ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

На правах рукописи

Крундышев Василий Михайлович

АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА КИБЕРУГРОЗ В КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург
2021

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.

Научный руководитель:
доктор технических наук, профессор Калинин Максим Олегович.

Официальные оппоненты:
доктор технических наук, профессор Петренко Сергей Анатольевич, Центр информационной безопасности автономной некоммерческой организации высшего образования «Университет Иннополис», руководитель.

кандидат технических наук Крюков Роман Олегович, Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военно-космическая академия имени А. Ф. Можайского» Министерства обороны Российской Федерации, преподаватель.

Ведущая организация:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет».

Защита состоится « 24 » декабря 2021 г. в __ 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, 29, ауд. 175).

С диссертацией 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 «__» _____ 2021 года.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Информационные и коммуникационные технологии становятся частью современных управляющих систем во всех отраслях экономики, сферах безопасности государства, жизни людей. Стратегией развития информационного общества в РФ на 2017 – 30 гг. определены задачи обеспечения устойчивого функционирования информационной инфраструктуры РФ, включая непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий. ФЗ-187 «О безопасности критической информационной инфраструктуры РФ» ставит задачу непрерывного обеспечения безопасности критической информационной инфраструктуры (КИИ) и устанавливает приоритет предотвращения компьютерных атак на КИИ.

Для современных систем поддержки Цифровой экономики, строящихся на базе Интернета вещей, индустриального Интернета, умных энергосетей, сенсорных сетей, межмашинных и конвергентных сетей, характерны уникальные свойства самоорганизации, реконфигурации, одноранговости взаимодействия, мобильности узлов и динамического изменения топологии, что расширяет существующее пространство киберугроз КИИ. Новые разновидности компьютерных атак, в т.ч. полиморфные целевые атаки, атаки на динамическую маршрутизацию, туннельные атаки, сложно определяются либо вовсе не определяются при помощи традиционных методов обнаружения и могут приводить не только к нарушениям конфиденциальности, целостности и доступности информационных ресурсов, но и к нарушениям непрерывного функционирования КИИ. Критическим становится противоречие между вариативностью действующих атак, скоростью их реализации и инертностью механизмов обнаружения, что ослабляет безопасность значимых объектов КИИ, используемых в банковской сфере, в системах транспорта, связи, энергетики, атомной и химической промышленности, усиливает социальные и техногенные риски.

Таким образом, актуальна и своевременна разработка решения, которое на основе анализа действующих киберугроз управляет обнаружением компьютерных атак в изменяющихся условиях функционирования КИИ для снижения риска реализации киберугроз.

Степень разработанности темы исследования. Научные подходы и практические решения в области защиты от компьютерных атак в КИИ до настоящего времени сводились к развитию технологий обнаружения, в т.ч. с привлечением методов машинного обучения. Созданию интеллектуальных систем анализа и предотвращения киберугроз посвящены работы таких ученых, как Д.П. Зегжда, И.В. Котенко, С.А. Петренко, А.Е. Кучерявый, А.И. Толстой, А.Я. Ометов, М. Герла, М. Цю. Совершенствованию детекторов атак с использованием методов искусственного интеллекта, машинного обучения и мягких вычислений посвящены работы А.А. Шелупанова, И.Б. Саенко, Н. Кумара, С. Верстега, Н. Карлини, Н. Мустафы. Динамически изменяющиеся внешние и внутренние факторы функциони-

рования КИИ затрудняют применение известных методов, доказавших свою эффективность в решении частных задач при фиксированном наборе признаков атак, наличии полных обучающих выборок, заранее известном множестве возможных состояний объекта защиты. Результаты диссертационной работы базируются на указанных исследованиях и развивают их в области адаптивного управления обнаружением компьютерных атак в изменяющихся условиях функционирования КИИ и действующих киберугроз.

Объектом исследования является КИИ, в отношении которой осуществляются компьютерные атаки.

Предметом исследования являются методы обнаружения компьютерных атак и методы управления обнаружением компьютерных атак.

Цель исследования — снижение риска реализации киберугроз в КИИ на основе разработки интеллектуальной системы, реализующей адаптивное управление обнаружением компьютерных атак адекватно изменяющимся условиям функционирования КИИ и действующим киберугрозам.

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

1. Анализ характерных особенностей КИИ и определение специфики защиты таких систем от новых разновидностей компьютерных атак.

2. Построение математической модели развития компьютерных атак на КИИ, описывающей динамику реализации атак в структуре КИИ, и определение критерия адекватности применяемых методов обнаружения атак изменяющимся условиям функционирования КИИ и действующим киберугрозам.

3. Разработка структуры базы методов обнаружения компьютерных атак на основе характерных параметров киберугроз и предложенной модели развития компьютерных атак на КИИ; создание комплекса интеллектуальных методов, позволяющих обнаруживать специфические киберугрозы современным КИИ.

4. Разработка адаптивной системы управления обнаружением компьютерных атак в КИИ, обеспечивающей адекватность применяемых детекторов изменяющимся условиям функционирования КИИ и действующим киберугрозам.

5. Разработка методики оценки снижения риска реализации киберугроз в КИИ на основе количественной адаптивной оценки риска, учитывающей особенности современных КИИ.

6. Построение архитектуры и макета автоматизированной системы анализа киберугроз в КИИ, реализующей непрерывный подбор, настройку и применение детекторов атак адекватно действующим киберугрозам и текущему состоянию КИИ.

Научная новизна диссертационной работы состоит в следующем:

1. Предложен новый подход к снижению риска реализации киберугроз в КИИ, заключающийся в адаптивном управлении обнаружением компьютерных атак на основе непрерывного выбора применяемых методов обнаружения атак, макси-

мально соответствующих типам действующих киберугроз и изменяющимся условиям функционирования КИИ.

2. Впервые предложена математическая модель развития компьютерных атак на КИИ на основе расширения базовой модели Лотки-Вольтерры. Модель применима для описания динамики компьютерных атак на объекты КИИ различной структурной и функциональной организации и для определения критерия адекватности применяемых методов обнаружения атак изменяющимся параметрам КИИ и уровню киберугроз.

3. Разработан комплекс новых методов обнаружения компьютерных атак в КИИ на базе методов машинного обучения, искусственных нейросетей, роевого интеллекта и биоинспирированных алгоритмов, покрывающих множество актуальных киберугроз современным КИИ и обеспечивающих высокую точность обнаружения.

4. Построена адаптивная система управления обнаружением компьютерных атак в КИИ, поддерживающая высокую точность обнаружения атак в изменяющихся условиях принятия решения за счет непрерывного нейро-нечеткого анализа киберугроз и параметров объекта защиты.

