МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

На правах рукописи

Штыркина Анна Александровна

СТРУКТУРНО-АДАПТИВНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ СПЕКТРАЛЬНОГО АНАЛИЗА МОДЕЛИРУЮЩИХ ГРАФОВ

2.3.6 - Методы и системы защиты информации, информационная безопасность (технические науки)

Направленность: 10.06.01_01 Методы и системы защиты информации, информационная безопасность

Академическая степень **Исследователь. Преподаватель-исследователь**

НАУЧНЫЙ ДОКЛАД

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ

Александрова Елена Борисовна

Санкт-Петербург, 2022

Научный доклад выполнен в Институте кибербезопасности и защиты информации федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ,
Александрова Елена Борисовна

Рецензент: д.т.н., доцент, профессор ИКиЗИ,
Полтавцева Мария Анатольевна

С научным докладом можно ознакомиться в библиотеке ФГАОУ ВО «Санкт–Петербургский политехнический университет Петра Великого» и на сайте Электронной библиотеки СПбПУ по адресу: http://elib.spbstu.ru.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы.

Усложнение современных технических систем различного назначения приводит к необходимости автоматизации протекающих в них процессов. Автоматизация осуществляется путем добавления информационной составляющей, которая используется для решения задач мониторинга, управления и принятия решений. Следствием цифровой трансформации является создание принципиально нового типа систем, характеризующихся интеграцией информационных и физических процессов, - киберфизических систем (КФС).

Концепция КФС применяется для построения объектов критической инфраструктуры, нарушение безопасности которых может негативно сказаться на задачах бизнеса, экологии, а также спровоцировать техногенные катастрофы. В связи с этим одной из актуальных задач является обеспечение информационной безопасности таких систем.

Обеспечение безопасности КФС является нетривиальной задачей и осложняется следующими факторами:

1. Отсутствие единой стандартизации для КФС. Большое количество типов подключаемых устройств, а также протоколов взаимодействия диктуют разработку универсальных подходов, учитывающих безопасность не только отдельного устройства, но и системы в целом.

2. Смещение цели атакующего от кражи информации в сторону нарушения корректного функционирования КФС. Таким образом, учета классических понятий информационной безопасности - конфиденциальности, целостности, доступности - недостаточно для безопасности КФС: требуется обеспечение ее устойчивого функционирования.

3. Увеличение числа устройств в КФС, которое приводит как к усложнению сетевой структуры системы, так и к росту объема анализируемых для задач безопасности данных. Такая тенденция ведет к тому, что когнитивных способностей аналитиков и специалистов по информационной безопасности

становится недостаточно для оперативного обнаружения и реагирования на инциденты безопасности.

Ряд работ, посвященных обеспечению безопасности КФС, направлен на предотвращение или обнаружение деструктивных воздействий на различных уровнях взаимодействия. Однако в случае, когда атакующее воздействие произошло, возникает необходимость в механизме автоматизированного восстановления эффективного функционирования КФС за счет включения резервных компонентов. В рамках данной работы предпринята попытка решить задачу минимизации ресурсов, необходимых для восстановления подвергшейся атаке КФС, на основе адаптивного изменения структурных свойств системы с учетом контроля спектральных характеристик графа, моделирующего КФС.

Степень разработанности темы исследования. Задаче обеспечения безопасности КФС посвящено множество работ российских и иностранных исследователей, среди который П. Д. Зегжда, Д. П. Зегжда, М. О. Калинин, Д. С. Лаврова, Е. Ю. Павленко, С. А. Саенко, И. В. Котенко. О. И. Шелухин, Д. Яакоуб, К. Гуо, Л. Джао.

Объектом исследования являются КФС с развитой сетевой структурой, в отношении которых осуществляются атаки, направленные на нарушение ее функционирования.

Предметом исследования являются методы и подходы к обеспечению безопасности КФС с развитой сетевой структурой, включающие в себя методы оценки и нейтрализации структурных нарушений КФС.

Целью работы является поддержание структурной устойчивости КФС на основе адаптивного изменения сетевой структуры системы, направленного на нейтрализацию последствий атаки.

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

1. Провести анализ топологий КФС с точки зрения спектральных характеристик моделирующих графов.

2. Разработать алгоритм, выполняющий отображение реальной КФС в абстрактный граф с учетом обнаруженных атакующих воздействий.

3. Выявить структурные изменения с помощью спектральных характеристик графа, моделирующего КФС.

4. Разработать метод адаптивной нейтрализации структурных нарушений КФС с учетом минимизации включаемых резервных компонентов КФС.

5. Разработка архитектуры системы поддержания структурной устойчивости КФС.

Методы исследования включают в себя теорию информационной безопасности, теорию графов, спектральную теорию графов, теорию вероятностей и математическую статистику, методы машинного обучения.

Научная новизна результатов:

1. Предложен подход к анализу структурной устойчивости КФС на основе спектрального анализа моделирующего графа в условиях деструктивных воздействий на систему.

2. Предложен метод обнаружения атак на КФС на основе байесовского алгоритма поиска разладки и дискретного вейвлет-преобразования временных рядов, результаты которого используются для отображения состояния устройств в атрибуты моделирующего КФС графа.

3. Предложен метод адаптивной нейтрализации структурных нарушений КФС на основе графовых нейронных сетей

Теоретическую значимость работы составляют метод обнаружения атак на КФС на основе метода поиска разладки и дискретного-вейвлет преобразования, метод адаптивной нейтрализации структурных изменений КФС на основе графовых искусственных нейронных сетей, линейная зависимость, полученная для изменения среднеквадратического отклонения для длины рабочего маршрута и связности графа.

Практическая значимость результатов работы заключается в возможности применения предложенных методов для разработки интеллектуальной системы безопасности КФС. Полученные результаты позволяют:

– обнаруживать атаки на устройства КФС на основе поиска разладки в коэффициентах детализации дискретного вейвлет-преобразования временных рядов, образованных параметрами системы;

– определять степень структурных нарушений КФС на основе спектрального анализа графа, моделирующего систему;

– поддерживать структурную устойчивость КФС путем включения необходимого количества резервных компонентов, определяемого с помощью адаптивного метода нейтрализации структурных нарушений системы.

Положения, выносимые на защиту

1. Подход к оценке структурных нарушений КФС на основе анализа графа, моделирующего систему.
2. Метод обнаружения атак на КФС на основе байесовского метода поиска разладки и дискретного вейвлет-преобразования.
3. Метод адаптивной нейтрализации структурных нарушений КФС.

