ISSN 2658-5014 (Print)
2024. Т. 6, № 4 (19). С. 14–31
СИИТ
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья
ISSN 2686-7044 (Online)
http://siit.ugatu.su

УДК 004.056 DOI 10.54708/2658-5014-SIIT-2024-no4-p14 EDN LTXBSG

Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем

Р. Р. Шамсутдинов • В. И. Васильев • А. М. Вульфин

Аннотация. Статья посвящена решению задачи обнаружения сетевых атак на системы промышленного Интернета вещей на основе комплексирования методов искусственного интеллекта, механизмов искусственной иммунной системы и методов корреляционного анализа данных. Подчеркивается, что системы промышленного Интернета вещей занимают важное место в Индустрии 4.0, однако они характеризуются как распределенные гетерогенные системы, обладающие в силу ряда обстоятельств недостаточно высоким уровнем защищенности от угроз информационной безопасности. Рассмотрены наиболее распространенные причины сложившейся ситуации, особенности мониторинга информационной безопасности промышленных сетей. Предложен подход к построению распределенной двухуровневой многоагентной системы обнаружения сетевых атак и аномалий сетевого трафика, основанной на комплексировании алгоритмов искусственных иммунных систем и методов машинного обучения, подчеркивается получаемый синергетический эффект от такого комплексирования. Рассматривается решение подзадачи нормализации анализируемых данных сетевого трафика. Разработана трехуровневая гибридная распределенная интеллектуальная система мониторинга информационной безопасности систем и устройств промышленного Интернета вещей, интегрирующая в себе двухуровневую искусственную иммунную систему, алгоритм случайного леса, искусственную нейронную сеть и подсистему корреляционного анализа данных. Эта система выполняет многоуровневое принятие решения: выявление аномалии с помощью агентов искусственной иммунной системы нижнего уровня; определение опасности аномалии и необходимости идентификации ее как атаки агентами искусственной иммунной системы верхнего уровня; определение класса атаки комитетом классификаторов; установление уровня значимости инцидента информационной безопасности на основе процедуры корреляционного анализа данных. Проведенные вычислительные эксперименты продемонстрировали достижение разработанной системой высоких значений показателей эффективности, превышающих значения таких показателей для каждого из рассмотренных интеллектуальных классификаторов в отдельности.

Ключевые слова: промышленный интернет вещей; информационная безопасность; искусственная иммунная система; интеллектуальная система; кибербезопасность.

Введение

Промышленное производство на современном этапе развития все шире использует киберфизические системы, инновационные информационные технологии, системы искусственного интеллекта и машинного обучения. Ключевые позиции в нарождающейся промышленной революции начинает занимать промышленный Интернет вещей (Industrial Internet of Things, IIoT). IIoT представляет собой систему объединенных компьютерных сетей и подключенных к ним промышленных (производственных) объектов со встроенными датчиками, программным обеспечением (ПО) для сбора и обмена данными, а также возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека. По данным [1], объем мирового рынка IIoT в 2023 г. уже достиг 255.3 млрд. долл., в дальнейшем ожидается устойчивый рост.

Важным условием работы сетей и систем промышленного Интернета вещей является обеспечение их информационной безопасности (ИБ). Согласно отчету фирмы Nokia «Threat Intelligence Report 2020» [2], в последние годы доля компьютерных атак на устройства IIoT в общем числе атак на мобильные устройства увеличилась и достигла значения 32.7 %.

По данным «Лаборатории Касперского», количество новых образцов вредоносного ПО для IIoT-устройств с каждым годом значительно возрастает: если в 2015 г. их число составляло 483, то в 2020 г. – уже 331 401 [3]. 55% респондентов опроса [4], проведенного этой организацией, характеризуют ИБ IIoT как один из главных факторов, определяющих кибербезопасность АСУ ТП, но в то же время только 14% организаций используют средства обнаружения сетевых аномалий и 19% – системы мониторинга сети и трафика. По данным Check Point [5], 67% предприятий уже сегодня столкнулись с инцидентами безопасности, связанными с применением IIoT-устройств.

Невысокая эффективность существующих систем обнаружения атак (СОА) в решении задач мониторинга ИБ сетей IIoT обусловливается рядом обстоятельств. Так, существуют атаки, эксплуатирующие специфичные уязвимости IIoT, например, атаки, приводящие к повышению расхода электроэнергии устройствами IIoT, в том числе сенсоров беспроводных сенсорных сетей, не выявляемые штатными средствами защиты промышленных систем. Существующие СОА, основанные на анализе сигнатур, в принципе не могут выявлять новые, не известные ранее атаки (атаки «нулевого дня»), а также новые виды уже известных атак, для которых пока не существует сигнатур. СОА на основе выявления злоупотреблений (аномалий) характеризуются большим количеством допускаемых ошибок. Существующие СОА, реализующие в том числе методы искусственного интеллекта, демонстрируют в целом более высокую, но пока еще недостаточную эффективность обнаружения сетевых атак и аномалий в сетях IIoT.

Поэтому проблема разработки и исследования новых методов и алгоритмов обнаружения сетевых атак и аномалий в работе систем и устройств IIoT с применением методов искусственного интеллекта, обеспечивающих повышения уровня их защищенности в условиях воздействия возможных внешних и внутренних угроз, является актуальной.

Текущее состояние проблемы обеспечения информационной безопасности сетей промышленного интернета вещей

Понятие промышленного Интернета вещей

Согласно предварительному национальному стандарту ПНСТ 643-2022. «Информационные технологии. Интернет вещей промышленный. Термины и определения» [6], промышленный Интернет вещей (IIoT) – это Интернет вещей, машин, компьютеров и людей, обеспечивающий интеллектуальные производственные операции с использованием расширенной аналитики данных для качественно новых результатов бизнеса. В качестве основных разновидностей «вещей», которые подключаются к сети IIoT, обычно рассматриваются различные типы датчиков (сенсоров) и приводов. Эти устройства, с одной стороны, имеют интерфейс с коммуникационной сетью, а с другой – интерфейс, обеспечивающий физическое взаимодействие с процессом, который требуется отслеживать. Коммуникационный интерфейс является необходимой компонентой IIoT. Это может быть проводной или беспроводной интерфейс. Но независимо от того, какая технология используется на канальном и физическом уровнях сети, устройства должны поддерживать протокол IP, чтобы интегрироваться в инфраструктуру IIoT.

В 2020 г. в РФ был выпущен предварительный национальный стандарт ПНСТ 420-2020 «Информационные технологии. Интернет вещей промышленный. Типовая архитектура» [7] (далее – ПНСТ 420-2020), который определяет типовую архитектуру промышленного Интернета вещей, структуру архитектуры IIoT, включающую каркас, основанный на интересах, точках зрения, видах моделей, заинтересованных сторонах. В стандарте представлен пример трехуровневой архитектуры промышленного Интернета вещей с точки зрения реализации архитектурных паттернов (шаблонов). Данная архитектура включает в себя следующие уровни:

- уровень предприятия, где реализованы приложения, системы поддержки принятия решений, интерфейсы для конечных пользователей (здесь осуществляется получение потоков информации с других уровней и выдача управляющих команд);

• уровень платформы, где агрегируется и обрабатывается информация граничного уровня, перенаправляются команды управления с уровня предприятия на граничный уровень;

• граничный уровень, где осуществляется сбор данных от граничных узлов посредством сети ближнего действия, а также реализация управляющих команд.

Обеспечение безопасности промышленного Интернета вещей

Одной из главных проблем в построении и эксплуатации промышленного Интернета вещей является обеспечение ИБ его устройств и систем. Наиболее распространенные причины недостаточно высокой защищенности IIoT:

- устаревшее системное и прикладное ПО устройств IIoT, недостаточное внимание к программным обновлениям;
- передача данных без шифрования;
- стандартные заводские настройки безопасности устройств;
- незащищенные интерфейсы;
- уязвимости в операционных системах (ОС) общего назначения;
- невозможность оснастить многие устройства встроенными средствами безопасности.

Специфика IIoT заключается в подключении промышленных систем к сети Интернет, возможности реализации удаленного управления ими, в том числе с устройств, находящихся за пределами предприятия; использовании облачных систем, в том числе арендованных; ограниченности вычислительных и энергетических ресурсов автономных IIoT-устройств; их слабой защищенности; отсутствии зачастую средств шифрования трафика.

Необходимо отметить, что в рамках IIoT часто используются беспроводные сенсорные сети (Wireless Sensor Networks, WSN), состоящие из большого числа автономных сенсорных узлов, собирающих различные данные и обменивающихся ими при помощи беспроводного соединения с более мощным узлом – базовой станцией. В связи с их распределенной открытой архитектурой и ограниченностью ресурсов сенсорных узлов такие сети являются очень уязвимыми для атак [8].

