Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

На правах рукописи

СКОПЦОВ
Алексей Михайлович

КОМПЛЕКСНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ ПРЕДПРИЯТИЯ

АВТОРЕФЕРАТ
диссертации на соискание степени магистра технических наук
по специальности 1–38 80 04 Технология приборостроения

Научный руководитель
канд. техн.наук, доцент
БОРОВИКОВ Сергей Максимович

Минск 2016

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель **Боровиков Сергей Максимович,**
кандидат технических наук, доцент, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент **БОНДАРИК Василий Михайлович,**
кандидат технических наук, доцент, доцент кафедры электронной техники и технологии, заместитель декана факультета непрерывного и дистанционного обучения учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «25» октября 2016 г. года в $14^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П.Бровки, 6, 1 уч. корп., ауд. 415, тел.: 293-20-80, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

СОГЛАСОВАНО:
_____С.М. Боровиков
«___» _____ 2016 г.

ВВЕДЕНИЕ

Современный этап развития информационных систем основан на достижениях телекоммуникационных технологий, применяемых для распределенной обработки информации. Это обусловило появление нового вида атак на информационные системы, распределенных как во времени, так и в пространстве.

Постоянно возникающие новые виды атак в совокупности с ростом общего количества атак на информационные системы обуславливает необходимость применения более гибких средств обнаружения и реагирования на атаки в качестве дополнения к статичным средствам защиты информации. В таких условиях актуальна разработка новых инструментов защиты информации. Этими средствами являются, в том числе, и системы обнаружения атак.

Таким образом, перед исследователями стоит цель изучить данную отрасль науки для получения максимально эффективных параметров разрабатываемых систем обнаружения атак. Для учета этих особенностей комплекс обнаружения компьютерных атак должен выполнять распределенный сбор из нескольких источников и интеллектуальный анализ информации, а также быть способным обнаруживать новые атакующие воздействия. Существующие системы выявления компьютерных атак не в полной мере обладают данными свойствами.

Для распределенного сбора и анализа информации современные программные и аппаратные комплексы обнаружения атак обладают набором датчиков. Так как различные датчики представляют собой независимые сущности, осуществляющие независимый сбор и интеллектуальный анализ данных, то они могут быть представлены агентами, а комплекс обнаружения атак – многоагентной системой. Для обнаружения новых атакующих воздействий должен применять адаптивный метод обнаружения атак.

Оптимизация средств обнаружения атак позволит решить огромный круг задач по обеспечению безопасности информационных систем предприятий.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Современные системы обнаружения вторжений в информационные структуры, представленные различными производителями на рынке Республики Беларусь, обладают или ограниченными возможностями по применению, либо имеют очень высокую стоимость.

В диссертации рассматриваются особенности функционирования информационных систем, наиболее распространенные компьютерные атаки на компьютерные сети, процессы реализации этих атак и существующие средства обнаружения вторжений.

Таким образом, актуальность темы обусловлена необходимостью разработки комплексной системы обнаружения компьютерных атак, позволяющей проводить интеллектуальный анализ данных следов атак и их совместный контроль.

Степень разработанности проблемы

Системы обнаружения вторжений в информационные структуры, представленные в Республике Беларусь, зачастую обладают недостаточным функционалом, либо имеют высокую стоимость в сочетании с избыточной производительностью. Поэтому существует необходимость разработки такого всестороннего решения, которое повысит эффективность обнаружения компьютерных атак на компьютерную сеть, будет обладать необходимой гибкостью и масштабируемостью, а также широким функционалом и простотой в использовании.

Цель и задачи исследования

Целью диссертации является разработка комплексной системы обнаружения атак на информационную систему предприятия, позволяющей проводить распределенный интеллектуальный анализ данных о наличии следов атак в основных компонентах информационной системы и их совместный анализ.

Для выполнения поставленной цели в диссертации были сформулированы следующие **задачи**:

– на основе анализа предметной области разработать подход к структуре и составу комплексной многоагентной системы обнаружения компьютерных атак;

– разработать методику совместного анализа агентами данных о состоянии информационной системы;

– провести оценку эффективности предложенной в диссертационном исследовании модели и метода совместного анализа, используя разработанные решения.

