На правах рукописи

ШАРАБЫРОВ Илья Викторович

СИСТЕМА ОБНАРУЖЕНИЯ АТАК В ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ ТЕХНОЛОГИЙ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2016

Работа выполнена в ФГБОУ ВПО «Уфимский государственный авиационный технический университет» на кафедре вычислительной техники и защиты информации

Научный руководитель:	доктор технических наук, профессор **Васильев Владимир Иванович**
Официальные оппоненты:	доктор технических наук, профессор **Чопоров Олег Николаевич** ФГБОУ ВО «Воронежский государственный технический университет», профессор кафедры систем информационной безопасности
	кандидат технических наук, доцент **Безукладников Игорь Игоревич** ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет», доцент кафедры автоматики и телемеханики
Ведущая организация:	ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (г. Казань)

Защита диссертации состоится «22» апреля 2016 г. в 10^{00} часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВПО «Уфимский государственный авиационный технический университет» по адресу: 450000, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «25» февраля 2016 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, доцент И.Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время беспроводные сети передачи данных, в том числе и локального типа, продолжают стремительно развиваться, что объясняется их доступностью, простотой подключения пользователей и распространением мобильных устройств. Однако беспроводная среда передачи в силу своих особенностей создает потенциальные условия для прослушивания сетевого трафика и неконтролируемого подключения к беспроводной сети злоумышленников, находящихся в ее зоне действия. Кроме того, данные сети подвержены, в том числе по причине несовершенства протоколов, множественным типам атак.

В последние годы атаки на беспроводные локальные сети стали обычным явлением. По статистическим данным "Лаборатории Касперского" (Kaspersky Security Bulletin), в 2014 г. было обнаружено и заблокировано более 6,1 млрд вредоносных атак на компьютеры и мобильные устройства пользователей, что значительно превышает аналогичный показатель 2013 г. – 5,1 млрд атак. Всего же за последние пять лет число сетевых атак выросло в 4,7 раза. Рядовые пользователи и небольшие организации, как правило, ограничиваются использованием антивирусного программного обеспечения, которое на современном этапе развития имеет ряд дополнительных модулей защиты (встроенные межсетевые экраны, проверка электронной почты и т.д.). Крупные предприятия вынуждены приобретать дорогостоящие системы обнаружения и предотвращения атак. Системы обнаружения атак могут быть реализованы как на основе модели обнаружения известных признаков (сигнатур), так и на основе обнаружения отклонений от нормального поведения (аномалий). Базы данных первых содержат тысячи признаков атак, при этом их использование повышает требования к аппаратному обеспечению и заметно замедляет скорость обработки сетевого трафика, поэтому зачастую большинство правил администратор информационной безопасности отключает, что ведет к повышению риска осуществления атаки. В свою очередь, технология обнаружения аномалий обеспечивает защиту от новых, неизвестных сетевых атак, но системы, построенные на основе этого метода, могут выдавать большое количество ошибочных предупреждений, что ведет к снижению восприимчивости к ним. В связи с этим решаемая в диссертационной работе задача, заключающаяся в разработке алгоритмического и программного обеспечения системы, позволяющей автоматизировать процесс обнаружения беспроводных атак на основе применения современных методов интеллектуального анализа параметров сетевого трафика, является актуальной.

Степень разработанности темы

В настоящее время в данной предметной области ведутся активные разработки, о чем свидетельствуют работы ведущих отечественных и зарубежных исследователей: Е.С. Абрамова, А.В. Аграновского, И.В. Аникина, С.В. Белима, В.И. Васильева, А.А. Владимирова, В.А. Галатенко, С.В. Гордейчика, С.А. Ермакова, П.Д. Зегжды, И.В. Котенко, А.В. Лукацкого, О.Б. Макаревича, А.А. Малюка, И.В. Машкиной, В.И. Никонова, Н.А. Соловьева, А.А. Шелупанова, В.Б. Щербакова, Ю.К. Язова, Д. Дасгупты, К. Лендвера, Д. Райта, Д. Росса и др.

В то же время, анализ публикаций в открытых источниках показал, что в области обнаружения атак в беспроводных локальных сетях на настоящий момент отсутствуют общепринятые стандарты, производители коммерческих средств, как правило, используют закрытые алгоритмы выявления и классификации атак, а многие заявленные функции носят исключительно рекламный характер. В ряде исследований представлены результаты применения методов интеллектуального анализа данных для повышения эффективности решения задачи обнаружения атак. Однако работы, посвященные целенаправленному применению данных методов для обнаружения атак, характерных для беспроводных локальных сетей, в доступной литературе отсутствуют. Поэтому тема диссертационной работы, посвященная разработке системы обнаружения атак в таких типах сетей на основе применения методов интеллектуального анализа данных, является актуальной.

Объектом исследования является система обнаружения атак в беспроводной локальной сети организации.

Предметом исследования являются методы и алгоритмы обнаружения атак в беспроводных локальных сетях с применением технологий интеллектуального анализа данных.

Целью работы является повышение эффективности обнаружения атак в беспроводной локальной сети организации путем разработки моделей и алгоритмов решения данной задачи на основе технологий интеллектуального анализа данных.

Задачи исследования

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

1. Исследовать особенности функционирования беспроводных локальных сетей организации с точки зрения их защищенности, сформировать перечень угроз и существующих методов защиты информации в беспроводных сетях.
2. Разработать системные модели процесса функционирования системы обнаружения атак в беспроводных сетях.
3. Разработать алгоритмы обнаружения атак в беспроводной сети на основе применения классифицирующей модели с использованием технологий интеллектуального анализа данных.
4. Предложить архитектуру интеллектуальной системы обнаружения атак, провести вычислительные эксперименты с целью оценки эффективности предложенных алгоритмов обнаружения атак.
5. Разработать программное обеспечение исследовательского прототипа интеллектуальной системы обнаружения атак, дать рекомендации по его практическому применению в реальных условиях эксплуатации.

