ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

На правах рукописи

Овасапян Тигран Джаникович

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ОБУЧАЮЩИХСЯ АВТОМАТОВ

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург
2022

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО СПбПУ) в Институте кибербезопасности и защиты информации, г. Санкт-Петербург.

Научный руководитель:
Кандидат технических наук Москвин Дмитрий Андреевич.

Официальные оппоненты:
Доктор технических наук, профессор Петренко Сергей Анатольевич, Центр информационной безопасности АНО ВО «Университет Иннополис», руководитель.

кандидат технических наук, доцент Красов Андрей Владимирович, ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», заведующий кафедрой защищенных систем связи.

Ведущая организация:
Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), г. Воронеж.

Защита состоится «30» марта 2022 г. в 14 ч.
на заседании диссертационного совета У.05.13.19 федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (195251, г. Санкт-Петербург, ул. Политехническая, д. 29, Главный корпус, ауд. 175).

С диссертацией и авторефератом можно ознакомиться в библиотеке и на сайте www.spbstu.ru федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Автореферат разослан "___" _____ 2022 г.

Ученый секретарь
диссертационного совета У.05.13.19,
кандидат физико-математических наук Шенец Николай Николаевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время наблюдается тенденция к применению устройств, способных взаимодействовать с внешней средой и обмениваться между собой информацией по внутренней сети или сети Интернет. Число подобных устройств непрерывно увеличивается, что свидетельствует о переходе к информационно-технологической концепции киберфизических систем (КФС).

Значимая часть устройств КФС является необслуживаемыми распределенными в пространстве вычислительными узлами. Объединение таких устройств в самоорганизующуюся систему сбора, обработки и передачи информации – беспроводную сенсорную сеть (БСС, Wireless Sensor Network, WSN) – позволит расширить возможности представления информации о производственных процессах, об окружающей среде, а также улучшить человеко-машинное взаимодействие.

Обеспечение безопасности играет решающую роль в использовании БСС, поскольку данный класс сетей применяется в критических сферах, напрямую связанных с жизнедеятельностью общества. Этому также свидетельствует ряд принятых законов Российской Федерации, таких как №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», постановления Правительства № 127, № 162, № 452, приказы ФСТЭК №31, №239, а также другие нормативно-правовые акты, связанные с безопасностью критически важной инфраструктуры. Таким образом, развитие БСС вынуждает разрабатывать эффективные методы противодействия угрозам безопасности.

Использование множества различных методов защиты от конкретных атак в БСС далеко не всегда является целесообразным из-за ограниченности узлов в ресурсах. Некоторые из методов защиты не имеют на сегодняшний день ни одной практической реализации. Другие методы противоречат друг другу, например, по требуемым протоколам маршрутизации, что делает невозможным их одновременную работу в рамках одной сети. К тому же обновление функционала, для противодействия новым атакам, требует физического доступа к некоторым узлам, что не всегда представляется возможным и увеличит стоимость обслуживания сети. В связи с этим необходим универсальный механизм безопасности, позволяющий защитить БСС как от искусственных угроз безопасности, так и от естественных. В рамках данной работы предлагается использовать адаптивную систему управления на базе обучающегося автомата, позволяющую узлам изменять правила взаимодействия с соседними узлами в зависимости от внешних факторов.

Степень разработанности темы исследования. Вопросам обеспечения безопасности КФС в целом и БСС в частности посвящены работы российских и иностранных ученых, таких как П.Д. Зегжда, Д.П. Зегжда, М.О. Калинин, И.Б. Саенко, И.В. Котенко, С.А. Петренко, Е.С. Абрамов, Е.С. Басан, Д.А. Заколдаев, С. Мишра, Х. Жу, А. Фатинавид, Н. Кумар.

Ряд работ посвящен применению обучающихся автоматов в области обеспечения безопасности БСС. В работах С. Мишры, П. Кришны, К. Абрахама предлагается система обнаружения вторжений на базе обучающегося автомата для выбора безопасного маршрута передачи данных. В работе Х. Жу предлагается применение адаптивного автомата для защиты от атак выборочной передачи пакетов (selective forwarding attack). Для обеспечения адаптивного поведения узлов БСС обучающийся автомат в данной работе применяется впервые. За счет использования адаптивного поведения узлы будут способны противодействовать как естественным угрозам безопасности, так и целенаправленным атакам злоумышленников.

Объектом исследования является БСС, в отношении которой совершаются деструктивные воздействия.

Предметом исследования являются подходы и методы противодействия угрозам безопасности в БСС.

Целью работы является поддержание защищенности и функциональной устойчивости БСС на основе интеллектуально-адаптивного управления правилами взаимодействия узлов в условиях угроз информационной безопасности.

Для достижения поставленной цели в работе решались следующие **задачи**:

1. Систематизация актуальных угроз и анализ существующих подходов к обеспечению функциональной устойчивости и защищенности БСС.
2. Разработка методики выявления угроз безопасности узлов БСС на основе интеллектуального анализа показателей функционирования.
3. Построение конечно-автоматной модели, описывающей динамически изменяемые правила взаимодействия узлов БСС.
4. Создание метода адаптивного управления работой БСС на основе обучающегося автомата, учитывающего показатели функционирования узлов и выполнение ими целевой функции.
5. Разработка архитектуры и макета системы поддержания защищённости и функциональной устойчивости БСС для оценки эффективности предложенного метода адаптивного управления.

Методы исследования включают в себя теорию информационной безопасности, теорию вероятностей, теорию автоматов, методы математического моделирования, методы машинного обучения.

Научная новизна полученных результатов:

1. Предложена методика выявления угроз безопасности узлов БСС различной архитектуры на основе предварительной обработки и анализа показателей функционирования с использованием технологий искусственного интеллекта.
2. Разработана модель обучающегося автомата для описания динамически изменяемых правил взаимодействия узлов БСС.
3. Сформулирована и доказана теорема о необходимом условии нахождения узла БСС в безопасном для взаимодействия с ним состоянии.

4. Предложен метод динамического управления работой БСС, позволяющий поддерживать защищенность и функциональную устойчивость сети.

Теоретическую значимость работы составляют предложенные показатели функционирования узлов БСС, формализация правил взаимодействия узлов с использованием обучающегося автомата, определение условий достижимости безопасного состояния узла в виде теоремы.

