьшением

числа генерируемых детекторов искусственной иммунной системы), вероятность пропуска неизвестных атак увеличивается, однако уменьшается вероятность ложных срабатываний системы, в результате которых легальные действия пользователя принимаются за атаку.

Таким образом, необходимо подобрать такие значения r и P_f, при которых работа системы активного аудита была бы наиболее эффективной. Очевидно, что наибольшая эффективность достигается при значениях P_f=0,2…0,3 и при r = 3. При этом значения ошибок первого и второго рода - минимамльны. В случае необходимости задачу выбора значений этих параметров можно возложить на администратора системы активного аудита.

При обнаружении атаки система активного аудита принимает решение о способе её нейтрализации. Система выработки решения построена на основе нечёткой логики, позволяющей выработать верное действие в зависимости от типа объекта, подвергающегося угрозе и условий выполнения атаки. Эти действия могут включать в себя: уведомление администратора системы активного аудита о происходящей атаке, блокирование работы пользователя в системе, перезагрузку рабочей станции, выгрузку программ из памяти рабочей станции и т.д.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработан комплекс системных моделей системы активного аудита ИС с применением SADT-методологии, позволивших выделить основные бизнес-процессы, лежащие в основе её функционирования, и сформулировать требования к реализации системы, исходя из современных требований к обеспечению защищенности ИС.

2. Предложены алгоритмы активного аудита ИС, основанные на применении технологий искусственных иммунных систем, что позволяет повысить эффективность обнаружения атак за счёт отказа от использования конечного множества сигнатур известных атак и выполнить переход к использованию более общего принципа распознавания «свой - чужой».

3. Предложен модифицированный алгоритм генерации детекторов системы обнаружения атак, основанный на использовании генетического алгоритма, что позволяет сократить сроки обучения и повысить эффективность функционирования системы активного аудита на основе механизмов искусственной иммунной системы.

4. Произведено сравнительное тестирование предложенных алгоритмов активного аудита ИС на основе искусственной иммунной системы и нейронной сети. Результаты тестирования показали преимущество

использования искусственной иммунной системы при решении задачи обнаружения атак. В частности, нейронная сеть показывала лучшее значение ошибки второго рода, однако не была способна с достаточной надёжностью обнаруживать неизвестные типы атак.

5. Разработан исследовательский прототип системы активного аудита ИС на основе технологии искусственных иммунных систем. Тестирование прототипа доказало эффективность его использования для обнаружения известных и неизвестных внутренних атак. В частности, в проведенных экспериментах разработанный прототип позволил обнаруживать до 85% атак, при этом в проведенных экспериментах ошибка второго рода не превысила 6%. Созданный прототип интеллектуальной системы активного аудита ИС может быть интегрирован в существующую инфраструктуру систем управления информационной безопасностью ИС, в том числе в гетерогенных ЛВС.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикация в периодическом издании из списка ВАК:

1. Комплексный подход к построению интеллектуальной системы обнаружения атак / Васильев В.И., Кашаев Т.Р., Свечников Л.А. // Системы управления и информационные технологии, №2, 2007. – С. 76-81.

Другие публикации:

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

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

4. Система обработки и анализа медицинской информации / Кашаев Т.Р., Кашаев М.Ш. // Вопросы теоретической и практической медицины: Материалы 69-й республиканской итоговой научно-практической конференции студентов и молодых учёных Республики Башкортостан с международным участием. – Уфа: БГМУ, 2004. – С. 255-256.

5. Система активного аудита / Кашаев Т.Р. // Информационная безопасность: Материалы VII Международной научно-практической конференции. – Таганрог: Изд-во ТРТУ, 2005. – С. 139-142.

6. Применение скрытых Марковских моделей для построения систем активного аудита / Кашаев Т.Р. // Компьютерные науки и информационные

технологии: Труды 7-го Международного семинара (CSIT-2005), Т. 3. –Уфа, 2005. – С. 224 - 227 (на англ. языке).

7. Использование адаптивных профилей для обнаружения внутренних атак в локальных вычислительных сетях / Васильев В.И., Кашаев Т.Р. // Информационная безопасность: Материалы VIII Международной научно-практической конференции. – Таганрог: Изд-во ТРТУ, 2006. – С. 177-180.

8. Обнаружение атак на основе профилей пользователя / Васильев В.И., Кашаев Т.Р. // Компьютерные науки и информационные технологии: Труды 8-го Международного семинара (CSIT-2006), Т.3. – Карлсруэ, Германия, 2006. – С. 224 – 227 (на англ. языке).

9. Применение нечетких сетей Петри для анализа безопасности локальной вычислительной сети / Васильев В.И., Кашаев Т.Р. // Вычислительная техника и новые информационные технологии: Межвузовский научный сборник. Вып. 6. – Уфа: УГАТУ, 2007. – С. 166 - 170.

10. Моделирование состояния безопасности локальной вычислительной сети / Кашаев Т.Р. // Интеллектуальные системы обработки информации и управления: Материалы 2-й региональной зимней школы-семинара аспирантов и молодых ученых. - Т.1. – Уфа: УГАТУ, 2007. – С. 171 - 174.

11. Автоматизированный анализ состояния безопасности ЛВС / Кашаев Т.Р. // Гагаринские чтения: Материалы XXXIII Всероссийской конференции. - Т.4. - М.: МАТИ, 2007. – С. 145.

12. Васильев В.И., Кашаев Т.Р. Свид. об офиц. рег. программы для ЭВМ № 2008611107. Модуль обнаружения атак и принятия решений системы активного аудита. М.: Роспатент, 2008. Зарег. 29.02.2008.

13. Применение искусственной иммунной системы для решения задачи обнаружения атак / Кашаев Т.Р. // Материалы 3-й Всероссийской зимней школы – семинара аспирантов и молодых ученых. – Уфа: УГАТУ, 2008. – С. 326-332.

КАШАЕВ Тимур Рустамович

АЛГОРИТМЫ АКТИВНОГО АУДИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

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

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати 12.09.2008. 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 №375.
ГОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К. Маркса, 12.