Научная новизна

– Разработан комплекс системных моделей процесса функционирования системы обнаружения атак в составе информационной системы организации, основанных на методологии IDEF0 и IDEF1X, детализирующих процесс выявления атак в беспроводных сетях и позволяющих интегрировать систему обна-

ружения атак с компонентами системы защиты информации в организации с учетом требований нормативных документов;

– предложены алгоритмы обнаружения атак в беспроводной сети на основе применения классифицирующей модели с использованием методов интеллектуального анализа данных, что в отличие от существующих алгоритмов позволяет повысить точность обнаружения атак и снизить количество ложных срабатываний за счет предварительного обучения и дообучения системы на данных реального сетевого трафика;

– предложена архитектура интеллектуальной системы обнаружения беспроводных атак, функционирующей на основе разработанных алгоритмов обнаружения атак и их объединения в ансамбль, применение которых позволяет с более высокой точностью и полнотой выявлять и блокировать атаки на беспроводной компонент информационной системы.

Практическая значимость

Практическая значимость полученных результатов заключается в применении технологии обнаружения беспроводных атак на базе методов интеллектуального анализа данных в качестве ядра или дополнительного модуля системы защиты от сетевых атак в организациях и на предприятиях, что обеспечивает повышение на 15÷18% точности обнаружения атак на беспроводной компонент информационной системы.

Методы исследования

В процессе исследования использовались методы теории графов, нейронных сетей, метод опорных векторов, метод k-ближайших соседей, деревья принятия решений. Для оценки эффективности предлагаемых решений применялись методы функционального, информационного и имитационного моделирования.

Положения, выносимые на защиту

1. Результаты анализа состояния проблемы информационной безопасности в области беспроводных локальных сетей, перечень угроз и существующих методов защиты информации в беспроводных сетях.

2. Системные модели процесса функционирования системы обнаружения атак в беспроводных сетях.

3. Алгоритмы обнаружения атак в беспроводной сети на основе применения классифицирующей модели с использованием технологий интеллектуального анализа данных.

4. Архитектура интеллектуальной системы обнаружения атак.

5. Программная реализация исследовательского прототипа интеллектуальной системы обнаружения атак в беспроводных локальных сетях.

Достоверность результатов

Достоверность научных положений и выводов и обоснованность полученных в диссертационной работе результатов подтверждается корректной постановкой задач, строгостью применяемого математического аппарата, результатами имитационного моделирования и результатами апробации программы, реализующей предложенные алгоритмы обнаружения атак.

Личный вклад

Все исследования, изложенные в диссертационной работе, проведены автором в процессе научной деятельности. Результаты, выносимые на защиту, получены автором лично, заимствованный материал обозначен в работе ссылками.

Апробация результатов

По теме диссертации опубликовано 10 научных статей и тезисов докладов, из них 3 статьи в изданиях, рекомендованных ВАК. Имеется свидетельство о государственной регистрации программы для ЭВМ.

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

– XIII Международная научная конференция «Компьютерные науки и информационные технологии» (CSIT'2011), г. Гармиш-Партенкирхен, Германия, 2011 г.;

– XII Международная научно-практическая конференция «Информационная безопасность – 2012», г. Таганрог, 2012 г.;

– VIII Всероссийская зимняя школа-семинар аспирантов и молодых ученых, г. Уфа, 2013 г.;

– V – VIII Всероссийские молодежные научные конференции «Мавлютовские чтения», г. Уфа, 2011–2014 гг.

Разработанный программный комплекс, реализующий прототип интеллектуальной системы обнаружения беспроводных атак, используется в филиале ФГБУ «ФКП Росреестра» по Республике Башкортостан.

Кроме того, результаты исследования используются в учебном процессе на кафедре «Вычислительная техника и защита информации» ФГБОУ ВПО «Уфимский государственный авиационный технический университет» при проведении лекций и лабораторных работ по курсам «Методы искусственного интеллекта» и «Искусственный интеллект в системах защиты информации» для студентов направлений 10.03.01 «Информационная безопасность» и 09.03.01 «Информатика и вычислительная техника» и специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

Объем и структура работы

Диссертационная работа включает введение, четыре главы основного материала, заключение и библиографический список. Работа изложена на 144 страницах машинописного текста, библиографический список включает 128 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении к диссертации обосновывается актуальность темы исследования, формулируется цель работы, решаемые в ней задачи, объект и предмет исследования, отмечается научная новизна работы, практическая значимость, положения, выносимые на защиту.

В первой главе проводится анализ последних достижений в области беспроводных технологий передачи информации, уровня защищенности локаль-

ных беспроводных сетей от различного рода угроз, современного состояния в области обеспечения информационной безопасности данного класса сетей, а также возможных подходов к решению проблемы повышения уровня защищенности беспроводных сетей. Анализируются рекомендации стандартов по обеспечению безопасности передачи информации в локальных беспроводных сетях, исследуются основные виды уязвимостей существующих сетевых протоколов, раскрывается специфика уязвимостей беспроводных сетей. Рассматриваются существующие технологии и средства защиты информации в локальных беспроводных сетях, включая системы обнаружения атак, анализируются их достоинства и недостатки. В результате проведенного анализа делается вывод о том, что существующие методы защиты, как правило, являются узкоспециализированными с точки зрения противодействия угрозам безопасности информации. Данный факт предопределяет необходимость разработки и реализации специализированной системы защиты информации в локальных беспроводных сетях, направленной на решение поставленных задач. В заключении главы формулируются цели исследования и задачи, решаемые в диссертационной работе.

Во второй главе строятся системные модели процесса функционирования системы обнаружения атак в локальных беспроводных сетях, модель нарушителя, модель угроз, формируется классификация атак, разрабатываются интеллектуальные алгоритмы обнаружения атак в беспроводных сетях.

Для анализа особенностей функционирования системы обнаружения атак (СОА) и степени ее влияния на защищаемый объект необходимо составить ее формализованное описание в виде функциональной модели. В данной работе использовано системное моделирование по методологии IDEF0 и IDEF1X. С помощью построенных моделей получено представление о структуре СОА, составе и функциях ее компонентов, а также о взаимосвязях между ними.

На рисунке 1 представлена функциональная модель системы обнаружения атак. Система включает в себя следующие компоненты:

– *сенсоры*: осуществляют сбор и первичную обработку данных о состоянии безопасности беспроводной локальной сети;

– *консоль управления*: предназначена для настройки администратором безопасности параметров СОА;

– *модуль обучения (дообучения)* СОА: выполняет построение классифицирующей модели на этапе обучения СОА, а также совершенствует модель в ходе дообучения на реальной сетевой активности;

– *база знаний*: содержит сигнатуры обучающей выборки, построенные классифицирующие модели, настройки компонентов системы;

– *модуль выявления атак*: производит анализ событий безопасности и на основе определенных критериев (правил) классифицирует вредоносную активность как атаку;

– *модуль принятия решений*: генерирует запросы/оповещения на консоль и вырабатывает список защитных мер для блокирования атаки.