Практическая значимость результатов работы заключается в возможности применения предложенных методов и алгоритмов для реализации интеллектуально-адаптивной системы управления для защиты БСС от угроз безопасности. Полученные в ходе работы результаты позволяют:

— выявить аномалии в работе БСС путем анализа показателей функционирования устройств;

— представить в виде автоматной модели процесс взаимодействия узлов друг с другом в БСС;

— сохранить устойчивость функционирования БСС в условиях угроз безопасности благодаря разработанному методу адаптивного управления правилами взаимодействия узлов.

Положения, выносимые на защиту:

1. Методика выявления угроз безопасности узлов БСС на основе интеллектуального анализа показателей функционирования устройств.
2. Модель обучающегося автомата, обеспечивающая устойчивость функционирования БСС путем изменения правил взаимодействия узлов друг с другом.
3. Метод адаптивного управления работой БСС на основе обучающегося автомата, учитывающего показатели функционирования и выполнения узлами целевой функции.
4. Теорема о необходимом условии нахождения узла БСС в безопасном для взаимодействия с ним состоянии.

Внедрение результатов работы. Полученные основные научные результаты диссертационного исследования использованы при реализации гранта Российского Фонда Фундаментальных Исследований 19-37-90027 «Разработка интеллектуально-адаптивного метода защиты беспроводной сенсорной сети», в проектной деятельности ФГУП «НИИ «Квант», ООО «ТехСистемС», а также нашли свое отражение в учебном процессе Института кибербезопасности и защиты информации ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» при организации дисциплины «Модели безопасности компьютерных систем», что подтверждается соответствующими актами о внедрении.

Достоверность и обоснованность результатов, представленных в диссертации, подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Соответствие специальности научных работников. Полученные научные результаты соответствуют следующим пунктам «Области исследования» паспорта специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность»: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса (п. 3); модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (п. 8).

Апробация работы. Основные результаты исследований и научных разработок докладывались и обсуждались на следующих конференциях: научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2017, 2018, 2019, 2020 и 2021 гг.), научно-практическая конференция «РусКрипто» (Москва, 2020 г.), научно-практическая конференция с международным участием «Неделя науки СПбГПУ» (Санкт-Петербург, 2017 г.), международная конференция «Региональная информатика (РИ-2016)» (Санкт-Петербург, 2016 г.), межрегиональная конференция «Информационная безопасность регионов России» (Санкт-Петербург, 2017 и 2021 гг.), межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий» (Севастополь, 2018 г.), международная конференция «Fourth World Conference on Smart Trends in Systems, Security and Sustainability WorldS4» (Лондон (Великобритания), 2020 г.), международная конференция «SIN 2020: 13th International Conference on Security of Information and Networks» (Турция, 2020 г.).

Исследования, лежащие в основе данной работы, победили в конкурсе грантов Правительства Санкт-Петербурга для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2017, 2018, 2019 и в 2020 годах.

Публикации. Результаты диссертационной работы отражены в 24 публикациях, в том числе в 6 публикациях в рецензируемых журналах из перечня ВАК РФ, 5 публикациях в изданиях из перечня Scopus и Web of Science, а также в 2 свидетельствах о регистрации программ для ЭВМ.

Объем и структура диссертации. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 170 наименований. Общий объем работы составляет 161 страницу, в том числе 32 рисунка и 7 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, поставлена цель работы, определены задачи. Выделены положения, выносимые на защиту, научная новизна и практическая значимость работы.

В первой главе представлены исследования, направленные на анализ принципов функционирования БСС, областей их применения, систематизацию угроз и определение специфики методов обеспечения их безопасности.

В ходе анализа существующих решений для построения БСС выделены основные сферы их применения. Наиболее критические задачи, с точки зрения влияния на безопасность общества и людей, выполняют сети из большого количества маломощных устройств, работающих на неохраняемом периметре.

На основе анализа принципов функционирования БСС выявлены особенности, влияющие на безопасность их функционирования. Сделан вывод, что БСС подвержены не только атакам злоумышленников, но и возникновению ошибок в сети без каких-либо вредоносных вмешательств (отказ части функционала узлов, неблагоприятная внешняя среда и т.п.).

Проведена систематизация угроз безопасности по уровням сетевой модели OSI. Основные угрозы направлены на нарушение доступности сети и целостности передаваемых данных между узлами. Данные угрозы реализуются в большинстве случаев за счет атак истощение энергоресурсов, зашумление канала связи, «черная/серая» дыра.

Выполнен обзор современных научных исследований и рассмотрены существующие подходы к обеспечению безопасности БСС. Проведен их сравнительный анализ, выявлены достоинства, недостатки и приемлемые условия для использования каждого из подходов.

Анализ работ показал, что существующие решения для БСС, в основном, позволяют идентифицировать выявленные угрозы безопасности. Их устранение осуществляется путем полного исключения атакующего или неисправного узла из сети. При этом подавляющее большинство подходов направлены на обеспечение защиты от целенаправленных атак вредоносных узлов, без учета возникновения в сети естественных угроз безопасности.

Основываясь на особенностях функционирования распределенных БСС, более целесообразным подходом к противодействию угрозам безопасности является использование гибкого управления правилами взаимодействия между узлами для сохранения работоспособности сети в условиях деструктивных воздействий.

Для сохранения отказоустойчивости предлагается использовать адаптивное поведение, в рамках которого узел будет изменять правила взаимодействия со своими соседями. Сохранение работоспособности сети обеспечивается за счет изменения поведения узла относительно вредоносного или неисправного узла на основе интеллектуального анализа входных сигналов (показателей).

Показатели, которые влияют на адаптивную работу предлагается разделить на две группы: показатели функционирования и показатели поведения (показывают корректность выполнения узлом целевой функции).

Во второй главе представлена разработанная методика выявления угроз безопасности узлов БСС путем сбора, обработки и интеллектуального анализа показателей функционирования узлов.