Производители, конечно, стараются решать проблемы безопасности IIoT. Так, по данным [9], в целях обеспечения ИБ IoT в облачной системе Microsoft Azure используется методика моделирования угроз STRIDE, которая рассматривает все уровни и компоненты IoT с точки зрения возникновения различных угроз, предлагаются меры защиты.

В [10] проводится сравнение возможностей обеспечения ИБ таких IoT-фреймворков, как AWS IoT от компании Amazon, ARM Bed от компании ARM, Azure IoT от «Microsoft», HomeKit от «Apple», Brillo/Weave «Google», SmartThings от «Samsung», Calvin от «Ericsson» и Kura от «Eclipse».

В [4] отмечается, что предотвратить угрозу выгоднее, чем компенсировать ущерб от последствий ее реализации. Сообщается, что Лабораторией Касперского разработан первый IT-продукт с кибериммунитетом – KISG 100. Данный продукт представляет собой шлюз данных для IoT. Однако, как показывает практика, существующих мер и средств всё ещё недостаточно.

Отметим, что в настоящее время с целью повышения уровня автоматизации процессов, связанных с управлением инцидентами ИБ, повышения эффективности реагирования на киберугрозы, обеспечения комплексной защиты компьютерных сетей создаются и используются ситуационные центры управления ИБ (Security Operation Center, SOC), рассматриваемые в [11]. По данным [12], большую часть времени оператор SOC-центра работает с системами управления безопасностью и событиями ИБ (Security Information and Event Management, SIEM). SIEM-системы осуществляют сбор данных о событиях ИБ по всей сети с различных источников, сопоставляют события между собой, выявляют подозрительные совокупности событий, которые вне этих совокупностей могут выглядеть вполне легитимными. На основе корреляционного анализа осуществляется более глубокая обработка данных о событиях и лучшее выявление инцидентов ИБ.

Мониторинг информационной безопасности сетей IIoT

Мониторинг ИБ сетей IIoT осуществляется на основе данных о сетевом трафике. Задача сбора этих входных данных усложняется использованием IIoT-устройствами различных протоколов и типов подключений. В системах IIoT применяются:

- беспроводные локальные сети (Wireless Local Area Network, WLAN), беспроводные персональные сети (Wireless Personal Area Network, WPAN), включая сети ближнего (малого и среднего) радиуса действия, такие протоколы, как: Wi-Fi, 6LoWPAN, ZigBee IP, Thread, Z-Wave, ZigBee, WirelessHart, BLE 4.2 (Bluetooth Mesh), MiWi;
- энергоэффективные глобальные сети (Low-Power Wide Area Network, LPWAN), технологии для передачи небольших данных на дальние расстояния: LoRaWAN, SIGFOX, CIoT, 4G LTE, 5G, NB-IoT и др. [13].

Сетевое взаимодействие относится к граничному уровню архитектуры IIoT, а системы управления, диагностики и мониторинга – к уровню платформы, описанных в ПНСТ 420-2020. В целях мониторинга ИБ сети IIoT с граничного уровня могут быть собраны данные о сетевом взаимодействии, состоянии IIoT-устройств, с уровня платформы – данные о текущем состоянии сетей и конечных точек IIoT, общем количестве инцидентов ИБ, поступающие от внешних систем мониторинга.

К таким системам могут относиться системы SIEM и SCADA, а также, к примеру, система обнаружения опасных состояний промышленных объектов, рассмотренная в [14], и др. Предполагается сбор данных о сетевом взаимодействии с канального по транспортный уровни сетевой модели OSI.

Мониторинг ИБ сети IIoT, в первую очередь, предполагает анализ состояния сетевого трафика IIoT, информация о котором включает:

- временные ряды технологических параметров (ВРТП), то есть параметры (данные), обрабатываемые с помощью мультисенсорных сетей;
- внутренний сетевой трафик IIoT, то есть данные, передаваемые по каналам связи на каждом из уровней управления IIoT и между уровнями управления, то есть в терминологии серии стандартов ГОСТ Р 62443 – трафик трактов;
- внешний сетевой трафик IIoT, то есть данные, поступающие из внешней среды (Интернет, передатчики, провайдеры и т. д.) и передаваемые во внешнюю среду;
- данные, поступающие от взаимодействующей SIEM-системы, о событиях (инцидентах) ИБ.

Таким образом, система мониторинга ИБ сети IIoT должна быть распределенной, учитывать характер собираемых входных данных, гетерогенность соответствующих источников. Необходимо учитывать разнородность входных данных также на этапе их нормализации, то есть приведения данных к единому формату представления.

Отметим также, что определение конкретного состава собираемых и анализируемых данных зависит от используемых протоколов и технологий конкретного объекта. В данной статье не предлагается какой-либо определенный состав параметров, наиболее универсальный для всех сетей IIoT или, наоборот, наиболее подходящий для определенной узкой области. Для обучения и работы СОА может быть использован любой набор параметров, достаточный для определения на его основе безопасности того или иного сетевого взаимодействия, выбранный экспертами в соответствии с используемыми на конкретном объекте сетевыми технологиями, протоколами, обеспечивающий возможность эффективной классификации.

Вместе с тем общий подход к нормализации данных должен включать в себя кодирование их качественных, текстовых или лингвистических значений числовыми параметрами, преобразование исходного диапазона количественных значений к используемому системой диапазону. Подробнее вопросы нормализации рассматриваются в [15, 16].

На этапе обучения и тестирования СОА применительно к сети IIoT будем отталкиваться от параметров, используемых в различных, наиболее часто используемых наборах данных

о сетевых соединениях, содержащих параметры трафика как для нормальных сетевых соединений, так и для различного рода атак – датасетах (ДС).

Применение искусственных иммунных систем для решения задачи обнаружения атак и аномалий сетевого трафика

Для лучшего понимания алгоритмов искусственной иммунной системы (ИИС) кратко рассмотрим работу естественной иммунной системы (ЕИС), служащей для защиты организма человека от чужеродных зловредных организмов – патогенов. В ЕИС выделяют две значимые подсистемы: врожденный иммунитет, приобретенный иммунитет. Первый передаётся по наследству, не меняется в течение жизни. Его механизмы обеспечивают первую линию защиты, включают механические барьеры (кожа, слизистые оболочки), гуморальные факторы (цитокины, система комплемента и пр.), клеточные механизмы. Второй осуществляет специфичный иммунный ответ на конкретный вид распознанного патогена с помощью специальных клеток – лимфоцитов. В ИИС чаще всего моделируются механизмы функционирования лимфоцитов, распознающих и атакующих «чужого», и дендритных клеток (ДК), осуществляющих анализ уровня опасности по объему повреждений тканей, запускающих или угнетающих деятельность лимфоцитов. Построение искусственной системы, обладающей всеми полезными свойствами и функционалом ЕИС, является пока нереализуемой задачей, но существуют алгоритмы, успешно имитирующие некоторые функции ЕИС, позволяющие решать в том числе задачи обнаружения сетевых атак и аномалий.

Основные алгоритмы теории искусственных иммунных систем. Алгоритм негативной селекции (Negative Selection Algorithm, NSA) нацелен на выполнение классификации «своего» и «чужого» [17]. Предполагает в первую очередь определение обучающих примеров «своего» (S) как совокупности строк длиной l, затем формирование случайным образом детекторов (D) таких, что ни один детектор не соответствует ни одной строке S. После чего анализируемые данные (A) приводятся к соответствующему строковому виду, и каждая строка A сравнивается с каждым детектором D. Если находится соответствие, то строка A_i считается «чужой». Для определения факта соответствия используются различные варианты оценки мер близости между точками или векторами в пространстве анализируемых параметров.

Модель гиперклетки представляет собой модификацию алгоритма NSA, при котором создается большая гиперклетка, покрывающая области как «своего», так и «чужого», затем от нее отсекаются части, покрывающие нецелевые области. Существуют различные вариации данного алгоритма: может изменяться форма гиперклетки, вид, критерий останова и пр. По данным [17], модель гиперклетки обладает более высокой скоростью обучения. Алгоритм NSA обеспечивает высокую эффективность СОА, однако может быть заменен также набором экспертных правил, создаваемых с помощью дерева решений, как это предложено в [18].

Алгоритм клональной селекции (Clonal Selection Algorithm, CSA) имитирует процесс пролиферации активированного B-лимфоцита. Существуют различные подходы к его реализации. Так, в [17] описывается создание детекторов, обнаруживающих нормальное состояние системы. Для этого детекторы генерируются случайно, определяется аффинность a_j как мера близости каждого детектора $\vec{d}_i$ и вектора данных нормального состояния $\vec{s}_j$. Детекторы с наибольшим значением a клонируются в количестве, прямо пропорциональном a. Каждый клон подвергается мутации, степень мутации обратно пропорциональна a. При этом на этапе анализа предполагается, что если ни один детектор не соответствует анализируемой строке, то она отмечается аномальной.

