На правах рукописи

Ву Вьет Тханг

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МНОГОЭТАПНОЙ СИСТЕМЫ АНАЛИЗА ТРАФИКА ЛОКАЛЬНОЙ БЕСПРОВОДНОЙ СЕТИ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И ЕЁ ПРИМЕНЕНИЕ В ЗАДАЧЕ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

05.13.01 – Системный анализ, управление и обработка информации (информационные и технические системы)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2019

Работа прошла апробацию на кафедре «Интегрированных киберсистем» Федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

Научный руководитель: доктор технических наук, профессор Пащенко Федор Федорович

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования "Липецкий государственный технический университет".

Защита состоится 19.11.2019 в 15:00 на заседании диссертационного совета ФРКТ.05.13.01.008 по адресу 141701, Московская область, г. Долгопрудный, Институтский переулок, д. 9.

С диссертацией можно ознакомиться в библиотеке и на сайте Московского физико-технического института (национальный исследовательский университет) https://mipt.ru/education/post-graduate/soiskateli-tekhnicheskie-nauki.php

Работа представлена «13» августа 2019 г. в Аттестационную комиссию федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)» для рассмотрения советом по защите диссертаций на соискание ученой степени кандидата наук, доктора наук в соответствии с п. 3.1 ст. 4 Федерального закона «О науке и государственной научно-технической политике».

Общая характеристика работы

Актуальность темы

В настоящий момент в результате широкого использования компьютерных сетей во всех сферах жизни человеческого общества обеспечение защищенности информационного пространства становится все более неотложным. Поэтому задача обнаружения атак на компьютерные сети является одной из самых актуальных. Существует множество уязвимостей в защищаемых системах: в программном обеспечении, операционной системе, веб-сайтах, линиях и средствах передачи данных и т. д. Широкое распространение мобильных устройств по всему миру является одной из причин большого спроса на беспроводные технологии, одна из которых – локальные беспроводные сети (ЛБС) стандарта IEEE 802.11 (Wi-Fi). В отличие от проводных сетей, в локальных беспроводных сетях 802.11 имеются специфичные проблемы, связанные со средой передачи сигнала. Поскольку передача данных в Wi-Fi осуществляется с помощью радиосигналов, то атака может производиться из различных удаленных мест в любое время.

Согласно последним статистическим данным, число атак на устройства ЛБС постоянно увеличивается. Например, согласно данным компании Symantec (Internet security threat report, volume 23, March 2018), число мобильных устройств в 2017 году, пораженных новыми атаками, увеличилось на 54% с 2016 года. По данным второго квартала 2018 года компании Kaspersky (Kaspersky Security Bulletin: Прогнозы на 2018г.), число мобильных устройств, пораженных зловредными пакетами программного обеспечения, услугами банковского программного обеспечения и троянцами-вымогателями, увеличилось на 25% по сравнению с первым кварталом 2018 и было выше пика 2017 года на 10%.

На данный момент существует множество методов и средств обеспечения сетевой безопасности, таких как шифрование, VPN, брандмауэры и т.д. Но все они слишком статичны, чтобы обеспечить эффективную защиту. Используемая

система должна иметь способность обновляться, так как мошенники постоянно меняют методы атаки на информационные ресурсы.

Современные исследования систем обнаружения вторжений (СОВ) пока не показали хороших результатов. Использование интеллектуальной модели может решить такую задачу. Системы обнаружения с интеллектуальной поддержкой обладают высоким потенциалом, поэтому исследования и разработка систем принятия решений в этой области активно ведутся в настоящее время.

Методы интеллектуального анализа данных (ИАД) в задаче прикладного применения для построения СОВ делятся на две группы: методы обнаружения злоупотреблений (misuse detection), которые позволяют построить модель атаки, а в процессе обнаружения использующие методы ИАД для классификации, и методы обнаружения аномалий (anomaly detection), используемые для построения модели нормальной активности, а в процессе обнаружения использующие методы ИАД в целях поиска аномалий.

Степень разработанности темы. На данный момент в области исследования методов ИАД для задач обнаружения вторжений и аномалий работают российские и зарубежные авторы, такие так И.В. Шарабыров, Е.С. Абрамов, Д.А. Андреев, М.Л. Евгеньевич, Д.Ю. Гамаюнов, А.Н. Назаров, Х.А. Фоелевич, А.А. Владимиров, В.А. Галатенко, С.В. Гордейчик, С.А. Ермакова, П.Д. Зегжда, И.В. Котенко, А.В. Лукацкий, Constantinos Kolias, Muhamad E. A., Kwangjo Kim, M. Usha и другие.

В диссертационном исследовании, проведенным автором И.В. Шарабыровым, была построена СОВ в ЛБС, но не были рассчитаны показатели точности обнаружения атак. Также для экспериментальной проверки использовался набор данных KDD'99, который был создан на базе трафика проводных сетей. В данной работе не проведено тестирование разработанной системы на основе трафика ЛБС. Разработанная им система не позволяет распознавать новые атаки. Добавление такой возможности было одной из задач данной диссертации упомянуто в качестве задачи дальнейших исследований.

В работе C. Kolias применяется множество методов для обнаружения вторжений в ЛБС, таких как метод дерева решений J48, Adaboost, Naive Bayes, Random Tree и т.д. В результате проведенных экспериментов получена невысокая точность обнаружения вторжений, особенно для вторжений "посредника".

В других работах задача обнаружения вторжений в ЛБС решалась только частично. Также существует много исследований, где задача решалась в иной среде передачи данных, например, в проводных сетях.

Анализ литературы показывает, что фактически не существует общего подхода к обнаружению вторжений, а системы с многоэтапными моделями для решения задачи обнаружения вторжений в ЛБС отсутствуют.

Таким образом, актуальным представляется исследование технологий ИАД для разработки методик и систем, автоматизирующих оценку и классификацию поведения пользователя посредством анализа трафика ЛБС с помощью многоэтапной интеллектуальной модели, основанных на данных технологиях ИАД и методах машинного обучения.

Целью работы является исследование, разработка и применение методов машинного обучения и технологий ИАД для анализа трафика локальной беспроводной сети для выявления аномалий и вторжений, а также повышение эффективности классификации вторжений в ЛБС.

Для достижения данной цели в работе решаются следующие задачи:

1. Проведение анализа существующих методов обеспечения информационной безопасности в ЛБС.
2. Проведение анализа существующих методик ИАД и машинного обучения в задаче обнаружения вторжений в ЛБС.
3. Разработка метода обнаружения аномалий Fast Local Density Score (FLDS) на основе метода оценки локальной плотности (Local Density Score, LDS), позволяющего повысить скорость выявления аномалий и обнаружить новые, ранее не определенные вторжения.

4. Разработка нового метода инкрементной кластеризации на основе графов с частичным привлечением учителя (IncrementalSSGC, ISSGC) на основе метода Semi-supervised Graph Based Clustering (SSGC), позволяющего повысить точность и скорость выявления вторжений по сравнению с аналогичными методами.