Объектом исследования является информационная система предприятия.

Предметом работы являются методы работы систем обнаружения атак.

Область исследования

Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 Технология приборостроения.

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области информационной безопасности корпоративных информационных систем, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Теоретической основой исследований являются методы теории графов, теории нейронных сетей, многоагентных систем, теории принятия решений. Для оценки эффективности предлагаемых решений используются методы математического и имитационного моделирования.

Данная область науки относительно молода, однако **методологическая основа** для проведения исследований в этой области уже сформирована. Об этом свидетельствуют работы таких ведущих исследователей, как А.В. Лукацкий,

А.В. Аграновский, В.А. Галатенко, А.А. Грушо, П.Д Зегжда, Е.В. Касперский, Ю.К. Язов, Д. Деннинг, К. Лендвер, М. Ранум и др.

Информационная база исследования сформирована на основе открытой информации, предоставляемой производителями систем обеспечения безопасности, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Инструментальной базой исследований являются приложения серверного программного обеспечения, системы управления базами данных *Postgre SQL*, *Microsoft SQL Server*, программные средства управления и мониторинга информационных систем.

Научная новизна

Научная новизна и значимость полученных результатов заключается в следующем:

– предложена структура и состав многоагентной системы обнаружения атак, позволяющей осуществлять сбор сведений из разных источников, и на основе анализа делать вывод о состоянии информационной системы;

– разработан подход к принятию агентами совместного решения, на основании которого происходит оценка состояния информационной системы в целом;

– разработана методика обнаружения компьютерных атак с использованием многоагентных технологий, позволяющая обучить комплексную систему обнаружения атак.

Теоретическая значимость диссертации заключается в том, что в ней предложена структура и состав комплексной системы обнаружения атак, позволяющей осуществлять сбор сведений из разных источников и, на основе анализа, делать вывод о состоянии информационной системы; разработана методика обнаружения атак с использованием многоагентных технологий, позволяющая обучить многоагентный комплекс обнаружения атак и использовать его для дальнейшего обнаружения вторжений.

Практическая значимость диссертации состоит в том, что использование разработанной комплексной системы обнаружения атак позволяет повысить эффективность обнаружения атак на информационную инфраструктуру предприятия, разработанный прототип может быть интегрирован в существующее информационное окружение и использоваться системой управления информационной безопасностью предприятия.

Основные положения, выносимые на защиту:

1. Комплексная система обнаружения атак, осуществляющая сбор сведений о состоянии информационной системы из нескольких источников и их нейросетевой анализ, позволяющая обнаружить атаки и информировать оператора системы о вторжении.

2. Алгоритмы анализа данных о состоянии информационной системы и принятия совместного решения, позволяющая реализовать функцию принятия решения в отношении обнаруженной угрозы.

3. Методика обнаружения атак на информационную систему, позволяющая использовать результаты работы для самообучения.

Апробация и внедрение результатов исследования

Результаты исследования неоднократно были применены при проектировании систем обеспечения информационной безопасности в Республике Беларусь на системах различного уровня и масштаба, имеется акт внедрения (использования) результатов научно-исследовательской работы в ООО «Студияя по разработке программного обеспечения».

Публикации

Основные положение работы и результаты диссертации изложены в четырех опубликованных работах общим объемом 6 страниц (авторский объем 6 страниц).

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен анализ информационных систем предприятий, рассмотрены типовые стадии компьютерных атак, а также исследованы существующие системы и методы обнаружения компьютерных атак. **Во второй главе** представлена структура комплексной многоагентной системы обнаружения атак и ее агентов, описываются ощущения агентов серверов, маршрутизаторов и сети, их убеждения и принципы взаимодействия. **В третьей главе** показывается принцип разработки архитектуры программной реализации агента, пользовательского интерфейса. Приведены результаты разработки модуля получения и обработки данных, модуля анализа. Описывается методика обнаружения компьютерных атак. **В четвертой главе** приведены результаты экспериментов, в ходе которых проводятся испытания разработанной комплексной системы обнаружения атак. **В приложении** представлены публикации автора и акт внедрения.