Разрастание количества детекторов в результате клонирования может негативно сказываться на производительности системы, поэтому часто ограничивают количество детекторов и срок их существования. Если срок существования детектора превышен, он уничтожается, вместо него генерируется новый. Если детектор обнаруживает аномалию, срок его существо-

вания значительно увеличивается. В целом алгоритм клональной селекции является адаптивным алгоритмом, позволяющим дообучать систему в процессе эксплуатации, но отдельно его применение не обеспечивает толерантности системы к «своим» данным.

В соответствии с теорией опасности иммунная система при определении необходимости своего реагирования использует не только обнаружение чужеродных патогенов, но и в большей степени учитывает опасность той или иной ситуации. То есть иммунитет должен более агрессивно реагировать не на «чужое, но безопасное», а, скорее, на «свое, но опасное» [19].

С теорией опасности тесно связан алгоритм дендритных клеток (ДК). ДК аккумулируют сигналы опасности, имеют три состояния: незрелое, полузрелое, зрелое. По данным [20], незрелое состояние – начальное состояние ДК, находящихся в поиске патогенов, полузрелое состояние устанавливается в случае обнаружения безопасного патогена, зрелое – опасного. В [20] предлагается предусмотреть для ДК три входа: сигнал опасности, сигнал безопасности, сигнал о наличии патогена (Pathogen-Associated Molecular Patterns, PAMP) и три выхода: сигнал о костимуляции, сигнал о полузрелом состоянии, сигнал о зрелом состоянии. Заметим, что алгоритм ДК и теория опасности позволяют сконцентрировать реагирование больше на действительные (реальные) угрозы, чем на случайные аномалии.

Теория идиотипической иммунной сети основана на предположении о функционировании иммунной системы как регулирующей сети антител, взаимно стимулирующих друг друга даже в отсутствие патогенов. Согласно данной теории, иммунная система активирует сама себя, обеспечивая поддержание детекторов в активном состоянии даже в отсутствие антигена, имитируя его присутствие. Предполагается, что лимфоциты, способные распознавать любые чужеродные антигены, должны распознавать и соответствующие им антитела, вырабатываемые другими лимфоцитами. В результате, антитела одних лимфоцитов распознаются другими лимфоцитами, что поддерживает активированное состояние последних. В [21] подробно описано формирование идиотипической сети. Механизмы идиотипической иммунной сети более актуальны для ЕИС, чем для ИИС, так как в ИИС для поддержания активности детектора достаточно программно задать соответствующие параметры, не нужно для этого имитировать вторжение.

В целом можно сделать вывод о том, что сегодня существуют различные подходы к построению ИИС, каждый из которых характеризуется определенными преимуществами и недостатками. Объединение рассмотренных подходов к построению ИИС в единую распределенную систему обнаружения атак и аномалий позволяет получить синергетический эффект, при котором на основе алгоритма негативной селекции возможно обнаружение в том числе неизвестных угроз при низком уровне ошибок первого рода, а наличие подсистемы клональной селекции обеспечивает адаптивность системы, что позволяет ей на основе выявленной неизвестной угрозы самообучиться лучшему выявлению подобных угроз.

Механизмы обновления и замены детекторов обеспечивают при этом стабильный размер популяции, не допуская перегрузку ими системы. Гибридизация алгоритмов негативной и клональной селекций сама по себе не нова, однако их дополнение модифицированной подсистемой дендритных клеток (ДК) позволяет обеспечить реагирование системы прямо пропорционально опасности. Предлагается модификация ДК-алгоритма, при которой ДК не накапливает сигналы безопасности, что в противном случае позволило бы злоумышленнику имитировать сигналы безопасности, выполняя активность, характерную для атаки, а ДК ассоциировала бы данную активность с сигналами безопасности и обеспечила толерантность системы к атаке, что в дальнейшем позволило бы злоумышленнику проводить атаку, на которую система бы уже не реагировала. Напротив, ДК должна только оценивать уровень опасности: если он нулевой или близкий к нему, то контрмеры должны быть минимальными, не «параноидальными». Если подобные или связанные аномалии встречаются чаще, то уровень ассоциированной с ними опасности накапливается, и соответственно инициируются более весомые контрмеры.

Результат применения такого объединения алгоритмов CSA и NSA с алгоритмом ДК для анализа датасета BotIoT опубликован нами в [19]. Построение подобной системы в виде архитектуры распределенных взаимосвязанных компонентов позволяет, в случае обнаружения неизвестной угрозы в одном сегменте сети, мгновенно обучить лучшему обнаружению подобных угроз все другие сегменты сети. Более того, единая подсистема ДК получает возможность оценивать сигналы опасности с разных сегментов, выстраивая общую картину безопасности.

Таким образом, особый интерес вызывает построение гибридной ИИС обнаружения сетевых атак и аномалий, объединяющей алгоритмы лимфоцитов и дендритных клеток в классе распределенной двухуровневой системы взаимодействующих агентов.

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМОВ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ

Решение задачи мониторинга ИБ систем IIoT усложняется использованием различных сетевых протоколов и технологий, однако в целом в процессе мониторинга ИБ решаются такие общие базовые задачи, как перехват сетевого трафика, его анализ, принятие решения о наличии и классе атаки (или ее отсутствии), протоколирование, оповещение.

Для решения рассматриваемого круга задач в работе предлагается многоуровневая схема интеллектуального анализа данных трафика, где на нижних двух уровнях используется распределенная двухуровневая искусственная иммунная система (ИИС), на верхнем – система классификации состояния сетевого трафика IIoT.

Двухуровневая искусственная иммунная система

Двухуровневая ИИС содержит агенты верхнего (второго) уровня, реализующие вычисления на основе принципов теории опасности в виде алгоритмов дендритных клеток (ДК), агрегирующие данные об атаках от подконтрольных агентов нижнего уровня, анализирующие уровень опасности. Двухуровневая ИИС содержит два вида агентов: первого и второго уровней, использующие методы классов «лимфоцит» и «дендритная клетка» соответственно. Агенты первого уровня анализируют сетевой трафик, выявляют аномалии, передают данные агентам второго уровня, которые реализует метод анализа класса дендритных клеток, оценивают уровень опасности тех или иных аномалий.

Таким образом, разработанная двухуровневая ИИС представляет собой многоагентную распределенную систему, схема реализации которой представлена на рис. 1. Агенты нижнего уровня распределены по подсетям, выполняют анализ посредством подсистем лимфоцитов, взаимодействуют друг с другом, взаимно обучают друг друга, выявляют атаки и аномалии. На верхнем уровне системы функционируют агенты, реализующие алгоритм ДК, они располагаются на границе сети, выполняют граничные вычисления, также взаимодействуют друг с другом.

Агенты нижнего уровня, в случае выявления неизвестной аномалии, направляют всем другим агентам нижнего уровня во всех сетях информацию о выявившем ее лимфоците. Другие агенты нижнего уровня осуществляют клональную селекцию данного лимфоцита и тем самым обучаются лучшему выявлению подобных аномалий, даже несмотря на то, что никогда с ней не встречались.

Агенты верхнего уровня, реализующие алгоритм ДК, устанавливаются на границах каждой сети, выполняют граничные вычисления, анализируют информацию от подсистем лимфоцитов, граничных маршрутизаторов, межсетевых экранов (МЭ), получают информацию от различных источников из Центра обработки данных (ЦОД), анализируют уровень опасности, сигнализируют о нем в консоли управления.