5. Разработка многоэтапной системы обнаружения вторжений, основанной на сочетании методов J48, IncrementalSSGC и FLDS.

6. Проведение экспериментальных исследований разработанных методик и многоэтапной системы обнаружения вторжений на реальных данных трафика локальной беспроводной сети (Wi-Fi).

Объектом исследования является трафик локальной беспроводной сети.

Предметом исследования является методы и алгоритмы интеллектуального анализа данных и машинного обучения для анализа трафика локальной беспроводной сети с целью выявления сетевых вторжений.

Методы исследования. Для решения поставленных задач используются методы машинного обучения (кластеризации, классификации обнаружения аномалий), компьютерных методов обработки и анализа информации, методы разработки приложений на языке программирования Java.

Научная новизна работы состоит в следующем:

1. Разработан метод обнаружения аномалий Fast Local density Score (FLDS), основанный на алгоритме Local Density Score (LDS), повышающий скорость обнаружения аномалий в 10-20 раз по сравнению с LDS, сохраняя при этом точность распознавания. Также FLDS обеспечивает возможность работы с большими объемами данных и наборами данных сложной формы.

2. Разработан метод инкрементной кластеризации на основе графов с частичным привлечением учителя (IncrementalSSGC) на основе метода SSGC, повышающий скорость и точность распознавания в 10-20 раз и на 15-20% соответственно.

3. Разработан комбинированный метод, основанный на сочетании метода обнаружения злоупотреблений при помощи дерева решений J48, метода с

частичным привлечением учителя IncrementalSSGC и метода обнаружения аномалий FLDS. Данный метод позволяет повысить точность обнаружения атак и аномалий на 10% по сравнению с использованием только алгоритма J48.

4. Разработана многоэтапная система на основе предложенных методик анализа трафика для повышения эффективности обнаружения вторжений в ЛБС, позволяющая повысить точность по сравнению с другими системами, распознавать неизвестные ранее вторжения, а также обладающая возможностью обновления базы данных маркированных атак для дополнительного обучения и настройки модулей обнаружения.

Теоретическая значимость диссертационной работы заключается в глубоком освещении проблемы исследования и разработки методов интеллектуального анализа данных и машинного обучения для обнаружения вторжений в ЛБС. В том числе созданы метод обнаружения аномалий Fast Local density Score (FLDS), метод инкрементной кластеризации на основе графов с частичным привлечением учителя (IncrementalSSGC), комбинированный метод на основе предложенных методов. Данные методы позволяют повысить скорость обнаружения аномалий в 10-20 раз, а точность обнаружения вторжений на 10% по сравнению с известными методами.

Практическая значимость полученных результатов состоит в повышении точности обнаружения вторжений по сравнению с другими методами классификации, в повышении скорости обнаружения вторжений, а также в возможности применения разработанной системы, метода обнаружения аномалий FLDS, метода инкрементной кластеризации с частичным привлечением учителя IncrementalSSGC для выявления вторжений и аномалий в ЛБС и построения СОВ в реальном времени, а также для решения других задач ИАД, таких как распознавание образов (изображений, лиц и др.).

Обоснованность и достоверность результатов и выводов определяется следующими факторами:

- Согласованностью теоретических положений с результатами экспериментов на реальных наборах данных CHAMELEON, ADFA, AWID и UCI.
- Публикациями результатов исследования в рецензируемых научных изданиях, входящих в перечень RSCI и в изданиях, индексируемых в международных базах данных (SCOPUS, Web Of Science).
- Практическим использованием результатов диссертационной работы, подтвержденным актом о внедрении.
- Свидетельством № 2019615700 о регистрации программы для ЭВМ**.**

Личный вклад соискателя состоит в:

1. Разработке метода обнаружения аномалий FLDS для распознавания новых или неизвестных вторжений.
2. Разработке метода инкрементной кластеризации с частичным привлечением учителя IncrementalSSGC для повышения точности распознавания вторжений в локальной беспроводной сети.
3. Разработке комбинированного метода выявления вторжений на основе сочетания методов J48, IncrementalSSGC и FLDS для повышения точности распознавания вторжений в задаче обнаружения вторжений в ЛБС.
4. Разработке многоэтапной системы анализа трафика ЛБС для обнаружения и классификации вторжений и аномалий, которая основана на предложенных методиках FLDS и IncrementalSSGC.

Апробация результатов работы

Основные положения, представленные в диссертационной работе, докладывались и обсуждались на следующих конференциях: Международная конференция «Инжиниринг и Телекоммуникации» (En&T-2015), Москва (18-19 ноября 2015 г.); XIII Всероссийская научная конференция «Нейрокомпьютеры и их применение», Москва (17 март 2015г.); Международная конференция «Инжиниринг и Телекоммуникации» (En&T-2016), Москва (29-20 ноября 2016 г.); XV Всероссийская научная конференция «Нейрокомпьютеры и их применение», Москва (14 марта 2017 г.); XI Международная отраслевая научно-техническая

конференция «Технологии информационного общества», Москва (15-16 марта 2017 г.); Международная конференция «Инжиниринг и Телекоммуникации» (En&T-2018), Москва (15-16 ноября 2018 г.); XVI Всероссийская научная конференция «Нейрокомпьютеры и их применение», Москва (13 марта 2018 г.).

Публикации автора по теме диссертации

По теме диссертации опубликовано 7 научных работ, из них три статьи [1-3] в рецензируемых научных изданиях, входящих в перечень RSCI, четыре статьи [4-7] в изданиях, индексируемых в международных базах данных (SCOPUS, Web Of Science). Получены свидетельство № 2019615700 о регистрации программы для ЭВМ, диплом первой степени за лучшую публикацию на конференции En&T-2015 и акт о внедрении результатов диссертации.

Основные положения диссертации, выносимые на защиту

1. Метод обнаружения аномалий FLDS.
2. Метод инкрементной кластеризации на основе графов с частичным привлечением учителя IncrementalSSGC.
3. Комбинированный метод на основе сочетания методов J48, IncrementalSSGC и FLDS.
4. Многоэтапная система анализа трафика ЛБС для обнаружения и классификации вторжений и аномалий.

Структура и объем работы

Диссертационная работа включает титульный лист, оглавление, введение, 4 главы, заключение, список литературы и приложения. Объем диссертации составляет 144 страниц формата А4, 34 рисунков и 27 таблиц. Список литературы включает 114 наименований.

Содержание работы

Во введении обоснована актуальность темы диссертации, определены её цель и задачи, сформулированы научная новизна, теоретическая и практическая значимость полученных результатов и приведен перечень научных результатов и положения, выносимые на защиту.

В первой главе проводится анализ современного состояния решения проблемы выявления вторжений в беспроводных сетях стандарта IEEE 802.11. Рассматриваются основные особенности беспроводных сетей стандарта IEEE 802.11, их устройство, архитектура и применяемые методы обеспечения безопасности. Переведены классификация и особенности наиболее распространенных вторжений в локальных беспроводных сетях. Показано, что на текущий момент существует множество видов вторжений, выявление которых существующими методами является сложной и трудоемкой задачей. Изучение данных вторжений с точки зрения методологии их осуществления, позволило выделить следующие основные их группы: пассивные атаки, инъекции (injection), флуд (flooding) и атаки посредника (impersonation).