Объем диссертационной работы составляет 84 страниц. Работа содержит 15 иллюстраций, 10 таблиц, библиографический список из 50 наименований, список собственных публикаций, акт внедрения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассматриваются общие вопросы построения комплексных систем обнаружения атак, дается краткая характеристика тенденциям и современной ситуации в области обеспечения безопасности, выделяется актуальность темы исследований.

В **общей характеристике работы** сформулированы ее цель и задачи, показана текущая ситуация в области построения систем обнаружения атак, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации, наличие публикаций, а также, структура и объем диссертации.

В **первой главе** проведен анализ информационных систем предприятий. По результатам анализа выделен типовой состав информационной системы предприятия: серверы, маршрутизаторы, разделяющие между собой подсети информационной системы, а также внешнюю сеть Интернет, рабочие станции.

Проведен анализ инцидентов информационной безопасности в информационных системах. По результатам анализа определено множество атак, принципы их работы и выделены основные элементы информационных систем, чаше всего подвергающиеся атакам. Проанализированы основные этапы атакующих воздействий и выделены основные пути реализации атак. Проанализированы основные группы методов обнаружения атак и выбраны группы, наиболее подходящие для обнаружения атак на различных стадиях.

Определены основные источники сведений о состоянии элементов информационной системы важные для задачи обнаружения атак: журналы событий и информация о процессах, происходящих на серверах информационной системы, журналы маршрутизаторов, пакеты, передаваемые по сети, журналы событий и информация о процессах, происходящих на рабочих станциях.

Проанализированы основные современные системы обнаружения компьютерных атак: *Snort, Bro, Prelude, OSSEC, Suricata*. Рассмотрены основные тенденции развития вышеперечисленных решений. Определен перечень критериев и их значений, которым должна удовлетворять система обнаружения атак:

– адаптивность, т.е. способность обнаруживать модифицированные реализации известных атак и новые виды атак;

– проактивность системы для реакции на атаку с помощью встроенных механизмов;

– открытость к добавлению новых анализируемых ресурсов информационной системы;

– централизованное и распределенное управление;

– защищенность компонентов системы обнаружения атак;

– многоуровневость системы обнаружения атак, которая должна собирать сведения о состоянии информационной системы из различных источников на различных уровнях наблюдения – уровень сети, сервера и хоста.

Во **второй главе** предложена архитектура многоагентной системы обнаружения атак, включающая в себя множество взаимодействующих интеллектуальных агентов и соответствующая выделенным в ходе анализа типовым компонентам информационной системы и источникам сведений, подлежащих анализу для задачи обнаружения атак (рисунок 1).

Рисунок 1 – Архитектура многоагентной системы обнаружения атак

В итоге многоагентная системы обнаружения атак имеет вид *MAS:*

$$MAS = (A_R, A_N, A_S, A_W),$$

где A_R – множество агентов маршрутизаторов, делится на подмножество агентов внешних маршрутизаторов A^0 и подмножество агентов A^v внутренних маршрутизаторов. Как на маршрутизаторах, так и на коммутаторах существует возможность ведения журнала событий. Агент маршрутизатора производит анализ сведений данного журнала;

A_N – множество агентов сети, анализирующие сведения о пакетах, передаваемых по сети. Для того чтобы анализировать сведения о пакетах, передаваемых по сети, сетевой агент работает как сниффер, т.е. перехватывает все пакеты и анализирует их. Однако подобные программы работают только в пределах одного сегмента сети. Поэтому данный агент располагается в каждом сегменте;

A_S – множество агентов серверов. На каждом сервере располагаются несколько агентов различных типов, которые анализируют события, наиболее критичные с точки зрения безопасности;

A_W – множество агентов рабочих станций. На каждой рабочей станции располагается несколько агентов различных типов A_W.