Рассмотрены особенности технической и программной реализации модулей и блоков, представленных на рисунке 1. Состав предлагаемой системы обнаружения атак в беспроводных сетях, в целом, схож со структурой традици-

онных СОА, за исключением наличия модуля обучения (дообучения) системы и особенностей реализации модуля выявления атак. Кроме того, в ходе проектирования возникает важная задача по выбору вектора признаков, специфичных для беспроводных сетей, для детального описания событий безопасности.

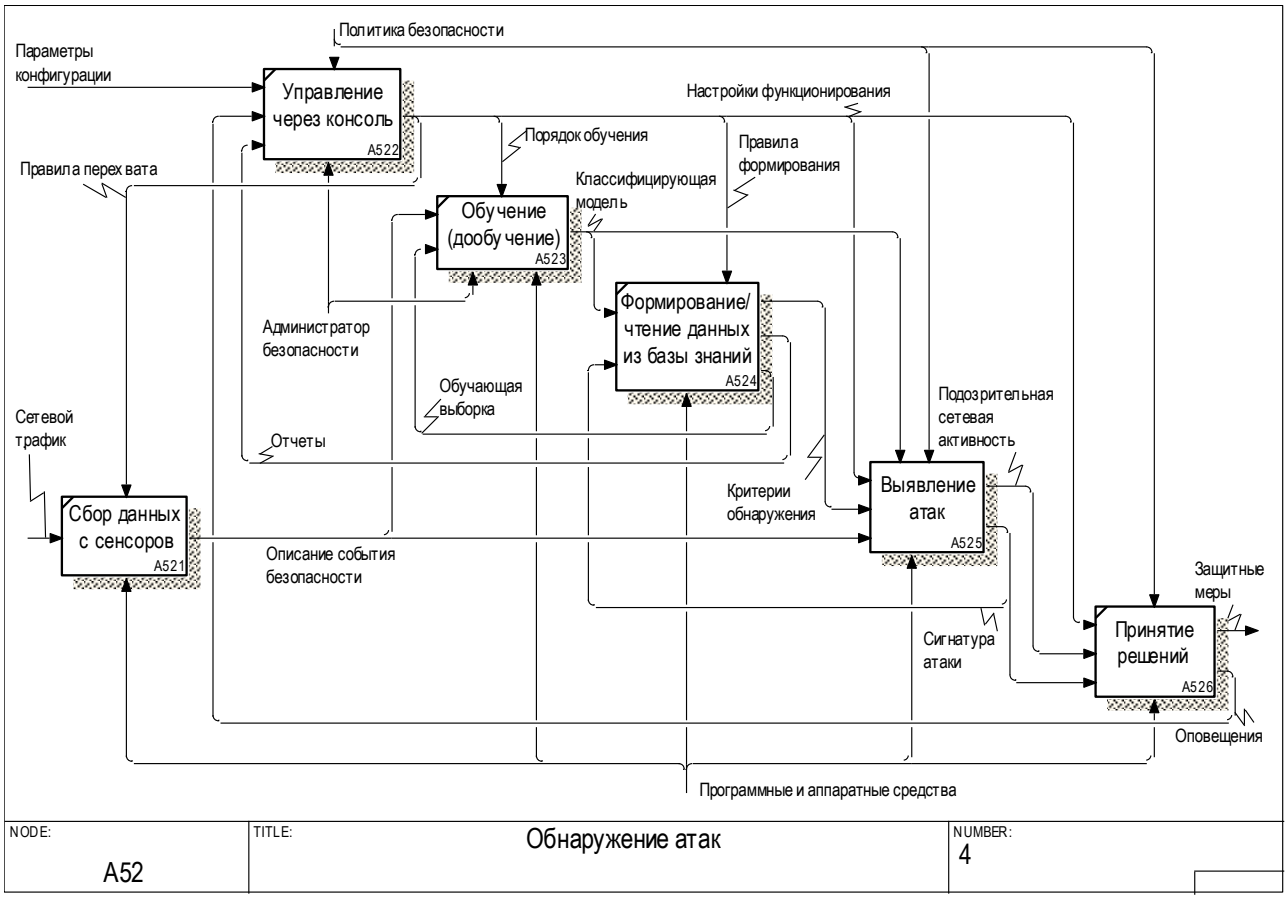

Рисунок 1 – Функциональная модель системы обнаружения атак

На основании проведенного анализа проблем защиты информации в беспроводных сетях выделен перечень возможных угроз информационной системе (ИС) организации:

- сканирование эфира;
- перехват, модификация, внедрение сетевого трафика;
- радиочастотное глушение точек доступа или клиентов;
- использование уязвимостей ПО точек доступа;
- внедрение ложного объекта сети (точки доступа или клиента);
- деавторизация санкционированного клиента беспроводной сети;
- подключение к беспроводной сети в обход процедуры аутентификации;
- получение сведений о владельце беспроводного устройства;
- навязывание ложного маршрута:
    а) удаленное изменение таблицы ARP (ARP-spoofing);
    б) внедрение ложного DHCP-сервера;
    в) внедрение ложного DNS-сервера, подмена DNS-ответов;
    г) изменение таблицы маршрутизации (ICMP Redirect);
- отказ в обслуживании:
    а) частичное исчерпание ресурсов;
    б) полное исчерпание ресурсов;

− удаленный запуск приложений путем рассылки файлов, содержащих деструктивный исполняемый код, вирусы или путем переполнения буфера серверного приложения;

− проникновение в ОС с использованием системного/прикладного ПО;

− выявление паролей;

− анонимное подключение к сети Интернет;

− хищение беспроводных устройств.

В основе атак на беспроводные сети лежит перехват сетевого трафика от/к точке доступа или трафика между двумя подключенными станциями, а также внедрение дополнительных (поддельных) данных в сеанс беспроводной связи. По своему происхождению, атаки против беспроводной сети могут быть пассивными и активными. Пассивная атака заключается в перехвате трафика с помощью сетевых анализаторов и его дальнейшем анализе злоумышленником. Как правило, данная атака осуществляется для сбора необходимой информации о беспроводной сети перед проведением активных действий. В ходе активной атаки злоумышленник осуществляет передачу данных в беспроводную среду.