Разработанная методика состоит из шести этапов, которые представлены на схеме (рисунок 1). Первые три этапа являются предварительными и предназначены для определения перечня анализируемых показателей функционирования и формирования

обучающих выборок. Далее, в зависимости от архитектуры сети, осуществляется обучение соответствующих методов искусственного интеллекта, и загрузка необходимых данных в прошивку узлов. Заключительным этапом является работа обученных методов в развернутой БСС.

Рисунок 1 – Схема методики выявления угроз БСС

В ходе работы определены показатели функционирования, которые можно получить из операционной системы каждого узла в режиме реального времени с определенной периодичностью: загрузка микроконтроллера, температура микроконтроллера, уровень заряда батареи, объем отправленного/полученного сетевого трафика, объем оперативной памяти. Любое вредоносное воздействие или атака отражается на значении показателей функционирования в виде аномалий, которые можно выявить.

В рамках задачи выявления аномалий проведен ряд исследований, в результате которых наилучший результат получен при использовании алгоритма классификации k-ближайших соседей (k-nearest neighbor, k-NN) с показателем количества соседей k = 10. Точность классификации (F-мера) в лучшем случае составляла 0.98 при проведении атак истощения энергоресурсов, зашумления канала связи, «черная/серая» дыра. Обучение основывалось на ранее собранных данных (69481 запись, где половина показателей

собрана при атаках, а другая половина при нормальной работе сети). Полученные данные были перемешаны случайным образом и разделены на обучающую выборку (75%) и тестовую выборку (25%).

При использовании метода k-NN важен размер выборки. Как правило, в связи с низкой периодичностью обмена данными в БСС, возникает ограничение, связанное с недостаточным количеством элементов в выборке для анализа методом машинного обучения в определенный момент времени. Для повышения количественного показателя выборки предложено использовать генеративно-состязательную сеть (generative adversarial network, GAN) для генерирования синтетических данных и дополнения ими анализируемых данных.

Генеративная-состязательная сеть включает в себя работу двух нейронных сетей - сверточной и сети-генератора. Работа метода описывается формулой (1) и заключается в попытке сверточной сети (дискриминатор, D) обмануть сеть-генератор (G) в процессе преобразования случайного шума в требуемые данные.

$$\min_G \max_D E_{x\sim p_{data}}[logD(x)] + E_{z\sim p(z)}[\log\left(1 - D\left(G(z)\right)\right)], \quad (1)$$

где $x\sim p_{data}$ – входные данные, $z\sim p(z)$ – случайный шум, $G(z)$ – данные, сгенерированные сетью G, $D(x)$ – результат работы дискриминатора, представляющий собой вероятность того, что данные, полученные на вход – настоящие.

В результате использования синтетических данных в некоторых случаях удалось добиться увеличения точности выявления аномалий. Так, при добавлении данных относительно расхода заряда батареи и нагрузки на процессор, точность выявления удалось повысить на 34%.

При полностью распределённой архитектуре сети, без базовых станций по всему периметру, использовать методы машинного обучения является нецелесообразным в связи с ограничениями ресурсов батареи и вычислительных ресурсов узлов. При такой конфигурации сети предлагается использовать радиально базисную нейронную сеть для прогнозирования значений показателей функционирования соседних узлов и выявления угроз безопасности. Задача прогнозирования данных сводится к задаче прогнозирования временных рядов. Процесс обучения осуществляется заранее до разворачивания сети в ходе имитационного моделирования. Таким образом, обученная сеть способна предсказать будущее значение показателя без накладных требований к вычислительным ресурсам узла.

Для решения задач прогнозирования используются сети на основе радиально-базисных функций. Такие сети строятся с использованием радиальных нейронов, функция активации которых имеет ненулевые значения только в окрестностях своего центра.

Прогнозирования каждого показателя осуществляет отдельно обученная нейронная сеть. Архитектура сети состоит из трех слоев: входной слой, который принимает получает N показателей, доступных на данный момент; скрытый слой с радиально-базисной активационной функцией; выходной слой, который выводит прогнозируемый показатель, представляющий собой взвешенную сумму сгенерированных скрытыми нейронами значений.

Число нейронов входного слоя соответствует числу подаваемых на вход показателей. Число нейронов скрытого слоя подбирается экспериментально в ходе имитационного моделирования по достижении требуемой точности.

Функция активации нейронов скрытого слоя основана на функции Гаусса:

$$\varphi_i(x) = \varphi(\bar{x}, \bar{c_i}) = \exp\left(-\frac{1}{2\sigma^2}||\bar{x} - \bar{c_i}||^2\right), i = 1, 2, \dots, K, \quad (2)$$

где x – входной вектор; σ и c – регулирующие параметры активационной функции, называемые шириной окна функции и центром соответственно. Коэффициенты σ и c вычисляются на этапе настройки сети. Вектор c принимает отдельные случайные значения из обучающей выборки. Ширина определяется в явном виде на основе эвристического подбора. Норма разности векторов рассчитывается как евклидово расстояние.

Нейроны скрытого слоя соединены по полносвязной схеме с нейроном выходного слоя, который осуществляет взвешенное суммирование по формуле:

$$y(x) = \sum_{i=1}^{K} \omega_i \varphi_i(x), \quad (3)$$

где ω – весовой вектор, являющийся центром радиально-базисной функции, соответствующей нейрону с номером i.

Точность прогнозирования оценивалась с использованием метрики качества MAE (средняя абсолютная ошибка, Mean Absolute Error). Наилучший показатель с результатом MAE=0.25 получен при использовании соотношения обучающая/рабочая выборка 0.2/0.8 соответственно.

На рисунке 2 представлен график зависимости реальных и спрогнозированных значений показателя функционирования.