Относительно задачи обнаружения атак с учетом предыдущих выводов предлагается использовать одинаковую структуру для всех типов агентов обнаружения атак и описывать их состоянием:

– P – ощущение, представляющее собой информацию об окружающей среде, собираемую агентом, т.е. набор входных данных агента, различается в зависимости от типа агента;

– B – множество убеждений, т.е. сведений и знаний об окружающей агента среде. Убеждения агента представляют собой нейронную сеть. На первом этапе агенты собирают сведения о нормальном функционировании информационной системы либо злоумышленных действиях, и на основе них создается обучающая выборка для нейронной сети;

– S – конкретное состояние среды, т.е. конкретные значения входных данных и результата классификации их нейронной сетью;

– G – цели, определяющиеся как желаемое состояние среды;

– I –намерения, т.е. множество возможных планов действий агента.

Архитектура управления агента обнаружения атак имеет следующий вид (рисунок 2):

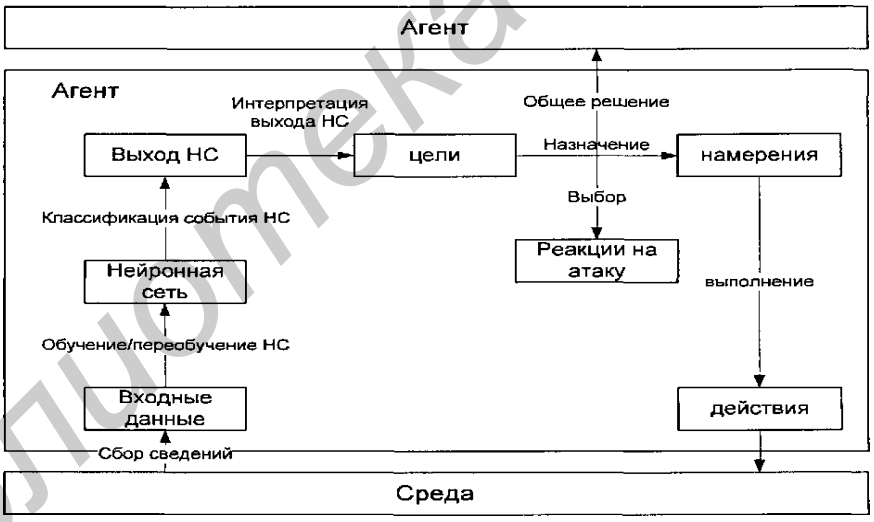

Рисунок 2 – Архитектура управления агента обнаружения атак

Показано, что агенты обнаружения атак обладают следующими базовыми функциями:

– сбор сведений, которые собираются как для обучения и в случае необходимости переобучения нейронной сети, так и для обнаружения атак;

– обучение и переобучение нейронной сети. Данная функция отвечает за формирование нейронной сети и, в случае необходимости пересмотра убеждений агента, построение новой нейронной сети;

– классификация события нейронной сетью. Получение результатов оценки собранных сведений об информационной системой нейронной сетью;

– интерпретация выхода нейронной сети. В зависимости от значения выхода нейронной сети агент выбирает набор элементарных действий, которые необходимо выполнить в данной ситуации;

– назначение на уровне локального планирования набора элементарных действий агента, которые необходимо выполнить. В случае необходимости задействуется уровень глобального планирования – взаимодействия с другими агентами. Агент принимает окончательный план действий, определяя последовательность элементарных действий;

– выполнение агентом выбранных элементарных действий.

В **третьей главе** предложена архитектура агента, имеющая следующий вид (рисунок 3):