На основе проведенного анализа исследованы функции и характеристики систем обнаружения вторжений в локальных беспроводных сетях, описана их классификация. Проанализированы достоинства и недостатки современных алгоритмов анализа данных, на основе которых создаются системы обнаружения вторжений.

Основными результатами исследования, проведенного в первой главе, являются сформированная классификация основных типов вторжений в беспроводных локальных сетях анализ современных методов и алгоритмов анализа сетевого трафика для задач обнаружения вторжений и систем обнаружения сетевых вторжений. На основе проведенного анализа делается вывод о целесообразности создания новых методов обнаружения вторжений, устраняющих недостатки рассмотренных методов, а также разработки системы, объединяющей достоинства новых методик, что позволит более эффективно выявлять сетевые атаки в локальных беспроводных сетях, обеспечив высокую точность обнаружения атак и низкую вычислительную сложность используемых алгоритмов анализа данных сетевого трафика. Сформулирована постановка задачи и частные задачи исследования.

Вторая глава посвящена рассмотрению вопросов построения моделей и алгоритмов анализа трафика ЛБС для обнаружения вторжений и аномалий в ЛБС. Рассматриваются различные подходы к анализу информации, передаваемых через компьютерную сеть, которые разделяются в зависимости от уровня сетевой модели OSI. Показано, что анализ передаваемой информации на канальном уровне в виде кадров является наиболее подходящим для задач выявления атак в ЛБС.

Проанализированы различные алгоритмы машинного обучения по выявлению аномалий. Показано, что в литературе недостаточно исследован вопрос обнаружения аномалий в ЛБС, а сами алгоритмы имеют высокую вычислительную сложность. Например, 99% времени вычислений алгоритма LDS и других аналогичных алгоритмов, таких как LOF, тратится для нахождения K-ближайших соседей для всех исходных данных, поэтому вычислительная сложность определяется как $O(n^2)$. В литературе предлагается несколько подходов для ускорения поиска K-ближайших соседей, такие как использование специальных структур Kd-tree или X-tree, но они применяются ко всем исходным данным, что оказывает негативное влияние на их производительность. По этой причине предлагается идея оптимизации поиска пространства K-ближайших соседей с помощью разбиения заданного пространства на подпространства.

Согласно идее разбиения пространства происходит оптимизация алгоритма. Для разбиения пространства выбран алгоритм K-средних, поскольку он имеет множество достоинств, таких как простота понимания, простота программирования и низкая вычислительная сложность ($O(k \times n)$, k – количество кластеров, n – количество записей исходных данных). Алгоритм K-средних является базовым и популярным алгоритмом для большого числа приложений, поэтому не излагается в данной работе.

Комбинацией алгоритмов LDS и K-средних получается гибридный алгоритм FLDS (Fast LDS) с низкой вычислительной сложностью $O(n^{1.5})$.

Алгоритм FLDS использует три параметра: k – количество кластеров алгоритма K-средних, k_{nn} – количество ближайших соседней, ε – порог для выбора кандидата, который является аномалией. Выбор параметра происходит экспериментально.

Перед изложением алгоритма FLDS дадим необходимые определения.

Определение 1. Для любой вершины x_i через $NN(x_i)$ обозначается множество *K*-ближайших соседей x_i, не включая x_i.

Определение 2. Длина ребра или значение веса между любой парой вершин (x_i, x_j) на графе обозначается $\omega(x_i, x_j)$ и определяется как количество общих точек двух множеств *K*-ближайших соседей $NN(x_i)$ и $NN(x_j)$:

$$\omega(x_i; x_j) = \left|NN(x_i) \cap NN(x_j)\right|. \quad (1)$$

Основная идея предлагаемого алгоритма заключается в том, что сначала заданное множество X разбивается с помощью алгоритма K-средних на k подмножеств $(X_1, X_2, X_3, \dots, X_k)$, соответствующих k кластерам. После этого применяется алгоритм LDS на каждом подмножестве X_i $(i = 1{:}\,k)$ для получения множества локальных аномалий E. Множество E является множеством кандидатов в глобальные аномалии. Для каждой локальной аномалии на множестве E на заданном множестве X величина локальной плотности *Score* любой вершины x пересчитывается по формуле:

$$Score(x) = \frac{\sum_{q \in NN(x)} \omega(x,q)}{k_{nn}}. \quad (2)$$

В результате получается множество величин *LDS*, в котором порог ε используется для выбора глобальной аномалии.

Алгоритм FLDS (Fast Local Density Score) **[1]**

Вход: множество исходных данных $X = \{x_1, x_2, \dots, x_n\}$, k – количество кластеров, k_{nn} – количество ближайших соседней, ε – порог;

Выход: G – множество глобальных аномалий.

Процесс:

Шаг 1: инициализация центров с помощью min–max-подхода [2, 3, 4, 5] либо случайного выбора из исходных данных.

Шаг 2: реализация метода K-средних с k центрами для разбиения X на k подмножеств.

Шаг 3: применение алгоритма LDS на каждом полученном подмножестве для получения множества локальной аномалии E.

Шаг 4: получение множества величин *Score* каждой локальной аномалии с помощью перевычисления всех локальных аномалий на 3-м шаге.

Шаг 5: получение множества G глобальных аномалий, которое является множеством записей, имеющих величину *Score* меньше ε.

Сложность FLDS составляет $O(n \times k) + O(k * (n/k)^2) + O(t \times n)$, где k – количество кластеров, t – количество локальных аномалий $(t \ll n)$, n – количество записей исходных данных. Значение t оценивается примерно равным k. Согласно исследованиям авторов Zhong C., Chaoji V. и их коллег, значение k может быть использовано до $n^{0.5}$ раз. Таким образом, сложность FLDS равна $O(n^{1.5})$.

Также во второй главе проанализированы методики классификации для решения задачи выявления сетевых вторжений. Показано, что в изученной литературе мало методов обнаружения аномалий в ЛБС и их эффективность невысока. Также в литературе не было найдено алгоритма инкрементной кластеризации с частичным привлечением учителя.

Новая инкрементная кластеризация с частичным привлечением учителя на основе графов (IncrementalSSGC), представленная в диссертационной работе, основана на методе кластеризации на основе графов с частичным обучением (SSGC) и использованием помеченных значений. Сложность алгоритма SSGC составляет $O(k_{nn} \times n^2)$. SSGC более эффективен по сравнению с кластеризацией на основе плотности с частичным обучением при обнаружении кластеров для больших объемов данных. Однако, он не адаптирован для потока данных или

хранилищ данных, поскольку в них происходит большое количество обновлений (операций вставки/удаления).