5. Предложена методика оценки снижения риска реализации киберугроз в КИИ на основе количественной адаптивной оценки риска, учитывающей типизацию и самоорганизацию сетевых структур и подсистем КИИ.

6. Разработана архитектура автоматизированной системы анализа киберугроз в КИИ на основе технологии программно-конфигурируемых сетей, позволяющая адаптировать обнаружение атак в вариативной среде КИИ адекватно уровню киберугроз, текущим размерности, динамике и нагрузке контролируемой сети объектов.

Теоретическая значимость работы. Впервые предложена математическая модель развития компьютерных атак на КИИ, основанная на расширении базовой модели Лотки-Вольтерры, позволяющая описать динамику развития компьютерных атак и подбирать наиболее эффективный метод обнаружения атак в текущих условиях функционирования КИИ и сведениях о киберугрозах. Для обнаружения полиморфных атак, атак на динамическую маршрутизацию, туннельных атак в реконфигурируемых сетевых инфраструктурах КИИ разработаны новые методы обнаружения на основе технологий искусственного интеллекта, обеспечивающие высокую точность и скорость работы. Построена адаптивная система управления обнаружением компьютерных атак в КИИ на основе аппарата нейро-нечеткой логики. Предложена методика количественной оценки риска реализации угроз в КИИ, учитывающая типизацию и самоорганизацию сетевых структур, позволяющая оценить снижение риска реализации киберугроз в КИИ.

Практическая значимость работы. Предложенные модель и методы могут быть использованы для практической реализации систем предотвращения киберугроз в современных и перспективных КИИ. Результаты работы обеспечивают:

– динамический выбор адекватного метода обнаружения атак, соответству-

ющего текущим параметрам КИИ и уровню киберугроз, за счет использования нейро-нечеткой системы управления;

– непрерывность, высокую точность и полноту обнаружения компьютерных атак в КИИ за счет применения интеллектуального управления обнаружением киберугроз адекватно динамике киберугроз и состояний КИИ;

– сокращение времени обнаружения компьютерных атак в КИИ за счет применения адаптивного управления и технологии программно-конфигурируемых сетей.

Методы исследования. Для решения поставленных задач использовались теория алгоритмов, методы математического и имитационного моделирования, теории управления, теории защиты информации, теории вероятностей.

Положения, выносимые на защиту:

1. Математическая модель развития компьютерных атак на КИИ, основанная на расширении базовой модели Лотки-Вольтерры.

2. Структура базы методов обнаружения компьютерных атак на основе характерных параметров киберугроз и предложенной модели развития компьютерных атак на КИИ.

3. Адаптивная система управления обнаружением компьютерных атак в КИИ на основе аппарата нейро-нечеткой логики.

4. Методика оценки снижения риска реализации киберугроз в КИИ на основе количественной оценки риска, учитывающей особенности КИИ.

5. Архитектура автоматизированной системы анализа киберугроз в КИИ на основе технологии программно-конфигурируемых сетей.

Соответствие специальности научных работников. Научные результаты соответствуют паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»: методы и модели выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса (п.3); анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения (п.6); модели и методы оценки защищенности информации и информационной безопасности (п.9).

Степень достоверности научных положений диссертации определяется строгим теоретическим обоснованием предлагаемого аналитического аппарата, эффективностью его использования при практическом воплощении и результатами экспериментальных исследований.

Внедрение результатов работы. Результаты работы использованы при выполнении исследований РФФИ №№18-29-03102, 19-37-90001; госзадания 075-ГЗ/Щ4575/784/2; гранта на осуществление господдержки создания и развития научных центров мирового уровня (проект «Интеллектуальное управление киберустойчивостью передовых цифровых технологий», НЦМУ СПбПУ), гранта на господдержку Центров НТИ (проект «Кибербезопасность и киберустойчивость новых

производственных технологий», ЦНТИ СПбПУ), ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-20 гг.» по соглашениям №№14.578.21.0224, 14.575.21.0131, 14.578.21.0231. Результаты работы использованы в проектной деятельности ООО «Акрибия. Исследования и разработки» и МРУ Росфинмониторинга по СЗФО, в учебном процессе Института кибербезопасности и защиты информации ФГАОУ ВО СПбПУ при организации дисциплин «Технологии машинного обучения в кибербезопасности», «Анализ рисков информационной безопасности», что подтверждено актами о внедрении.

Апробация работы. Основные результаты работы докладывались и обсуждались на межрегиональных научно-практических конференциях «Информационная безопасность регионов России» (СПб, 2017г.), «Перспектива» (Таганрог, 2019г.), «Цифровая экономика, умные инновации и технологии» (СПб, 2021г.), «Методы и технические средства обеспечения безопасности информации» (СПб, 2017-21гг.), на международных конференциях International Conference on Security of Information and Networks (2017-20гг.), International Conference on Industrial Cyber-Physical Systems (2018-19гг.), International Russian Automation Conference (2018, 2020гг.), Digital Transformation on Manufacturing, Infrastructure and Service (2019г.), International Scientific Conference on Telecommunications, Computing and Control (2019г.), World Conference on Smart Trends in Systems, Security and Sustainability (2019-21гг.). Работа поддержана грантами для аспирантов вузов, отраслевых и академических институтов, расположенных на территории С.-Петербурга в 2019-20 гг., стипендией Президента РФ молодым ученым и аспирантам в 2019-21 и 2021-23 гг. Разработка отмечена серебряной медалью международная выставки «Высокие технологии. Инновации. Инвестиции (HI-TECH)» (СПб, 2018г.).

Публикации. По теме диссертации опубликовано 74 научных работ, в т.ч. 8 в изданиях из Перечня ВАК, 26 в изданиях, индексируемых в базах Scopus и WoS, 3 патента РФ на изобретения, раздел монографии, 19 свидетельств о регистрации программ для ЭВМ.

Объем и структура. Диссертация состоит из введения, 5 глав, заключения и списка литературы из 141 наименования.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулированы цели и задачи работы, изложены полученные основные результаты исследований, показана их новизна, теоретическая и практическая значимость, отражены основные положения, выносимые на защиту.

В главе 1 приведен анализ типовых объектов КИИ различных категорий значимости, в результате которого установлено, что для таких систем свойственны неоднородность сетевой инфраструктуры, постоянная реорганизация, мобильность узлов и быстроменяющаяся топология. Вариативность объекта защиты и широкий спектр возможных киберугроз усложняют решение проблем кибербезопасности.

Сформулированы требования адаптивности, полноты и оперативности к разрабатываемой системе анализа киберугроз в КИИ. Задача обеспечения безопасности КИИ в условиях вариативности киберугроз и объекта защиты является наиболее критичной. Для ее решения необходима универсальная модель развития компьютерных атак на КИИ, которая позволит описать динамику развития атак и определить критерий адекватности применяемых методов обнаружения атак изменяющимся условиям функционирования КИИ и действующим киберугрозам.