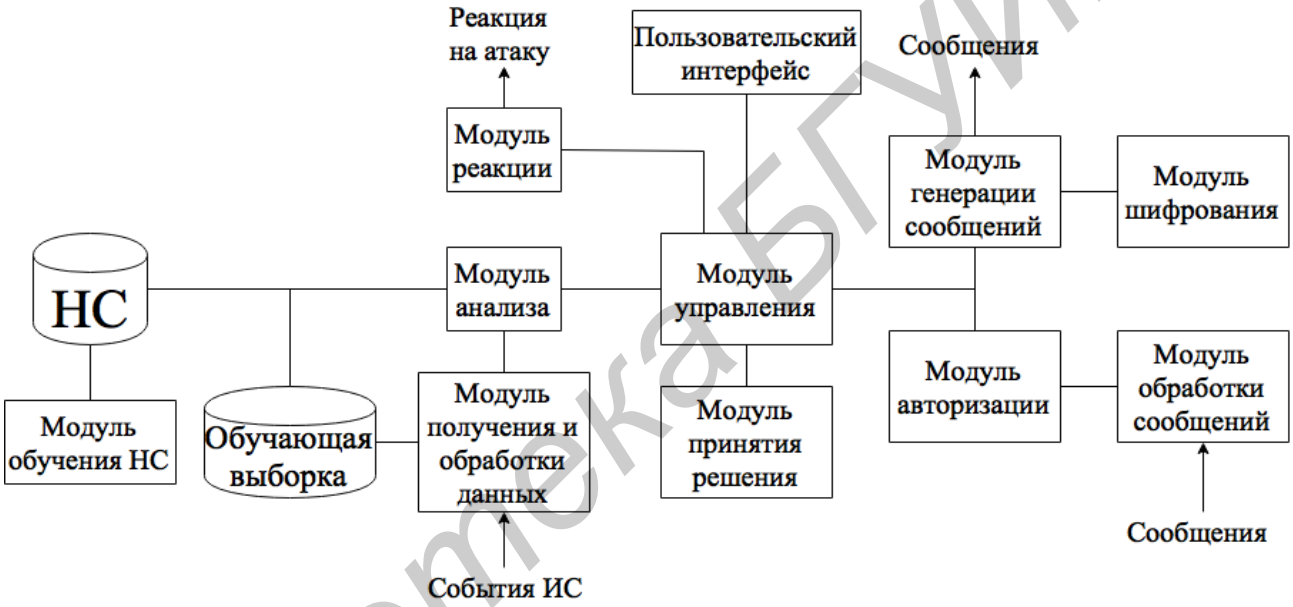

Рисунок 3 – Архитектура агента обнаружения вторжений

Раскрыто содержание модулей, входящих в структуру агента обнаружения вторжений.

Модуль управления осуществляет получение настроек из пользовательского интерфейса и передачу результатов анализа сведений о состоянии информационной системы агентом на пользовательский интерфейс. Также он производит аутентификацию субъекта взаимодействия, общую настройку агента, запуск процесса анализа, процесса принятия общего решения, передачу данных и инициацию процесса генерации сообщений, управляет реакцией агента.

Модуль получения и обработки данных получает данные из определенного источника сведений о состоянии информационной системы, проводит их преобразование в вид, необходимый для передачи на вход нейронной сети. Полученные данные передаются на вход модулю анализа и записываются в базу данных – обучающую выборку.

Модуль обучения нейронной сети получает данные из базы данных, хранящей обучающую выборку за определенный период времени и запускает процедуру обучения обратного распространения ошибки. Результатом выполнения данной процедуры является нейронная сеть.

Модуль анализа передает данные, полученные от модуля получения и обработки данных, и передает их для анализа на вход нейронной сети. Получив результат анализа, выход нейронной сети записывается в базу данных и интерпретируется, и событие либо игнорируется, либо формируются упорядоченные предпочтения агента и управление передается на модуль управления для инициации принятия общего решения агентами, либо управление передается модулю управления для формирования реакции агента на атаку.

Модуль реакции осуществляет выполнение намерений агента. В зависимости от типа агента и настроек, агент может сообщить сведения об атаке специалисту по защите информации, отправить сетевой пакет, сообщающий атакующему узлу о недоступности узла, сети или сервиса, или приостановить или завершить процесс.

Модуль принятия общего решения формирует упорядоченные предпочтения агента и инструктирует модуль управления сгенерировать и отравить сообщения своим соседям об инициации процедуры принятия общего решения. После получения наборов упорядоченных предпочтений, модуль проводит процедуру голосования. В случае если совместное решение показало ошибку агента, запускается таймер. По истечению времени таймера процедура повторяется снова, но не более *n* раз. Если после повторений процедуры, будет подтверждена ошибка агента, уменьшается его показатель качества.