Внедрение результатов работы. Полученные основные научные результаты научно-квалификационной работы использованы при реализации гранта Российского Фонда Фундаментальных исследований № 20-37-90109 «Моделирование инфраструктуры защищенной киберфизической системы с использованием графового представления».

Достоверность и обоснованность результатов, представленных в научно-квалификационной работе, подтверждается их внутренней непротиворечивостью, проведенным анализом научных работ и полученными в результате экспериментов экспериментальными данными.

Соответствие специальности научных работников. Полученные научные результаты соответствуют следующим пунктам паспорта специальности научных работников 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

– модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты

(системы, цепей поставки) вне зависимости от области их функционирования (п. 7);

– модели противодействия угрозам нарушения информационной безопасности для любого вида информационных системы, позволяющие получать оценки показателей информационной безопасности (п. 9);

– модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании (п. 18).

Апробация работы. Основные результаты исследований и научных разработок докладывались и обсуждались на международной конференции SHS Web of Conference (Санкт-Петербург, 2018), на научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2018, 2019 и 2022 гг.), международной конференции CEUR Workshop Proceedings (Санкт-Петербург, 2019), международной конференции «2nd International Conference on Cyber-Physical Systems & Control» (Санкт-Петербург, 2021).

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 2019, 2021 годах.

Публикации. Результаты диссертационной работы отражены в 11 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 3 свидетельствах о регистрации программ для ЭВМ.

Объем и структура научно-квалификационной работы. Научно-квалификационная работа состоит из введения, 4 глав, заключения и списка литературы из 58 наименований. Общий объем работы составляет 70 страниц, в том числе 28 рисунков.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, выполнена постановка цели работы, определены задачи. Выделены положения, выносимые на защиту, научная новизна и практическая значимость работы.

В первой главе рассмотрены особенности современных КФС с точки зрения обеспечения информационной безопасности. Выявлены факторы, осложняющие задачу обеспечения информационной безопасности КФС: отсутствие единой стандартизации, что связано с высокой вариативностью подключаемых моделей устройств и протоколов обмена информацией; смещение цели злоумышленников от кражи информации к нарушению устойчивого функционирования; рост числа подключаемых устройств, что ведет к усложнению структуры КФС. Перечисленные ограничения затрудняют как этапы предотвращения и раннего обнаружения атакующих воздействий, так и этап нейтрализации нарушений, полученных в результате атаки.

Приведен обзор угроз безопасности на КФС. Выделены угрозы, приводящие к нарушению информационного обмена, что приводит к потере или задержке информационных потоков внутри системы, и, как следствие, к снижению эффективности функционирования КФС.

Поскольку качество информационного обмена тесно связано со структурными свойствами графа, было приведено исследование спектральных свойств сетевых топологий КФС различной сложности и области применения.

Приведен анализ современных исследований, посвященных обеспечению информационной безопасности КФС. Особое внимание уделено работам, связанным с оценкой последствий нарушения системы, а также с разработкой механизмов нейтрализации деструктивных воздействий. К недостаткам перечисленных методов можно отнести отсутствие учета структурных характеристик КФС при анализе нарушений и выработке сценариев противодействия, а также высокую сложность работы.

Для решения поставленной задачи предлагается подход, заключающийся в формировании абстрактного графа по реальной функционирующей КФС, анализе

структурных свойств полученного графа на основе спектрального анализа и реализации метода адаптивной нейтрализации структурных нарушений с учетом структуры системы и масштабом последствий атакующего воздействия.

Во второй главе изложен алгоритм формирования абстрактного графа по реально функционирующей КФС с учетом состояния устройств и каналов связи, отражающихся в атрибутах компонент графа.

Структурные свойства КФС могут быть учтены, если задавать систему графом $G =< V, E >$ где множество вершин V задает множество устройств, а множество ребер E - связи между ними. В ходе функционирования КФС выполняет набор операций над данными. Для сложного преобразования такие операции декомпозируются в набор последовательно выполняемых функций. Каждая функция в ходе работы может менять свойства данных: аналитическое устройство может принимать на вход набор данных, а на выходе выдавать поток команд для соответствующих устройств.

Для моделирования работы КФС процесс функционирования рассматривается как последовательное преобразование данных функциями, заданными на устройствах системы. Пусть $type\_list = \{type_1, , \dots, type_l\}$ - набор типов данных, которые передаются между устройствами. Каждая единица данных, передаваемых по ребру, характеризуется набором атрибутов $attributes = = \{attr_1, \dots, attr_m\}$. В качестве атрибутов может выступать, например, объем данных. Таким образом, каждое ребро графа предлагается задавать как матрицу $D^{l \times m}$. Элементы матрицы являются атрибутами данных $attr_i, 0 \le i \le m$, для каждого типа $type_j, 0 \le j \le l$. Пусть $F = \{f_1, f_2, .., f_k\}$ - множество функций, которые могут выполнять устройства системы. Каждой вершине сопоставляется набор функций, которые может реализовывать соответствующее вершине устройство. Функция f_i выполняет преобразование данных, в ходе которого могут измениться как свойства, так и тип данных: $f_i: D\left[type_j\right] \to D[type_z]$ для $0 \le i \le k$ и $0 \le j, z \le l$.

Тогда процесс функционирования КФС описывается последовательностью операций преобразования данных на устройствах системы. Такой процесс задается

маршрутом на графе, который проходит через вершины, содержащие необходимые для обработки данных функции в своих атрибутах, и соответствующим потоком данных.

Для формирования графа необходимо корректно определять состояния устройств, в частности, подверглись ли они атакующим воздействиям. Информация об атаках на устройство может быть доступна из логов системы мониторинга, антивирусных средств. Однако приведенные источники могут не выявлять атаки на раннем этапе с высокой скоростью.

Для современных КФС обнаружение атак осложняется ростом объема циркулирующих в КФС данных за счет усложнения функции систем и увеличения числа компонентов и большим разнообразием типов устройства и протоколов их взаимодействия. Таким образом, метод обнаружения атак на устройства системы должен обеспечивать быстрое время работы и быть адаптивным с точки зрения различной природы анализируемых данных.

В работе предлагается метод на основе вейвлет-анализа временных рядов, образованных параметрами функционирования КФС. Использование временных рядов позволяет рассматривать специфичные для системы параметры функционирования: начиная с характеристик сетевого трафика и заканчивая показателями датчиков.

Дискретное вейвлет-преобразование выполняется путем применения набора фильтров к анализируемой последовательности: применение высокочастотных фильтров позволяет получить коэффициент детализации, а применение низкочастотных – коэффициенты аппроксимации. Коэффициенты детализации подчиняются нормальному распределению с средним, равным нулю. Для поиска аномалий предлагается отслеживать изменение дисперсии полученной последовательности.