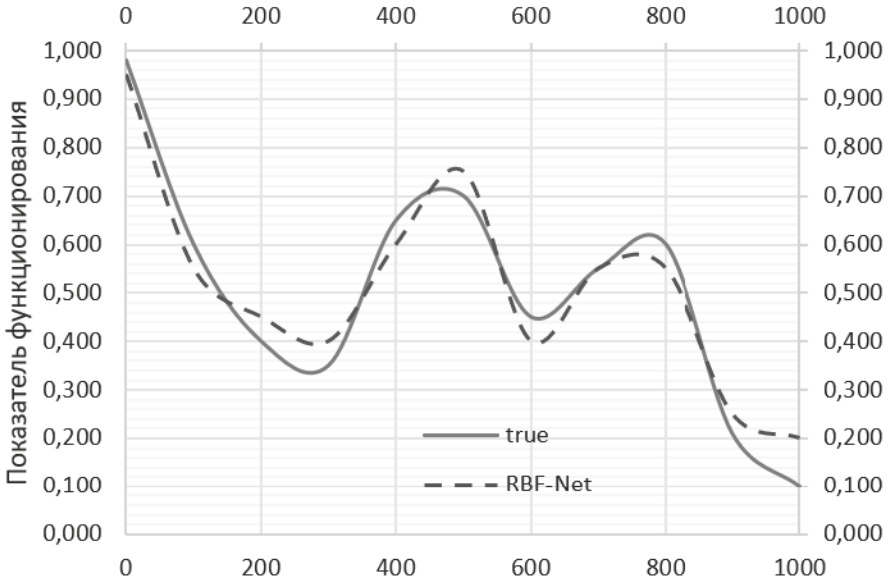

Рисунок 2 – График зависимости реальных и спрогнозированных значений показателя функционирования

Предложенная методика выявления угроз БСС реализована в программах для ЭВМ №2021669906 «Программа интеллектуальной идентификации киберугроз в интернете вещей с дообучением на синтетических наборах данных» и №2021617986 «Программа обнаружения нарушений безопасности и аномалий функционирования в беспроводных сенсорных сетях на основе интеллектуального анализа параметров работы устройства».

В третьей главе представлены результаты построения конечно-автоматной модели, описывающей динамически изменяемые правила взаимодействия узлов БСС и позволяющей узлам изменять правила взаимодействия со своими соседями.

Приведена классификация адаптивных систем управления по задаче адаптации и по характеру настройки. Определены наиболее подходящие характеристики системы с учетом особенностей БСС. По первому критерию наиболее подходящей является система с оптимизацией управления, а по второму критерию система должна быть обучающейся.

В качестве математической модели, удовлетворяющей двум указанным выше критериям и позволяющей достичь интеллектуально-адаптивного поведения узлов, используется обучающийся автомат (ОА, Learning Automaton, LA).

Обучающийся автомат представляет собой модель, которая способна самообучаться в процессе взаимодействия с внешней средой и адаптироваться к изменениям. У каждого узла есть набор вероятных действий относительно соседнего узла. Эти же действия представлены в автомате. Вероятности действий в автомате обновляются на основе полученного сигнала подкрепления. Сигнал подкрепления формируется в зависимости от полученных показателей соседних узлов в процессе работы сети.

Проведен анализ математического аппарата ОА. Выявлены и проанализированы возможные типы и характеристики автоматов данного класса. Определены необходимые характеристики в рамках решаемой задачи:

— тип автомата – стохастический;

— структура – переменная;

— модель оценивания - P-модель;

— комбинированная модель обучения: поощрение-ε-штраф ($L_{П-εШ}$, a<<b) и поощрение-штраф ($L_{ПН}$, b = 0) a – параметр поощрения b – параметр штрафа.

Обновление вектора вероятностей осуществляется с использованием систем уравнений:

$$P_j(n+1) = \begin{cases} P_j(n) + a\left(1 - P_j(n)\right), \; j = i \\ P_j(n) - aP_j(n), \;\; \forall j, \; j \neq i \end{cases}, \tag{4}$$

$$P_j(n+1) = \begin{cases} (1-b)P_j(n), \; j = i \\ \dfrac{b}{r-1} + (1-b)P_j(n), \;\; \forall j, \; j \neq i \end{cases}, \tag{5}$$

где $P_j(n)$ – вероятность действия в момент времени n; a, b – коэффициенты, значения которых зависит от выбранной модели обучения.

Система уравнений (4) используется в случае выигрыша, система уравнений (5) – в случае проигрыша автомата.

С учетом ранее определенных параметров и особенностей работы БСС разработана графовая модель обучающегося автомата, представленная на рисунке 3.

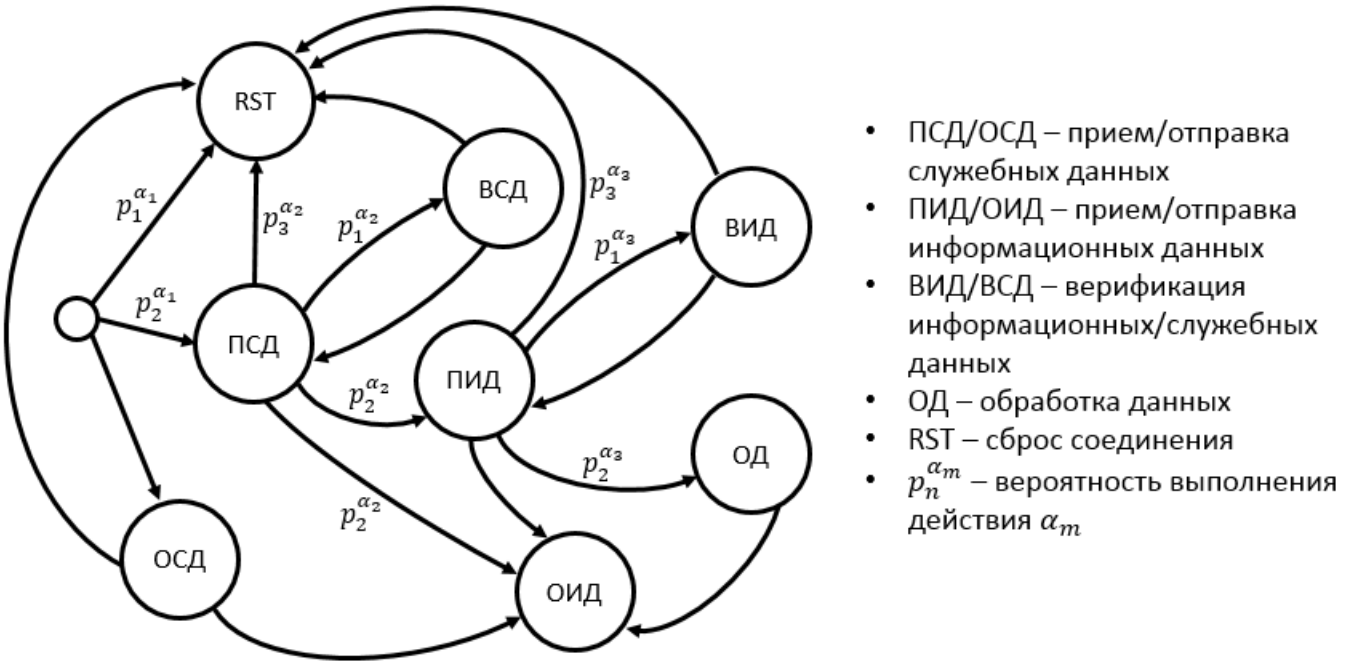

Рисунок 3 – Графовая модель обучающегося автомата

Модели обучения автомата:

— $L_{П-\varepsilon Ш}$ для действий α_1 и α_2;

— $L_{ПН}$ для действия α_3.