Модуль генерации сообщений в зависимости от запроса формирует сообщите, содержащее настройки, сообщение, запрашивающее ситуацию, сообщение, инициирующее принятие общего решения.

Модуль обработки сообщений в зависимости от пришедшего сообщения передает полученные настройки модулю управления, передает запрос модулю управления на отправку ситуации или упорядоченных предпочтений в ответ на запрос.

Модуль шифрования используется для шифрования сообщений, которыми обмениваются агенты.

Модуль аутентификации используется для идентификации и аутентификации других агентов и специалиста по защите информации, пытающегося получить доступ к агенту.

На основе разработанных модулей агентов комплексной системы обнаружения компьютерных атак реализуется механизм обнаружения вторжений и реакции в соответствии с принятыми убеждениями агентов.

В **четвертой главе** был проведен ряд экспериментов на программно реализованном исследовательском прототипе системы обнаружения компьютерных атак. Эксперименты проводились на фрагменте сети ООО «Студия по разработке программного обеспечения», состоящей из сервера, двух маршрутизаторов, двух подсетей и 4 рабочих станций.

Были установлены 4 агента рабочей станции, 2 агента сети, 2 агента маршрутизатора и 1 агент сервера – по одному агенту на каждый элемент инфраструктуры (рисунок 4):

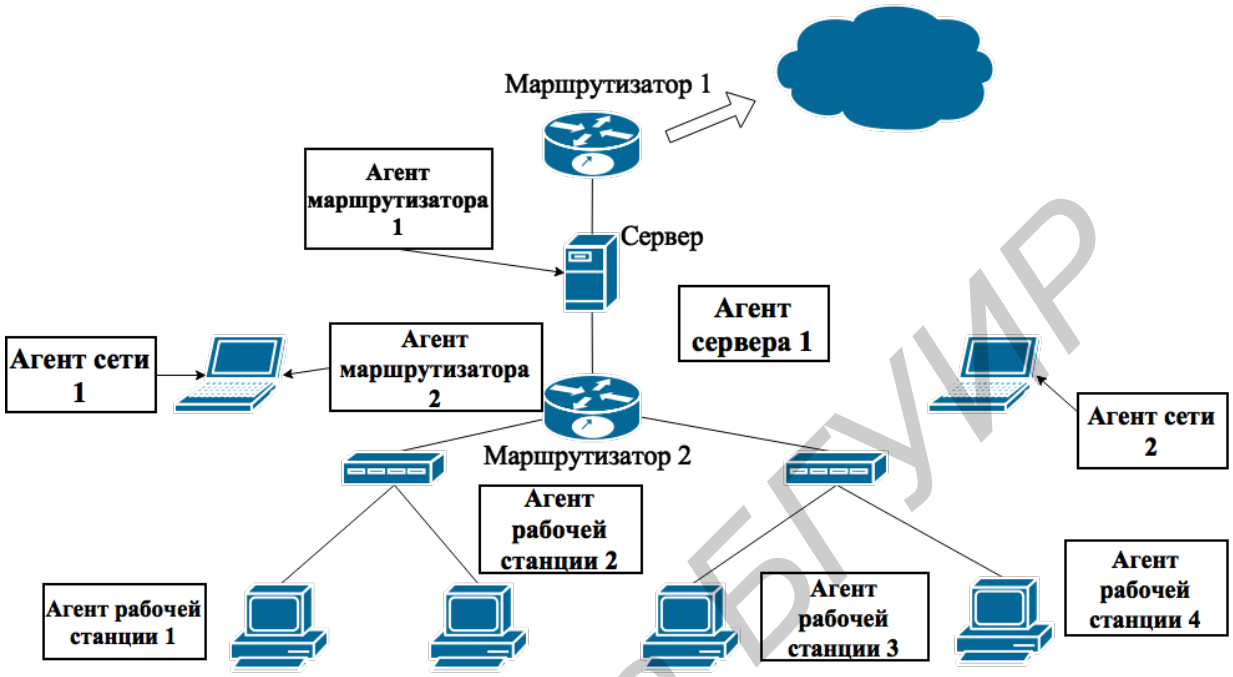

Рисунок 4 – Архитектура тестовой сети

В ходе первого эксперимента проверяется возможность обнаружения атак и адаптивность нейросетевого анализа. В рамках первой группы испытаний проверяется реакция системы на атаки, внесенные в обучающие выборки нейросети агентов (рисунок 5).