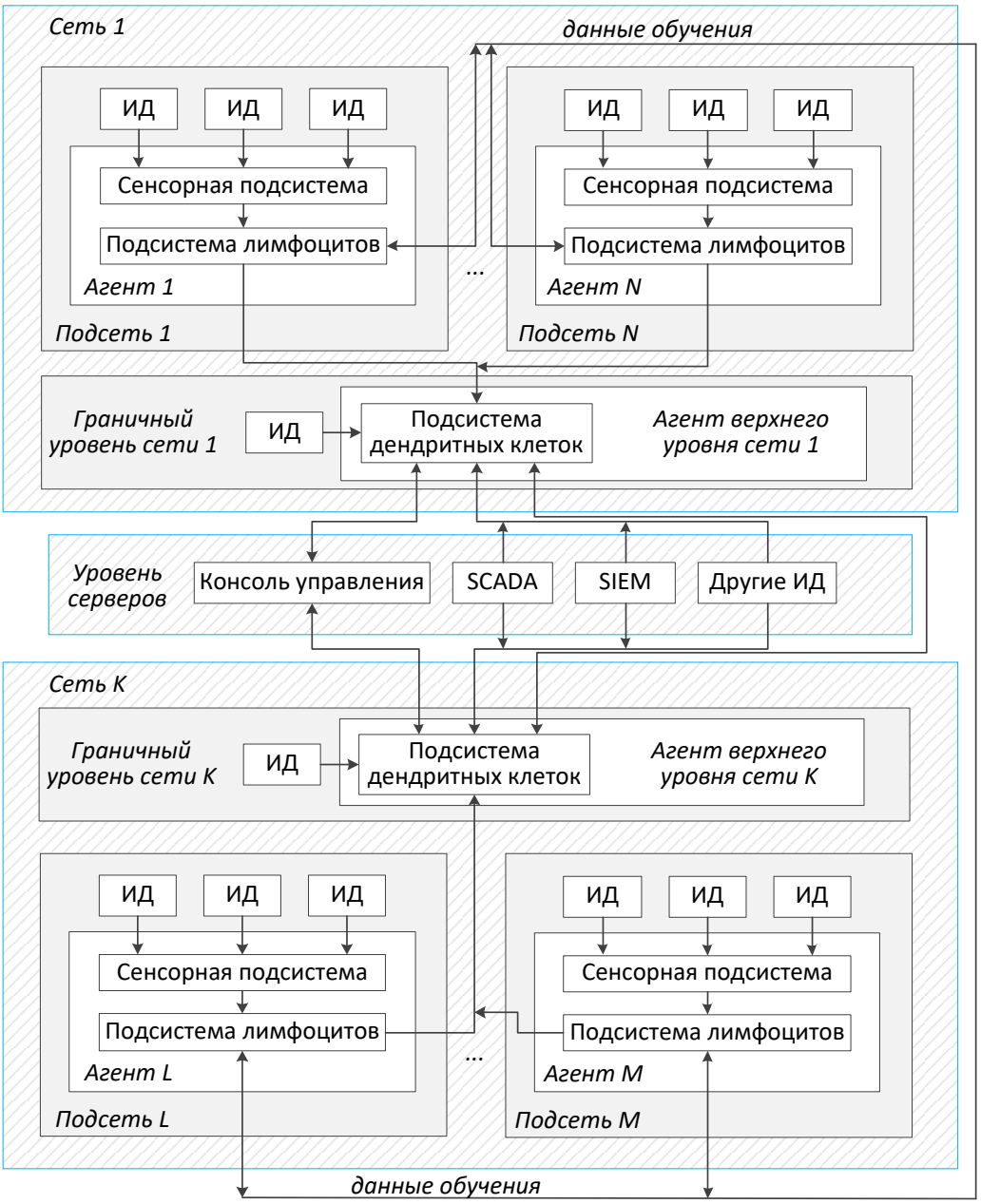

Рис. 1 Схема реализации многоагентной распределенной двухуровневой ИИС (ИД – источник данных).

Сбор и предварительная обработка данных о сетевом трафике промышленного Интернета вещей

В данной работе была использована следующая процедура определения информативных (значимых) параметров датасета. Лингвистические данные были кодированы целыми неотрицательными числами, получился диапазон значений [0; 65]; десятичные дроби, округленные до сотых, были умножены на 100; флаговые значения оставлены без изменений; остальные целочисленные неотрицательные значения – распределены в диапазоне [0; 255] следующим образом.

Для каждого параметра было выбрано пороговое значение, близкое к некоторому максимальному. Если исходное значение строго равно нулю, то «сжатое» значение также равно нулю. Если исходное значение больше нуля и не превышает порогового, то сжатие осуществляется равномерно так, чтобы сжатое значение лежало в диапазоне [1; 254]. Если исходное значение превышает пороговое, то сжатое равно 255. То есть:

$$y_i = \begin{cases} 255, & \text{если } x_i > P_i \\ 1 + \left\lfloor x_i : \left(\frac{P_i}{253}\right) \right\rfloor & \text{если } 0 < x_i \le P_i, \\ 0, & \text{если } x_i = 0 \end{cases} \quad (1)$$

где y_i – значение параметра после сжатия; x_i – значение параметра до сжатия; P_i – пороговое значение параметра.

В итоге значение каждого параметра после нормализации представляет собой целое неотрицательное число в диапазоне значений одного байта. Таким образом, исходный набор данных был нормализован, разделен на данные об атаках (A) и о нормальном состоянии (N). Для каждой строки A_i была найдена максимально похожая строка N_j в датасете, в качестве меры близости использовалось расстояние Хэмминга. Совпадающие параметры для каждой такой пары строк были отмечены. После чего был выполнен расчёт частоты совпадений по каждому параметру, ранжирование по наименьшей частоте совпадений.

На следующем этапе предполагается обучение используемого классификатора (СОА) на основе выбранного количества ранжированных параметров и оценка точности классификации. При ее недостаточности требуется увеличение числа параметров. Если точность классификации достаточна, стоит уменьшить количество параметров и повторить эксперимент для определения рационального количества анализируемых параметров.

Обработка трафика является двухуровневой: в первую очередь извлекаются выбранные параметры из файлов с расширением pcap (.pcap–файлов), NetFlow или других источников; если требуется, вычисляются дополнительные параметры. Затем параметры приводятся к анализируемому формату представления. Данные сетевого трафика должны поступать анализатору непрерывно, аналогично поступлению данных в SIEM-систему.

Данный алгоритм не предполагает какой-либо балансировки данных, содержащихся в датасете. Для многих интеллектуальных классификаторов необходимо наличие определенного количества образцов атак каждого класса для эффективного обучения, однако большинство датасетов содержит в том числе атаки, для которых представлено недостаточное количество образцов.

Данная проблема решается в [22], где предлагается применение алгоритма генеративных состязательных сетей для дополнения малочисленных атак сгенерированными образцами. В рамках выполненных в работе вычислительных экспериментов по оценке эффективности использования ИИС для обнаружения сетевых атак и аномалий использовались несбалансированные датасеты для дополнительного определения возможности ИИС выявлять атаки, представленные в малом количестве.

Результаты вычислительных экспериментов по оценке эффективности искусственной иммунной системы

Для оценки эффективности системы использовались следующие метрики [23, 24]:

- False Negatives (FN) – количество образцов атак, определенных как норма (ошибки второго рода);
- False Positives (FP) – количество образцов нормальной активности, определенных как атаки (ошибки первого рода);
- True Negatives (TN) – количество верно определенных образцов нормальной активности;
- True Positives (TP) – количество верно выявленных атак;
- False Negative Rate (FNR) – уровень ошибок второго рода:

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TP+FN}}; \quad (2)$$

- False Positive Rate (FPR) – уровень ошибок первого рода:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{TN+FP}}; \quad (3)$$

- True Negative Rate (TNR) – доля верно определенных образцов нормальной активности:

$$\mathrm{TNR} = \frac{\mathrm{TN}}{\mathrm{TN+FP}}; \quad (4)$$

- Recall (полнота, True Positive Rate, TRP, также обозначается как Sensitivity – чувствительность) – доля верно выявленных атак среди всех атак:

$$\mathrm{Recall} = \mathrm{TRP} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}; \quad (5)$$

- Precision (точность) – доля верно выявленных атак среди всех образцов, определенных как атаки:

$$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP+FP}}; \quad (6)$$

- Accuracy – доля верно классифицированных образцов среди всех образцов:

$$\mathrm{Accuracy} = \frac{\mathrm{TP+TN}}{\mathrm{TP+FP+TN+FN}}; \quad (7)$$

- F_1 score – среднее гармоническое точности (Precision) и полноты (Recall):

$$\mathrm{F_1score} = \frac{2\cdot\mathrm{Precision}\cdot\mathrm{Recall}}{\mathrm{Precision+Recall}}. \quad (8)$$

Эффективность ИИС была протестирована на датасете NSL-KDD в двух сериях экспериментов. В первой ИИС обучалась на половине данных датасета, включая и данные об атаках, и данные о нормальном состоянии сетевого взаимодействия, во второй – ИИС обучалась только с использованием половины данных о нормальном состоянии сетевого взаимодействия, и все атаки датасета являлись неизвестными для ИИС. Достигнутые значения показателей эффективности представлены в табл. 1.

Таблица 1

Значения показателей эффективности ИИС

№ серии экспериментов	FNR	FPR	TNR	TPR (Recall)	Precision	Accuracy	F_1 score
1	0.003	<0.001	0.999	0.997	0.999	0.998	0.998
2	0.005	<0.001	0.999	0.995	0.999	0.997	0.997

Таким образом, ИИС демонстрирует достижение высоких значений показателей эффективности как при обнаружении известных атак, так и при обнаружении неизвестных атак.

Гибридная распределенная интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей

Гибридная распределенная интеллектуальная система мониторинга (РИСМ) атак и аномалий сетевого трафика IIoT базируется на интеграции нескольких взаимодействующих между собой систем – распределенной многоагентной двухуровневой ИИС, системы классификации событий ИБ в виде комитета классификаторов и подсистемы корреляционного анализа данных (КАД) об инцидентах ИБ, в том числе полученных от внешней SIEM-системы. Структура РИСМ представлена на рис. 2.