Данную задачу предлагается решить с помощью метода, предложенного в работе Д. С Лавровой. Суть метода заключается в поиске точки разладки - момента времени, в которое произошло изменение статистических свойств анализируемой последовательности. В качестве метода обнаружения разладки используется

байесовский онлайн алгоритм, который позволяет работать со временными рядами в режиме реального времени. Суть алгоритма заключается в вычислении распределения длины временного периода без изменения статистических свойств относительно поступивших данных на основе формулы Байеса:

$$P(r_t|x_{1:t}) = \frac{P(x_t|r_{t-1}, x_{1:t-1}) \sum_{r_{t-1}} P(r_t|r_{t-1}) P(r_{t-1}|x_{1:t-1})}{P(x_{1:t})},$$

где $P(x_t|r_{t-1}, x_{1:t-1})$ – вероятность того, что поступившие данные удовлетворяют текущим значениями параметров распределения, $P(r_t|r_{t-1})$ – вероятность отсутствия точки разладки на шаге t, $P(r_{t-1}|x_{1:t-1})$ – апостериорная вероятность на шаге $t-1$, или априорная вероятность на шаге t.

Однако в оригинальной работе априорная вероятность $P(r_t|r_{t-1})$ задается показательным распределением с фиксированным параметром λ, таким образом фиксируя временную разницу между точками разладки значением λ. Однако, интенсивность атак на различные виды информационных систем, в том числе, КФС не определяется через фиксированный параметр: на частоту атак могут влиять временные показатели (время суток, года и т.д.), политические и иные мировые события. Для адаптации метода под изменяющиеся значения интенсивности потока атак метод предлагается дополнить модулем отслеживания изменения параметра λ.

Экспериментальные исследования показали применимость предложенного метода для обнаружения атак (рис. 1).

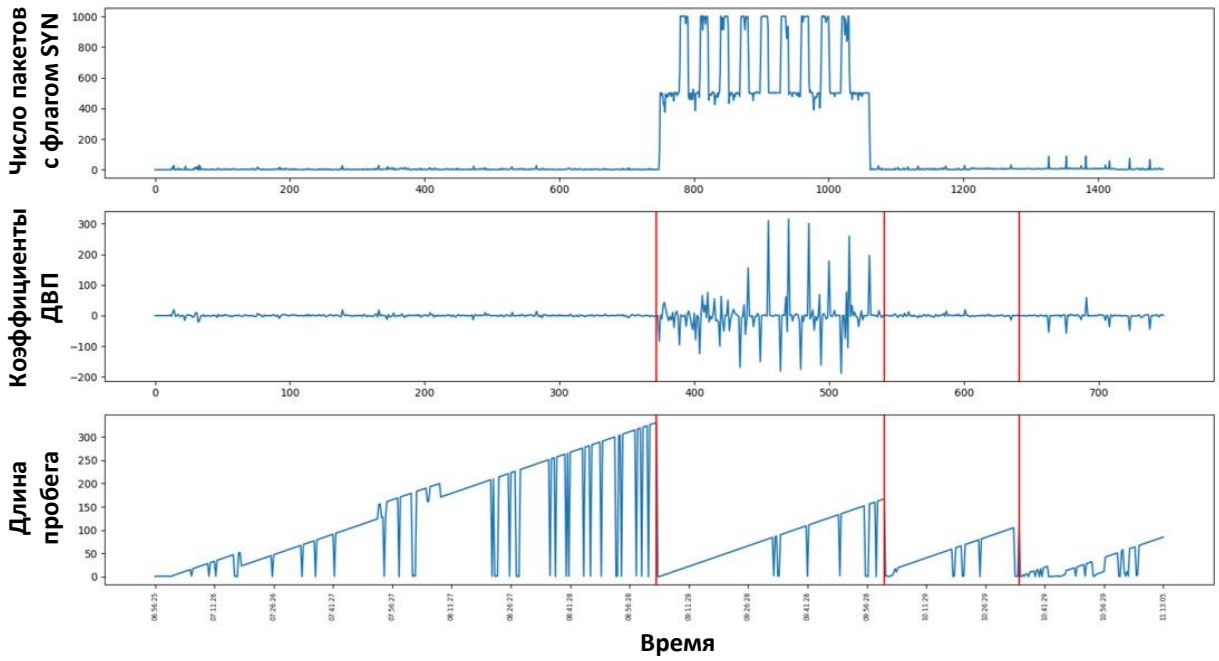


Рисунок 1 – Обнаружение атаки SYN Flood с помощью байесовского метода поиска разладки и вейвлет-преобразования

Тогда алгоритм формирования абстрактного графа по функционирующей КФС состоит из следующих шагов (рис. 2):

1. Опрос системы мониторинга и антивирусных средств для выявления зараженных или вышедших из строя устройств и связей.
2. Формирование временных рядов по заданным характеристикам системы.
3. Выявление атак на основе ДВП и алгоритма поиска разладки.
4. Если нарушения обнаружены, то в модуль внесения изменений передается информация о необходимости изоляции устройства и/или связи.
5. Формирование графа с атрибутами, отображающими доступность устройства и интенсивность потока данных в канале связи.