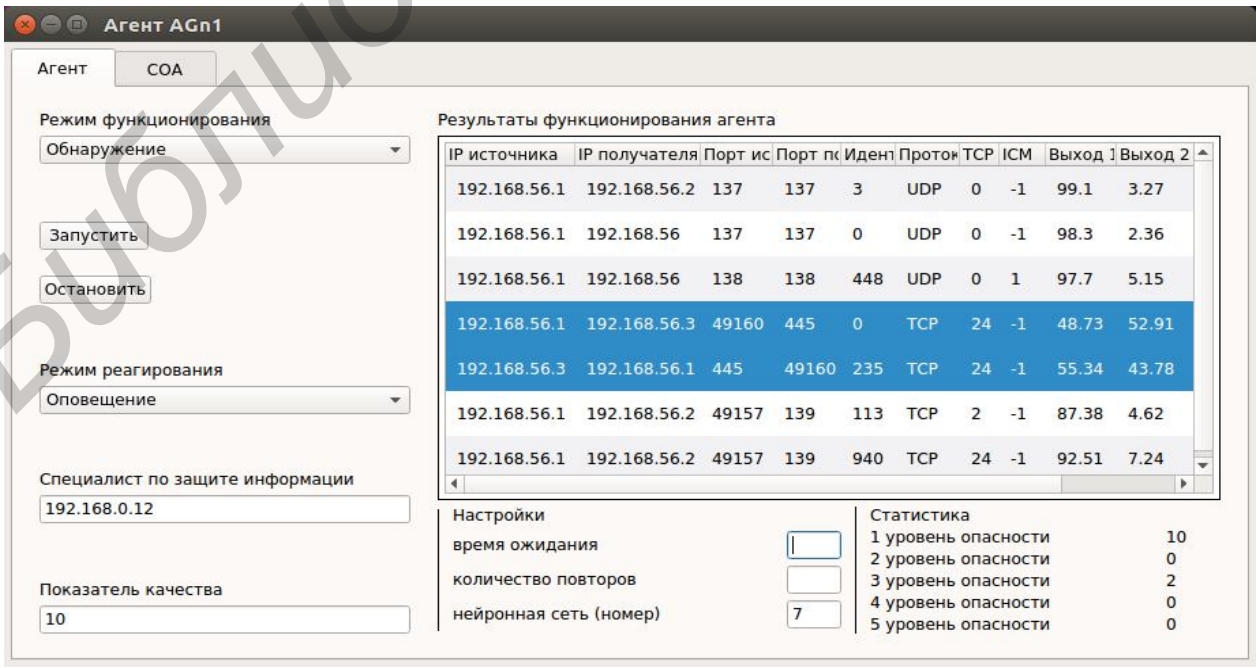

Рисунок 5 – Результат реакции системы на атаки

Во втором эксперименте проверяется предложенный алгоритм принятия совместного решения, проверяется реакция системы обнаружения атак на атакующие воздействия, не внесенные в обучающие выборки нейронной сети агентов.

Злоумышленник, находясь на рабочей станции №1 под учетной записью user1, осуществляет успешную попытку доступа к файлу паролей сервера.

В результате принятия общего решения уровень опасности для ИС был определен как «выше среднего», и было отправлено извещение специалисту по защите информации.

В **заключении** сформулированы основные научные и практические результаты.

ЗАКЛЮЧЕНИЕ

1. Разработаны подходы к структуре и составу комплексной многоагентной системы обнаружения компьютерных атак, включающей в себя агентов рабочих станций, серверов, маршрутизаторов и сетей и позволяющей осуществлять сбор сведений из разных источников и, анализируя их совместно, делать вывод о состоянии информационной системы.

2. Разработана методика принятия агентами совместного решения, позволяющий сформировать круглый стол агентов и на основании результатов анализа сведений, полученных из различных источников, оценить состояние информационной системы в целом.