В IncrementalSSGC помеченные значения будут использоваться для обучения графа k-ближайших соседей для построения связанных компонентов и определения значения θ как в алгоритме SSGC. Граф k-ближайших соседей понимается взвешенный неориентированный граф, в котором каждая вершина представляет точку данных и имеет не более k_{nn} ребер для своих ближайших соседей. Ребро создается между парой точек x_i и x_j тогда и только тогда, когда x_i и x_j принадлежат множествам k-ближайших соседей друг друга. Вес ребра $\omega(x_i; x_j)$ между двумя точками x_i и x_j определяется как число общих ближайших соседей, которые разделяют две точки, согласно формуле (1).

Как и в других алгоритмах инкрементной кластеризации, IncrementalSSGC включает две процедуры: вставку и удаление.

Алгоритм IncrementalSSGC [6]: процесс вставки

Вход: новый объект данных x_{new}; набор текущих кластеров C, список, содержащий ребра для каждой точки текущих кластеров L, θ (пороговое значение) и количество ближайших соседей k_{nn}.

Выход: метка для x_{new}.

Процесс:

1: Создать список k-ближайших соседей ребер (LE) между x_{new} и всеми текущими кластерами.

2: Удалить все $(u, v) \in LE : \omega(u, v) < \theta$.

3: **если** $(LE = \emptyset)$, **тогда**

x_{new} назначается метка ближайшего кластера, к которому относится точка с ребром к x_{new} с наибольшим весом.

4: **иначе если** x_{new} имеет соединения с точками, относящимися к одному и тому же кластеру, **тогда**

x_{new} назначается метка того же кластера.

5: **иначе если** x_{new} относится к двум или более компонентам с другой меткой, **то**

Удалить ребра из LE в порядке возрастания веса до нового соединения с компонентами, имеющими не более одного вида меток.

6: **конец если (5)**

7: конец если (4)

8: Получить метку для x_{new}.

9: Обновить список L: добавление x_{new} и ребер, связанных с x_{new}, в L; некоторые ребра между x_t и x_lтакже будут пересчитаны, если x_{new} появится в списке ближайших соседей x_t или x_l.

10: **конец если (3)**

Следующий алгоритм подробно описывает процесс удаления. Когда требуется исключить точку x_{del} из текущих кластеров, то необходимо удалить x_{del} и все ребра, связанные с x_{del} в графе. Шаг 2 алгоритма показывает процесс обновления. На этом этапе необходимо обновить все ребра, на которые влияет x_{del}. Это означает, что все ребра между x_i и x_j должны быть обновлены, если x_{del} появится в списке ближайших соседей. Наконец, на шаге 3 удаляются все ребра, которые имеют вес меньше, чем θ.

Алгоритм IncrementalSSGC [6]: процесс удаления

Вход: объект x_{del}, подлежащий удалению; список текущих кластеров C, список ребер каждой точки кластера L, θ (пороговое значение).

Выход: обновленные списки C и L

Процесс:

1: Удалить x_{del} и все ребра, связанные с x_{del} и L

2: Обновить все веса $(u, v) \in C: x_{del} \in NN(u) \cap NN(v)$

3: Удалить все обновленные (на шаге 2) $(u, v) \in L: \omega(u, v) < \theta$

Анализ сложности. Теперь проанализируем сложность IncrementalSSGC. Напомним, что сложность SSGC – $O(k_{nn} \times n^2)$, где n – число объектов в наборе

данных, k_{nn} – число ближайших соседей. Предполагая, что имеются текущие кластеры, включающие n объектов, проанализируем далее сложность процесса вставки и удаления IncrementalSSGC на шаге (n + 1).

Вычислительная сложность IncrementalSSGC составляет $O\big((1+q)\times n\times k_{nn}\big)$ (n – число объектов в наборе данных, k_{nn} – число ближайших соседей, q – среднее значение количества вызванных процессов удаления и фактически, q определяется путем проведения экспериментов), что значительно меньше по сравнению с SSGC ($O(k_{nn}\times n^2)$).

Третья глава посвящена проектированию и проведению экспериментов по проверке эффективности разработанных методик FLDS и IncrementalSSGC, а также их применимости для задач выявления аномалий и сетевых вторжений в ЛБС.

Для экспериментальной проверки предложенного алгоритма FLDS были взяты для сравнения алгоритмы LDS и LOF, которые также были применены для набора данных CHAMELEON, созданного автором Karypis G. и коллегами для тестирования эффективности алгоритмов кластеризации и поиска аномалий. Результат обнаружения аномалий в графическом виде представлен на рисунке 1. Сравнение времени выполнения алгоритмов показано на рисунке 2.

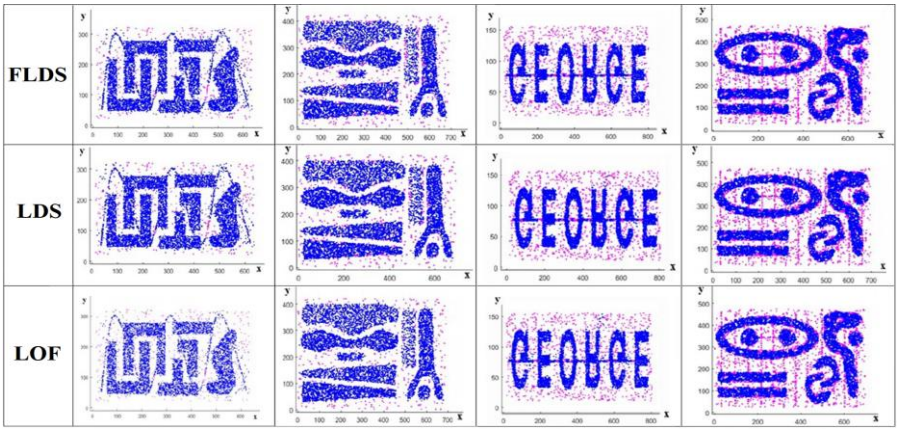

Рисунок 1 – Эксперименты по проверке FLDS. Набор данных CHAMELEON

Из рисунка 1 понятно, что аномалии, обнаруженные обоими методами, в основном схожи. Можно объяснить результаты тем фактом, что стратегия оценки того, является точка аномалией или нет, основана на локальном показателе плотности.

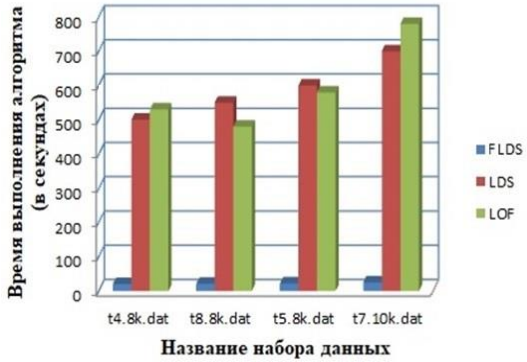

Рисунок 2 – Эксперименты по проверке FLDS. Набор данных CHAMELEON. Время обнаружения аномалий

Также для оценки качества работы предложенного алгоритма обнаружения аномалий используется ROC-кривая (receiver operating characteristic curves). Основой этого метода оценки является анализ графика ROC-кривой, при построении которого используется два показателя: коэффициент обнаружения (Detection Rate – DR) и коэффициент ложноположительных ошибок (False Alarm Rate – FAR). По оси абсцисс графика кривой откладываются значения коэффициента ложноположительных ошибок, по оси ординат – значения коэффициента обнаружения. Каждому результату работы алгоритма на таком графике будет соответствовать одна точка. При этом в зависимости от параметров алгоритма получается множество точек. Кроме того, важной характеристикой ROC-кривой является то, что чем больше площадь фигуры под ROC-кривой, тем эффективнее соответствующий ей алгоритм. ROC-кривые представлены на рисунке 3.

