АДАПТИВНАЯ СИСТЕМА ЗАЩИТЫ СЕНСОРНЫХ СЕТЕЙ ОТ АКТИВНЫХ АТАК

Басан А.С.[1], Басан Е.С.[2], Пескова О.Ю.[3], Сушкин Н.А.[4], Шулика М.Г.[5]

Цель: *Разработка архитектуры адаптивной системы защиты сенсорных сетей и киберфизических систем для обнаружения аномалий на основе сбора и анализа киберфизических параметров системы.*

Методы исследования: *Метод основывается на использовании математического аппарата теории вероятностей, математической статистики и теории информации. Мера энтропии и нормализация необработанных данных позволяют унифицировать данные и оценивать их с точки зрения обнаружения аномалий.*

Результаты: *Выполнен анализ существующих решений по защите киберфизических систем от внешних активных атак злоумышленника. Предложена архитектура адаптивной системы защиты киберфизической системы. В рамках представления подсистемы сбора и анализа данных узла предложен метод оценки киберфизических параметров с целью обнаружения вторжений. В данном исследовании подробно изучались изменения трех параметров для четырех сценариев поведения. Уже на этом этапе по трем параметрам можно определить разницу между атаками и вариантами нормального поведения. Можно оценить не только факт изменения параметра, но и степень его изменения. При этом узел автономно сравнивал свои изменения с изменениями соседнего узла и мог выявить влияние атаки на соседа.*

Научная новизна *состоит прежде всего в том, что разработан метод определения аномальной активности киберфизической системы на основе оценки параметров системы с использованием меры энтропии и нормализации необработанных данных, что позволяет достичь высокого уровня обнаружения известных и неизвестных атак режиме реального времени. Этот метод может эффективно использоваться в том числе и для автономных систем. Также предложена оригинальная архитектура адаптивной системы защиты киберфизической системы, проработаны ее основные компоненты. При реализации атаки в распределенной системе, данная разработка позволит обнаруживать аномалии узлу не только автономно, но и распределено, то есть обнаруживать воздействие на соседние узлы.*

Вклад каждого соавтора: *Басан Е.С. — общее руководство проектом, разработка структурной схемы предлагаемой системы защиты КФС, разработка метода определения аномальной активности киберфизической системы; Басан А.С. — разработка структуры и механизмов подсистемы сбора и анализа данных, а также подсистемы обнаружения атак и вторжений; Пескова О.Ю. – проведение анализа существующих методов и систем киберфизической безопасности; Сушкин Н.А. — проведение эксперимента, анализ результатов; Шулика М.Г. — подготовка наборов данных для проведения и анализа результатов эксперимента.*

Ключевые слова: *анализ данных, статистика, аномалии, атаки, риски, кибер-физические системы.*

DOI:10.21681/2311-3456-2022-6-22-39

Введение

В данном исследовании сенсорная сеть рассматривается как часть киберфизической системы. На сегодняшний день киберфизические системы внедряются в различные сферы деятельности человека. Умные датчики используются для построения систем интернета вещей (IoT), групп мобильных ро-

1 Басан Александр Сергеевич, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: asbasan@sfedu.ru.

2 Басан Елена Сергеевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

3 Пескова Ольга Юрьевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: oyupeskova@sfedu.ru, ORCID 0000-0002-6397-6970.

4 Сушкин Никита Андреевич, аспирант кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: sushkin@sfedu.ru.

5 Шулика Мария Геннадьевна, аспирант кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: mshulika@sfedu.ru.

ботов, умных автомобилей и т. д. [1]. В процессе создания и эксплуатации этих систем ключевым понятием становится кибербезопасность [2]. Поскольку киберфизические системы (КФС) строятся на новых архитектурных решениях и принципах, то им свойственны новые угрозы кибербезопасности [3]. Например, для построения КФС часто используется кластеризация, иногда в кластере выбирается лидер. Внедрение злоумышленника в такую схему может привести к тому, что он станет лидером кластера или повлияет на разбиение узлов по группам. В результате не только будут нарушены информационные потоки и процессы, но и будет оказано влияние на физический мир. Эта проблема особенно актуальна для систем, управляющих физическим объектом или активом [4].

Некоторые решения по защите КФС включают использование технологии блокчейн, которая должна обеспечивать доверенное использование инфраструктуры на базе сенсорной сети, что, в итоге, повышает безопасность [5]. Блокчейн является достаточно сложной и ресурсоемкой технологией, при этом доверие достигается путем использования подписей, как и в классической криптографии [6].

Еще одним популярным решением для обеспечения безопасности КФС являются методы аутентификации на основе глубокого обучения [7]. В то же время исследователи ищут новые признаки оценки поведения, которые легли бы в основу аутентификации [8]. Однако криптографические методы и методы аутентификации не всегда могут обеспечить полную безопасность системы. Нередко сенсорная система может располагаться вне контролируемой зоны, в природных условиях или на открытом воздухе. Узлы системы могут быть мобильными, архитектура системы может периодически обновляться и дополняться новыми узлами [9]. Кроме того, многие сенсорные системы основаны на беспроводных сетях, которые не защищены физически [10]. Даже если узлы шифруют трафик и аутентифицируют друг друга, это не защитит их от активных атак, деструктивных воздействий и не поможет обнаружить внешние воздействия [11].