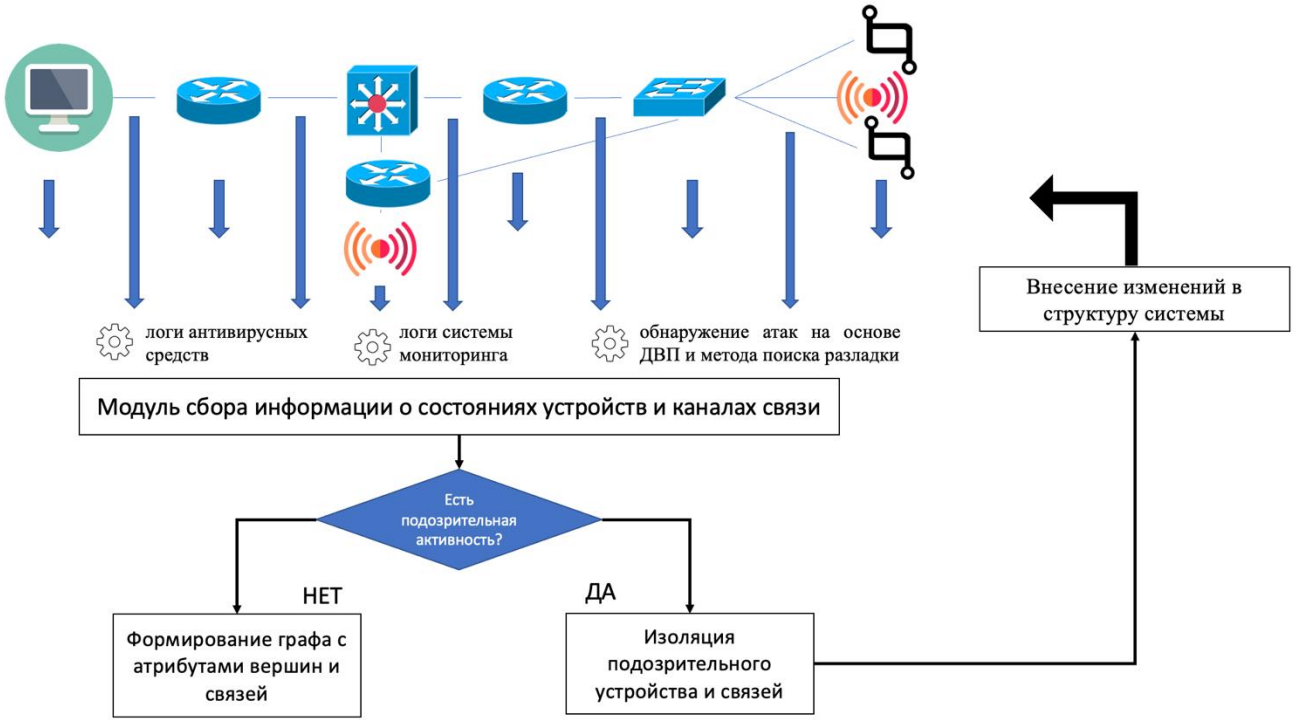


Рисунок 2 – Алгоритм формирования абстрактного графа из функционирующей КФС

Предложенный алгоритм позволяет адекватно описывать текущее поведение КФС, задавая систему в виде графа с атрибутами, описывающими состояние компонент системы.

В третьей главе описан метод оценки структурных нарушений графа, моделирующего КФС, в ходе деструктивных воздействий на систему. Поскольку процесс функционирования на графе задается с помощью маршрута, наличие большого количества альтернативных маршрутов определяет эффективный информационный обмен в КФС: при выходе из строя одного маршрута целевая функция может быть выполнена по альтернативному. С ростом размерности и сложности графа процесс вычисления количества альтернативных маршрутов усложняется. Чем нетривиальнее целевая функция и чем больше соответствующих ей альтернативных маршрутов на графе, тем сложнее структура графа, моделирующего КФС.

Структурные свойства предложено оценивать через спектральные характеристики графа. Пусть граф с n вершинами задается матрицей смежности $A^{n\times n}$. Тогда спектр графа определяется через собственные значения этой матрицы

$S(G) = \{\lambda_1, \lambda_2, .., \lambda_n\}$. Спектр графа также может задаваться собственными значениями матрицы Лапласа, в таком случае он называется спектром Лапласа.

Для случайного графа, построенного по алгоритму Барабаши-Альберта, спектр подчиняется нормальному распределению. Показано, что с изменением структуры графа, заключающемся в последовательном удалении 10% связей на каждой итерации атаки, среднеквадратическое отклонение распределения компонент спектра графа изменяется (рис. 2).

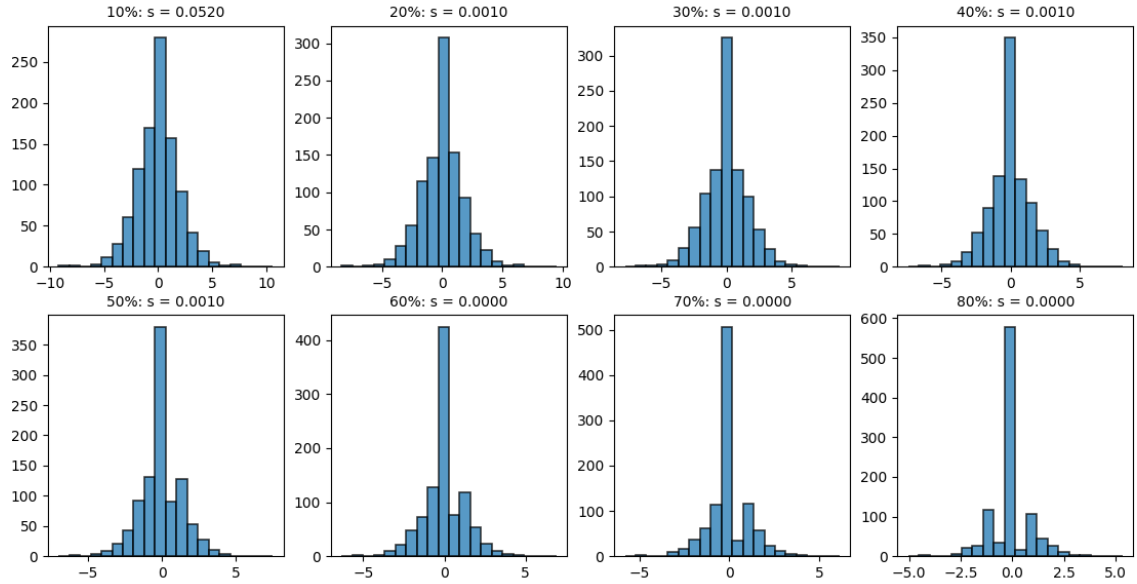
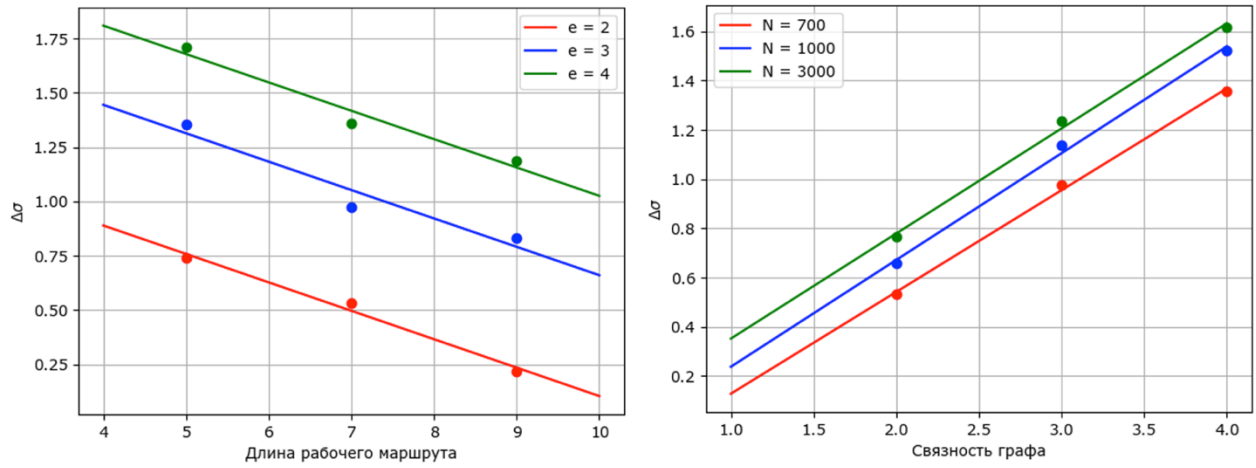