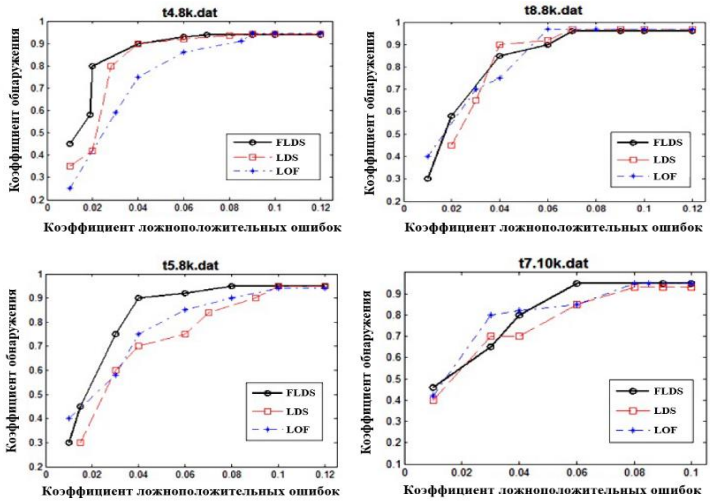

Рисунок 3 – Эксперименты по проверке FLDS. Набор данных CHAMELEON. Эффективность обнаружения аномалий

На рисунках 4 и 5 приведены результаты экспериментов на наборе данных ADFA, созданном авторами Creech G. и Hu J. для задачи выявления аномалий с целью обнаружения атак на информационные ресурсы. Он состоит из тысяч записей (traces) системных вызовов, собранных с локального сервера Linux, подвергнутого шестью типами современных кибератак, таких как Hydra-FTP, Hydra-SSH, Adduser, Java-Meterpreter, Meterpreter и Webshell. Из представленных на рисунках результатов видно, что алгоритм FLDS можно успешно применять для решения задачи обнаружения компьютерных вторжений. Достигнутая средняя точность обнаружения составила 95% при сокращении времени обработки более чем в 20 раз по сравнению с алгоритмами LDS и LOF.

На рисунке 6 показано сравнение времени работы алгоритмов FLDS и LOF на наборе данных AWID. AWID был разработан автором Kolias и коллегами для задачи выявления вторжений в локальные беспроводные сети Wi-Fi. Данный набор данных состоит из записей трафика, передаваемого по локальной беспроводной сети в виде кадров данных. AWID содержит как примеры обычного

трафика пользователей, так и большое количество сетевых вторжений различного типа.

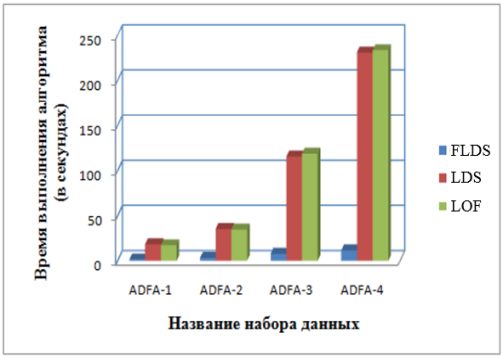

Рисунок 4 – Сравнение времени выполнения трех алгоритмов в зависимости от объема набора данных (для лучших по точности результатов)

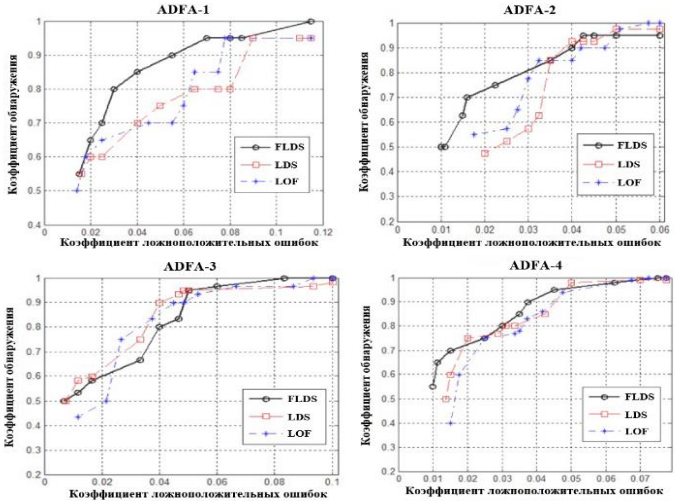

Рисунок 5 – Сравнение точности трех алгоритмов на наборе данных ADFA

Из рисунка 6 видно, что для четырех наборов данных время расчета FLDS примерно в 12 раз меньше, чем время работы LOF. Это может быть объяснено тем фактом, что сложность FLDS составляет всего $O(n^{1.5})$ по сравнению с $O(n^2)$ для LOF.

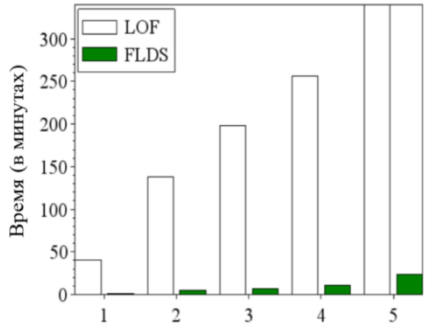

Рисунок 6 – Сравнение времени выполнения алгоритмов FLDS и LOF для пяти наборов данных AWID

Чтобы объединить значения частоту ложноположительных срабатываний (ложных тревог) (*FPR* – False Positive Rate) и частоту ложноотрицательных срабатываний (злонамеренный трафик принят за нормальный) (*FNR* – False Negative Rate), был рассчитан половинный общий коэффициент ошибок (*HTER* – Half Total Error Rate), который определяется по формуле:

$$HTER = \frac{FPR+FNR}{2}. \quad (3)$$

В таблице 1 приведены значение показателя *HTER* для LOF и FLDS для наборов данных AWID (чем меньше значение, тем лучше).

Таблица 1 – Показатель HTER для LOF и FLDS для наборов данных AWID

Алгоритм	O-AWID1	O-AWID2	O-AWID3	O-AWID4	O-AWID5
FLDS	0.13	0.12	0.10	0.11	0.06
LOF	0.23	0.11	0.11	0.09	0.09

Чтобы показать эффективность IncrementalSSGC, будут рассмотрены два аспекта: время работы и точность. Для тестирования IncrementalSSGC и IncrementaDBSCAN будут использованы 5 наборов данных UCI и 3 набора данных AWID.