Одним из решений повышения безопасности КФС может стать модернизация архитектуры сети, улучшение ее физических свойств. В статье [12] авторы предлагают модифицировать концепцию безопасности для архитектуры систем разработанных с учетом концепции четвертой промышленной революции (Индустрия 4.0) и внедрять решения безопасности на аппаратном уровне.

Поведенческие меры безопасности и алгоритмы для сети автомобилей были предложены в [13]. Авторы концентрируются на оценке поведения транспортных средств самими элементами сети. Выявляются различные типы поведения автомобиля, которые в итоге влияют на уровень доверия к нему. При этом необходимо соблюдать определенные условия, такие, например, как расстояние до соседнего автомобиля и количество соседей. Авторы утверждают, что даже если количество злоумышленников превысит 50%, то система сможет их обнаружить.

В статье [14] авторы используют статистические методы и методы машинного обучения для выявления аномалий. При этом авторы анализируют временные ряды, классифицируя их следующим образом: периодические, стационарные, непериодические и нестационарные временные ряды. Затем к разным классам временных рядов применяются разные схемы для обнаружения аномалий. Авторы заявляют, что их метод Tri-CAD дает наилучшие результаты оценки.

Авторы работы [15] анализируют безопасность и производительность наиболее популярных протоколов безопасной маршрутизации Low-Energy Adaptive Clustering Hierary (LEACH) [16] и Energy-Efficient Sensor Routing (EESR), подкластера LEACH. Они доказывают, что наиболее успешным решением является метод LEACH классификации ближайших соседей – Large margin nearest neighbor (LMNN), который показывает наилучшую производительность [17]. Авторы также предлагают систему обнаружения вторжений. Они используют методы нормализации данных и кодирования для лучшей обработки данных.

Шнайдер и др. [18] используют готовый набор данных для оценки своего метода [19]. Авторы анализируют различные методы обнаружения атак и аномалий, основанные на алгоритмах машинного обучения для защиты от угроз кибербезопасности Интернета вещей. В отличие от существующих работ, использующих отдельные классификаторы, они также анализируют ансамблевые методы, такие как упаковка, усиление и суммирование, для повышения производительности системы обнаружения [20–23]. Авторы объединяют набор функций: перекрестную проверку и мультиклассовую классификацию для области кибербезопасности. Экспериментальные результаты, выполненные с использованием общедоступного набора данных об атаках, показывают, что этот метод может эффективно выявлять кибератаки.

Таким образом, следует отметить актуальность темы обеспечения информационной безопасности

КФС, и, в частности, обнаружения аномалий. Однако авторы часто акцентируют внимание на методах машинного обучения, а не на критериях классификации. В большинстве исследований для анализа и выявления аномалий берутся готовые базы данных. При этом от качества используемых данных будет в большей степени зависеть конечный результат обнаружения. Данное исследование концентрируется на выявлении признаков атаки.

Одной из задач исследования является изучение изменений киберфизических параметров под влиянием атаки при нормальном функционировании и с дополнительной нагрузкой. Необходимо выявить признаки воздействия, которые могут дать новый толчок к исследованию аномалий в сенсорной системе. Кроме того, исследование должно дать возможность создания собственной базы данных, которую можно считать достоверной для обучения искусственного интеллекта. Полученную базу данных можно также использовать для тестирования различных методов классификации.

Приоритетной задачей исследования является определение признаков атаки и анализ киберфизических параметров, как нового вектора оценки атаки. В этой статье также затрагиваются вопросы нормализации данных. Предполагается, что за счет нормализации и выявления пороговых значений на этапе эксперимента в дальнейшем метод можно будет применять к любой КФС без предварительного обучения.

Рис. 1. Блок-схема системы адаптивной защиты сенсорного узла в киберфизической системе на примере БПЛА

1. Адаптивная защита киберфизической системы для обнаружения аномалий

Основные задачи, которые решает система:

— Детектирование аномалий с помощью анализа параметров узла системы;
— Своевременное оповещение оператора и соседних узлов о возможном инциденте;
— Определение типа атаки.

Общая структурная схема предлагаемой системы защиты представлена на рис. 1. На этой схеме показаны основные модули и подсистемы, а также их интеграция в систему датчиков.

Предлагаемая система адаптивной защиты функционирует следующим образом. Подсистема анализа данных узла собирает информацию об изменении киберфизических параметров. Данная подсистема получает данные от оборудования, из которого состоит узел (это могут быть как компоненты самого узла, так и сенсоры и актуаторы, которые связаны с узлом). Идея состоит в том, что, анализируя киберфизические параметры на протяжении всей работы сенсорной системы, можно обнаружить наличие аномалий, которые могут быть признаками активной атаки на сенсорную систему. Под киберфизическими параметрами в данном случае подразумеваются параметры, отражающие изменения как в программном обеспечении, так и в физических компонентах узла.

В состав подсистемы сбора и анализа данных узла кроме модуля сбора данных также входит модуль обработки и нормализации данных. Использование необработанных данных может быть неэффективным по нескольким причинам. Во-первых, необработанные данные требуют больше памяти и вычислительной мощности. Во-вторых, в процессе использования необработанных данных могут возникать ложные срабатывания, также может усиливаться влияние неточности измерений, что должно быть сглажено.