Рисунок 2 - Распределение собственных значений графа при итерациях атаки

При анализе результатов экспериментальных исследований выявлены линейные зависимости для приращения среднеквадратического отклонения распределения спектра графа $\Delta\sigma$:

– при фиксированной размерности N и связности графа $\Delta\sigma$ убывает линейно при увеличении длины рабочего маршрута с коэффициентом $C_e = -0.13$ (рис. 3а);

– при фиксированной размерности N графа и длине рабочего маршрута $\Delta\sigma$ увеличивается линейно с ростом связности графа с коэффициентом $C_l = 0.44$ (рис. 3б).



а) б)

Рисунок 3 – Выявленные зависимости для изменения среднеквадратического отклонения распределения спектра графа

Поскольку не для каждого типа графов распределение спектра можно выразить аналитической функцией, возникает необходимость в отслеживании универсальных для любого спектра характеристик. По аналогии с информационными системами эффективность информационного обмена в графе предложено оценивать следующими спектральными характеристиками: обобщенный структурный показатель, алгебраическая связность, константа Чигера, показатель внутренней устойчивости. Выбранные характеристики реагируют на изменения структуры графа так же, как и изменение числа альтернативных маршрутов. Данная зависимость проиллюстрирована на примере графа со свойством «малого мира», для которого распределение спектра не выражается известной функцией: в ходе эксперимента производилось удаление вершин графа и вычислялись структурные характеристики (рис. 4).

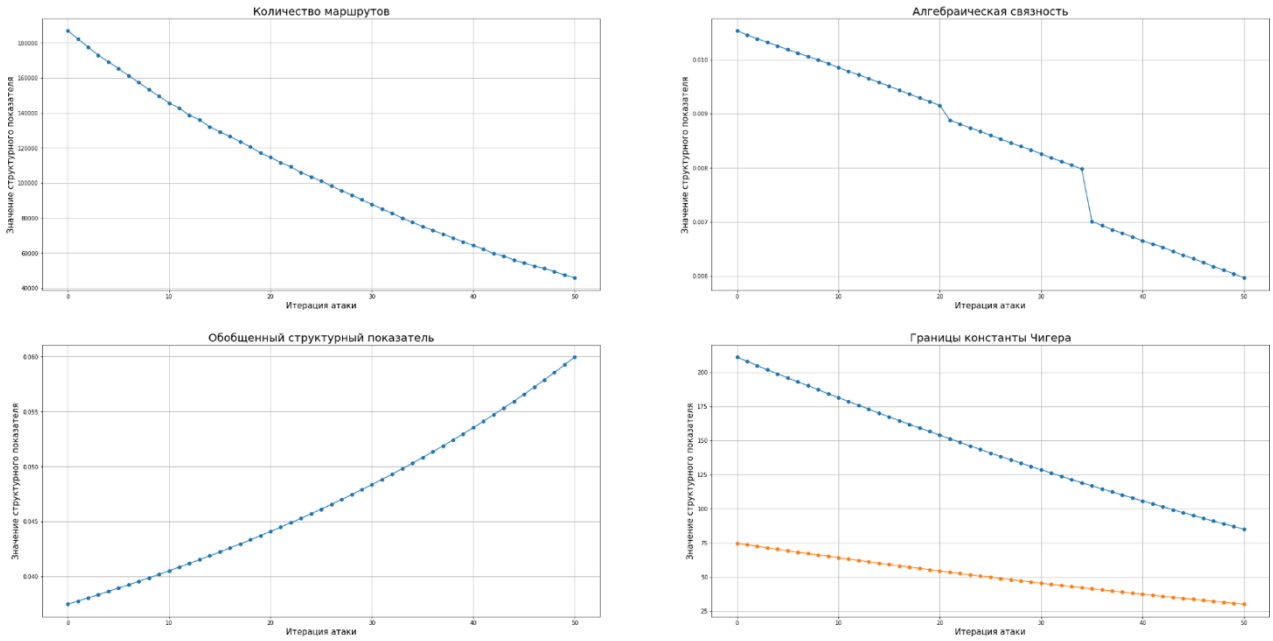


Рисунок 4 – Изменение структурных показателей графа в результате атаки путем удаления вершин

Экспериментальные исследования показали применимость анализа спектральных характеристик графа для оценки структурных нарушений КФС.

В четвертой главе предложен метод адаптивной нейтрализации последствий деструктивных воздействий на граф, моделирующий КФС. Предложенный метод основан на применении графовых искусственных нейронных сетей (ИНС) для генерации графа на основе топологии подаваемого на вход графа.

Рассмотрены архитектуры графовых ИНС и области их применения. Среди основных видов графовых ИНС выделяют: графовые рекуррентные ИНС (graph recurrent network, GRN), графовые сверточные ИНС (graph convolutional network), пространственно временные графовые ИНС (spatial-temporal graph neural network), графовые автоэнкодеры (graph autoencoder, GAe). В работе предлагается рассматривать архитектуру GCN, использующие в работе спектральные характеристики графа.

В качестве архитектуры для решения поставленной задачи предложено использовать графовую ИНС NEC-DGT, которая решает задачу трансляции графа. Такая задача заключается в поиске отображения, переводящего входной граф в выходной. Архитектура NEC-DGT расширяет возможности сверточных и

рекуррентных графовых ИНС и позволяет выполнять трансляцию графа не только с точки зрения топологии, но с точки зрения изменения атрибутов вершин и связей графа. Авторы NEC-DGT, К. Гуо и др., использовали такой подход для прогнозирования процесса изменения графа, моделирующего сетевую инфраструктуру Интернета Вещей в результате инфицирования устройств: инфицированные устройства изолировались, а связанные с ними незащищенные устройства инфицировались. Эксперименты проводились на полносвязных графах размерности 20, 40 и 60 вершин.