Далее приведено сравнение производительности предложенного алгоритма и алгоритма IncrementalDBSCAN. IncrementalDBSCAN можно рассматривать как

один из наилучших среди предложенных ранее инкрементных методов кластеризации. Он может обнаруживать кластеры с различным размером, формой и с шумами. Поскольку и SSGC, и IncrementalSSGC дают одинаковые результаты, то приводятся результаты только для IncrementalSSGC и IncrementalDBSCAN. Результаты показаны на рисунке 7.

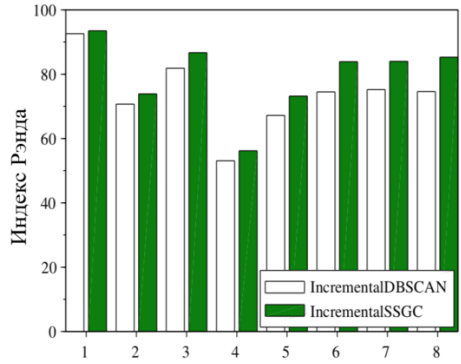

Рисунок 7 – Эксперименты по проверке IncrementalSSGC. Наборы данных UCI и AWID

Из рисунка видно, что IncrementalSSGC показывает лучшие результаты по сравнению с IncrementalDBSCAN. Это может быть объяснено с тем фактом, что IncrementalDBSCAN не может обнаружить кластеры с различной плотностью. В отличие от IncrementalDBSCAN, алгоритм IncrementalSSGC не зависит от плотности данных, поскольку используемый показатель сходства основан на совместных ближайших соседях.

На рисунках 8 и 9 показано время выполнения алгоритмов InternmentalSSGC и IncrementalDBSCAN для трех наборов данных AWID и 5 наборов данных UCI. Видно, что время выполнения обоих алгоритмов одинаково. Это можно объяснить тем, что для поиска кластеров оба алгоритма на каждой итерации используют метод k-ближайших соседей. Для справочных целей на рисунках 8 и 9 также показано время работы алгоритма SSGC.

В четвертой главе рассматриваются задачи проектирования и создания многоэтапной системы обнаружения и классификации злонамеренных действий в

ЛБС, основанная на разработанных методиках FLDS и IncrementalSSGC [1,4,6,7]. Приведены результаты экспериментальных исследований, проведенных на наборе данных реального трафика ЛБС AWID.

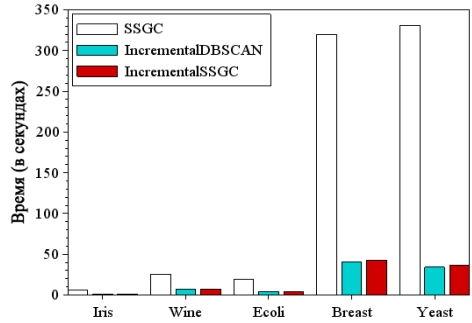

Рисунок 8– Сравнение времени выполнения алгоритмов SSGC, IncrementalSSGC и IncrementalDBSCAN. Наборы данных UCI

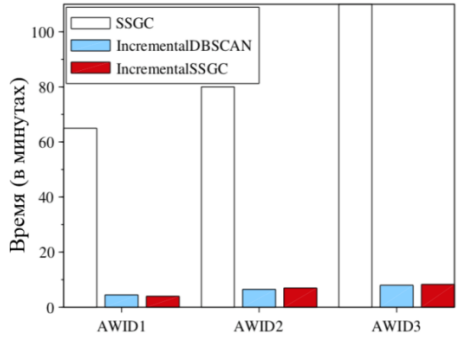

Рисунок 9 – Сравнение времени выполнения алгоритмов SSGC, IncrementalSSGC и IncrementalDBSCAN. Наборы данных AWID

Состав и схема работы системы представлен на рисунке 10.

Для задачи обнаружения вторжений в разработанной системе используется три основных компонента.

1. Классификатор (модель обучения с учителем) J48 в качестве базового компонента обнаружения вторжений в ЛБС.

2. Алгоритм инкрементной кластеризации для обнаружения атак посредника (Impersonation) на основе предложенного в диссертации метода IncrementalSSGC.

3. Метод обнаружения аномалий для выявления новых атак в ЛБС, основанный на предложенном в диссертационной работе алгоритме FLDS.

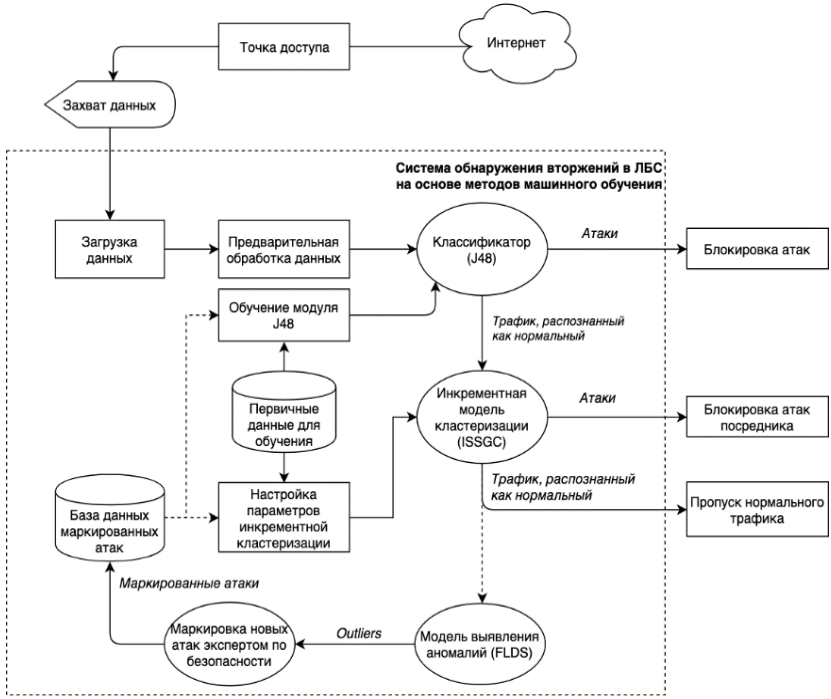

Рисунок 10 – Состав и схема работы предлагаемой СОВ в ЛБС

Основные этапы работы системы:

1. Первичный сбор данных трафика, передаваемого по ЛБС. Захват данных осуществляется сторонними инструментами, такими как tcpdump, Wireshark, NetFlow.

2. Загрузка собранных данных в СОВ, в ходе которой производится извлечение информации из исходных файлов, выборка параметров, необходимых для дальнейшего проведения анализа, и сохранение их в память программы.

3. Предварительная обработка, состоящая из двух шагов: преобразование символьных параметров в числовые значения и нормализация числовых значений в значения от нуля до единицы.

4. Обработка данных классификатором. В результате работы анализируемый трафик разделяется на нормальный и атакующий.