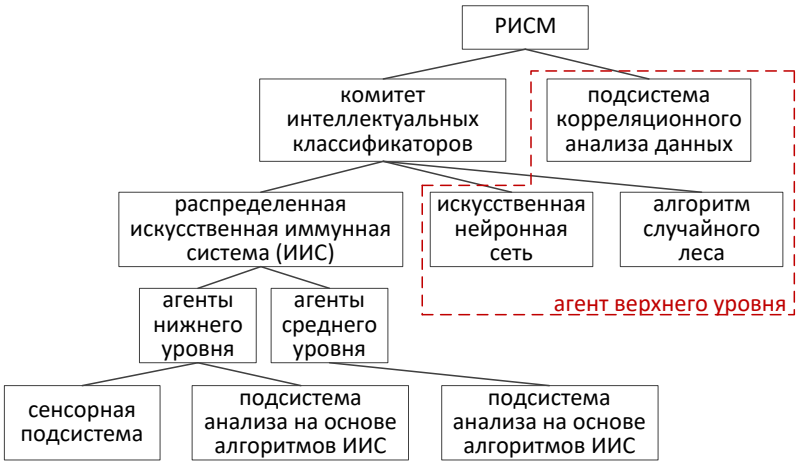

Рис. 2 Структура РИСМ.

Взаимодействие ИИС с подсистемой КАД схематично представлено на рис. 3.

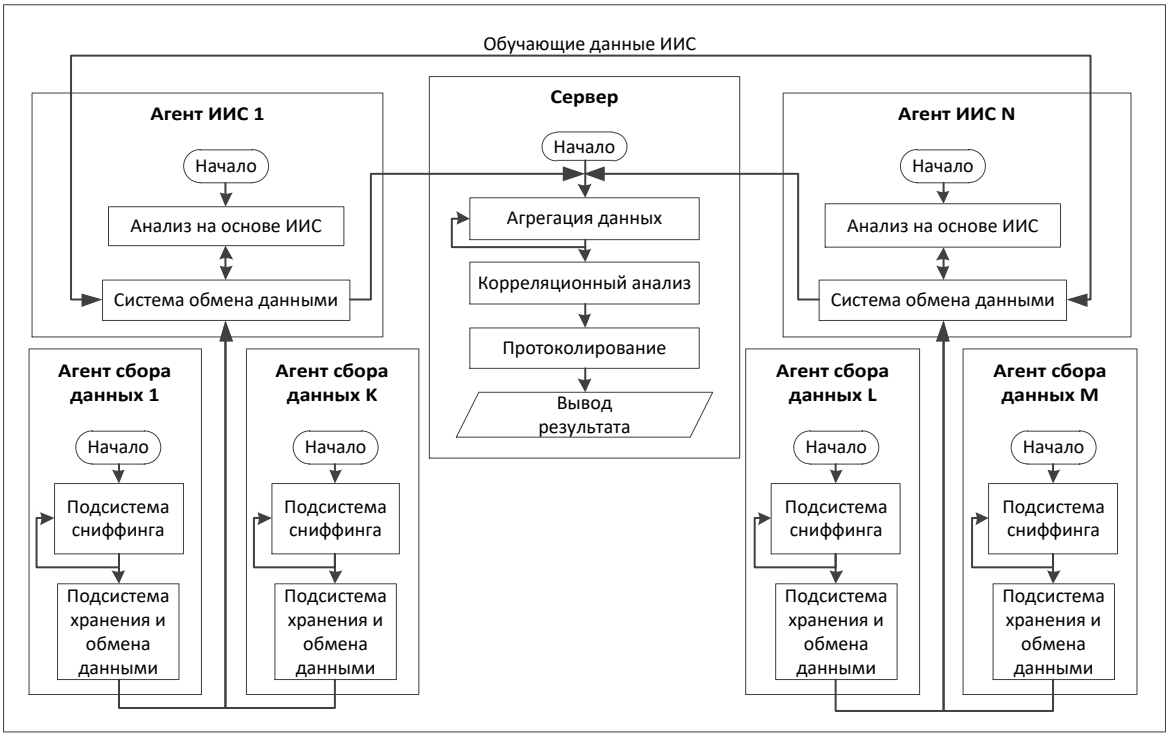

Рис. 3 Схема взаимодействия ИИС и подсистемы КАД.

На рис. 4 представлен пример отчета, формируемого подсистемой КАД.

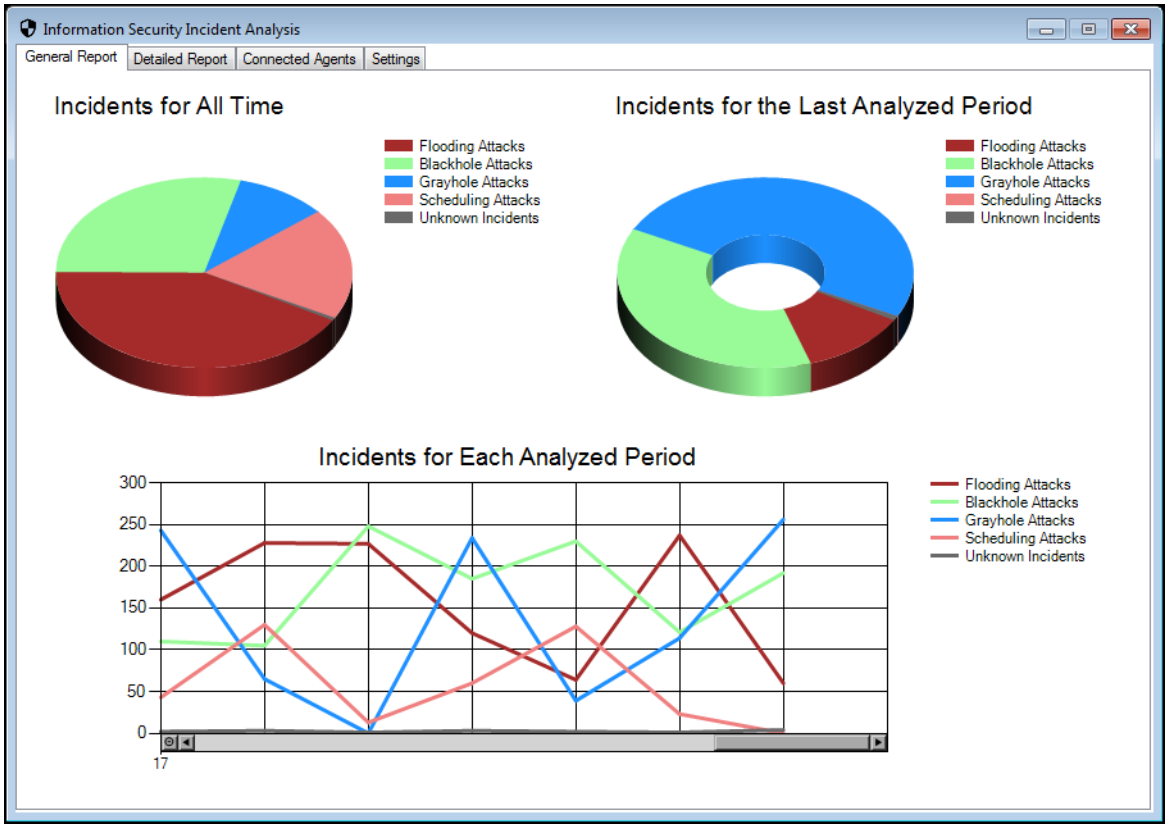

Рис. 4 Отчет, формируемый подсистемой корреляционного анализа инцидентов ИБ (опубликован в [25]).

Применение комитета классификаторов обусловлено выводами известной теоремы Кондорсе [26] о комитете экспертов (присяжных), согласно которой, если компетентность экспертов выше 0.5, то увеличение числа экспертов всегда приводит к повышению точности результата. Анализ литературных источников показал, что, как правило, в числе лидеров по эффективности обнаружения атак (без учета ИИС) оказываются такие методы машинного обучения, как искусственная нейронная сеть (ИНС) и алгоритм случайного леса (СЛ). Классификаторы были объединены в комитет согласно схеме, представленной на рис. 5.