В рамках модели выделены основные действия узла. Модель автомата является базовой и не привязана к протоколу маршрутизации. При использовании определенного протокола состояния автомата расширяются в зависимости от спецификации протокола.

Передаваемые между узлами сообщения разделены на два типа: информационные и служебные. Информационные данные включают в себя информацию, необходимую для выполнения сетью целевой задачи. Сообщения со служебными данными содержат информацию, необходимую для работы протокола маршрутизации, а также передают информацию о состоянии сети и узлов.

Описание правил работы узлов с использованием ОА позволило сформулировать теорему о необходимом условии нахождения узла сенсорной сети в безопасном для взаимодействия с ним состоянии.

Теорема. Узел находится в безопасном для взаимодействия с ним состоянии, если математическое ожидание штрафа автомата, которым описываются правила работы с узлом, удовлетворяет условию:

$$M < \frac{1}{n}\sum_{i=1}^{n} c_i\,, \tag{6}$$

где c_i – вероятность штрафа при выполнении действия α_i.

Доказательство основано на эргодичности модели обучающегося автомата и на применении метода от противного.

В четвертой главе описан разработанный метод адаптивного управления правилами взаимодействия узлов БСС на основе обучающегося автомата, учитывающего показатели функционирования узлов и показатели поведения (корректность выполнения целевой функции). Также представлена разработанная архитектура макета системы поддержания защищённости и функциональной устойчивости БСС и экспериментальная оценка его эффективности.

Разработанный метод обеспечивает адаптивность в поведении за счет изменения вероятностей переходов между состояниями ОА. Изменение происходит в зависимости от значения комплексного показателя *Q*, который вычисляется по формуле:

$$Q^{i,j} = \frac{\sum_{i=1}^{m} g_i(1-q^{i,j})q^{i,j}}{\sum_{i=1}^{m} g_i(1-q^{i,j})}. \tag{7}$$

Комплексный показатель вычисляется с использованием текущего качества узла q_i и коэффициента устаревания g_i.

Текущее качество узла складывается из взвешенной суммы комплексного показателя показатель поведения и показателя функционирования по формуле:

$$q_j = z_1 BI^{i,j} + z_2 PI_j. \tag{8}$$

Показатель функционирования вычисляется путем взвешенного суммирования с плавающим окном показаний классификатора или радиально базисной нейронной сети в зависимости от архитектуры БСС.

Комплексный показатель поведения вычисляется формулой (9) и состоит из прямого показателя поведения и косвенного, полученного от других узлов.

$$BI^{i,j} = C^{i,j} * DI^{i,j} + (1 - C^{i,j}) * II^{i,j}, \tag{9}$$

где $DI^{i,j}$ – показатель прямого поведения; $II^{i,j}$ – показатель косвенного поведения; $C^{i,j}$ – коэффициент достоверности.

Показатели поведения описывают выполнение узлом возложенной на него целевой функции.

Прямой показатель поведения вычисляется узлом самостоятельно путем анализа поведения своего соседа. Например, узел отслеживает факт передачи соседним узлом пакета, который тот ему передал (проверка корректной ретрансляции пакета по сети).

Выделены следующие показатели, использование которых позволяет защититься от актуальных угроз безопасности:

— передача (ретрансляция) пакетов – после передачи пакета соседнему узлу, узел отправитель переходит в режим мониторинга для отслеживания факта ретрансляции

своего пакета дальше по сети. Используется для противодействия узлам, которые ретранслируют пакеты выборочно или вовсе этого не делают (злонамеренно или нет);

— сохранения целостности пакета – помимо проверки факта ретрансляции, узел-отправитель также проверяет контрольную сумму пакета, отправленный соседом дальше по сети;

— интенсивность генерирования узлом данных – показатель определяется как количество полученных от узла пакетов за определенный установленный промежуток времени и призван защитить узлы от атак истощение энергии и засорение канала;

— объем отправляемых данных – аналогично предыдущему показателю учет объема отправляемых соседними узлами данных позволит защититься от атак исчерпания ресурсов.

Значения показателей «передача пакета» и «целостность пакета» определяются по формуле (10) и представляют собой отношение успешных событий взаимодействия ко всем событиям.

$$I_m^{i,j} = \frac{S_m^{i,j}}{S_m^{i,j} + F_m^{i,j}}, \tag{10}$$

где $S_m^{i,j}$ – количество удачных событий между узлами i и j в контексте показателя; $F_m^{i,j}$ – количество неудачных событий.

Показатели оцениваются на основе введенных пороговых значений. Пороговые значения также зависят от области применения сети и типа передаваемых данных.

Для получения комплексного показателя поведения $DI^{i,j}$ значение каждого показателя суммируется с учетом веса по формуле (11). Вес показателя зависит от типа и области применения БСС.

$$DI^{i,j} = \sum_{m=1}^{N} \left(W_m * I_m^{i,j}\right), \tag{11}$$

где N – число показателей поведения, W_m – вес показателя, $I_m^{i,j}$ – значение показателя по определенному аспекту поведения относительно узла j.