В главе 2 представлена разработанная математическая динамическая модель развития компьютерных атак на КИИ. За основу взята модель Лотки-Вольтерры, обобщающая долговременные отношения между видами хищника и жертвы в экосистеме. Преимуществами выбранной модели являются ее универсальность, интерпретируемость и возможность описания динамики взаимодействий и состояний системы легитимных и атакующих узлов. В модели определены следующие понятия.

Жертва – узел, который выполняет свою целевую функцию и не осуществляет деструктивных воздействий по отношению к КИИ.

Хищник – узел, который осуществляет целенаправленные компьютерные атаки на КИИ, маршрутизацию и отдельные узлы-жертвы.

Инфицированный узел – устройство «зомби», которое осуществляет деструктивное воздействие на КИИ и находится под управлением злоумышленника.

Вакцинированный узел – устройство, которое в период действия вакцины является более защищённым от компьютерных атак за счет использования дополнительных средств обеспечения безопасности.

Выведенный из строя узел – устройство, неспособное в полной мере выполнять целевую функцию (в терминах модели Лотки-Вольтерры – мертвая жертва).

Узлы КИИ разбиты на классы Z и Q (хищники); X, W и Y (жертвы) (рис. 1).

Рисунок 1 – Классы узлов КИИ в модели развития компьютерных атак

Узлы классов X и W успешно выполняют целевую функцию, при этом узлы класса X являются «вакцинированными». Узлы класса Y выведены из строя, при этом они не представляют угрозы для других узлов и могут быть либо восстановлены в класс W, либо со временем перейти в состояние D (терминальное состояние, описывающее выход узла из строя). Узлы класса Z находятся под прямым управлением нарушителей, реализуют компьютерные атаки и стремятся перевести узлы из классов X и W в классы Q и Y в зависимости от целей и мотивов. Узлы класса Q являются «узлами-зомби», реализуют компьютерные атаки на узлы классов X и W, стремясь перевести их в класс Y, при этом они могут быть восстановле-

ны в класс W. Узлы класса Y переходят в это состояние, если они не были своевременно восстановлены в класс W, а узлы классов Q и Z при успешной работе системы обнаружения киберугроз. На рис. 2 представлена диаграмма состояний КИИ.

Узлы классов Q и Y могут быть восстановлены в класс W с вероятностями r_1 и r_2. Узлы класса Z инфицируют узлы X и W с вероятностями τ_1 и τ_2. Под воздействием узлов из классов Q и Z жертвы из классов W и X могут перейти в класс Y с коэффициентами ε_1 и ε_2. μ, a, c – коэффициенты вымирания узлов класса Y, Q, Z. Узлы класса W становятся вакцинированными (переходят в класс X) с вероятностью β. Устойчивость к заражению (вакцинация) пропадает со скоростью прямо пропорциональной коэффициенту η. Узлы классов Q и Z могут вымирать только под воздействием системы обнаружения киберугроз – «охотника», которая напрямую влияет на значение коэффициентов a и c.

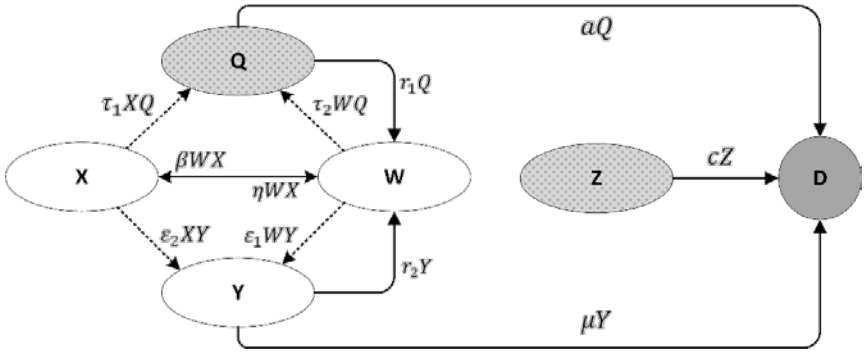

Рисунок 2 – Диаграмма состояний узлов КИИ в терминах модели развития компьютерных атак

Универсальное формальное описание динамики состояний КИИ и развития компьютерных атак представляется в виде системы уравнений (1).

$$\begin{cases} \frac{dW}{dt} = w_g W\left(1-\frac{W}{N_w}\right) + WX(\eta-\beta) - \varepsilon_1 WY - \tau_2 WQ + r_2 Y + r_1 Q - m_W W \\ \frac{dX}{dt} = x_g X\left(1-\frac{X}{N_X}\right) + WX(\beta-\eta) - \varepsilon_2 XY - \tau_1 XQ - m_X X \\ \frac{dY}{dt} = y_g Y\left(1-\frac{Y}{N_Y}\right) + \varepsilon_1 WY + \varepsilon_2 XY - r_2 Y - Y(\mu + m_Y) \\ \frac{dQ}{dt} = q_g Q\left(1-\frac{Q}{N_Q}\right) + \tau_2 WQ + \tau_1 XQ - r_1 Q - aQ \\ \frac{dZ}{dt} = z_g Z\left(1-\frac{Z}{N_Z}\right) - cZ \end{cases} . \quad (1)$$

N_w, N_X, N_Y, N_Q, N_Z – количество узлов, принадлежащих классу W, X, Y, Q, Z соответственно. w_g, x_g, y_g, q_g, z_g – коэффициенты, характеризующие рост количества узлов в классах W, X, Y, Q, Z соответственно. m_X, m_Y, m_W – вероятность промаха охотника (попадания по узлам из классов X, Y, W).