В данном исследовании для нормализации данных использовались методы теории вероятностей. Для определения типов распределения вероятностей для каждого параметра были построены квантильные диаграммы. Метод квантильных диаграмм помогает определить тип распределения случайной величины.

Подсистема сбора и анализа данных узла собирает информацию от аппаратных устройств, датчиков и исполнительных устройств об использовании ЦПУ, энергопотреблении и ресурсах памяти, сетевом трафике и т. д. Затем данные нормализуются и передаются в модуль анализа данных сенсорного узла.

Преимущества использования подсистемы сбора и анализа данных заключаются в следующем:

— возможность передачи собранных и нормализованных данных в другие подсистемы;
— возможность просто представить собранные данные в удобном для анализа формате.

На рис.1, представленном выше, показана схема использования киберфизических параметров и аппаратной части сенсорного узла модулями системы адаптивной защиты. Из этой схемы видно, что к аппаратному обеспечению обращается только подсистема анализа данных сенсорного узла, именно она снимает показания с датчиков, вычислительных ресурсов, исполнительных механизмов и получает набор киберфизических параметров. Остальные модули системы обращаются только к сетевому адаптеру для передачи и получения сообщений и работают с обработанными данными.

Таким образом, преимуществом подсистемы сбора и анализа данных сенсорного узла является использование одного набора данных для решения разных задач обеспечения защиты, а также уменьшение количества обращений программных модулей к аппаратным средствам. Во-первых, это обеспечивает большую надежность, поскольку сенсорный узел во многом является интеллектуальной системой и описывается процессами, при этом необходимо рассматривать разные процессы в рамках единой системы управления. Если говорить о построении системы защиты, то каждый процесс должен быть авторизован, а его доступ к оборудованию должен контролироваться и фиксироваться; в противном случае возможен сбой системы, и т. д. Следовательно, чем меньше будет таких обращений, тем проще с точки зрения безопасности будут обрабатываться эти события. Во-вторых, работа программных модулей с подготовленными наборами данных ускоряет процесс принятия решений, что уменьшает время отклика и, в то же время, увеличивает производительность системы. Злоумышленник может проводить целенаправленные атаки на определенные киберфизические параметры, а может проводить атаки, косвенно влияющие на физические свойства системы [24]. Например, есть атака на исчерпание заряда аккумулятора устройства, а есть атака на переполнение сети с ложными запросами на подключение к узлу, которым может быть узел сети. При этом эффект от обеих атак может быть схожим, например, в том, что в обоих случаях аккумулятор быстрее расходует заряд, а может и различаться, к примеру в том, что атака на переполнение ложными запросами еще и влияет на сетевой трафик.

В зависимости от того, какие киберфизические параметры изменили свое значение и в какой степени, можно определить не только тип или класс атаки, но и установить, какая конкретно атака была реализована на систему.

В основе обнаружения атак и вторжений для подсистемы адаптивной защиты узла лежит детектирование аномалий или аномального поведения. В результате деструктивного воздействия состояние сенсорной системы изменяется и переходит из нормального состояния в аномальное.

Основные задачи подсистемы:

— обнаружение аномалий и установление связи между аномалией и атакой;
— обмен информацией с другими модулями системы.

Аномалии и отказы в обслуживании могут возникать не только в результате преднамеренной атаки, но и вследствие внешних природных воздействий или сбоев, связанных с ошибками, допущенными при проектировании системы. Необходимо исследовать процесс диагностики, прогнозирования, мониторинга и принятия решений в режиме реального времени с использованием данных, полученных как от отдельного сенсорного узла, так и от системы в комплексе.

Подсистема обнаружения атак и вторжений на систему классифицирует обнаруженную аномалию, как атаку и определяет ее тип. Узел может быть захвачен злоумышленником и использован в качестве атакующего узла. Либо злоумышленник может использовать его с целью нанести ущерб остальной части системы из-за технического, системного сбоя. Тип атаки определяется исходя из того, какие киберфизические параметры и в какой степени затронуты. Данный модуль получает данные от модуля принятия решений о наличии аномалий и использует их для дальнейшего анализа.

Модуль оповещения предназначен для отправки сообщений оператору, который может контролировать и координировать работу сенсорной системы. Модуль может быть полезен при смешанном управлении, когда оператор отдает команды, а узлы их выполняют уже в автономном режиме. Также данный модуль может быть полезен в случае, когда узлы действуют автономно, но оператору нужно знать о возникновении неисправностей во время выполнения миссии.

Если предусмотрено, что узлы разделяют задачи и действуют как группа, координируя задачи между собой, то этот модуль будет уведомлять не только об аномалиях, обнаруженных для отдельного узла, но и об аномалиях, обнаруженных соседними узлами.

2. Метод определения аномальной активности киберфизической системы

Нормальное распределение сглаживает изменение случайной величины, и время начала атаки может быть незафиксированным, если распределение перестраивается каждый временной интервал [25]. Если разброс значений значительный, то атака будет пропущена из-за того, что стандартное отклонение резко возрастет и может даже превысить ожидаемое значение.