Показатель косвенного поведения вычисляется по формуле (12) на основе показателей прямого поведения, полученных от всех соседних узлов относительно узла для которого вычисляется показатель.

$$II^{i,j} = \frac{\sum_{l=1}^{n}\left(DI^{i,k_l} * DI^{k_l,j}\right)}{\sum_{l=1}^{n} DI^{i,k_l}}, \tag{12}$$

где DI^{i,k_l} – значение прямого показателя относительно узла k; $DI^{k_l,j}$ – значение показателя узла k относительно узла j; n – количество узлов, предоставивших свое значение.

Данный показатель введен с целью компенсирования недостаточных данных для вычисления корректного значения прямого показателя. С течением времени, при увеличении числа взаимодействий, вес у значения прямого показателя становится больше, чем вес косвенного.

Схема разработанного метода представлена на рисунке 4.

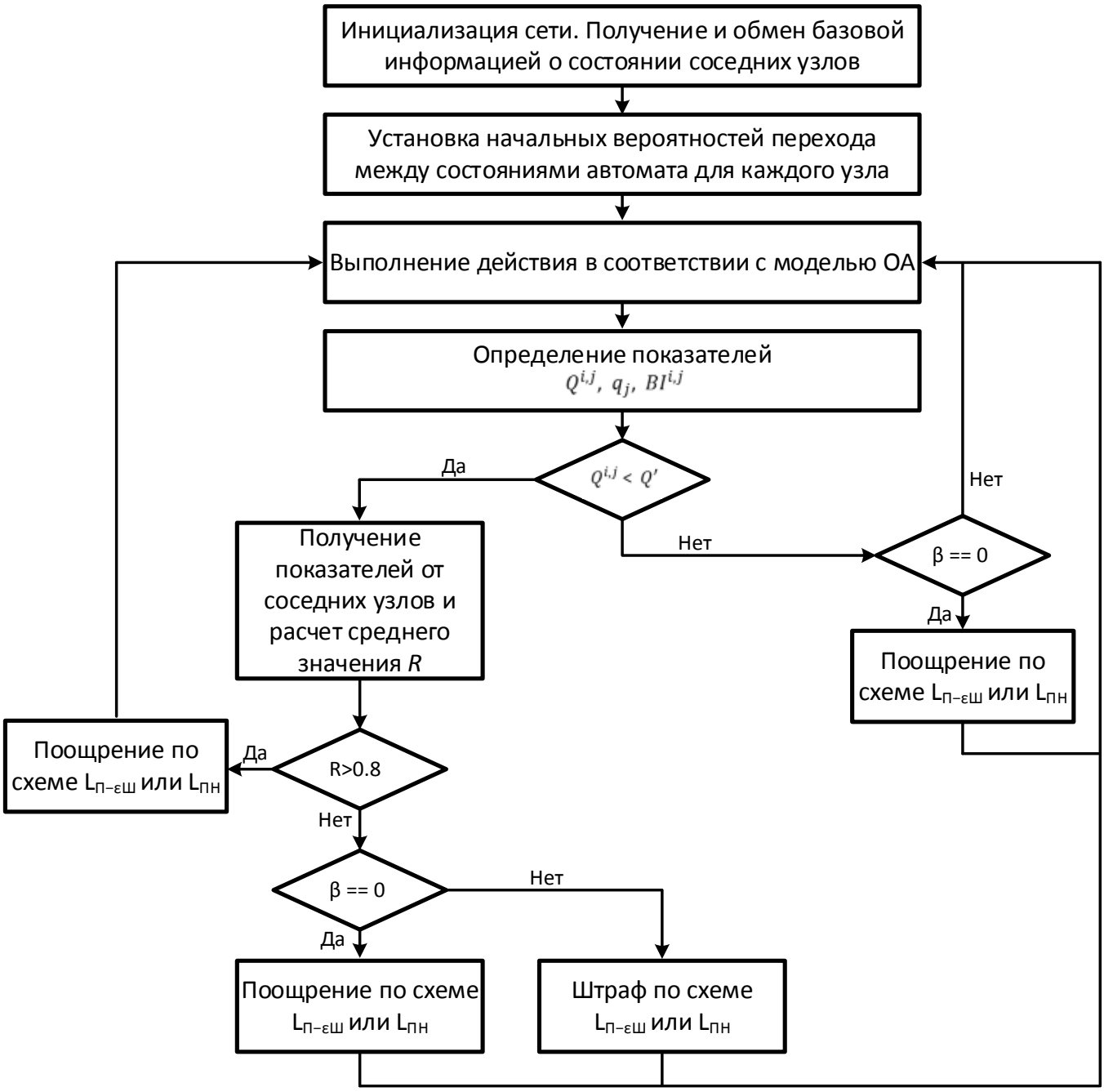

Рисунок 4 – Схема разработанного метода

На основе разработанной методики проверки безопасности беспроводных сенсорных сетей, а также методе адаптивного управления правилами взаимодействия узлов на основе ОА, создана система защиты. Архитектура системы представлена на рисунке 5.