Согласно предложенной модели, решаемой задачей является максимизация коэффициентов вымирания для классов Z и Q, при этом вероятности промаха должны стремится к нулю (2). Кроме того, учитывая, что узлы Q могут быть восстановлены в класс W, то относительно класса Q появляется также коэффициент r_1, который наравне с a, должен стремиться к своему максимуму:

$$\begin{cases} \begin{cases} m_W \to 0 \\ m_X \to 0 \\ m_Y \to 0 \end{cases}. \\ \begin{bmatrix} r_1 \to \infty \\ a \to \infty \end{bmatrix} \\ c \to \infty \end{cases} \quad (2)$$

Для оценки эффективности системы анализа киберугроз определена точка устойчивости системы – идеал. Идеалом системы (1) является состояние, при котором в модели присутствуют узлы классов X и W, выполняющие свою целевую функцию, а узлы классов Q, Z и Y отсутствуют. Точка устойчивости системы $P_0(W_0, X_0, Y_0, Q_0, Z_0) = P_0(W_0, X_0, 0, 0, 0)$ достижима при значениях (3).

$$\begin{cases} W_0 = N_w + \frac{N_w(N_X x_g w_g - N_X N_w(\eta-\beta)(w_g - m_W) - m_X N_X w_g)(\eta-\beta)}{x_g {w_g}^2 + w_g N_X N_w (\eta-\beta)^2} - \frac{N_w m_W}{w_g} \\ X_0 = \frac{N_X x_g w_g - N_X N_w(\eta-\beta)(w_g - m_W) - m_X N_X w_g}{x_g w_g + N_X N_w (\eta-\beta)^2} \\ Y_0 = 0 \\ Z_0 = 0 \\ Q_0 = 0 \end{cases}. \quad (3)$$

Для достижения точки устойчивости необходимо решить задачу оптимизации функции «охотника»:

$$h_\Phi(t) \to opt. \quad (4)$$

Функция $h_\Phi(t)$ зависит от времени и имеет динамический параметр $\Phi = \{\varphi_1, \dots, \varphi_n\}$, который представляет собой исследуемый в данный момент времени t набор входных данных: параметры КИИ, доступные вычислительные ресурсы, текущий уровень киберугроз, параметры действующих атак и т. д. На основе входных данных $\{\Phi_0, t_0\}$ функция $h_\Phi(t)$ определяет, какой из методов обнаружения атак должен быть выбран и применен для обеспечения наиболее точной и быстрой реакции.

Критерием адекватности применяемых методов обнаружения атак в изменяющихся условиях функционирования КИИ и действующих киберугроз служит система (5) (скорость вымирания узлов-злоумышленников выше, чем скорость перехода узлов из нормального состояния в выведенное из строя, при этом количество ложных срабатываний не должно превышать λ, при $N_Q > 0$ и $N_Z > 0$).

$$\begin{cases} \begin{cases} m_W \le \lambda \\ m_X \le \lambda \\ m_Y \le \lambda \end{cases}. \\ a > \eta \\ c > \eta \end{cases} \quad (5)$$

Таким образом, в соответствии с данной моделью необходимо разработать такую систему управления обнаружением компьютерных атак в КИИ, которая обеспечит выполнение критерия (5).

<u>В главе 3</u> представлена система управления обнаружением компьютерных атак в КИИ, реализующая выбор детекторов атак в режиме реального времени, за счет комбинирования искусственных нейросетей и аппарата нечеткой логики (рис. 3). Использование гибридной нейро-нечеткой системы позволяет явным образом

отразить в структуре нейросетей систему нечетких правил вывода, которые автоматически корректируются в процессе обучения.

Для динамического выбора метода обнаружения компьютерных атак использована нейро-нечеткая модель, основанная на адаптивной системе нейро-нечеткого вывода ANFIS на базе алгоритма Такаги-Сугено-Канга, основным преимуществом которого является высокая производительность и точность. Данная нечеткая адаптивная сеть базируется на следующих положениях: входные переменные являются четкими, функции принадлежности всех перечисленных множеств определены функцией Гаусса. Обучение адаптивной нечеткой системы, по сравнению с обучением традиционных нейросетей, более сложное и трудоемкое – оно состоит из генерации лингвистических правил (задачи переборного типа) и корректировки функций принадлежности (задачи оптимизации в непрерывных пространствах).

На этапе генерации лингвистических правил определены входные переменные следующих типов: сетевые характеристики, доступные вычислительные ресурсы, допустимое время реакции системы, стоимость активов и текущий уровень киберугроз. На выходе система определяет с учетом модели развития компьютерных атак на КИИ и критерия (5) оптимальный метод обнаружения компьютерных атак для КИИ в данных условиях. Для каждого из признаков определено терм-множество вида {Н (низкий), С (средний), В (высокий)}, а также задана функция принадлежности, ставящая в соответствие значению терм. Например, количество узлов в сети считается низким, когда в сети менее 100 узлов. Представление общей структуры базы методов обнаружения компьютерных атак на основе характерных параметров актуальных киберугроз и построенной модели развития компьютерных атак на КИИ осуществляется с помощью модифицированных нечетких правил (табл. 1):

Таблица 1 – Общая структура базы методов обнаружения компьютерных атак

Входные переменные															**Выходная переменная**
Сетевые характеристики			Вычислительные ресурсы			Экономические параметры		Время реакции	Уровень киберугроз			Параметры типов атак			Методы обнаружения атак
Кол-во узлов	Скорость передачи данных	…	ЦП	ОП	Диск	Стоимость активов	…	Временные задержки	DoS-атака	Черная дыра	…	Цель воздействия	Активное воздействие	…	Нейросетевой метод
Н	Н	…	Н	Н	Н	Н	…	Н	Н	Н	…	Н	Н	…	Метод машинного обучения
С	С	…	С	С	С	С	…	С	С	С	…	С	С	…	Роевой интеллект
В	В	…	В	В	В	В	…	В	В	В	…	В	В	…	Метод выравнивания
															…

Общее количество правил в базе знаний рассчитывается по формуле:

$$N = \mu f^{Inputs} \quad (6)$$

где N – количество нечетких правил, μf – количество функций принадлежности на входе и $Inputs$ – количество входов. В работе построена модель с 3 функциями принадлежности и 16 входными переменными ($N = 3^{16}$).

Сформированные правила сохраняются в виде структуры нейросети. Отраженные в информационных полях нейросети, правила описывают классификационные заключения, устанавливающие соответствие между одним из методов обна-

ружения компьютерных атак и перечисленными признаками. На этапе оптимизации нечетких правил параметры исходного нечеткого множества уточняются с помощью нейросетевых методов. Правила, полученные на этапе генерации, используются для построения нейросети с пятью слоями. Структура построенной нейро-нечеткой системы управления обнаружением компьютерных атак представлена на рис. 3.