После определения начальных условий строится нормальное распределение:

$$f(s) = \frac{1}{\sigma_s \sqrt{2\pi}} e^{-\frac{(s-M_S)^2}{2\sigma_s^2}}, \quad (1)$$

где *f(s)* и *f(r)* — функции нормального распределения случайной величины (в данном случае количества отправленных и полученных пакетов соответственно) в заданные интервалы времени, M_s и M_r — математические ожидания для отправленных и принятых пакетов соответственно, рассчитываемых одинаково для пересылаемых и отбрасываемых пакетов, σ_s и σ_r — стандартные отклонения для тех же параметров.

Распределение Пуассона можно использовать для оценки киберфизического параметра загрузки ЦПУ [26]. Модель Пуассона описывает схему редких событий: количество событий, произошедших за фиксированный период или в фиксированной области пространства, часто подчиняется распределению Пуассона:

$$P(K_n) = \frac{\lambda^{K_n}}{K_n!} e^{-\lambda}, \quad (2)$$

где P — функция вероятности распределения случайной величины по распределению Пуассона; K_n — процент от общего количества процессорного времени между n и n–1, который процессор тратит на обработку процессов, работающих в режиме ядра; λ — математическое ожидание, представляющее собой среднее число наступлений интересующего события в единицу времени; e — число Эйлера.

Анализ нормализованных киберфизических параметров показал, что распределения вероятности для параметров жертвы и параметров, полученных при оценке нормального состояния, часто близки друг к другу, а аномальное состояние существенно отличается. Для измерения разницы между распределениями функций используется мера энтропии Кульбака-Лейблера.

Энтропия случайной величины — это мера неопределенности случайной величины, или количество информации, необходимой в среднем для описания

случайной величины. Относительная энтропия является мерой расстояния между двумя распределениями [27]. В статистике это выглядит как ожидаемый логарифм отношения правдоподобия [28]. Относительная энтропия D(p||q) является мерой неэффективности, если предполагается, что распределение равно q, но истинное распределение равно p. Например, если известно истинное распределение p случайной величины, то можно построить код со средней длиной описания H(p). Если бы вместо этого использовался код для распределения q, то для описания случайной величины потребовалось бы в среднем H(p)+D(p||q) битов. Относительная энтропия впервые была определена Кульбаком и Лейблером [29,30].

Определение меры энтропии для киберфизического параметра «уровень загрузки ЦПУ»:

$$D_{ij} = \sum PK_{ni}(x) \ln \frac{PK_{ni}(x)}{PK_{nj}(x)} dx \quad (3)$$

,

$$D_{ji} = \sum PK_{nj}(x) \ln \frac{PK_{nj}(x)}{PK_{ni}(x)} dx \,, \quad (4)$$

где PK_{ni} — функция вероятностного распределения загрузки процессора случайной величиной узла-датчика i на текущем временном интервале, PK_{nj} — функция вероятностного распределения загрузки процессора случайной величиной узла-датчика j в текущий интервал времени, D_{ij} — степень отклонения распределений узла i от узла j; D_{ji} — степень отклонения распределений узла j от узла i.

Определение меры энтропии для киберфизического параметра «сетевой трафик»:

$$DL_{ij} = \int f(s,r)_{ni} \ln \frac{f(s,r)_{ni}}{f(s,r)_{nj}} d(s,r) \,, \quad (5)$$

$$DL_{ji} = \int f(s,r)_{nj} \ln \frac{f(s,r)_{nj}}{f(s,r)_{ni}} d(s,r) \,, \quad (6)$$

где $f(s,r)_{ni}$ — функция нормального распределения сетевого трафика сенсорного узла i на текущем интервале времени, $f(s,r)_{nj}$ — функция нормального распределения сетевого трафика случайной величины *j* на текущем интервале времени, DL_{ij} — степень отклонения распределений узла *i* от узла *j*; DL_{ji} — степень отклонения распределений узла j от узла i.

Таким образом, с помощью этого метода можно определить, в какой степени поведение узла *i* отличается от поведения соседнего узла *j*, и выявить аномалии.

3. Экспериментальное исследование и его результаты

Основные задачи экспериментального исследования заключались в следующем:

- подтверждение эффективности метода выявления аномалий киберфизической системы;
- сбор данных для формирования набора данных для обучения нейронной сети с целью классификации атак;
- анализ границ значений дивергенции для принятия решений о наличии аномалий и атак в киберфизической системе.

Экспериментальное исследование проводилось с использованием испытательного стенда, разработанного авторами ранее и представленного в работе [31]. Тестовый стенд представляет собой набор одноплатных компьютеров с установленной операционной системой на базе Linux. Стенд включает в себя 4 узла, которые обмениваются полезной информацией по заданному алгоритму, при этом между узлами создается беспроводная ячеистая сеть (mesh-сеть).