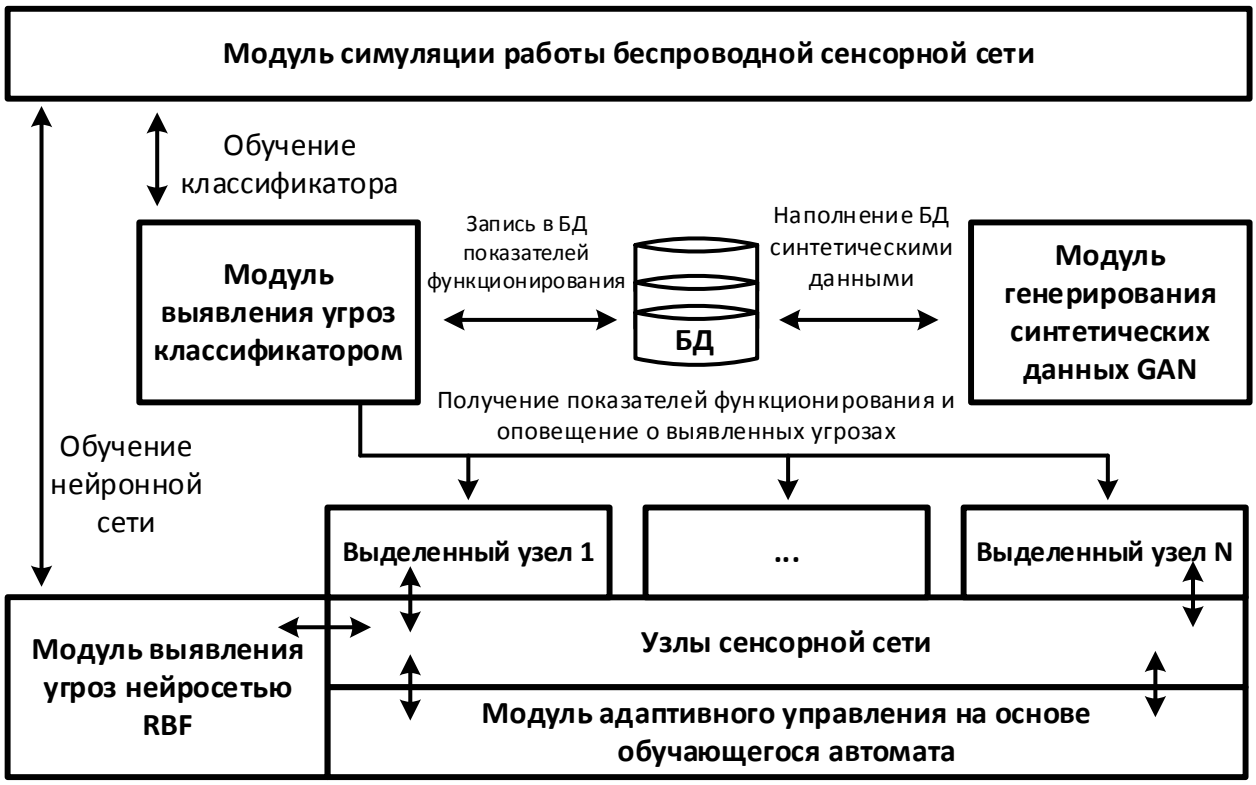

Рисунок 5 – Архитектура системы защиты

Важным аспектом для экспериментальной оценки метода является возможность симулировать работу сети. В ходе работы проведен сравнительный анализ среди существующих симуляторов для ad-hoc сетей по ряду критериев. В результате сравнения выбран симулятор NS-3.

Одним из наиболее существенных параметров оценки любого метода в контексте БСС является расход заряда батареи. Ни в одной из проанализированных симуляторов, включая NS-3, функционал по учету расхода заряда не был реализован достаточно корректно и полно. В связи с этим для NS-3 была доработана модель потребления энергии, позволяющая учесть затраты энергии на вычисления, связанные с протоколом маршрутизации.

Для оценки эффективности смоделирована сеть из 500 узлов сенсорных узлов, расположенных случайным образом в области размером 1000x500 метров.

Моделировались атаки, связанные с влиянием на работу сети (истощение энергии) и на целостность данных (выброс пакетов, черная/серая дыра). В атаках выброса пакетов узлы отбрасывали пакеты с вероятностью 0.8.

График зависимости количества атакующих узлов от доставленных до базовой станции пакетов представлен на рисунке 6 слева. Как видно из графика, сеть с разработанной системой защиты работает лучше, чем обычный протокол маршрутизации с точки зрения доставки корректных пакетов до базовой станции. Процент потерь остается ниже 20%, при количестве вредоносных узлов 20% от общего числа узлов. В аналогичной

ситуации обычная сеть без системы защиты с атакующими узлами теряет более 70% пакетов, что является критичным для исследуемого типа сетей.

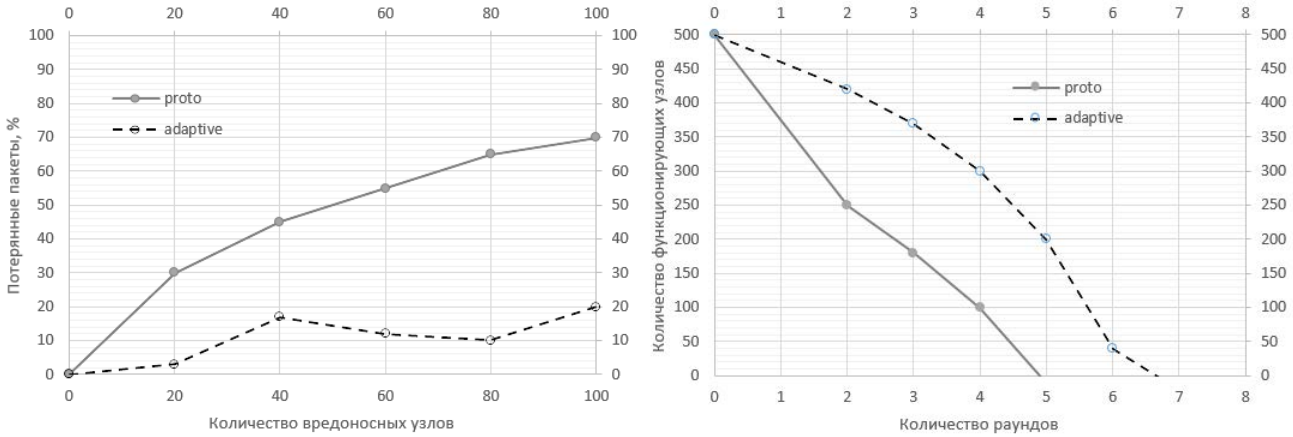

Рисунок 6 – Результаты экспериментальной оценки эффективности разработанного метода защиты

График зависимости количества функционирующих узлов от количества пройденных раундов с учетом совершения атак исчерпания ресурсов представлен на рисунке 6 справа. Под раундом понимается определенный период времени, в течение которого узлы передают пакеты (100 секунд). Как видно из графика, время работы сети с активной системой защиты больше на 30%. Легитимные узлы успешно обнаруживают вредоносные узлы и перестраивают процесс взаимодействия с ними, тем самым не расходуя ресурсы своей батареи.