Пусть входной и выходной графы задаются кортежами $G\left(V_{0,}E_0, V_{attr_0}, E_{attr_0}\right)$, $G\left(V_{t,}E_t, V_{attr_t}, E_{attr_t}\right)$, где $V_0,\ V_t -$ множества, состоящие из N вершин, $E_0, E_t -$ множество связей размерности $N \times N$, $V_{attr_0}, V_{attr_t} -$ матрицы атрибутов вершин размерности $N \times D$, $E_{attr_0}, E_{attr_t} -$ тензоры атрибутов связей размерности $N \times N \times K$. Вектор C размерности $N \times L$ задает контекстную информацию. Тогда процесс трансляции графа определяется как отображение вида: $\mathcal{T}: \left(V_{0,}E_0, V_{attr_0}, E_{attr_0}\right); C \rightarrow \left(V_{t,}E_t, V_{attr_t}, E_{attr_t}\right)$.

Логично, что наиболее оптимальным с точки зрения информационного обмена граф – это полносвязный граф, так как каждая вершина связана с любой маршрутом единичной длины. Однако включение каждого нового компонента сети сопряжено со дополнительными затратами: сверхизбыточность не является оптимальным решением в условиях ограниченности ресурсов. Поэтому топология графа, который генерируется в ходе работы модели, должна быть близкой к исходному графу. Такой эффект достигается за счет регуляризации $\mathfrak{R}$ с использованием спектра Лапласа:

$$\mathfrak{R}\left(G(V_{attr}, E_{attr})\right) = \sum_{s=1}^{S} \mathfrak{R}_\theta \left(G\left(V_{attr_s}, E_{attr_s}\right)\right) + \mathfrak{R}(\theta),$$

где $S -$ количество блоков в ИНС, $\theta -$ параметры спектральной регуляризации графа , V_{attr_s}, E_{attr_s} соответствуют сгенерированным атрибутам вершин и связей на блоке под номером S, соответственно. Тогда функция потерь будет вычисляться следующим образом:

$$\hat{\mathcal{L}} = \mathcal{L}\left(\mathcal{T}\left(G\left(V_{attr_0}, E_{attr_o}\right), C\right), G(V_{attr_t}, E_{attr_t})\right) + \beta\Re(G(V_{attr}, E_{attr})),$$

где β – соотношение между функцией потерь и спектральной регуляризацией графа. Модель обучается путем минимизации среднеквадратической ошибки (mean squared error, MSE) атрибутов вершин (V_{attr_0} и V_{attr_t}) и атрибутов связей (E_{attr_0}, E_{attr_t}).

Графовая ИНС NEC-DGT принимает на вход атрибуты вершин, атрибуты связей и вектор контекста и производит над ними операции в нескольких блоках ИНС.

Для преобразования атрибутов связи сначала вычисляется функция влияния, которая кодирует каждую пару атрибутов вершины-связи в числовой вектор – «влияние». Далее по всем «влияниям» для конкретной связи вычисляется функция обновления атрибутов связи. Для вычисления новых атрибутов вершин «влияние» вычисляется и агрегируется в функции обновления на основе информации от смежных вершин.

Описанный подход был применен для задачи изменения структуры КФС. Пусть система задается в виде графа $G =< V, E, V_{attr}, E_{attr} >$. Атрибуты вершины задают ее текущее состояние: $V_{attr} = \{-1, 0, 1\}^N$. Если $v_{att_i} = -1$, то устройство выведено из строя и восстановлению на текущий момент времени не подлежит. Если $v_{att_i} = 0$, то устройство находится в резерве и может быть подключено. Значение $v_{att_i} = 1$ задает работающее устройство. Атрибуты ребер задают количество информации, передаваемое по каналу связи: $e_{att_i} = 0$ определяет канал передачи информации, который не используется (например, справедливо для ребер, смежных с вышедшими из строя вершинами), $e_{att_i} = -1$ определяет отсутствие возможности связи между устройствами, $e_{att_i} > 0$ показывает количество передаваемой по каналу связи информации, которое определяется значимостью ребра для информационного обмена.

Вышедшие из строя устройства накладывают ограничения на пропускную способность оставшихся каналов из-за снижения эффективности информационного обмена. Таким образом в ходе подобных атак возникает

необходимость в подключении резервных устройств для улучшения структурных характеристик графа, определяющих эффективность информационного обмена.

Тогда задача, которую должна решить графовая ИНС, заключается в перемещении множества значимых с точки зрения информационного обмена резервных вершин и связей, в множество рабочих. Включение самых значимых компонентов позволит оптимизировать информационный обмен в системе и таким образом минимизировать затрачиваемые на восстановление системы ресурсы. В рамках данной работы значимыми считались вершины, обладающие большей центральностью по посредничеству.

Графовая ИНС NEC-DGT обучалась с помощью оптимизатора Адама для графов размерности 45, в результате чего была получена точность для вершин, равная 0,89, и точность для ребер – 0,86. Величина среднеквадратической ошибки (MSE) для ребер получилась равной 241,4. Поученная MSE сопоставима с ошибкой, полученной NEC-DGT при решении задачи трансляции графа размерности 40 при распространении вируса в системе Интернета Вещей.

Обученной ИНС удалось корректно прогнозировать добавление значимых с точки зрения информационного обмена вершин и связей (рисунок 5).

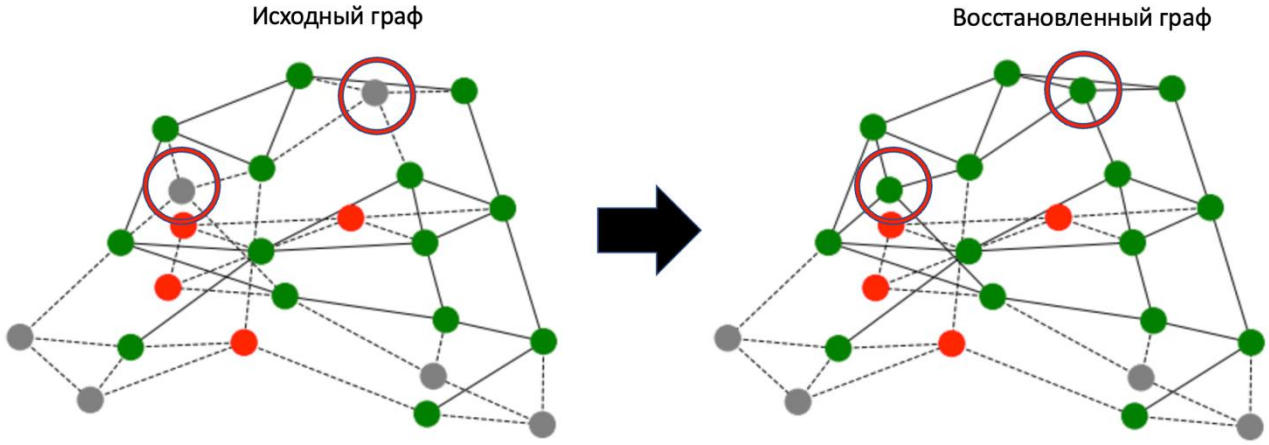


Рисунок 5. Результат преобразования графа с помощью обученной графовой ИНС NEC-DGT

Для графов из тестового набора спектральные характеристики показали улучшения с точки зрения эффективности информационного обмена (рисунок 6).