Атаки могут быть реализованы на разных уровнях модели OSI: прикладном, транспортном, сетевом, канальном и физическом. Специфичными для беспроводных сетей являются физический и канальный уровни, на использовании которых основан стандарт IEEE 802.11. Именно использование уязвимостей протоколов и технологий этих уровней является основой проведения атак на беспроводную локальную сеть и первоначальной стадией атак на информационную систему через несанкционированное получение доступа в беспроводную сеть.

Для наглядного представления механизма распространения атак на компоненты беспроводной локальной сети организации в работе использована технология построения деревьев атак. В качестве основного представлено дерево атак, целью которых является получение доступа к корпоративной сети, после чего дальнейшие действия злоумышленника могут быть направлены, например, на сканирование объектов сети и получение доступа к защищаемым корпоративным серверам (серверу баз данных, файловому серверу и др.).

Для обнаружения беспроводных атак в данной работе разработаны соответствующие алгоритмы построения классифицирующей модели, составляющей ядро базы знаний системы обнаружения атак, на основе методов интеллектуального анализа данных (ИАД): метода опорных векторов, метода k-ближайших соседей, деревьев принятия решений, а также нейронных сетей.

На рисунке 2 приведена обобщенная блок-схема обнаружения атак в локальной беспроводной сети. На первом этапе формируются массивы для записи прослушанных в эфире кадров F и выделенных из них параметров P, а также массив $P_{ЭТ}$, в который сохраняются эталонные значения параметров, измеренные в режиме обучения СОА. Также формируются массив T, в который набирается статистика сетевой активности на заданном интервале времени Δt, массив данных о вещающих беспроводных точках доступа M и заполняется перечень информации о доверенных корпоративных точках доступа $M_{ЭТ}$: MAC-адрес, номер занимаемого радиоканала, разрешенные к использованию протоколы шифрования и аутентификации и др.

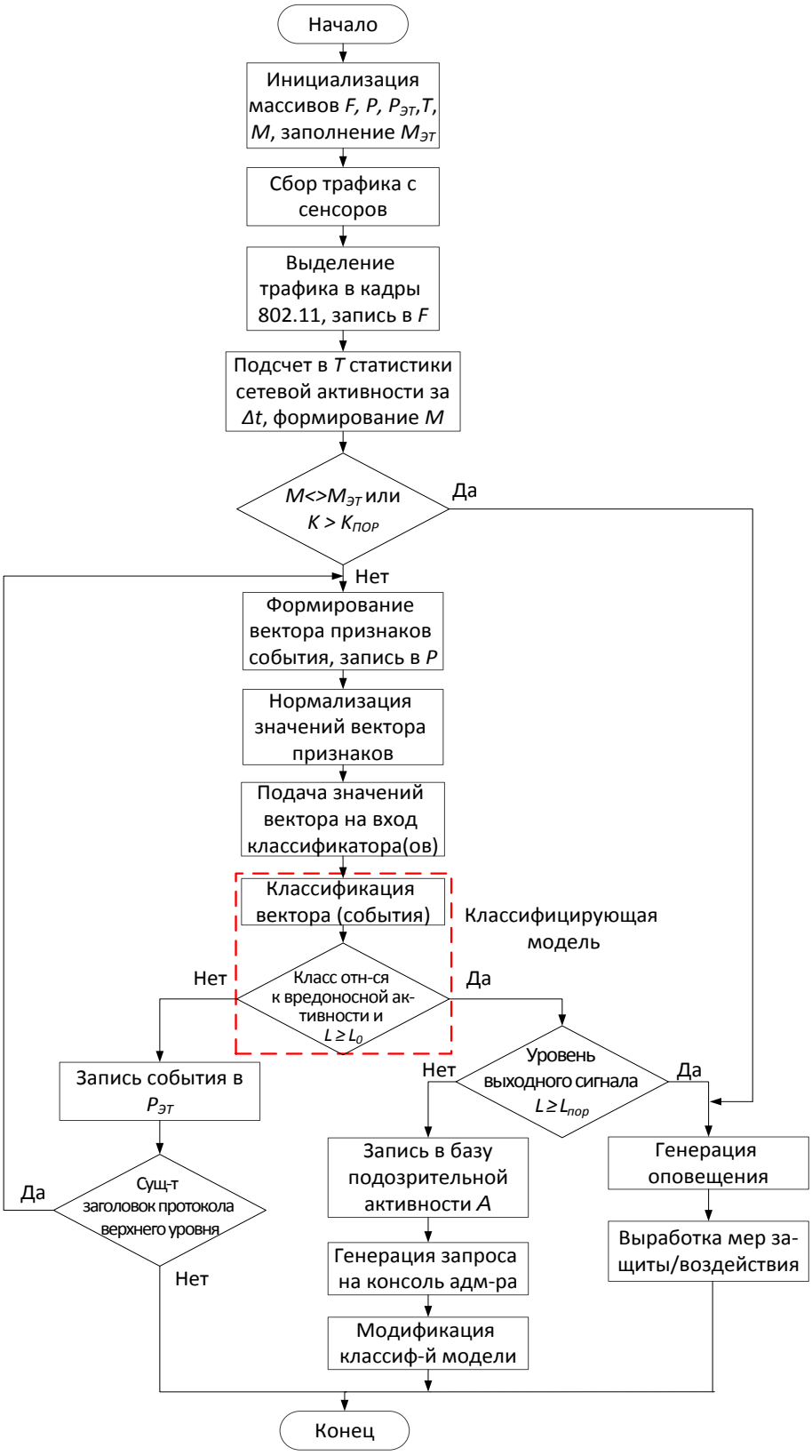

Рисунок 2 – Блок-схема обнаружения беспроводных сетевых атак

Далее производится сбор данных с сенсоров, их первичный анализ с целью выделения трафика в отдельные кадры формата 802.11 и сохранение их в массив *F*. Затем осуществляется формирование векторов признаков событий и запись их в массив *P*, нормализация значений признаков и подача *P* на вход классификатора(ов) модуля выявления атак. Соответствующий блок производит классификацию событий безопасности на базе классифицирующей модели,