В заключении представлены основные результаты и выводы, полученные в ходе выполнения диссертационного исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Исследованы особенности функционирования БСС с точки зрения обеспечения безопасности, выявлены и систематизированы угрозы, проведен сравнительный анализ существующих подходов к обеспечению безопасности.
2. Разработана методика выявления угроз безопасности узлов БСС на основе интеллектуального анализа показателей функционирования. Определен перечень показателей функционирования, анализ которых позволяет выявить аномалии в работе узлов БСС. В рамках разработанной методики в зависимости от архитектуры сенсорной сети применяются определенные методы искусственного интеллекта: для полностью распределенной сети используются радиально-базисные нейронные сети, а для сетей с иерархической архитектурой используется связка методов машинного обучения - генеративно-состязательные сети и k-ближайших соседей.
3. Построена модель обучающегося автомата, описывающая динамически изменяемые правила взаимодействия узлов и позволяющая узлам изменять их. Определены необходимые параметры обучающегося автомата с учетом особенностей

функционирования БСС. Сформулирована и доказана теорема о необходимом условии нахождения узла сенсорной сети в безопасном для взаимодействия с ним состоянии.

4. Создан метод адаптивного управления работой БСС на основе обучающегося автомата, учитывающего показатели функционирования узлов и выполнение ими целевой функции. Адаптивное поведение узлов достигается за счет изменения вероятностей между состояниями в автомате.

5. Разработана архитектура и макет системы поддержания защищённости и функциональной устойчивости БСС. Выполнен сравнительный анализ существующих средств имитационного моделирования работы распределенных сетей, внесены изменения в существующее средство для более корректного учета энергопотребления узлов сети при симулировании их работы. Проведена экспериментальная оценка эффективности предложенного метода адаптивного управления узлами.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня ВАК РФ:

1. **Овасапян Т.Д.** Обеспечение безопасности WSN-сетей на основе модели доверия / Овасапян Т.Д., Иванов Д.В. // Журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехн. ун-та, 2017. - №4. - С. 64-72.

2. **Овасапян Т.Д.** Применение нейронных сетей для выявления внутренних нарушителей в VANET-сетях / Овасапян Т.Д., Москвин Д.А., Калинин М.О. // Журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехн. ун-та, 2018. - №1. - С. 68-73.

3. **Овасапян Т. Д.** Применение аппарата нечеткой логики для противодействия атакам внутренних нарушителей в WSN-сетях / Овасапян Т. Д. // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 2. – С. 65-72.

4. **Овасапян Т. Д.** Применение taint-анализа для исследования безопасности программного обеспечения устройств Интернета вещей, построенных на базе архитектуры ARM / Овасапян Т. Д., Князев П. В., Москвин Д. А. //Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 4. – С. 84-91.

5. **Овасапян Т. Д.** Применение методов генерации синтетических данных в задачах выявления сетевых атак на устройства Интернета вещей / Овасапян Т. Д., Данилов В. Д., Москвин Д. А. // Проблемы информационной безопасности. Компьютерные системы. – 2020. – №. 4. – С. 26-34.

6. **Овасапян Т. Д.** Применение технологии Honeypot с адаптивным поведением для сетей Интернета вещей / Овасапян Т. Д., Никулкин В. А., Москвин Д. А. // Проблемы информационной безопасности. Компьютерные системы. – 2021. – №. 2. – С. 135-144.

Публикации из перечня SCOPUS и Web of Science:

1. **Ovasapyan T.** Using Neural Networks to Detect Internal Intruders in VANETs / Ovasapyan T. D., Moskvin D. A., Kalinin M. O. // Automatic Control and Computer Sciences. – 2018. – Т. 52. – №. 8. – С. 954-958.

2. **Ovasapyan T.** Security Provision in Wireless Sensor Networks on the Basis of the Trust Model / Ovasapyan T. D., Ivanov D. V. // Automatic Control and Computer Sciences. – 2018. – Т. 52. – №. 8. – С. 1042-1048.

3. **Ovasapyan T.** Security Provision in WSN on the Basis of the Adaptive Behavior of Nodes / Ovasapyan T., Moskvin D. // 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). – IEEE, 2020. – С. 81-85.

4. **Ovasapyan T.** Application of Taint Analysis to Study the Safety of Software of the Internet of Things Devices Based on the ARM Architecture / Ovasapyan T. D., Knyazev P. V., Moskvin D. A. //Automatic Control and Computer Sciences. – 2020. – Т. 54. – №. 8. – С. 834-840.

5. **Ovasapyan T.** Detection of attacks on the Internet of Things based on intelligent analysis of devices functioning indicators / Ovasapyan T., Moskvin D., Tsvetkov A. //13th International Conference on Security of Information and Networks. – 2020. – С. 1-7.

Наиболее значимые публикации в других изданиях:

1. **Овасапян Т.Д.** Обеспечение безопасности WSN-сетей на основе модели доверия / Овасапян Т.Д., Иванов Д.В., Зегжда Д.П. // Информационная безопасность регионов России (ИБРР-2017). И 74 Юбилейная X Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 1-3 ноября 2017 г.: Материалы конференции/СПОИСУ. – СПб., 2017.

2. **Овасапян Т.Д.** Применение распределенной модели доверия для обеспечения безопасности беспроводных сенсорных сетей / Овасапян Т.Д., Иванов Д.В. // Неделя науки СПбПУ. Санкт-Петербург, 13-19 ноября 2017г.: Материалы научной конференции с международным участием. – СПб.: Издательство Политехнического университета, 2018.

3. **Овасапян Т.Д.** Выявление внутренних нарушителей в VANET-сетях с использованием нейронных сетей / Овасапян Т.Д., Москвин Д.А. // IV Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Севастополь, 18-22 сентября 2018 г.

4. **Овасапян Т. Д.** Применение адаптивной системы управления для противодействия атакам внутренних нарушителей в беспроводных сенсорных сетях / Овасапян Т. Д., Москвин Д. А., Иванов Д. В. // Методы и технические средства обеспечения безопасности информации. – 2019. – №. 28. – С. 40-41.

5. **Овасапян Т. Д.** Исследование эффективности применения алгоритмов генерации синтетических данных для увеличения точности выявления сетевых атак на интернет вещей / Овасапян Т. Д., Данилов В. Д., Иванов Д. В. // Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 24-25.

6. **Овасапян Т. Д.** Применение обучающихся автоматов для обеспечения безопасности WSN-сетей / Овасапян Т. Д., Москвин Д. А. // Методы и технические средства обеспечения безопасности информации. – 2021. – №. 30. – С. 99-100.