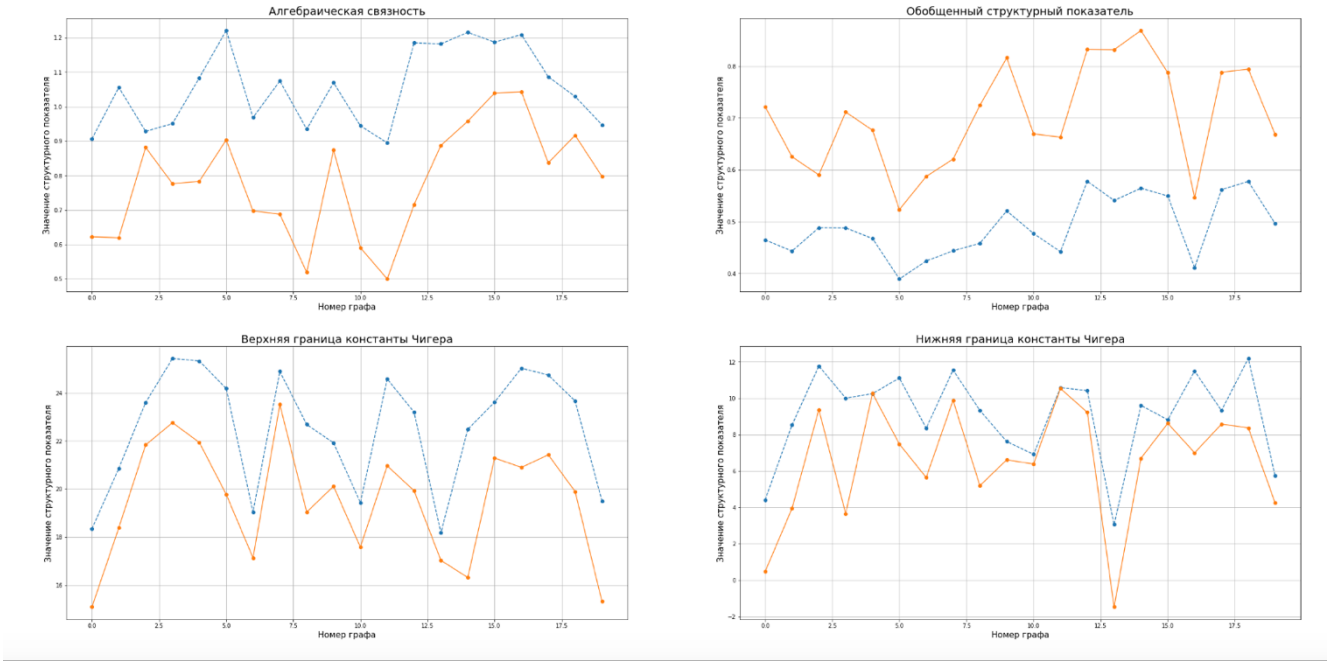


Рисунок 6. Сравнение спектральных характеристик исходного (сплошная линия) и сгенерированного ИНС (пунктирная линия) графов.

Разработана архитектура системы управления безопасностью КФС, выполняющей нейтрализацию негативных последствий атак, заключающихся в нарушении эффективности информационного обмена (рисунок 7).

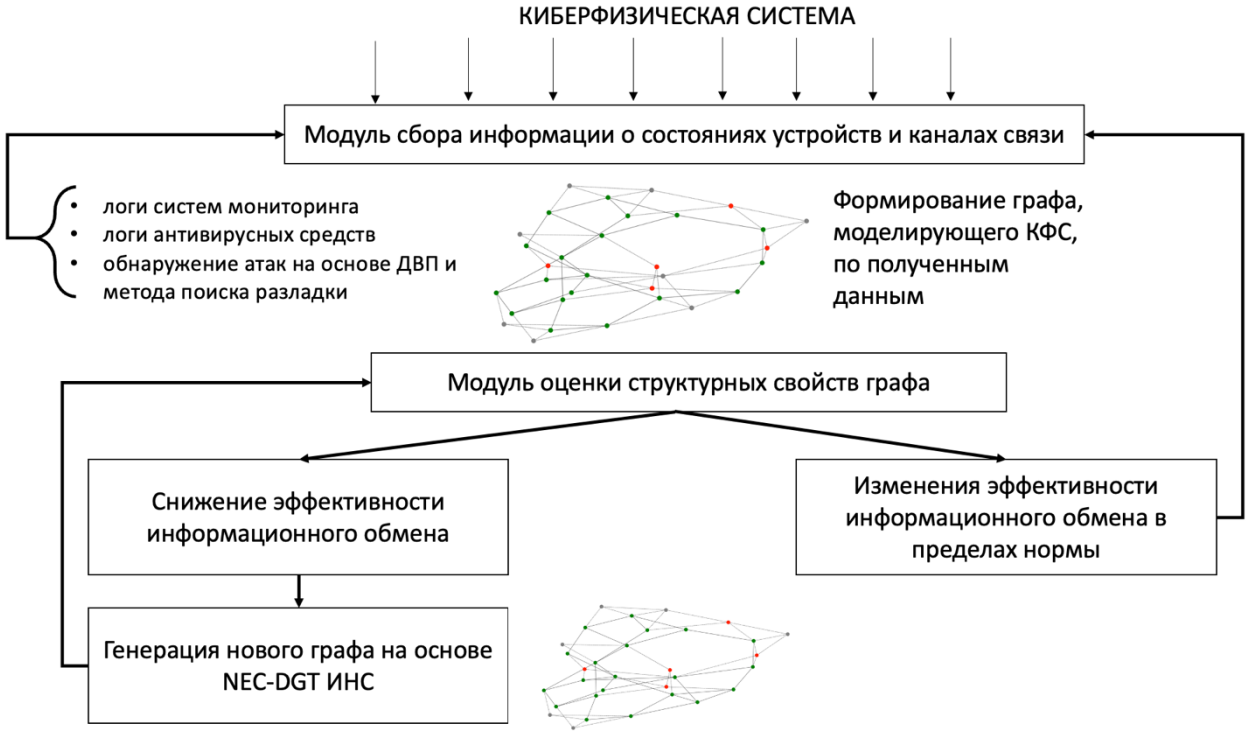


Рисунок 7. Архитектура системы нейтрализации структурных нарушений КФС

В ходе функционирования системы происходит непрерывный мониторинг состояния устройств системы. С заданной периодичностью со всех устройств и каналов связи собирается статистика о текущей работоспособности. Сбор статистики осуществляется встроенными агентами. При отсутствии отклика от устройства, наличии подтвержденного факта инфицирования, полученного по логам системы, или в результате подозрения на атакующие воздействия в ходе анализа сетевого трафика, узел помечается выведенным из строя. Смежные связи также отключаются.