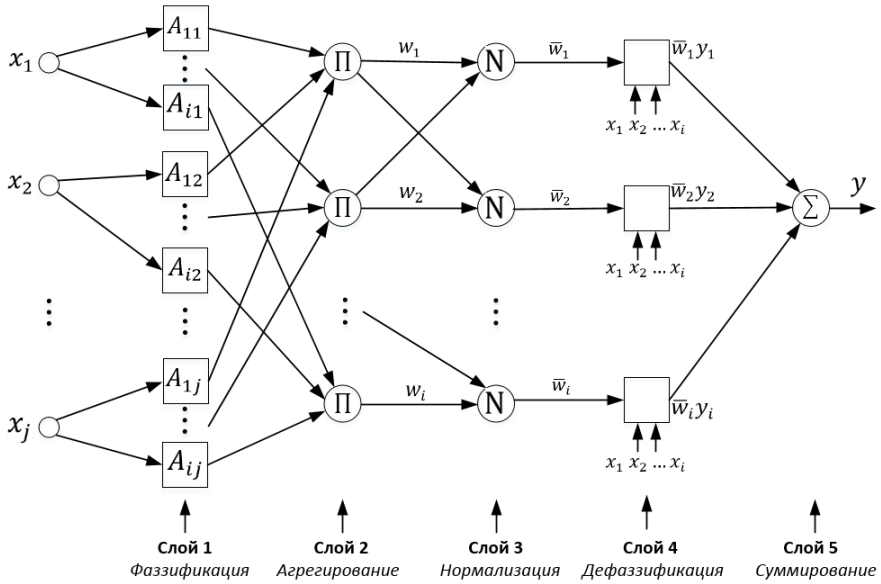

Рисунок 3 – Структура построенной нейро-нечеткой системы управления обнаружением компьютерных атак

Выбор адекватных методов обнаружения компьютерных атак в режиме реального времени осуществляется следующим образом:

1. На вход нейро-нечеткой системы поступает вектор четких входных значений $X = (x_1, x_2, \dots, x_n)$.

2. Элементы слоя фаззификации вычисляют значения степеней принадлежности $\mu_{A_i^j}(x_j)$, заданных гауссовскими функциями с параметрами a_{ij} и b_{ij}.

3. Второй слой реализует вычисление весов путем умножения выходных значений всех функций принадлежности (7). Выходы нейронов данного слоя представляют уровень активации правил.

$$w_i = \prod_{j=1}^{n} A_i^j\,(x_j) \qquad (7)$$

4. Узлы третьего слоя являются фиксированными, как и узлы второго слоя. Нормализованные уровни активизации правил ($\bar{w}_i$) вычисляются по формуле:

$$\bar{w}_i = N(w_i) = w_i / \sum_{i=1}^{c} w_i, \qquad (8)$$

где c – количество функций принадлежности для каждого входа.

5. Узлы четвертого слоя являются адаптивными узлами. Выходные данные каждого узла являются произведением нормализованного веса из предыдущего слоя и полинома первого порядка:

$$\bar{y}_i = \bar{w}_i y_i = \bar{w}_i (b_{i,0} + b_{i,1} x_1 + \dots + b_{i,j} x_j) \qquad (9)$$

6. Последний слой состоит из одного выходного нейрона, который формирует выходное значение – выбранный метод обнаружения компьютерных атак:

$$y = \sum_{i=1}^{m} \bar{y}_i \qquad (10)$$

Обучение данной системы выполняется с помощью метода обратного распространения ошибки с корректировкой функций принадлежностей A_i^j.

Разработан комплекс интеллектуальных методов обнаружения компьютерных атак в КИИ на основе методов машинного обучения, искусственных нейросетей, роевого интеллекта и биоинспирированных алгоритмов, обеспечивающих высокую точность и скорость обнаружения полиморфных целевых атак, атак на динамическую маршрутизацию, туннельных атак (представлены в патентах РФ на изобретения, программах для ЭВМ, в т.ч. №2668222 «Способ безопасной маршрутизации в одноранговых самоорганизующихся сетях», №2020617065 «Программа типизации киберугроз критическим информационным инфраструктурам по оценке близости признаковых пространств», №2019664316 «Программа выявления киберугроз в промышленных системах с помощью генеративных соревнующихся нейросетей», №2021660868 «Программа выявления угроз безопасности в неоднородных киберсредах с помощью запоминающей нейросетевой модели», №2019664596 «Программа обнаружения кибератак в динамических промышленных системах с помощью сетей глубокого обучения»).

Применение выбранного детектора атак, адекватного изменяющимся условиям, позволяет снизить риск реализации киберугроз в КИИ.

В главе 4 описана разработанная методика оценки снижения риска реализации киберугроз в КИИ на основе количественной адаптивной оценки риска, учитывающей типизацию и самоорганизацию сетевых структур КИИ (рис. 4).

Рисунок 4 – Схема применения методики оценки снижения риска реализации киберугроз в КИИ

Разработанная методика основана на адаптивной количественной оценке риска, которая является легко и быстро вычислимой. Для оценки риска выполняется выявление всех устройств (активов КИИ), имеющих ценность для КИИ, и определяются типы устройств (активов КИИ) $T = \{T_i\}$, $1 \le i \le n$, где n – количество выделенных типов устройств (активов КИИ). $|T_i| = n_{T_i}$ – количество устройств (активов КИИ) в типе T_i. Выполняется анализ пространства действующих киберугроз

$U = \{U_j\}$, $1 \le j \le m$, где m – количество идентифицированных киберугроз, и затем соотносятся киберугрозы $U_j \in U$ с типами устройств (активов КИИ) $T_i \in T$, которые им подвержены. Значение риска при реализации угрозы $U_j \in U$ для устройства (актива КИИ) типа $T_i \in T$ рассчитывается по формуле:

$$R(U_j)T_i = P(U_j)\sum_{k=1}^{n} I_{T_iT_k} C_{T_iT_k} \times Q_{T_k}. \quad (11)$$

$P(U_j)$ – вероятность реализации угрозы $U_j \in U$, которая показывает, какую долю занимают успешные реализации угрозы $U_j \in U$ от общего числа успешных реализаций угроз U. Для определения количественного значения вероятности киберугроз в КИИ используются актуальные экспертные оценки и статистические данные.

$I_{T_iT_k}$ – коэффициент влияния устройств (активов КИИ) типа $T_i \in T$ на устройства (активы КИИ) типа $T_k \in T$. Для вычисления $I_{T_iT_k}$ (12) определяется тип сообщений, которыми обмениваются устройства.

$$I_{T_iT_k} = \frac{N_{\text{значимые}}}{N_{\text{общее}}}, \quad (12)$$

где $N_{\text{значимые}}$ и $N_{\text{общее}}$– соответственно количество значимых и количество всех переданных сообщений, которыми обмениваются устройство (актив КИИ) типа $T_i \in T$ с устройством (активом КИИ) типа $T_k \in T$.

$C_{T_iT_k}$ – коэффициент количества взаимодействий устройств (активов КИИ) друг с другом, который показывает количество устройств типа $T_k \in T$, с которыми взаимодействует устройство типа $T_i \in T$.

Q_{T_k} – размер возможного ущерба (при реализации угрозы).

По завершении методики выполняется сопоставление полученной оценки риска с приемлемым уровнем риска и предпринимаются меры, включающие донастройку нейро-нечеткой системы управления обнаружением компьютерных атак, переобучение разработанных методов обнаружения компьютерных атак, расширение базы методов защиты.