3. Проведена оценка эффективности всех предложенных в диссертационном исследовании методов, используя разработанные решения.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1–А] Скопцов, А. М. Структура агентов системы обнаружения вторжений в информационную систему / А. М. Скопцов // Материалы работы конференции «Актуальные вызовы современной науки. Выпуск 3». – Переяслав-Хмельницкий. – 2016 – С. 44-46.

[2–А] Скопцов, А. М. Типовые стадии компьютерных атак / А. М. Скопцов // Материалы работы конференции «Актуальные вызовы современной науки. Выпуск 4». – Переяслав-Хмельницкий. – 2016 – С. 85-88.

[3–А] Скопцов, А. М. Основные принципы организации защищенных информационных систем / А. М. Скопцов // Материалы работы конференции «Актуальные научные исследования в современном мире». – Киев – 2016 – (в печати).

[4–А] Скопцов, А.М. Структурно-организационные меры при организации защищенных информационных систем/ А.М. Скопцов. // Материалы работы XII международной научно-практической конференции «теоретические и практические проблемы развития современной науки» – НИЦ «Апробация.рф» – (в печати).

РЭЗЮМЭ

Скапцоў Аляксей Міхайлавіч

Комплексная сістэма выяўлення нападаў на інфармацыйную сыстэму прадпрыемства

Ключавыя словы: інфармацыйная сістэма, інфармацыйная бяспека, выяўленне нападаў, шматагентная сістэма.

Мэта работы: распрацоўка сістэму выяулення нападкаў, якая дазваляе праводзіць размеркаваны інтэлектуальны аналіз дадзеных аб наяўнасці слядоў нападаў у асноўных кампанентах інфармацыйнай сістэмы і іх сумесны аналіз.

Атрыманыя вынікі і іх навізна

Прапанаваная структура і склад шматагентнай сістэмы, якая дазваляе ажыццяўляць збор звестак з розных сродкаў і, аналізуючы іх сумесна, рабіць выснову пра стан інфармацыйнай сістэмы. Распрацавана методыка выяўлення нападаў з выкарыстаннем шматагентных тэхналогій, якая дазваляе навучыць шматагентную сістэму выяўлення нападаў і выкарыстоўваць яе для далейшага выяўлення нападаў.

Ступень выкарыстання: вынікі ўкаранены ў працэс распрацы сістэмы інфармацыйнай бяспекі на «Студыя распрацоўкі праграммных сродкаў»

Вобласць ужывання: распрацоўка сістем інфармацыйная бяспекі, інфармацыйная бяспека прадпрыемств.

РЕЗЮМЕ

Скопцов Алексей Михайлович

Комплексная система обнаружения атак на информационную систему предприятия

Ключевые слова: информационная система, информационная безопасность, обнаружение атак, многоагентная система.

Цель работы: разработка системы обнаружения атак, позволяющей проводить распределенный интеллектуальный анализ данных о наличии следов атак в основных компонентах информационной системы и их совместный анализ

Полученные результаты и их новизна

Разработана методика обнаружения атак с использованием многоагентных технологий, позволяющая обучить многоагентную систему обнаружения атак и использовать ее для дальнейшего обнаружения атак.

Степень использования: результаты внедрены в процесс разработки системы информационной безопасности в ООО «Студия по разработке программного обеспечения», г. Минск.

Область применения: разработка систем иноформационной безопасности, информационной безопасности предприятий.

SUMMARY

Skaptsou Aliaksei Mikhailavich

Complex intrusion detection system of enterprise system

Keywords: information system, information security, detection of intrusions, multiagent system.

The object of study: the development of intrusion detection system that allows for distributed intelligent analysis of data on the presence of traces of attacks in the main components of information systems and it's joint analysis.

The results and novelty

There was developed the method of attack detection with the use of multiagent technology system allows train detection of attacks and use it for further intrusion detection.

Degree of use: results are implemented in process of developing of system of information security at «Studia po razrabotke programmnogo obespecheniya» LLC.

Sphere of application: information security system design, enterprise information security.