По заранее заданной топологии сети формируется граф, атрибутами вершин которого является вектор текущего состояния устройств, а атрибутами ребра – интенсивность потока трафика по соответствующему каналу связи. Полученный граф подается в модуль вычисления спектральных свойств для оценки эффективности информационного обмена.

Полученные оценки сопоставляются с историческими оценками; при отклонении значений более чем на заданными порог инициируется процесс оптимизации топологии сети с помощью графовой ИНС NEC-DGT. Полученный в ходе анализа ИНС граф используется для подключения прогнозируемых резервных вершин.

В заключении приведены основные результаты, полученные в ходе выполнения научно-квалификационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В ходе выполнения научно-квалификационной работы были исследованы методы и средства обеспечения информационной безопасности КФС, и получены следующие результаты:

1. Проведен анализ распространенных атак на КФС. Сделан вывод о влиянии таких атак на эффективность информационного обмена.

2. Проведен анализ спектральных свойств различных сетевых топологий, использующихся при построении КФС. Показано, что структура графа отражается

на его спектре. Предложен подход к обеспечению безопасности КФС на основе спектрального анализа графа.

3. Разработан алгоритм отображения функционирующей КФС в абстрактный граф. В случае, обнаружения атаки, устройство (и смежные с ним связи) должны быть изолированы из системы. Для обнаружения атак на КФС был улучшен метод на основе поиска разладки в коэффициента дискретного вейвлет-преобразования временных рядов, сформированных параметрами системы.

4. Была показана применимость спектрального анализа для выявления структурных изменений КФС. Атакующие воздействия были обнаружены в ходе анализа распределения спектра графа, алгебраической связности, обобщенного структурного показателя, границ константы Чигера.

5. Разработан метод адаптивной нейтрализации структурных изменений графа, моделирующего КФС, на основе графовой ИНС NEC-DGT. Обученная ИНС показала точность 0,89 для вершин, и 0,86 – для ребер.

6. Разработана архитектура системы поддержания структурной устойчивости КФС.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня ВАК РФ:

1. **Штыркина А. А.** Обеспечение устойчивости киберфизических систем на основе теории графов //Проблемы информационной безопасности. Компьютерные системы. – 2021. – №. 2. – С. 145-150.

2. Павленко Е. Ю., **Штыркина А. А.,** Зегжда Д. П. Оценка устойчивости киберфизических систем на основе спектральной теории графов //Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 1. – С. 60-68.

3. Зегжда П. Д., Александрова Е. Б., Лаврова Д. С. **Штыркина А.А.** Обнаружение аномалий в сетевом трафике с использованием дискретного вейвлет-преобразования и метода разладки //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 4. – С. 14-21.

4. Лаврова Д. С., Алексеев И. В., **Штыркина А. А.** Анализ безопасности на основе контроля зависимостей параметров сетевого трафика с использованием

дискретного вейвлет-преобразования //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 2. – С. 9-15.

5. Лаврова Д. С., Попва Е. А., **Штыркина А. А.,** Штеренберг С.И. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 3. – С. 70-77.

6. Зегжда Д. П., Павленко Е. Ю., Лаврова Д. С., **Штыркина А.А.** Подход к созданию критерия устойчивого функционирования киберфизических систем //Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 2. – С. 156-163.

Публикации из перечня SCOPUS и Web of Science:

1. Pavlenko E., Zegzhda D., **Shtyrkina A**. Estimating the sustainability of cyber-physical systems based on spectral graph theory //2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). – IEEE, 2019. – С. 1-5.

2. Lavrova D. S., Alekseev I. V., **Shtyrkina A. A**. Security analysis based on controlling dependences of network traffic parameters by wavelet transformation //Automatic Control and Computer Sciences. – 2018. – Т. 52. – №. 8. – С. 931-935.

3. Zegzhda D. P., Pavlenko E., **Shtyrkina A.** Cybersecurity and Control Sustainability in Digital Economy and Advanced Production //The Economics of Digital Transformation. – Springer, Cham, 2021. – С. 173-185.

4. Lavrova D. S., Popova E. A., **Shtyrkina A. A.** Prevention of DoS Attacks by Predicting the Values of Correlation Network Traffic Parameters //Automatic Control and Computer Sciences. – 2019. – Т. 53. – №. 8. – С. 1065-1071.

5. Pavlenko E., Zegzhda D., **Shtyrkina A.** Criterion of cyber-physical systems sustainability //CEUR Workshop Proc. – 2019. – Т. 2603. – С. 60-64.

Наиболее значимые публикации в других изданиях:

1. **Штыркина А. А.,** Павленко Е. Ю., Лаврова Д. С. Подход к оценке структурной устойчивости киберфизических систем на основе спектральной

теории графов //Методы и технические средства обеспечения безопасности информации. – 2019. – №. 28. – С. 21-23.

2. Алексеев И.В., Зегжда П.Д., Лаврова Д.С., **Штыркина А.А.** Анализ безопасности магистральных каналов связи на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования //Методы и технические средства обеспечения безопасности информации. – 2018. – №. 27. – С. 16-17.

В свидетельствах о регистрации программы для ЭВМ

1. Зегжда Д.П., Лаврова Д.С., Павленко Е.Ю., **Штыркина А.А.** Программа для оценки устойчивости функционирования киберфизической системы на основе вычисления спектральных характеристик моделирующего ее графа: RU 2019660900. – зарегистр. 06.08.2019.

2. Лаврова Д. С., **Штыркина А. А**. Программа для моделирования функционирования распределенной киберфизической системы с использованием ее графового представления: RU 2021610368 . – зарегистр.: 07.12.2020.

3. Павленко Е. Ю., **Штыркина А. А.** Программа для оценки динамики участия устройств распределенной киберфизической системы в реализации целевой функции: RU 2020667012 . – зарегистр. 07.12.2020.