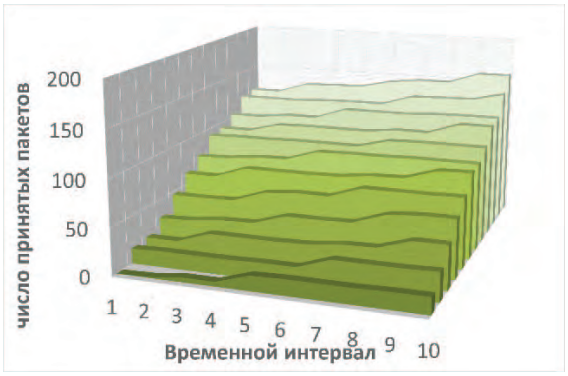
Экспериментальное исследование проводилось по четырем направлениям:

- Фиксирование штатной работы системы, когда узлы обмениваются информацией по заданному алгоритму с использованием протокола UDP, TCP [32], между узлами используется протокол маршрутизации OLSR [33]. При этом никакого дополнительного воздействия на сенсорную систему не оказывается.
- Добавление полезной нагрузки к нормальной работе узла. В качестве полезной нагрузки использовался протокол ICMP, а сообщения запрос/ответ отправлялись на соседний узел.
- Атака типа «отказ в обслуживании», направленная на перегруз узла. Для реализации данного сценария использовалась атака SYN-flood, атаке подвергался открытый порт жертвы, в данном случае порт 22 [34]. Во время атаки на узел-жертву поступило множество запросов на подключение, из-за чего очередь сообщений переполнилась, и узел был заблокирован, при этом сеть оставалась доступной.
- Атака типа «отказ в обслуживании» на блокирование канала. Для реализации этого сценария использовалась атака деаутентификации, когда один из узлов блокировался и терялась его связь с другими узлами, пакеты между соседними узлами не передавались [35]. При этом ра-

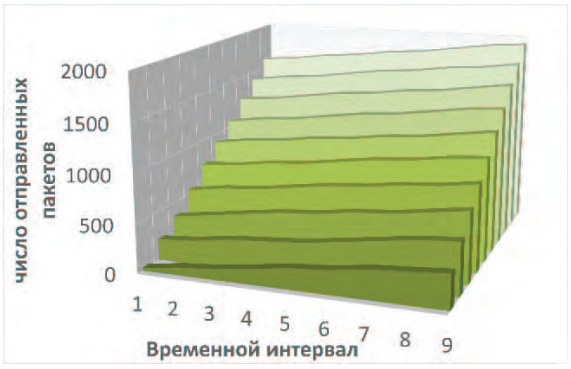
бота самого узла не блокировалась, он просто не мог получить ответ на передаваемые ему сообщения.

3.1. Анализ поведения узла при нормальной работе

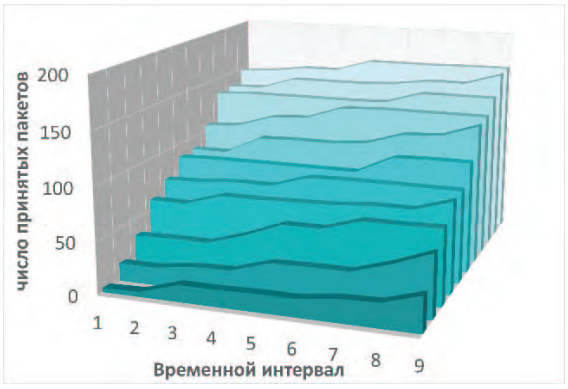
Как упоминалось ранее, узлы обмениваются сообщениями в соответствии с заранее определенным алгоритмом. Они отправляют пакеты на основе своих расчетов, а не равномерно. Поэтому, как видно из рисунка 2, картина трафика не выглядит прямолинейно. От одного временного ряда к другому наблюдаются небольшие изменения. Как правило, количество переданных и полученных пакетов со временем растет.



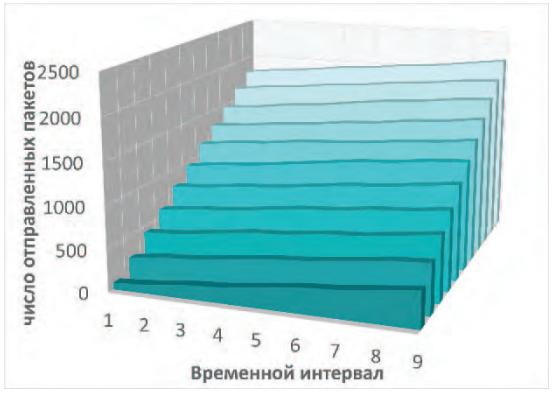
(а)



(б)



(в)



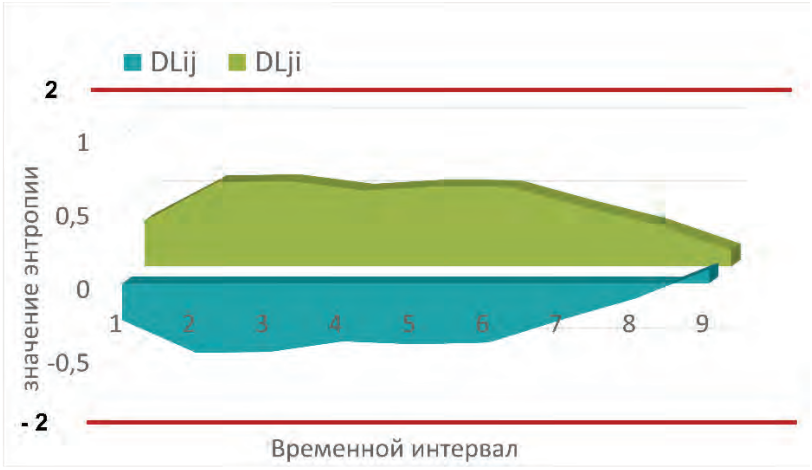
(г)