5. Дополнительная проверка данных на предмет наличия атак посредника, осуществляемая методом IncrementalSSGC. Трафик, распознанный инкрементной моделью кластеризации как нормальный, должен быть пропущен СОВ.

6. Обнаружение новых атак при помощи алгоритма выявления аномалий FLDS.

7. После анализа трафика ЛБС с помощью FLDS, система сохраняет данные о выявленных аномалиях. Данная информация должна быть изучена экспертом по сетевой безопасности. По результатам исследования эксперт маркирует кадры аномального трафика, являющегося злонамеренным, и сохраняет помеченные данные в базу данных маркированных вторжений. Далее обновленная база данных используется для дополнительного обучения модуля J48, а также для настройки параметров инкрементной кластеризации в модели ISSGC. Это позволяет в дальнейшем автоматически обнаруживать новые типы сетевых атак.

На рисунках 11 и 12 показаны примеры интерфейса разработанной программы для обнаружения вторжений в ЛБС.

Для проверки разработанной системы были проведены эксперименты на наборе данных AWID. Матрицы ошибок по результатам работы модулей J48 и ISSGC приведены в таблицах 2 и 3.

После того, как модуль FLDS обнаружил новые атаки, СОВ может быть обновлена. Во время эксперимента по результатам работы FLDS были добавлены новые атаки в данные обучения модуля J48. Таким образом, модуль J48 был обновлен, после чего проведено новое тестирование с первоначальными данными. Результаты тестирования показывают, что обновленный модуль J48 смог обнаружить новые атаки, в результате суммарная точность обнаружения

возросла до 96,41%. В таблице 4 приведен суммарный результат работы модуля J48 до и после обновления, а также модуля ISSGC.

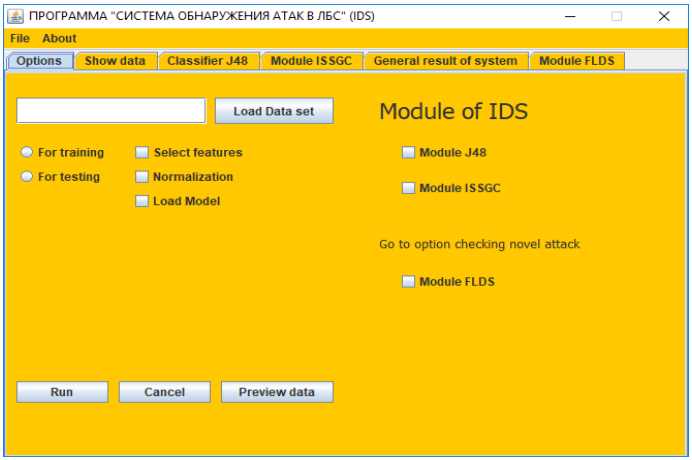

Рисунок 11 – Интерфейс окна настроек СОВ в ЛБС

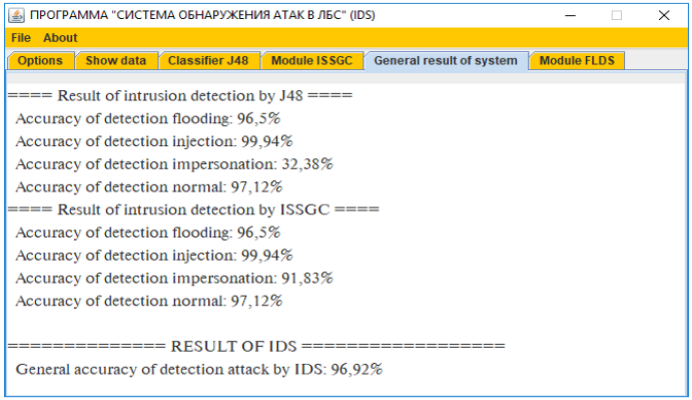

Рисунок 12 – Интерфейс окна с результатами работы СОВ в ЛБС

Таблица 2 – Матрица ошибок по результатам работы модуля J48 системы обнаружения вторжений в ЛБС

Нормальный трафик	Атаки «Флуд»	Атаки «Инъекции»	Атаки «Посредника»	*Распознан как:*
14568	431	0	1	Нормальный трафик
70	1930	0	0	Атаки «Флуд»

2	0	3348	0	Атаки «Инъекции»
1623	0	0	777	Атаки «Посредника»

Таблица 3 – Матрица ошибок по результатам работы модуля ISSGC системы обнаружения вторжений в ЛБС

Нормальный трафик	Атаки «Флуд»	Атаки «Инъекции»	Атаки «Посредника»	*Распознан как:*
14279	431	0	290	Нормальный трафик
70	1930	0	0	Атаки «Флуд»
2	0	3348	0	Атаки «Инъекции»
23	0	0	2377	Атаки «Посредника»

Таблица 4 – Суммарный результат работы двух модулей J48 и ISSGC

Группа трафика	Точность обнаружения на выходе алгоритма		
	J48 (до обновления)	ISSGC (после работы J48)	J48 после обновления
Атаки «Флуд»	96.5%	96.5%	96.5%
Атаки «Инъекции»	99.94%	99.94%	99.94%
Атаки «Посредника»	32.38%	92.12%	99.04%
Нормальный трафик	97.12%	97.12%	95.19%
Суммарная точность:	90.65%	96.95%	96.41%

Как показали проведенные эксперименты, разработанная система позволяет повысить точность обнаружения вторжения на 10% по сравнению с использованием только алгоритма J48. Сравнение производится с данным алгоритмом как наиболее известным и эффективным алгоритмом для решения задач выявления атак в ЛБС.

Следует отметить, что для реальных приложений, в момент возникновения атаки система должна немедленно выдавать предупреждение. Предложенная многоэтапная система, основанная на методах машинного обучения, дает основу

для построения систем IDS/IPS в реальном времени, что является одной из наиболее важных задач в сфере обеспечения безопасности компьютерных сетей.

В заключении приводятся результаты работы и делаются выводы.

Основные результаты диссертации

Проведен анализ современного состояния решения проблемы обнаружения вторжений в локальных беспроводных сетях стандарта IEEE 802.11. Рассмотрены классификация и особенности наиболее распространенных вторжений. Показано, что на текущий момент существует множество видов вторжений, выявление которых существующими методами является сложной, трудоемкой, а иногда и неразрешимой задачей.

Проведен анализ существующих методов и средств по выявлению вторжений в локальных беспроводных сетях. Рассмотрены достоинства и недостатки современных алгоритмов анализа данных, на основе которых создаются системы обнаружения вторжений.

Проанализированы особенности различных подходов к анализу трафика в локальных беспроводных сетях. Подробно рассмотрены алгоритмы машинного обучения по выявлению аномалий и методики классификации для решения задачи обнаружения сетевых вторжений.

Предложен алгоритм обнаружения аномалий FLDS, который имеет вычислительную сложность $O(n^{1.5})$, что значительно меньше по сравнению с наиболее известным алгоритмом оценки локальной плотности (LDS) и алгоритмом фактора локального отклонения (LOF).