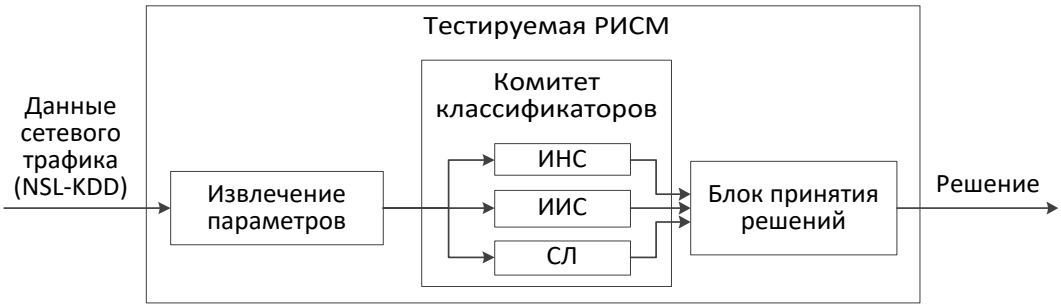

Рис. 5 Построение классификаторов в составе РИСМ.

Что касается механизма голосования, то, в первую очередь, была протестирована наиболее простая схема независимого голосования трех классификаторов по мажоритарному принципу, в соответствии с моделью простого объединения на уровне принятия решений. Взвешенное голосование не применялось, так как точность классификаторов была сопоставимо высокой.

Выбранный датасет NSL-KDD подвергся дополнительному балансированию с применением ресемплирования – SMOTE с KNN, для аугментации (расширения) маленьких классов до 5000 примеров и отбора по 15 000 примеров из двух классов с большим количеством исходных данных.

Система была обучена заново. ИИС была построена в варианте, предполагающем возможность классификации известных атак. Реализован алгоритм СЛ с оптимизацией гиперпараметров (перекрестная проверка, выбор по метрике F_1 score). Параметры СЛ оценены на тестовой выборке, не участвовавшей в оптимизации гиперпараметров.

Созданная ИНС была обучена на данных с контролем переобучения и ранним остановом. ИНС, аналогично СЛ, была проверена на основе тестовой выборки. Произведен выбор параметров архитектуры ИНС: количество нейронов в скрытом слое и коэффициент прореживания связей. По результатам экспериментов установлено, что оптимальной является архитектура с 32 нейронами в скрытом слое, использование которой обеспечивает минимальный уровень ошибок. Полученные значения показателей эффективности использования ИНС и СЛ представлены в табл. 2.

Таблица 2

Значения показателей эффективности ИНС, СЛ

Классификатор	FNR	FPR	TNR	TPR (Recall)	Precision	Accuracy	F_1 score
ИНС	0.003	0.013	0.987	0.997	0.985	0.992	0.991
СЛ	0.001	0.003	0.997	0.999	0.996	0.998	0.997

Доля верно классифицированных атак каждого i-го класса рассчитывается следующим образом:

$$P_i = \frac{A_i}{A_{0,i}} \times 100\%, \tag{9}$$

где $A_{0,i}$ – общее количество атак класса i; A_i – количество верно классифицированных атак класса i. Значение данного показателя по каждому классификатору и каждому анализируемому виду атак представлено на рис. 6.

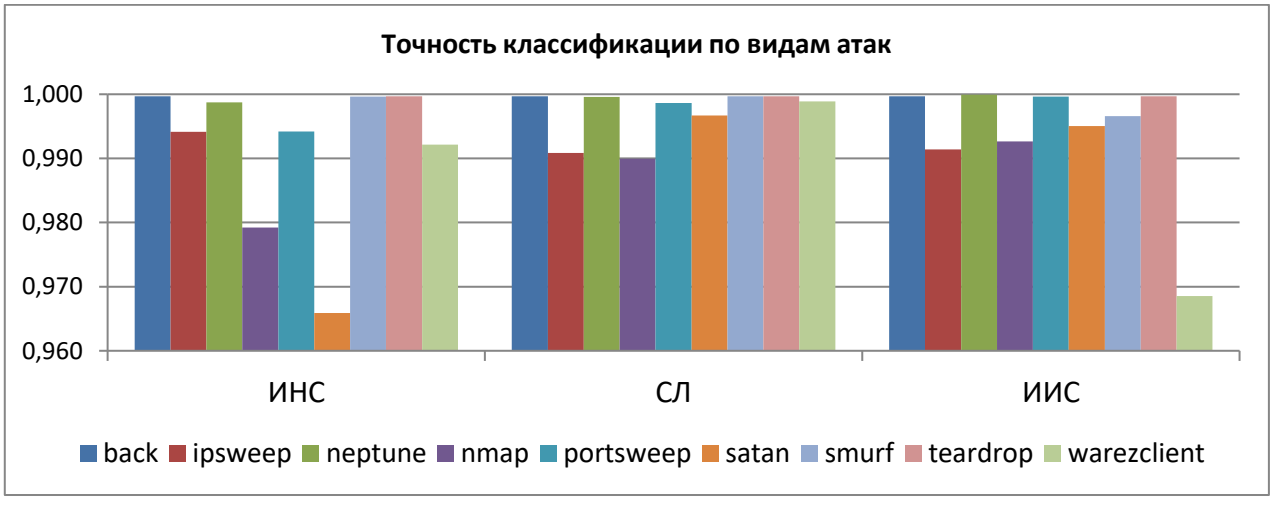

Рис. 6 Точность классификации по видам атак.

Полученные показатели эффективности комитета классификаторов представлены в табл. 3.

Таблица 3

Значения показателей эффективности ИИС, ИНС, СЛ и комитета классификаторов при принятии решений по мажоритарному принципу

Классификатор	FNR	FPR	TNR	TPR (Recall)	Precision	Accuracy	F_1 score
ИНС	0.003	0.013	0.987	0.997	0.985	0.992	0.991
СЛ	0.001	0.003	0.997	0.999	0.996	0.998	0.997
ИИС	0.002	0.001	0.999	0.998	0.999	0.999	0.998
Комитет классификаторов	0.001	0.002	0.998	0.999	0.998	0.998	0.998

Таким образом, по показателям FPR, TNR, Precision, Accuracy лучшие значения демонстрирует ИИС. Проведенный анализ показал, что ИИС благодаря негативной селекции допускает меньше ошибок первого рода. В абсолютных значениях ИИС выдала ошибку первого рода (False Positive) по 25 проанализированным образцам трафика, в то время как СЛ совершил 101 такую ошибку, а ИНС – 136. Таким образом, возникали ситуации, когда ИИС верно определяла экземпляр легитимного трафика, а СЛ и ИНС одновременно ошибались, что при голосовании на основе большинства давало в результате ошибку, и значения некоторых показателей эффективности комитета оказывались ниже, чем у ИИС. Поэтому механизм голосования был пересмотрен.

Рассматривался вариант увеличения веса мнения ИИС, но, с другой стороны, в точности классификации атак по 5 видам из 10 ИИС уступала другим классификаторам. Поэтому было принято решение – организовать механизм голосования на основе двухуровневой схемы: на первом этапе учитывается мнение ИИС: если она считает, что трафик соответствует нормальному (штатному) сетевому взаимодействию, то этого достаточно для определения экземпляра как соответствующего нормальному сетевому трафику. В противном случае, данные считаются соответствующими одной из атак и классифицируются на основе мнений большинства. Если все три классификатора выдают три разных решения, приоритет отдается мнению СЛ, так как его точность классификации атак выше. Полученные результаты при использовании двухуровневой схемы голосования представлены в табл. 4.

Таблица 4

Значения показателей эффективности ИИС, ИНС, СЛ и комитета классификаторов при двухуровневом принятии решения

Классификатор	FNR	FPR	TNR	TPR (Recall)	Precision	Accuracy	F_1 score
ИНС	0.003	0.013	0.987	0.997	0.985	0.992	0.991
СЛ	0.001	0.003	0.997	0.999	0.996	0.998	0.997
ИИС	0.002	0.001	0.999	0.998	0.999	0.999	0.998
Комитет классификаторов	0.001	0.001	0.999	0.999	0.999	0.999	0.999

Таким образом, при данном подходе комитет классификаторов демонстрирует наилучшие значения показателей эффективности.

Эффективность предлагаемой РИСМ оценивалась на тестовой IIoT-системе контроля уровня и мутности воды в резервуаре, которая, в свою очередь, входит в состав автоматизированной системы очистки и распределения воды в промышленных резервуарах. Проводились вычислительные эксперименты по обнаружению атак на основе датасета WUSTL-IIOT-2021, созданного его авторами на основе сетевого взаимодействия элементов указанной IIoT-системы, в том числе во время имитированных сетевых атак. Рассматривались несколько вариантов построения ИИС, ИНС, СЛ, оценивались значения показателей эффективности отдельных алгоритмов и комитета классификаторов. Совокупность показателей эффективности комитета классификаторов оказалась выше. По метрикам: Precision, Recall, Accuracy, F_1 score, TNR, TPR достигнуты значения 0.999 на основе тестового набора данных.