Рис. 2. Изменения в структуре трафика при анализе необработанных данных о: (а) принятых пакетах узла i; (б) пакетах, отправленных из узла i; (в) принятых пакетах узла j; (г) пакетах, отправленных от узла j, во время нормальной работы сенсорной сети

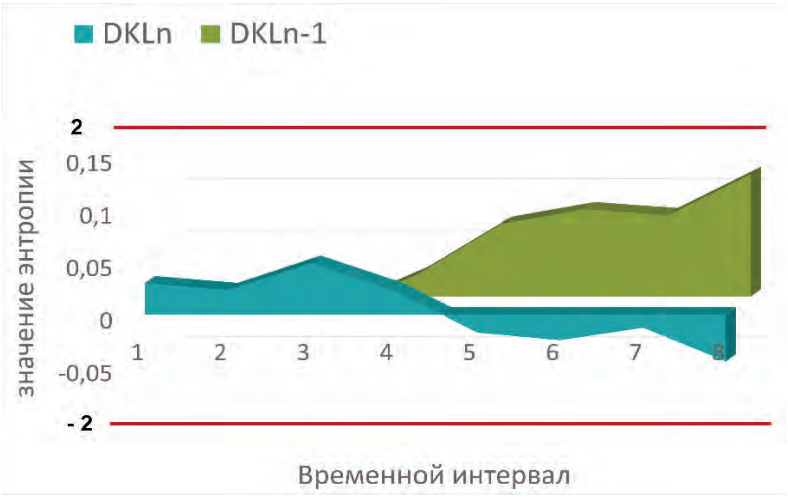
Получив информацию о трафике, модуль анализа данных нормализует ее, после чего по алгоритму, описанному выше, вычисляется энтропия. Результат расчета энтропии соседними узлами показан на рисунке 3. На рисунке 3 (а) показан результат расчета энтропии для входящего трафика. Наблюдаются небольшие отклонения, а пиковое значение достигает 0,5. Эта ситуация является нормальной и не указывает на проводимое воздействие. На рис. 3(б) показан результат вычислений для полученных пакетов.

Как видно из рисунков, для принимаемых пакетов значения энтропии ниже, чем для отправленных. Эта ситуация коррелирует с картиной трафика, полученной для необработанных данных. Рис. 2 показывает, что изменения трафика немного больше для полученных пакетов, хотя из рисунка 2(б) видно, что количество самих отправленных пакетов намного больше, чем количество полученных. Таким образом, метод позволяет выявлять отклонения вне зависимости от количества пакетов, а именно — от поведения узла при их отправке/получении. При этом отсутствуют ложные срабатывания и превышения порога. Важно отметить, что по этому методу узлы анализируют не сами себя, а друг друга. На рис. 3 видно, что разницы между отправленными пакетами двух узлов практически нет, графики близки, хотя количество пакетов разное. Графики полученных пакетов отличаются больше, но незначительно.

Рассмотрим возможность изменения параметра загрузки ЦПУ. В данном исследовании загрузка определяется не в процентах, а в тактах процессора за доли секунды. Уровень загруженности ЦПУ не может быть одинаковым в разные промежутки времени, так



(а)



(б)

Рис. 3. Результат расчета энтропии для: (а) принятых пакетов и (б) отправленных пакетов, узлом i относительно узла j (отмечено синим цветом) и узлом j относительно узла i (отмечено зеленым цветом)

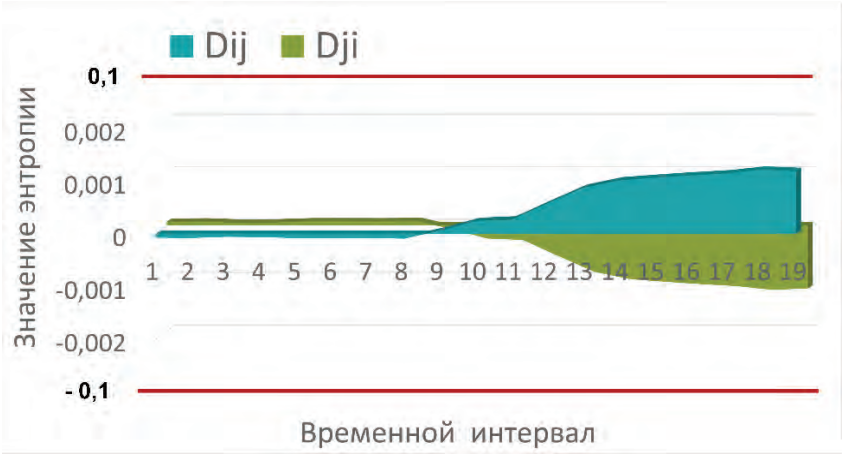


Рис. 4. Результат расчета энтропии уровня загрузки ЦПУ узлом i относительно узла j (отмечен синим цветом) и узлом j относительно узла i (отмечен зеленым цветом)