представляющей собой набор решающих правил, неявно сравнивая значения признаков с соответствующими значениями в массиве $P_{ЭТ}$. При выявлении соответствия вектора признаков какому-либо типу вредоносной активности производится анализ уровня выходного сигнала классификатора(ов) L. В случае достижения или превышения порогового уровня сигнала $L_{пор}$ информация о событии передается в модуль принятия решений, который генерирует оповещение на консоль администратора, а также на основании предустановленных настроек вырабатывает меры защиты или воздействия на устройство злоумышленника. В ином случае, если $L_0 \leq L < L_{пор}$, где L_0 – минимально допустимый уровень сигнала, свидетельствующий о подозрительной сетевой активности, то анализируемый вектор признаков события сохраняется в базе подозрительной активности A для дальнейшего анализа методами ИАД. По достижении порогового количества однотипных событий генерируется запрос на консоль администратора, который определяет наличие или отсутствие вредоносной активности в данных событиях. На основании его решения производится модификация классифицирующей модели (дообучение) и добавление записей о событиях в базу сигнатур S.

Кроме того, для обнаружения отдельных типов атак в массив T набирается статистика количества кадров определенного типа на заданном интервале времени Δt. Дополнительно в процессе функционирования СОА производится пополнение массива данных о вещающих беспроводных точках доступа M. При превышении порогового значения $K_{ПОР}$ количества кадров K одинакового типа генерируется оповещение на консоль администратора о возможной DoS-атаке для дальнейшего обнаружения и физического устранения ее источника. При несовпадении данных массива M с заданными значениями $M_{ЭТ}$ генерируется оповещение о ложном устройстве в радиоэфире.

Построение классифицирующей модели происходит на стадии обучения системы обнаружения атак. Для обучения СОА необходима обучающая выборка, состоящая из записей о текущих беспроводных сетевых соединениях. Каждое соединение имеет характерный набор признаков (входных параметров) и присвоенную метку класса.

После построения классифицирующей модели на стадии обучения СОА переводится в режим полнофункциональной работы и на входы сенсоров подается реальный сетевой трафик. При этом по мере функционирования происходит дообучение СОА при анализе подозрительной сетевой активности.

В третьей главе проводится анализ эффективности разработанных алгоритмов обнаружения атак, основанных на применении технологий интеллектуального анализа данных, представлены результаты проведенных экспериментов, выявлены сравнительные достоинства и недостатки предлагаемых алгоритмов.

На основании классификации атак, построенной в предыдущей главе работы, атаки на локальные беспроводные сети разделены на две группы:

– атаки физического и канального уровня, являющиеся специфичными для беспроводных сетей;

– атаки с сетевого по прикладной уровни, присущие любой технологии организации локальных сетей, в том числе Ethernet.

В качестве образцов атак с сетевого по прикладной уровни предложено воспользоваться усовершенствованной базой сигнатур NSL KDD-2009, постро-

енной на основе базы KDD-99, созданной по инициативе американского агентства перспективных оборонных исследовательских проектов (DARPA).

Однако для обучения и тестирования СОА в беспроводной сети необходима также выборка беспроводных атак, специфичных для сетей 802.11, т.е. атак канального уровня. Для решения задачи формирования такой выборки в работе была использована тестовая локальная беспроводная сеть государственной организации с технологией защиты доступа WPA 2-Enterprise. Средой генерации атак служил ноутбук с установленным дистрибутивом Kali Linux версии 1.1.0 с набором специальных утилит для тестирования на проникновение в сеть и беспроводным адаптером Atheros AR9485 в режиме мониторинга. Для перехвата и анализа кадров с целью формирования базы сигнатур атак использовался второй ноутбук с Windows 7 и беспроводным адаптером Atheros AR9285 в пассивном режиме мониторинга. Собранные кадры были проанализированы и промаркированы, т.е. каждый кадр обозначен как нормальный либо как указывающий о проведении какого-либо типа атаки, относящегося к одной из следующих четырех категорий атак:

- нарушение периметра сети (Perimeter Violation);
- нарушение целостности (Integrity Violation);
- нарушение конфиденциальности (Confidentiality Violation);
- нарушение доступности (Denial of Service).

Соотношение числа атак разных типов в базе сигнатур показано в таблице 1.

Таблица 1

Соотношение количества сигнатур атак в обучающей и тестовой базе

Обучающая база		*Тестовая база*	
Класс	Кол-во	Класс	Кол-во
Normal	114959	Normal	27886
Perimeter Violation		Perimeter Violation	
rogue_client	131	rogue_client	225
MAC_spoofing	106	MAC_spoofing	12
fake_auth	81	fake_auth	9
caffe_latte	198	caffe_latte	22
chopchop	202	chopchop	22
client_fragment	56862	client_fragment	6318
AP_fragment	3552	AP_fragment	395
Confidentiality Violation		Confidentiality Violation	
evil_twin_AP	1344	evil_twin_AP	149
Integrity Violation		Integrity Violation	
data_replay	75785	data_replay	8420
EAP_replay	75	EAP_replay	8
Denial of Service		Denial of Service	
beacon_flood	1761	beacon_flood	2153
auth_flood	569	auth_flood	74
deauth_flood	10940	deauth_flood	1216
EAPOL_start_flood	16345	EAPOL_start_flood	1816
EAPOL_logoff_flood	1923	EAPOL_logoff_flood	2425
RTS/CTS_flood	1831	RTS/CTS_flood	2237

В таблице 2 приведены компоненты вектора признаков для описания атак канального уровня. В качестве признаков выбраны значения полей MAC-заголовка кадра формата IEEE 802.11, радио информация заголовка физического уровня (PLCP) и некоторые статистические признаки. Согласно алгоритму, представленному на рисунке 2, радио информация (номер канала, уровень сигнала передатчика, скорость передачи) совместно с другими данными массива *M* используется, в основном, для выявления ложных устройств в радиоэфире, а статистические признаки – для обнаружения DoS-атак, характеризующихся резким увеличением количества кадров на заданном временном интервале.