Разработанная РИСМ была также протестирована на основе данных испытательного стенда беспроводной сенсорной сети, состоящей из 100 сенсорных узлов, объединенных в 5 кластеров. На основе взаимодействия элементов этой сети, в том числе во время имитированных сетевых атак, авторами стенда был создан датасет WSN-DS, содержащий атаки на протокол LEACH, часто используемый в WSN. Проведены ряд вычислительных экспериментов по оценке эффективности РИСМ в выявлении атак WSN-DS, в том числе с применением различных мер близости в ИИС. Результаты экспериментов показали рациональность применения расстояния Хэмминга, а также комитета классификаторов: ИИС, ИНС, СЛ, продемонстрировавшего высокую эффективность обнаружения и классификации атак на WSN.

Таким образом, разработана гибридная распределенная интеллектуальная система мониторинга информационной безопасности сетей промышленного Интернета вещей, которая выполняет многоуровневое принятие решения: выявление аномалии агентами искусственной иммунной системы нижнего уровня, определение опасности аномалии и необходимости идентификации ее как атаки агентами искусственной иммунной системы верхнего уровня, определение класса атаки комитетом классификаторов, установление уровня значимости инцидента ИБ на основе корреляционного анализа данных. Проведенные вычислительные эксперименты продемонстрировали достижение разработанной системой высоких значений показателей эффективности, превышающие значения таких показателей для каждого интеллектуального классификатора по отдельности.

Благодарности и поддержка

Работа выполнена при поддержке гранта РФФИ № 20-37-90024. Авторы также отмечают работы [27–32], оказавшие косвенное влияние на данное исследование.

Список литературы / References

1. Industrial Internet of Things – IIoT. Промышленный Интернет вещей [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:IIoT_–_Industrial_Internet_of_Things_(Промышленный_интернет_вещей) (дата обращения: 12.08.2024) [[(2024, August 12). Industrial Internet of Things – IIoT. [Online], (in Russian). URL: https://www.tadviser.ru]]
2. Threat intelligence report. Nokia.com, 2020. [Online]. Available: https://pages.nokia.com/T005JU-Threat-Intelligence-Report2020.html?_ga=2.216248470.1653315497.1608038999-829562352.1608038999 (Accessed Sept. 23, 2021).
3. Что угрожает промышленному Интернету вещей и как от этого защититься [Электронный ресурс]. URL: https://vc.ru/kaspersky/265770-chto-ugrozhaet-promyshlennomu-internetu-veshchey-ikak-ot-etogo-zashchititsya (дата обращения: 30.07.2021). [[(2021, July 30). What Threatens the Industrial Internet of Things and How to Protect It [Online], (in Russian). URL: https://vc.ru/kaspersky/265770-chto-ugrozhaet-promyshlennomu-internetu-veshchey-ikak-ot-etogo-zashchititsya]]
4. Лаборатория Касперского: распространение умных устройств в промышленности повлечёт за собой смену подхода к киберзащите [Электронный ресурс]. URL: https://www.kaspersky.ru/about/pressreleases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-vpromishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite (дата обращения: 30.07.2021). [[(2021, July 30). Kaspersky Lab: The spread of smart devices in industry will lead to a change in the approach to cybersecurity [Online], (in Russian). URL:https://www.kaspersky.ru/about/pressreleases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-vpromishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite]]
5. Check Point IoT Protect // CheckPoint.com [webcite]. Available: https://www.checkpoint.com/downloads/products/cp-iot-security-solution-brief.pdf (Accessed: March 13, 2021).

6. ПНСТ 643-2022 Информационные технологии. Интернет вещей промышленный. Термины и определения: предварительный национальный стандарт РФ. [[PNST 643-2022. Preliminary national standard of Russian Federation. Information technology. Industrial Internet of Things. Terms and definitions, (in Russian).]]
7. ПНСТ 420-2020 Информационные технологии. Интернет вещей промышленный. Типовая архитектура: предварительный национальный стандарт РФ. [[PNST 420-2020. Preliminary national standard of the Russian Federation. Information technology. Industrial Internet of Things. Typical architecture, (in Russian).]]
8. Sen J. Security in wireless sensor networks // Wireless Sensor Networks: Current Status and Future Trends. New York: CRC Press, 2012. Pp. 407–460.
9. Информационная безопасность цифрового пространства / Е. В. Стельмашонок, И. Н. Васильева. СПб.: Изд-во СПбГЭУ, 2019. 155 с. [[Information security of digital space, (in Russian) / E. V. Stelmashonok, I. N. Vasileva. St. Petersburg, 2019.]]
10. Ammar M., Russello G., Crispo B. Internet of things: a survey on the security of IoT frameworks // Journal of Information Security and Applications. 2003. No. 38. Pp. 8–27.
11. Милославская Н. Г. Центры управления информационной безопасностью // Безопасность информационных технологий. 2016. № 4(23). С. 38–51. [[Miloslavskaya N. G. // Bezopasnost' informatsionnykh tekhnologiy, 2016, vol. 4(23), pp. 38-51, (in Russian).]]
12. Березин Д. Как сегодня строится центр оперативного управления информационной безопасностью (SOC-центр) [Электронный ресурс]. URL: https://habr.com/ru/company/croc/blog/353324/ (дата обращения 31.05.2020). [[D. Berezin. (2020, May 31). How a Security Operations Center (SOC) is built today [Online]. URL: https://habr.com/ru/company/croc/blog/353324 (In Russian).]]
13. Кушнир Е. Протоколы Интернета вещей: как обмениваются данными IoT-устройства, серверы и пользовательские приложения [Электронный ресурс]. URL: https://mcs.mail.ru/blog/protokoly-interneta-veschej (дата обращения: 11.06.2023). [[E. Kushnir (2023, June 11). [Online]. (In Russian). URL:https://mcs.mail.ru/blog/protokoly-interneta-veschej]]
14. Сычугов А. А. Информационная система оперативного обнаружения опасных состояний промышленных объектов // Известия ТулГУ. Технические науки. 2021. № 10. С. 401–406 [[Sychugov A. A. // Izvestiya TulGU. Tekhnicheskie nauki, no. 10, pp. 401–406, 2021. (In Russian).]]
15. Старовойтов В. В., Голуб Ю. И. Нормализация данных в машинном обучении // Информатика. 2021. Т. 18. № 3. С. 83–96. [[V. V. Starovoitov, Yu. I. Golub // Informatika. 2021, Vol. 18, no. 3, pp.83–96. (in Russian).]]
16. Умная нормализация данных [Электронный ресурс]. URL: https://habr.com/ru/articles/527334/ (дата обращения 11.06.2023). [[(2023, June 11). Smart Data Normalization [Online], (in Russian). URL: https://habr.com/ru/articles/527334]]
17. Брюхомицкий Ю. А. Искусственные иммунные системы в информационной безопасности. Ростов н/Д; Таганрог: ЮФУ, 2019. 142 с. [[Yu. A. Bryukhomitskii. Artificial Immune Systems in Information Security, (in Russian). Rostov-on-Don–Taganrog: SFU, 2019.]]
18. Бурлаков М. Е., Ивкин А. Н. Система обнаружения вторжения на основе искусственной иммунной системы // Вестник ПНИПУ. 2019. № 29. С. 209–224. [[M. E. Burlakov, A. N. Ivkin, “Intrusion detection system based on artificial immune system” // Vestnik PNIPU. No. 29, pp. 209–224, 2019. (In Russian).]]
19. Васильев В. И., Вульфин А. М., Гвоздев В. Е., Шамсутдинов Р. Р. Комплексирование механизмов искусственных иммунных систем в составе интегрированной системы обнаружения атак на промышленный Интернет вещей // МОИТ. 2022. Т. 10. № 4(39). С. 13–14. DOI 10.26102/2310-6018/2022.39.4.001. EDN JTHNVH. [[V. I. Vasil'ev, A. M. Vul'fin, V. E. Gvozdev, R. R. Shamsutdinov // MOIT, vol. 10, no. 4, 2022. DOI 10.26102/2310-6018/2022.39.4.001. EDN JTHNVH. (In Russian).]]
20. Еременко Ю. И., Глущенко А. И. О решении неформализуемых и плохоформализуемых задач методами иммунных алгоритмов // Информационные технологии. 2011. № 7. С. 2–7. [[Yu. I. Eremenko , A. I. Glushchenko // Informatsionnye tekhnologii, no. 7, pp. 2–7, 2011. (In Russian).]]
21. Частикова В. А., Картамышев Д. А. Искусственные иммунные системы: основные подходы и особенности их реализации // Научные труды КубГТУ. 2016. № 8. С. 193–208. [[V. A. Chastikova, D. A. Kartamyshev (in Russian) // Nauchnye trudy KubGTU, no. 8, pp. 193-208, 2016.]]
22. Сычугов А. А., Греков М. М. Применение генеративных состязательных сетей в системах обнаружения аномалий // МОИТ. 2021. № 9(1). [[A. A. Sychugov, M. M. Grekov // MOIT, no. 9(1), 2021. (In Russian).]]
23. Основные метрики задач классификации в машинном обучении // Webiomed [Электронный ресурс]. URL: https://webiomed.ru/blog/osnovnye-metriki-zadach-klassifikatsii-v-mashinnomobuchenii/ (дата обращения 24.05.2023). [[(2023, May 24). Key Metrics for Classification Problems in Machine Learning // Webiomed [website], (in Russian). URL: https://webiomed.ru/blog/osnovnye-metriki-zadach-klassifikatsii-v-mashinnomobuchenii]]
24. Karabiber F. Precision and recall // LearnDataSci [website]. Available: https://www.learndatasci.com/glossary/precision-and-recall/ (Accessed May 24, 2023).
25. Vasilyev V., Shamsutdinov R. Security analysis of wireless sensor networks using SIEM and multi-agent approach // Proceedings 2020 Global Smart Industry Conference. GloSIC. Chelyabinsk. 2020. Nov 17–19, 2020. Chelyabinsk, 2020. Pp. 291–296. DOI 10.1109/GloSIC50886.2020.9267830. EDN QNOXGT.
26. Estlund D.M. Opinion leaders, independence, and Condorcet's jury theorem // Theory and Decision. 1994. Vol. 36. Pp. 131–162.
27. Бакулин М. А. Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры // СИИТ. 2023. Т. 5. № 5(14). С. 78–87. EDN CRVUZJ. [[Bakulin M. A. “Risk management