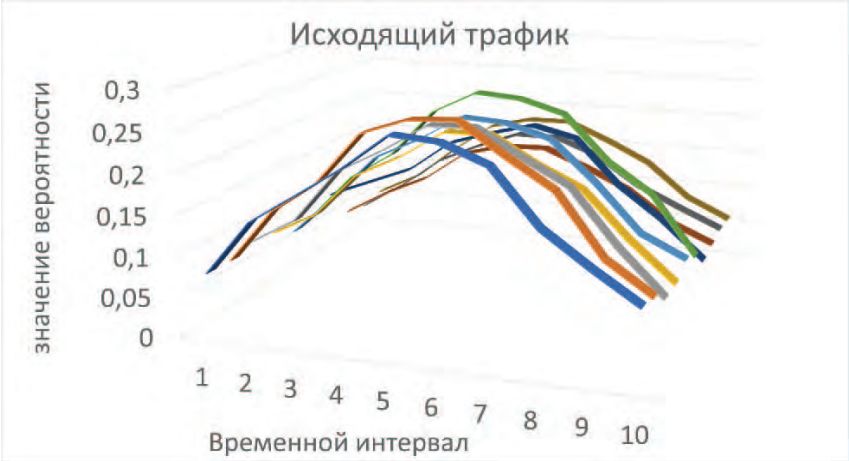


Рис. 5. Результат расчета функции вероятности Гаусса исходящего трафика без атаки

как по своей природе этот параметр меняется скачкообразно.

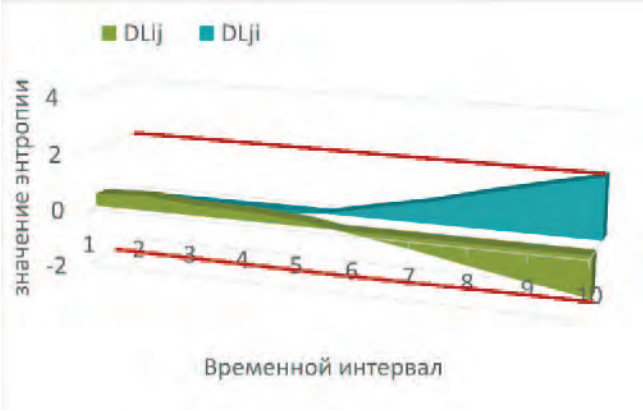
Результат расчета энтропии по узлу i для узла j представлен на рис. 4. Из рис. 4 видно, что небольшая разница в значениях наблюдается на временных интервалах, начиная с 10-го, что коррелирует с необработанными данными.

3.2. Анализ поведения узла с дополнительной полезной нагрузкой

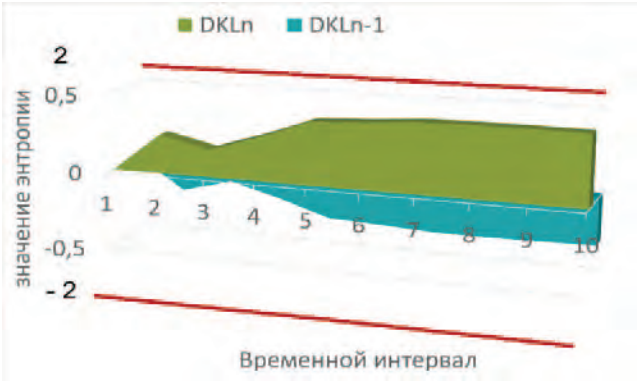
При предоставлении дополнительной полезной нагрузки, не являющейся атакой, в сенсорной системе наблюдались некоторые изменения. Дополнительная полезная нагрузка заключалась в том, что узел отправлял эхо-запросы с помощью команды ping. На рис.5 показан результат вычисления функции Гаусса для узла, на который была оказана дополнительная нагрузка.

На рис. 5 показано, что для исходящего трафика узла i функция Гаусса в некоторых точках имеет разницу около 10–15 процентов. Такие отклонения допустимы для киберфизической системы при дополнительной нагрузке, так как она изменяет ход работы устройства, но незначительно. Это смещение повлияет на расчет энтропии. Результат расчета энтропии показан на рис. 6, – на рисунке видно, что наблюдается небольшой рост значений исходящего трафика.

В предыдущих исследованиях авторами был определён условный порог энтропии, равный двум. Когда значение не превышает двух, то условно сеть работает в штатном режиме. В этом случае заметно небольшое превышение, которое можно интерпретировать как изменение режима работы или дополнительную нагрузку. Как видно из рисунка 7, после увеличения значения наблюдается спад. Это означает, что система приходит в стационарное состояние. На рис. 8 показан результат вычисления энтропии для загрузки ЦПУ. График очень похож на результат вычисления энтропии для нормального состояния. Значения энтропии достигают 0,1. Однако это значение далеко от



(а)



(б)

Рис. 6. Результат вычисления энтропии для: (а) принятых пакетов и (б) отправленных пакетов узлом i относительно узла j (обозначен зеленым цветом) и узлом j относительно узла i (обозначен синим цветом) с добавлением полезной нагрузки