В главе 5 представлена разработанная архитектура и результаты реализации автоматизированной системы анализа киберугроз в КИИ.

Автоматизированная система анализа киберугроз в КИИ (рис. 5), реализующая в адаптивном режиме непрерывный подбор, настройку и применение детекторов атак адекватно действующим киберугрозам и текущему состоянию КИИ, построен на платформе эластичных вычислений, образованной облачной средой, на базе которой развернута вычислительная инфраструктура контроллера программно-конфигурируемой сети (ПКС-контроллера). ПКС-контроллер выполняет управление обнаружением атак и автоматически адаптирует мощности под текущие размерность, динамику и нагрузку контролируемой сети КИИ.

Для оценки точности обнаружения различных компьютерных атак выполнена серия экспериментов с использованием наборов данных IoT Network Intrusion (IEEEDataPort), Malware on IoT (Stratosphere Lab) и The BoT-IoT (NSW Canberra). В экспериментах оценивалось качество классификации на основе ошибок I и II рода.

Комплекс методов обнаружения атак на КИИ обеспечивают точность 95-100%, при этом количество ложных срабатываний не превышает 2% (рис. 6).

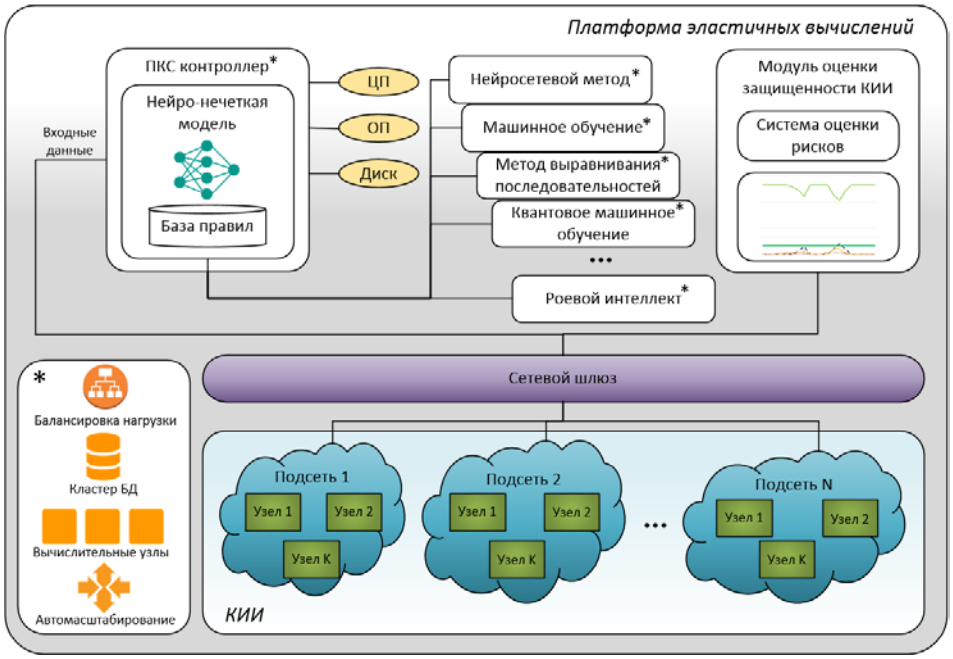

Рисунок 5 – Архитектура системы анализа киберугроз в КИИ

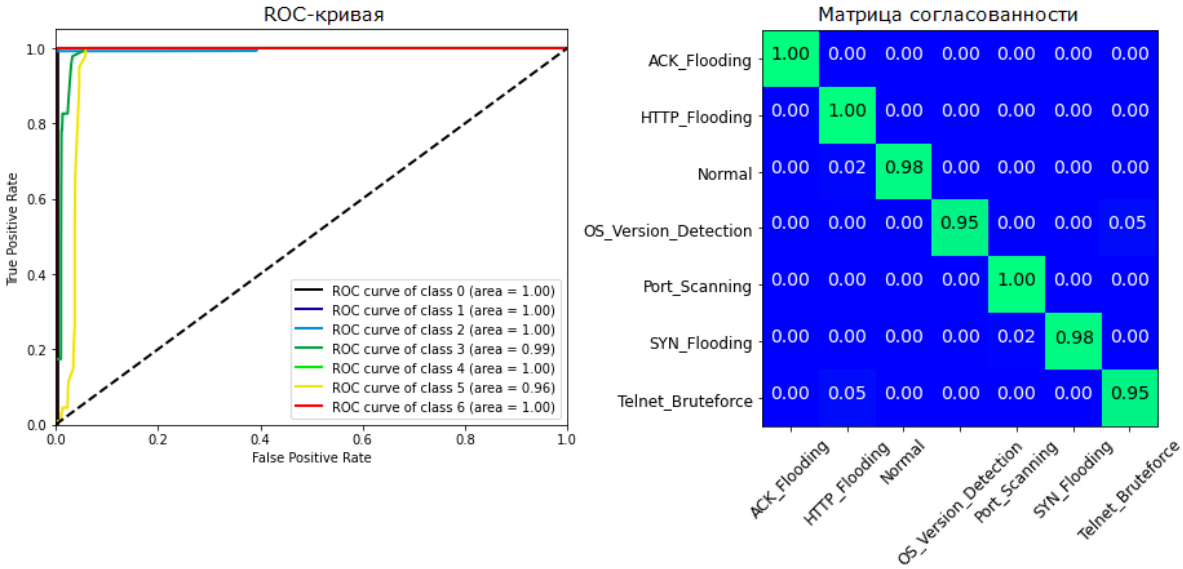

Рисунок 6 – Результаты оценки точности обнаружения компьютерных атак

С использованием сетевого эмулятора NS-3 разработан полигон КИИ, включающий имитационные модели типовых инфраструктур: сети транспортных средств (VANET/FANET), промышленный Интернет (IIoT) и умный город (smart city). На рис. 7 представлены результаты исследований функционирования КИИ (в терминах модели развития компьютерных атак на КИИ показана динамика изменения популяций узлов КИИ) при фиксированном методе обнаружения атак на основе роевого интеллекта (левая часть рис. 7) и при включении системы анализа киберугроз (правая часть рис. 7) На рис. 7 представлен фрагмент сценария атаки: на 40 с инициирована атака «Черная дыра», на 220 с –атака «Отказ в обслуживании»).