of information security breaches of significant objects of critical information infrastructure" // SIIT. 2023. Vol. 5, No. 5(14). pp. 78-87. EDN CRVUZJ. (In Russian).]]

28. Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // СИИТ. 2023. Т. 5. № 4(13). С. 50–76. EDN FJPFKC. [[Vulfin A. M. "Models and methods for comprehensive assessment of security risks of critical information infrastructure facilities based on intelligent data analysis" // SIIT. 2023. Vol. 5, No. 4(13), pp. 50-76. EDN FJPFKC. (In Russian).]]
29. Кириллова А. Д. Оценка рисков информационной безопасности АСУ ТП промышленных объектов методами когнитивного моделирования // СИИТ. 2023. Т. 5. № 4(13). С. 77–93. EDN CUEUUP. [[Kirillova A. D. "Assessment of information security risks of industrial control systems using cognitive modeling methods" // SIIT. 2023. Vol. 5, No. 4(13), pp. 77-93. EDN CUEUUP. (In Russian).]]
30. Махмутов А. Р., Вульфин А. М., Миронов К. В. Исследование возможностей автономной работы конечных устройств интернета вещей // СИИТ. 2023. Т. 5. № 1(10). С. 41–47. EDN DPEMFA. [[Makhmutov A. R., Vulfin A. M., Mironov K. V. "Study of the possibilities of autonomous operation of end devices of the internet of things" // SIIT. 2023. Vol. 5, No. 1(10), pp. 41-47. EDN DPEMFA. (In Russian).]]
31. Fabarisov T., Siedel G., Vock S., Morozov A. Aspects of Industrial CPS critical for risk assessment methods // SIIT. 2021. Vol. 3. No. 3(7). Pp. 23–29. DOI 10.54708/26585014_2021_33723. EDN JUPLEJ.
32. Васильев В. И., Картак В. М. Применение методов искусственного интеллекта в задачах защиты информации (по материалам научной школы УГАТУ) // СИИТ. 2020. Т. 2. № 2(4). С. 43–50. EDN ZTQFCW. [[Vasiliev V. I., Kartak V. M. "Application of artificial intelligence methods in information security problems (based on the materials of the scientific school of Ufa State Aviation Technical University)" // SIIT. 2020. Vol. 2, No. 2(4), pp. 43-50. EDN ZTQFCW. (In Russian).]]

Поступила в редакцию 17 августа 2024 г.

МЕТАДАННЫЕ / METADATA

Title: Intelligent system for monitoring information security of the industrial internet of things using artificial immune systems mechanisms.

Abstract: The article is devoted to solving the problem of detecting network attacks on Industrial Internet of Things systems based on the integration of artificial intelligence methods with the use of artificial immune system mechanisms. It is emphasized that Industrial Internet of Things systems occupy an important place in Industry 4.0, are widely used to overcome production challenges, and are characterized as heterogeneous distributed systems that still have an insufficient level of protection against information security threats. The article discusses the most common reasons for the poor security of such systems, their specificity, and features of monitoring the information security of their networks. The possibility of using a distributed two-level multi-agent system for detecting network attacks based on the integration of the main algorithms and approaches of the theory of artificial immune systems is considered. The resulting synergistic effect of such integration is emphasized. The solution to the subtask of normalizing the analyzed network traffic data is considered. A series of computational experiments have been conducted, which showed the high efficiency of the proposed solution. A three-level hybrid distributed intelligent system for monitoring the information security of the industrial Internet of Things has been developed, integrating the developed two-level artificial immune system, a random forest algorithm, an artificial neural network, and a data correlation analysis subsystem. This system performs multi-level decision making detecting anomalies by lower-level the agents of artificial immune system, determining the danger of anomalies and the need to identify them as attacks by upper-level agents of the artificial immune system, determining the attack class by a committee of classifiers, and establishing the level of incident significance based on data correlation analysis.

Key words: Industrial Internet of Things; Information Security; Artificial Immune System; Intelligent System; Cybersecurity

Язык статьи / Language: русский / Russian.

Поддержка/Support: РФФИ, грант № 20-37-90024.

Об авторах / About the authors:

ШАМСУТДИНОВ Ринат Рустемович
Уфимский университет науки и технологий, Россия.
Каф. вычислительной техники и защиты информации. Дипл. магистр по информ. безопасности (Уфимск. гос. авиац. техн. ун-т, 2018). Канд. техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. ун-т науки и технологий, 2023). Иссл. в обл. обнаружения сетевых атак.
E-mail: shrr2019@yandex.ru
ORCID: https://orcid.org/0000-0002-4178-5284
URL: https://elibrary.ru/author_items.asp?authorid=909032

ВАСИЛЬЕВ Владимир Иванович
Уфимский университет науки и технологий, Россия.
Проф. каф. вычислительной техники и защиты информации. Дипл. инж. по пром. электронике (Уфимс. авиац. ин-т, 1970). Д-р техн. наук по управлению в техн. системах (ЦИАМ, 1990).

SHAMSUTDINOV Rinat Rustemovich
Ufa University of Science and Technology, Russia.
Dept of Computer Science and Information Security. Master's degree in information security (Ufa State Aviation Technical University, 2018). Cand. of Technical Sciences in methods and systems of information security (Ufa University of Science and Technology, 2023). Research in the field of network attack detection.
E-mail: shrr2019@yandex.ru
ORCID: https://orcid.org/0000-0002-4178-5284
URL: https://elibrary.ru/author_items.asp?authorid=909032

VASILYEV Vladimir Ivanovich
Ufa University of Science and Technology, Russia.
Prof., Dept. of Computer Technology and Information Security. Dipl. Eng. on industrial electronics (Ufa Aviation Institute, 1970). Dr. of Tech. Sci. (CIAM, 1990). Research in the field of intelligent

Иссл. в обл. интел. систем управления сл. орг.-техн. объектами, информ. безопасности.
E-mail: vas0015@yandex.ru
ORCID: http://orcid.org/0000-0002-1825-0097
URL: https://elibrary.ru/author_items.asp?authorid=111073

ВУЛЬФИН Алексей Михайлович
Уфимский университет науки и технологий, Россия.
Проф. каф. вычислительной техники и защиты информации. Дипл. инж.-программист (Уфимск. гос. нефтяной техн. ун-т, 2008). Д-р техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. гос. авиац. техн. ун-т, 2022). Иссл. в обл. информ. безопасности, интел. систем, нечеткого и нейросетевого моделирования.
E-mail: vulfin.alexey@gmail.com
ORCID: https://orcid.org/0000-0001-5857-2413
URL: https://elibrary.ru/author_profile,asp?id=1051942

control systems for organizational and technical objects, information security.
E-mail: vas0015@yandex.ru
ORCID: http://orcid.org/0000-0002-1825-0097
URL: https://elibrary.ru/author_items.asp?authorid=111073

VULFIN Alexey Mikhailovich
Ufa University of Science and Technology, Russia.
Prof., Dept. of Computer Technology and Information Security. Dipl. software engineer (Ufa State Oil Techn. Uni., 2008). Dr. of Technical Sciences in information security methods and systems (Ufa State Aviation Technical Univ., 2022). Research in the field of information security, intelligent systems, fuzzy and neural network modeling.
E-mail: vulfin.alexey@gmail.com
ORCID: https://orcid.org/0000-0001-5857-2413
URL: https://elibrary.ru/author_profile,asp?id=1051942