Таблица 2

Значимые параметры трафика для канального уровня

Характеристика	*Описание*	*Тип*
Характеристики протоколов 802.11		
frame_ type/subtype	Тип/подтип кадра	текстовый
protocol_type	Тип протокола канального уровня	текстовый
source_address	MAC-адрес источника	текстовый
destination_address	MAC-адрес назначения	текстовый
length	Размер кадра, байт	численный
SSID	Значение тега SSID	текстовый
sequence_number	Номер кадра	численный
fragment_number	Номер фрагмента	численный
BSSID	MAC-адрес точки доступа	текстовый
DS_status	Участие распределенной системы в обмене	численный
more_fragments	Еще фрагменты для передачи, 0 иначе	бинарный
retry	Повторная передача предыдущего кадра, 0 иначе	бинарный
pwr_mgt	Клиент в режиме энергосбережения, 0 иначе	бинарный
more_data	Буферизованные кадры для передачи, 0 иначе	бинарный
protected_flag	Данные кадра зашифрованы, 0 иначе	бинарный
order_flag	Обработка кадров строго по порядку, 0 иначе	бинарный
duration	Продолжительность передачи ACK+SIFS, мкс	численный
chan_number	Номер канала	численный
signal	Уровень сигнала передатчика, %	численный
TX_rate	Скорость передачи, Мбит/с	численный
cipher	Используемый протокол шифрования	текстовый
reason_code	Код причины деаутентификации	численный
Статистика за 2 секунды		
mng_frm_count	Число управляющих кадров	численный
ctrl_frm_count	Число контрольных кадров	численный
probe_count	Число запросов на подключение	численный
frag_count	Среднее число фрагментированных пакетов	численный
malformed_count	Число поврежденных кадров	численный
retry_count	Число повторных передач кадров	численный
avg_tx_rate	Средняя скорость передачи данных, Мбит/с	численный
client_count	Общее число подключенных клиентов	численный

Имитационное моделирование осуществлялось с целью проверки работоспособности предложенных моделей и алгоритмов обнаружения атак в реальной беспроводной локальной сети. Моделирование проводилось с помощью разработанного исследовательского прототипа СОА в две стадии. В ходе пер-

вой стадии одновременно с передачей данных легальными пользователями осуществлялся набор различных категорий атак, представленных в предыдущей главе, на локальную беспроводную сеть с технологией защиты доступа WPA 2-Enterprise. Беспроводной трафик прослушивался сенсорами СОА, которые собирали кадры данных, создавали по ним модели соединений между абонентами, формировали описание событий с набором характерных признаков и передавали их в модуль выявления атак для анализа.

Вторая стадия тестирования состояла собственно в проверке способности системы к обнаружению атак. В ходе нее производилось обучение системы на обучающей выборке с целью построения классифицирующей модели различными методами ИАД. Затем на вход модуля выявления атак подавались тестовые данные, перехваченные сенсорами. Данный модуль проводил классификацию событий безопасности на основании классифицирующей модели по критериям, содержащимся в базе знаний, и присваивал метку класса сетевой активности.

Была произведена оценка корректности распознавания рассмотренных типов атак с помощью СОА путем сравнения между собой результатов классификации, полученных с помощью различных методов ИАД. Эффективность разработанных алгоритмов оценивалась по следующим критериям:

1. Общий процент корректно классифицированных атак *A (accuracy)*:

$$A = \frac{TP + TN}{N}, \quad (1)$$

где *TP* и *TN* – общее количество истинных записей;

N – общее количество классифицированных записей.

2. Точность классификации *P (precision)*:

$$P = \frac{TP}{TP + FP}, \quad (2)$$

где *TP* – количество истинно-положительных записей*;*

FP – количество ложно-положительных записей.

3. Полнота классификации *R (recall)*:

$$R = \frac{TP}{TP + FN}, \quad (3)$$

где *FN* – количество ложно-отрицательных записей.

4. Метрика F_1 – среднее гармоническое значение величин *P* и *R*:

$$F_1 = 2 \cdot \frac{P \cdot R}{P + R} \quad (4)$$

Ниже приведены средние значения метрик эффективности сравниваемых алгоритмов при обнаружении атак с сетевого по прикладной уровни (таблица 3) и при обнаружении атак канального уровня (таблица 4).

Таблица 3

Средние значения метрик сравниваемых алгоритмов

Алгоритм	Корректно классифицировано	Точность	Полнота	Метрика F_1
Метод опорных векторов (SVM)	93,67%	83,27%	83,61%	83,44%
k-ближайших соседей (kNN)	93,69%	84,89%	84,65%	84,77%
Нейронная сеть (NN)	90,70%	70,19%	70,38%	70,28%
Дерево принятия решений (DT)	92,69%	79,58%	79,58%	79,58%

Таблица 4

Средние значения метрик сравниваемых алгоритмов

Алгоритм	Корректно классифицировано	Точность	Полнота	Метрика F_1
Метод опорных векторов (SVM)	94,41%	81,61%	84,90%	83,23%
k-ближайших соседей (kNN)	95,05%	82,79%	88,07%	85,35%
Нейронная сеть (NN)	92,20%	70,92%	82,62%	76,33%
Дерево принятия решений (DT)	95,07%	85,46%	90,40%	87,86%

В связи с различием показателей эффективности обнаружения атак для разработанных алгоритмов в зависимости от уровня модели OSI, на котором реализуется атака, предложено использовать ансамбль из четырех разработанных алгоритмов и одного арбитра, определяющего итоговый класс сетевой активности методом взвешенного голосования (рисунок 3).

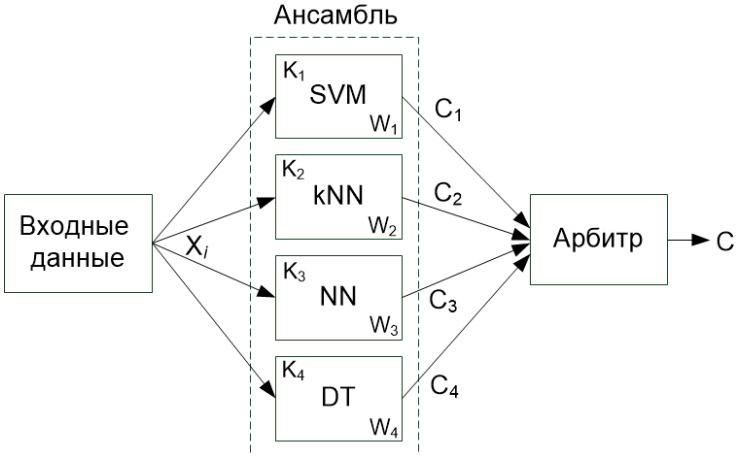

Рисунок 3 – Схема построения интеллектуальной СОА с использованием ансамбля алгоритмов

Идея состоит в том, чтобы не полагаться на результат работы только одного алгоритма, а учитывать решения всех классификаторов в формулировании окончательного вывода о принадлежности сетевой активности тому или иному классу. При этом каждому алгоритму для каждого класса сетевой активности назначается свой вес (по шкале от 0 до 1) исходя из значений его показателей на обучающих данных. Таким образом, если для конкретной записи входных данных $X_i = \{x_1,...,x_m\}$ классификаторы указывают различные классы C_j, то учитываются значения их весов W_j и результат работы классификатора с наибольшим весом принимается в качестве выходного значения C всего ансамбля:

$$C = C_l \mid W_l = \max_j \{W_j\}, \qquad (5)$$

где j=1, .., 4 – порядковый номер классификатора K.