Разработан инкрементный метод кластеризации с частичным обучением на основе графов (IncrementalSSGC), который позволяет повысить эффективность обнаружения вторжений в локальных беспроводных сетях. Его сложность составляет $O\big((1+q)\times n\times k_{nn}\big)$, где n – число объектов в наборе данных, k_{nn} – число ближайших соседей, q – среднее значение количество вызванных процессов удаления.

Проведена экспериментальная проверка предложенного алгоритма быстрой оценки локальной плотности FLDS на наборах данных CHAMELEON, ADFA и AWID, которая подтвердила его эффективность. Результаты экспериментов показывают, что предложенный алгоритм реализует точное обнаружение аномалий, а также работает быстрее в 10-20 раз и более по сравнению с алгоритмами LDS и LOF.

Проведена экспериментальная проверка инкрементного метода кластеризации с частичным привлечением учителя на основе графов IncrementalSSGC на наборах данных AWID и UCI. Результаты экспериментов подтвердили высокую эффективность методики в части выявления вторжений посредника. Точность распознавания IncrementalSSGC на 15-20% выше, скорость распознавания выше в 10-20 раз по сравнению с SSGC.

Разработана многоэтапная система “Программа-модуль обнаружения атак в локальной беспроводной сети на основе методов машинного обучения” на основе алгоритма J48 и предложенных в настоящей работе алгоритма быстрой оценки локальной плотности (FLDS) и метода инкрементной кластеризации на основе графов с частичным привлечением учителя (IncrementalSSGC).

Испытания предложенной многоэтапной системы обнаружения аномалий и вторжений в локальных беспроводных сетях проведены на наборах данных AWID. Результаты испытаний показали, что многоэтапная система обеспечивает высокую эффективность обнаружения вторжений в ЛБС (96-97%). Это на 10% лучше по сравнению с системой Kolias C., использующей алгоритм J48.

Разработанная многоэтапная система может являться основой для построения систем обнаружения вторжения в реальном времени, а также для решения других задач ИАД, таких как распознавание образов (изображений, лиц и др.).

Разработанная система установлена и запущена в эксплуатацию в центре сетевой безопасности «Телекоммуникации FPT» (Вьетнам).

Основные результаты опубликованы

В рецензируемых научных изданиях, входящих в перечень RSCI:

1. By B. T., Пантюхин Д. В., Назаров А. Н. FLDS: Оптимизация пространства поиска для ускорения алгоритма оценки локальной плотности (Local Density Score) // Труды Московского физико-технического института. – 2016. – Т. 8. – №. 3. – С. 65-78.

2. By B. T., Пантюхин Д. В., Галушкин А. И. Гибридный алгоритм кластеризации FASTDBSCAN // Журнал «Труды Московского физико-технического института». – 2015. – Т. 7. – №. 3 (27). – С. 77-81.

3. By B. T. Ускорение алгоритма кластеризации DBSCAN за счет использовании алгоритма K-means // Журнал «Информационные технологии». – 2016. – Т. 22. – №. 2 (27). – С. 109-115.

В изданиях, индексируемых в международных базах данных (SCOPUS, Web Of Science):

4. Vu V. T., Pantiukhin D. V., Nazarov A. N. FLDS: fast outlier detection based on local density score // 3th International Conference on Engineering and Telecommunication (EnT). – IEEE, 2016. – С. 137-141.

5. Vu V. T., Pantiukhin D. V., Galushkin A. I. A Hybrid Clustering Algorithm: The FastDBSCAN // 2015 International Conference on Engineering and Telecommunication (EnT). – IEEE, 2015. – С. 69-74.

6. Vu V. T., Pashchenko F. F. A new incremental semi-supervised graph based clustering // 5th International Conference on Engineering and Telecommunication (EnT). – IEEE, 2018. – С. 210-214.

7. Vu V. T., Pashchenko F. F. Multistage system-based machine learning techniques for intrusion detection in Wifi network // Journal of Computer Networks and Communications, Special Issue Advances in Machine Learning for Cybersecurity. – Volume 2019, Article ID 4708201, 13 pages. https://doi.org/10.1155/2019/4708201.

Заявка на свидетельство о регистрации программы для ЭВМ

8. Ф.Ф. Пащенко, By Вьет Тханг. «Программа-модуль обнаружения атак в локальной беспроводной сети на основе методов машинного обучения»// Роспатент, регистрационный № 2019615700, 07.05.2019.

Публикации в материалах конференций

9. By B. T., Чан Ван Нгиа. «Ускорение алгоритма кластеризации DBSCAN за счет использования алгоритма K-Means» // Сборник «Международная конференция Инжиниринг & Телекоммуникации». – М.: МФТИ. – 18-19 ноября 2015г.

10. D. V. Pantiukhin, By B. T. «Применение нейронной сети типа многослойный персептрон для распознавания типа атаки на информационную систему на примере базы KDD'99» // Сборник XIII всероссийская научная конференция «Нейрокомпьютеры и их применение» 17 марта 2015 года.

11. By B. T., D. V. Pantiukhin; A.N. Nazarov. «O-LDS: Оптимизация пространства поиска для ускорения алгоритма оценки локальной плотности (Local Density Score)» // Сборник «Международная конференция Инжиниринг & Телекоммуникации». – М.: МФТИ. – 29-20 ноября 2016 г..

12. D. V. Pantiukhin, By B. T. «Ускорение кластеризации методом DBSCAN за счет использования алгоритма K-means» // Сборник XV всероссийская научная конференция «Нейрокомпьютеры и их применение» 14 марта 2017 года.

13. A.N. Nazarov, By B. T. «Применимость метода покрытий для синтеза функций защиты от информационных атак объекта риска информационно-телекоммуникационной системы» // Сборник XI отраслевая научно-техническая конференция «Технологии информационного общества» 15-16 марта 2017 г.

14. By B. T. «Повышение эффективности обнаружения атак «Impersonation» в беспроводных сетях стандарта 802.11 на основе нейронной сети и обнаружения аномалий O-LDS» // Сборник XVI всероссийская научная конференция «Нейрокомпьютеры и их применение» 13 марта 2018г.

15. By B. T., Ф.Ф. Пащенко. «Новая инкременная кластеризация с частичным обучением на основе графа» // Сборник «Международная конференция Инжиниринг & Телекоммуникации». – М.: МФТИ. – 15-16 ноября 2018 г.

Научное издание

Ву Вьет Тханг

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МНОГОЭТАПНОЙ СИСТЕМЫ АНАЛИЗА ТРАФИКА ЛОКАЛЬНОЙ БЕСПРОВОДНОЙ СЕТИ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И ЕЁ ПРИМЕНЕНИЕ В ЗАДАЧЕ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Федеральное государственное автономное образовательное учреждение

высшего образования

Московский физико-технический институт

(национальный исследовательский университет)

141701, Московская область, г. Долгопрудный,

Институтский переулок, д. 9

https://mipt.ru