Атака «Черная дыра» в обоих случаях успешно обнаружена, но за счет гибкого управления ресурсами при использовании разработанной системы анализа киберугроз восстановление КИИ произошло быстрее. При атаке «Отказ в обслуживании» разработанная система, основываясь на изменившихся характеристиках КИИ, изменила режим работы, определив нейросетевой ансамбль из базы методов в качестве оптимального для новых условий. Высокая скорость обнаружения и нейтрализация узлов-злоумышленников обеспечивает безопасность КИИ в условиях действия различных киберугроз.

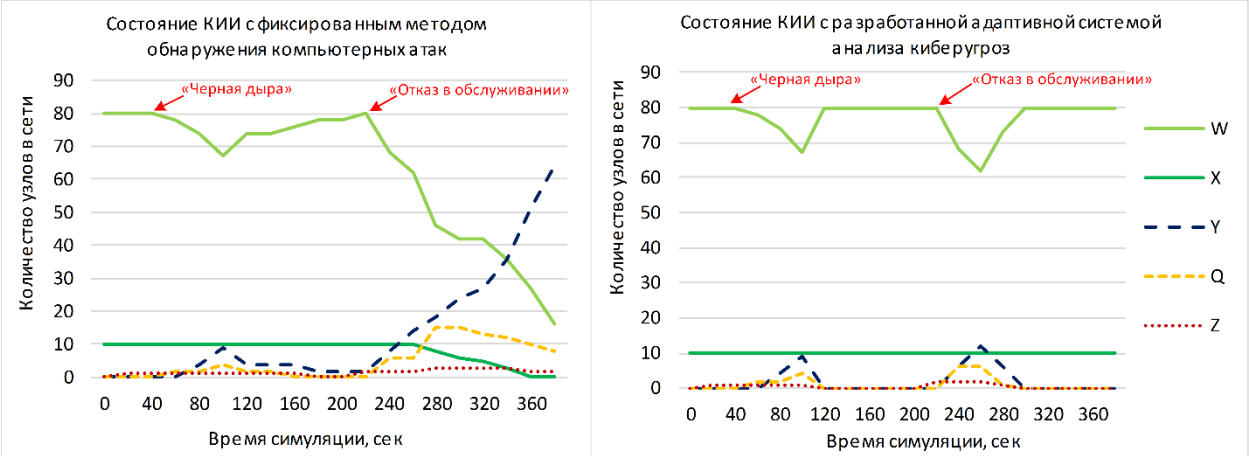

Рисунок 7 – Сравнение состояний КИИ при жестком (слева) и адаптивном (справа) обнаружении компьютерных атак

В заключении приведены основные результаты, полученные автором в ходе выполнения работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Определена задача обеспечения непрерывного функционирования КИИ в условиях целенаправленных компьютерных атак; сформулированы требования адаптивности, полноты и оперативности обнаружения компьютерных атак в вариативных условиях функционирования КИИ.

2. Предложена математическая модель развития компьютерных атак на КИИ, основанная на расширении базовой модели Лотки-Вольтерры. На базе модели предложен критерий адекватности применяемых методов обнаружения атак изменяющимся параметрам КИИ и действующим киберугрозам.

3. Построена структура базы методов обнаружения компьютерных атак в КИИ на основе характерных параметров актуальных киберугроз и модели развития компьютерных атак на КИИ. Разработан комплекс из 10 интеллектуальных методов обнаружения компьютерных атак в КИИ на основе методов машинного обучения, искусственных нейросетей, роевого интеллекта и биоинспирированных алгоритмов, обеспечивающих высокую точность и скорость обнаружения полиморфных целевых атак, атак на динамическую маршрутизацию, туннельных атак.

4. Построена адаптивная система управления обнаружением компьютерных атак в КИИ на базе нейро-нечеткого анализа вариативных пространств киберугроз и параметров объекта защиты с помощью автоматически реконфигурируемой системы нейро-нечеткого вывода ANFIS и нечеткого базиса Такаги-Сугено-Канга, что обеспечивает высокую динамику и точность обнаружения атак в изменяющихся условиях принятия решения.

5. Разработана методика оценки снижения риска реализации киберугроз в КИИ, основанная на адаптивной быстровычислимой количественной оценке риска, которая учитывает типизацию и самоорганизацию сетевых структур КИИ.

6. Разработаны архитектура и макет автоматизированной системы анализа киберугроз в КИИ на базе технологии программно-конфигурируемых сетей. Система осуществляет выбор, настройку и применение детекторов атак с учетом изменяющегося уровня киберугроз и состояния контролируемой сети объектов КИИ.

Перспективы дальнейшей разработки темы диссертации заключаются в развитии предлагаемых методов для выявления компьютерных атак в других системах сложной структуры, а также в масштабировании предложенных методов в условиях КИИ сверхбольших размеров.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ

в 74 научных работах, наиболее значимыми из которых являются:

В рецензируемых журналах из Перечня ВАК:

1) Калинин, М.О. Архитектуры построения защищенных транспортных сетей на основе технологии SDN / М.О. Калинин, **В.М. Крундышев**, П.В. Семьянов // Проблемы информационной безопасности. Компьютерные системы. – 2017. – №3. – С. 53-61.

2) Калинин, М.О. Иерархическое программно-конфигурируемое управление безопасностью крупномасштабных динамических сетей / М.О. Калинин, **В.М. Крундышев**, Е.Ю. Резединова, Д.В. Решетов // Проблемы информационной безопасности. Компьютерные системы. – 2018. – №1. – С. 82-88.

3) **Крундышев, В. М.** Выявление киберугроз в современных промышленных системах с помощью сетей глубокого обучения / В.М. Крундышев // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №4. – С. 76-83.

4) **Крундышев, В. М.** Подготовка наборов данных для обучения нейросетевой системы обнаружения вторжений в промышленных системах / В.М. Крундышев // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №4. – С. 108-113.

5) **Крундышев, В. М**. Обеспечение кибербезопасности цифрового производства с помощью современных нейросетевых методов / В.М. Крундышев // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №3. – С. 85-92.

6) Калинин, М. О. Разработка системы обнаружения вторжений в сетях Интернета вещей на основе алгоритма выравнивания последовательностей / М.О. Калинин, **В.М. Крундышев**, Б.Г. Синяпкин // Проблемы информационной безопасности. Компьютерные системы. – 2020. – №3. – С.50-58.

7) **Крундышев, В. М.** Выявление киберугроз в сетях промышленного Интернета вещей на основе нейросетевых методов с использованием памяти / В.М. Крундышев //

Проблемы информационной безопасности. Компьютерные системы. – 2020. – №1. – С. 89-95.

8) Калинин, М. О. Анализ сверхвысоких объемов сетевого трафика на основе квантового машинного обучения / М.О. Калинин, **В.М. Крундышев** // Проблемы информационной безопасности. Компьютерные системы. – 2021. – №1. – С. 39-49.