Проведенные тесты показали, что применение ансамбля алгоритмов позволяет обнаружить до 93,5% атак на беспроводной компонент информационной системы с точностью до 93,6%, общий процент корректно классифицированных записей составил 96,7%. Вероятность возникновения ошибок первого рода не превышает 1,6%, ошибок второго рода – 1,7%.

В четвертой главе сформулированы требования к реализации разрабатываемого прототипа интеллектуальной системы обнаружения атак, ее отдельным модулям (подсистемам). Приведены результаты оценки эффективности разработанной СОА, даны рекомендации по ее применению.

Предложено оценивать степень соответствия СОА предъявляемым требованиям на основе двух наборов показателей. В качестве первого набора выступает ряд показателей для оценки функциональных возможностей СОА (функциональные показатели), которые подразделены на следующие группы:

1. Показатели обнаружения – определяют соответствие СОА требованиям, предъявляемым к методам выявления и распознавания атак.

2. Показатели безопасности – определяют соответствие СОА требованиям, предъявляемым к аппаратному и программному обеспечению защищаемого объекта с целью предотвращения попыток получения несанкционированного доступа к информации.

3. Показатели реагирования – определяют соответствие СОА требованиям к предпринимаемым ею защитным мерам в случае обнаружения атаки на защищаемый объект.

Второй набор показателей характеризует производительность СОА и особенности ее применения для обнаружения атак на защищаемый объект (количественные показатели):

1. Скорость обработки кадров СОА.
2. Задержка, вносимая СОА в процесс функционирования ИС.
3. Производительность сенсора при сборе кадров.
4. Количество ошибок первого и второго рода.
5. Полнота и точность распознавания атак.

Основу предложенной архитектуры интеллектуальной СОА составляет модульная схема организации взаимодействия между компонентами, представленными на рисунке 1, с выделенной подсистемой сенсоров и централизованным управлением через консоль администратора (рисунок 4).

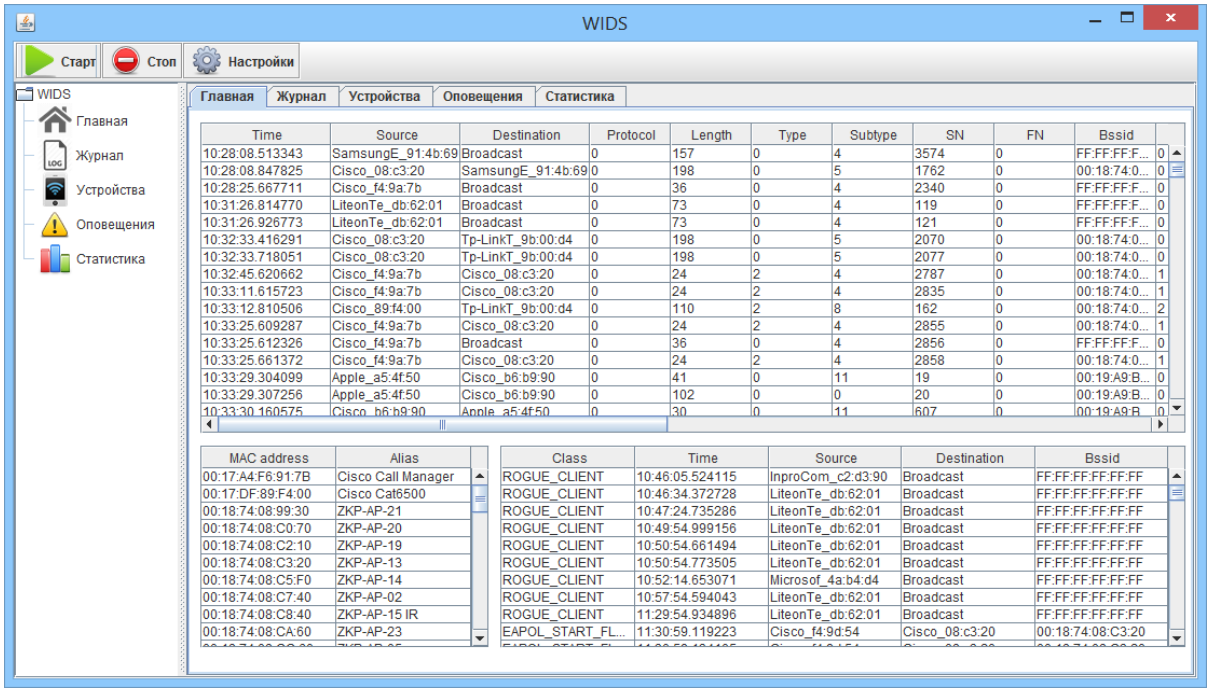

Рисунок 4 – Главное окно консоли управления

Отличительной особенностью предлагаемой архитектуры является наличие модуля обучения (дообучения) системы и технология реализации модуля выявления атак, основанная на применении алгоритмов на базе методов ИАД. Таким образом, СОА, классифицирующая модель которой строится на основе сигнатур обучающей выборки, имеет возможность обучаться в процессе работы на реальном сетевом трафике, что позволяет обнаруживать изначально неизвестные системе модификации атак.

Сравнение эффективности разработанного прототипа производилось с некоммерческими СОА Wireless IDS и «Wireless Auditing, Intrusion Detection and Prevention System». В результате проведенного сравнения выявлено, что показатель точности обнаружения атак разработанного прототипа СОА превышает аналогичные показатели сравниваемых систем на 15,1% и 18,1% соответственно.