<u>В изданиях, индексируемых Scopus и/или Web of Science:</u>

1) Kalinin, M. Architectures for building secure vehicular networks based on SDN technology / M. Kalinin, V. Krundyshev, P. Semianov // Automatic Control and Computer Sciences. - 2017. - Vol. 51. - P. 907-914.

2) **Krundyshev, V.** Artificial swarm algorithm for VANET protection against routing attacks / V. Krundyshev, M. Kalinin, P. Zegzhda // IEEE International Conference on Industrial Cyber-Physical Systems, May 15-18, 2018, Saint Petersburg, Russia. – P. 795-800.

3) Belenko, V. Synthetic datasets generation for intrusion detection in VANET / V. Belenko, **V. Krundyshev**, M. Kalinin // 11th International Conference on Security of Information and Networks, September 10, 2018, Cardiff, UK. – Article number a9.

4) Belenko, V. Evaluation of GAN applicability for intrusion detection in self-organizing networks of cyber physical systems / V. Belenko, V. Chernenko, M. Kalinin, **V. Krundyshev** // 2018 International Russian Automation Conference, September 9-16, 2018, Sochi, Russia. – P. 1-7.

5) Kalinin, M. Hierarchical Software-Defined Security Management for Large-Scale Dynamic Networks / M. Kalinin, **V. Krundyshev**, E. Rezedinova, D. Reshetov // Automatic Control and Computer Sciences. - 2018. - Vol. 52. – P. 906-911.

6) **Krundyshev, V.** Hybrid neural network frame work for detection of cyber attacks at smart infrastructures / V. Krundyshev, M. Kalinin // 12th International Conference on Security of Information and Networks, September 12-15, 2019, Sochi, Russia. – Article number 3357623.

7) **Krundyshev, V.** Identifying Cyberthreats in Modern Industrial Systems by Means of Deep-Learning Networks / V. Krundyshev // Automatic Control and Computer Sciences. - 2019. - Vol. 53. – P. 1006-1011.

8) **Krundyshev, V.** Preparing Datasets for Training in a Neural Network System of Intrusion Detection in Industrial Systems / V. Krundyshev // Automatic Control and Computer Sciences. - 2019. - Vol. 53. – P. 1012-1016.

9) Kalinin, M. Sequence Alignment Algorithms for Intrusion Detection in the Internet of Things / M. Kalinin, **V. Krundyshev** // Nonlinear Phenomena in Complex Systems. – 2020. – Vol. 23. – No 4. – P. 397-404.

10) Ivanov, D. Automatic security management of smart infrastructures using attack graph and risk analysis / D. Ivanov, M. Kalinin, **V. Krundyshev**, E. Orel // 4th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), July 27-28, 2020, London, UK, –P. 295-300.

11) **Krundyshev, V.** The Security Risk Analysis Methodology for Smart Network Environments / V. Krundyshev, M. Kalinin // 2020 International Russian Automation Conference (RusAutoCon), September 6-12, 2020, Sochi, Russia, – P. 437-442.

12) **Krundyshev, V.** Prevention of cyber attacks in smart manufacturing applying modern neural network methods / V. Krundyshev, M. Kalinin // International Scientific Conference on Digital Transformation on Manufacturing, Infrastructure and Service 2019, DTMIS 2019, November 21-22, 2019, Saint Petersburg, Russia. – Article number 012011.

13) **Krundyshev, V.** Neural network approach to assessing cybersecurity risks in large-scale dynamic networks / V. Krundyshev // 13th International Conference on Security of Information and Networks, November 4-6, 2019, Merkez, Turkey. – Article number 3433603.

14) Kalinin, M. Development of the Intrusion Detection System for the Internet of Things Based on a Sequence Alignment Algorithm / M. Kalinin, **V. Krundyshev**, B. Sinyapkin // Automatic Control and Computer Sciences. - 2020. - Vol. 54. – P. 993-1000.

15) **Krundyshev, V.** Identification of Cyber Threats in Networks of Industrial Internet of Things Based on Neural Network Methods Using Memory / V. Krundyshev // Automatic Control and Computer Sciences. - 2020. - Vol. 54. – P. 900-906.

16) **Krundyshev, V.** Ensuring Cybersecurity of Digital Production Using Modern Neural Network Methods / V. Krundyshev // Automatic Control and Computer Sciences. - 2020. - Vol. 54. – P. 786-792.

17) Kalinin, M. Detection and Prediction of Safety Faults in Inter-Device Networks Applying a Set of Data-Driven Methods / M. Kalinin, **V. Krundyshev**, V. Belenko and V. Chernenko // Smart Innovation, Systems and Technologies. – 2021. – Vol. 220. – P. 15-25.

18) Kalinin, M. Cybersecurity risk assessment in smart city infrastructures / M. Kalinin, **V. Krundyshev**, P. Zegzhda // Machines. – 2021. – Vol. 9. – No 4. – P. 78.

19) Kalinin, M. Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions / M. Kalinin, **V. Krundyshev** // 5th World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), July 29-30, 2021, London, UK, – P. 118-122.

20) Zegzhda, D. Application of bioinformatics algorithms for polymorphic cyberattacks detection / D. Zegzhda, M. Kalinin, **V. Krundyshev**, D. Lavrova, D. Moskvin, E. Pavlenko // Informatics and Automation. - 2021. - Vol. 20, – P. 820-844.

В разделе монографии: Крундышев, В.М. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д.П. Зегжда, Е.Б. Александрова, М.О. Калинин и др. // М.: Горячая линия – Телеком, 2019. – 640 с.: ил. – (ISBN 978-5-9912-0826-0).

В патентах РФ на изобретения:

1) Способ управления связностью одноранговой межмашинной сети передачи данных: патент на изобретение №2666306 / Д.П. Зегжда, М.О. Калинин, П.Д. Зегжда, **В.М. Крундышев**. – зарегистр. 27.12.2017.

2) Способ безопасной маршрутизации в одноранговых самоорганизующихся сетях: патент на изобретение №2668222 / Д.П. Зегжда, М.О. Калинин, **В.М. Крундышев**, А. А. Минин. – зарегистр. 27.12.2017.

3) Способ контроля доступа между устройствами в межмашинных сетях передачи данных: патент на изобретение №2714853 / М.О. Калинин, **В.М. Крундышев**, Е.Ю. Резединова, П. Д. Зегжда. – зарегистр. 27.12.2018.

Подписано к печати	11.2021	Печ. л. – 1,0
Печать – ризография	Бумага для множит. апп.	Формат 60x84 1/16
Тираж 100 экз.	Заказ №	

СР ПГУПС, 190031. С.-Петербург, Политехническая ул, 29Б