Разработанный прототип СОА обладает хорошей масштабируемостью и функциональной гибкостью, может использовать в качестве входных данных дамп-файл перехваченных беспроводных кадров формата .cap или .ncf, формируемый как бесплатным ПО, так и коммерческими продуктами. Прототип имеет возможность встраивания в качестве ядра или дополнительного модуля в систему защиты от сетевых атак в организациях и на предприятиях.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ существующих методов и средств защиты локальных беспроводных сетей Wi-Fi, в том числе коммерческих систем обнаружения атак, который выявил отсутствие предоставления полноценной защиты от вредоносной сетевой активности в таких типах сетей.

2. Разработан комплекс системных моделей процесса функционирования системы обнаружения атак в составе ИС, основанных на методологии IDEF0 и IDEF1X, детализирующих процесс выявления атак в беспроводных сетях и позволяющих интегрировать СОА с компонентами системы защиты информации в организации с учетом требований нормативных документов.

3. Предложены алгоритмы обнаружения атак в беспроводной сети на основе применения классифицирующей модели с использованием методов интеллектуального анализа данных, которые в отличие от существующих алгоритмов обнаружения атак позволяют повысить точность обнаружения атак и снизить количество ложных срабатываний за счет предварительного обучения и дообучения системы на данных реального сетевого трафика.

4. Предложена архитектура интеллектуальной системы обнаружения беспроводных атак, функционирующей на основе разработанных алгоритмов обнаружения атак и их объединения в ансамбль, применение которых позволяет с более высокой точностью и полнотой выявлять и блокировать атаки на беспроводной компонент информационной системы.

5. Разработано программное обеспечение исследовательского прототипа интеллектуальной системы обнаружения беспроводных атак. Эффективность разработанного прототипа подтверждена методом имитационного моделирования атак на сегмент локальной беспроводной сети организации с использованием реального сетевого трафика, перехваченного сенсорами СОА. Прототип обеспечивает повышение на 15÷18% точности обнаружения атак на беспроводной компонент информационной системы.

Перспективы дальнейших исследований

Дальнейшие исследования предполагается продолжить в направлении изучения новых типов атак в локальных беспроводных сетях, а также совершенствования архитектуры системы, повышения показателей эффективности и доработки алгоритмов системы обнаружения атак с использованием рассмотренных в данной работе методов ИАД.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Васильев В.И., Шарабыров И.В. Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа данных // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». №2 (151). Таганрог: Изд-во ТТИ ЮФУ, 2014. С. 57–67.

2. Шарабыров И.В. Интеллектуальный анализ данных в задачах обнаружения атак на локальные беспроводные сети // Естественные и технические науки. № 11 (89). М.: Изд-во Спутник+, 2015. С. 479–481.

3. Васильев В.И., Шарабыров И.В. Интеллектуальная система обнаружения атак в локальных беспроводных сетях // Вестник УГАТУ. 2015. Т. 19. № 4 (70). С. 91–102.

Объекты интеллектуальной собственности

4. Свид. о гос. регистрации программы для ЭВМ № 2012615568. Управляемая кластеризация объектов / И.В. Шарабыров. Зарег. 20.06.2012 г. – М.: Роспатент, 2012.

В трудах международных и всероссийских конференций

5. Дополнения к алгоритму обучения на основе прямоугольников с максимальным зазором / Миронов К.В., Шарабыров И.В., Кирмзе М., Петерсон У. // Компьютерные науки и информационные технологии *CSIT*‘2011 (г. Гармиш-Партенкирхен, Германия, 27.09 – 2.10.2011): тр. 13-й междунар. науч. конф. Уфа: Изд-во УГАТУ, 2011. Т. 2–3. С. 26–31 (на англ. яз.).

6. Миронов К.В., Шарабыров И.В. Гибридный алгоритм обучения, основанный на методе опорных векторов и построении дерева принятия решений // Мавлютовские чтения: Всероссийская молодежная научная конференция: Сб. науч. трудов. Уфа: Изд-во УГАТУ, 2011. Т. 3. С. 42–43.

7. Васильев В.И., Машкина И.В., Миронов К.В., Шарабыров И.В. Разработка модели обнаружения сигнатур атак на основе метода опорных векторов // Материалы XII Международной научно-практической конференции «Информационная безопасность–2012». Ч.1. Таганрог: Изд-во ТТИ ЮФУ, 2012. С. 192–201.

8. Миронов К.В., Шарабыров И.В. О применении метода опорных векторов в системах обнаружения атак // Мавлютовские чтения: Всероссийская молодежная научная конференция: Сб. науч. трудов. Уфа: Изд-во УГАТУ, 2012. Т. 3. С. 28–30.

9. Шарабыров И.В. Атаки в локальных беспроводных сетях // Актуальные проблемы в науке и технике: Информационные и инфокоммуникационные технологии: Сб. науч. трудов Восьмой Всероссийской зимней школы-семинара аспирантов и молодых ученых (Уфа, 19.02–20.02.2013). Уфа: Изд-во УГАТУ, 2013. Т. 1. С. 371–373.

10. Шарабыров И.В. Проблемы обнаружения атак в сетях Wi-Fi // Мавлютовские чтения: Всероссийская молодежная научная конференция: Сб. науч. трудов. Уфа: Изд-во УГАТУ, 2013. Т. 3. С. 42–43.

11. Шарабыров И.В. Применение интеллектуального анализа данных для обнаружения атак в локальных беспроводных сетях // Мавлютовские чтения: Всероссийская молодежная научная конференция: Сб. науч. трудов. Уфа: Изд-во УГАТУ, 2014. Т. 3. С. 47–48.

Диссертант  И.В. Шарабыров

ШАРАБЫРОВ Илья Викторович

СИСТЕМА ОБНАРУЖЕНИЯ АТАК В ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ ТЕХНОЛОГИЙ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 16.02.2016. Формат 60×84 1/16
Бумага офсетная. Печать плоская. Гарнитура *Times New Roman*.
Усл. печ. л. 1,0. Уч.-изд. л. 0,9.
Тираж 100 экз. Заказ № 40.

ФГБОУ ВПО «Уфимский государственный авиационный технический университет»
450000, Уфа-центр, ул. К. Маркса, 12