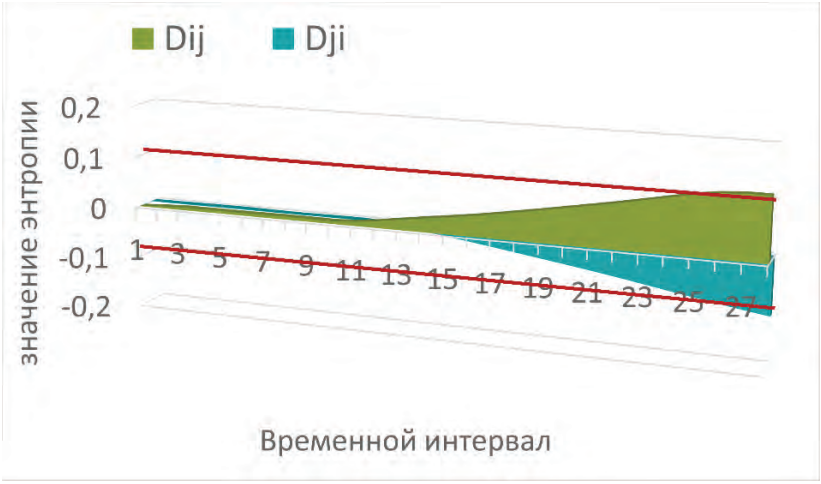


Рис. 7. Результат расчета энтропии для уровня загрузки ЦПУ узлом i относительно узла j (отмечен зеленым цветом) и узлом j относительно узла i (отмечен синим цветом) с дополнительной полезной нагрузкой

порогового значения 0,5. Это говорит о том, что некоторая дополнительная активность присутствует, но не является ненормальной.

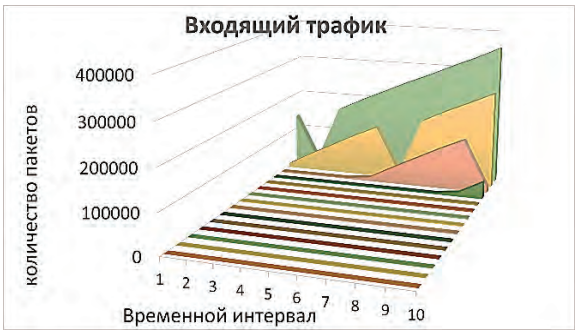
Таким образом, только один параметр из трех показал превышение порога, — исходящий трафик. Остальные параметры были в пределах нормы, хотя и немного увеличились.

3.3. Анализ поведения узла при атаке типа «отказ в обслуживании» — SYN-флуд

Атака SYN-flood начинается не сразу, а спустя три минуты после начала эксперимента. До тех пор сенсорная система работает нормально. На рисунке 8 показано, что изменения начинаются в пятом временном ряду как для входящего, так и для исходящего трафика.

Изменения сопровождаются не только резким увеличением количества пакетов, но и изменением картины трафика. Если сравнить структуру трафика при атаке и при нормальной работе, то увидим, что графики стали более прямолинейными. Это связано с тем, что трафик, связанный с атакой, перекрывает полезный и зашумляет полосу пропускания. На рис. 9 показан результат расчета энтропии для входящего и исходящего трафика узлом i относительно узла j и наоборот.

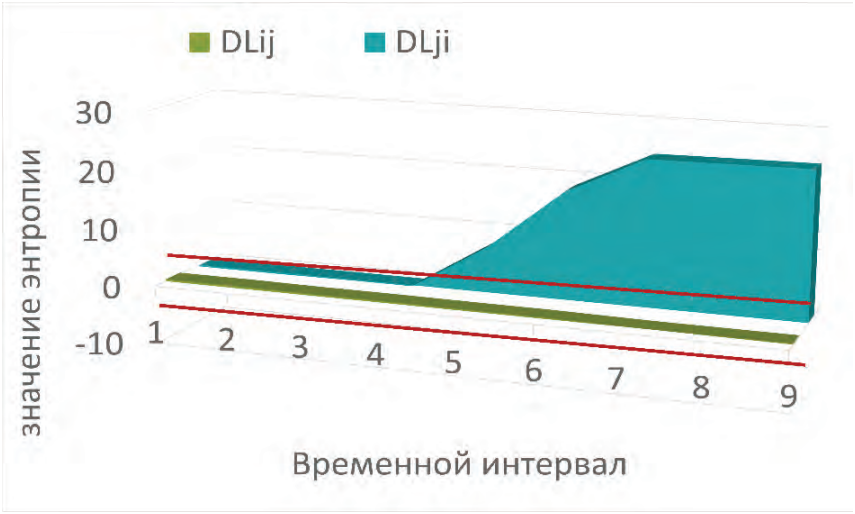
Цифры показывают значительное увеличение значения энтропии. При этом обнаружить аномалию для входящего трафика удается узлу j, а для исходящего трафика — узлу i. На рис. 10 показан результат вычисления функции Гаусса для исходящего трафика атакуемого узла. При вычислении энтропии сравниваются именно результаты вычисления функции распределения Гаусса для трафика или Пуассона для ЦПУ. Именно потому, что значения распределения во время атаки становятся слишком различными друг от друга, узел i при сравнении их с узлом j фиксирует аномалию, и в обратном направлении все работает, и узел j обнаруживает аномалию.



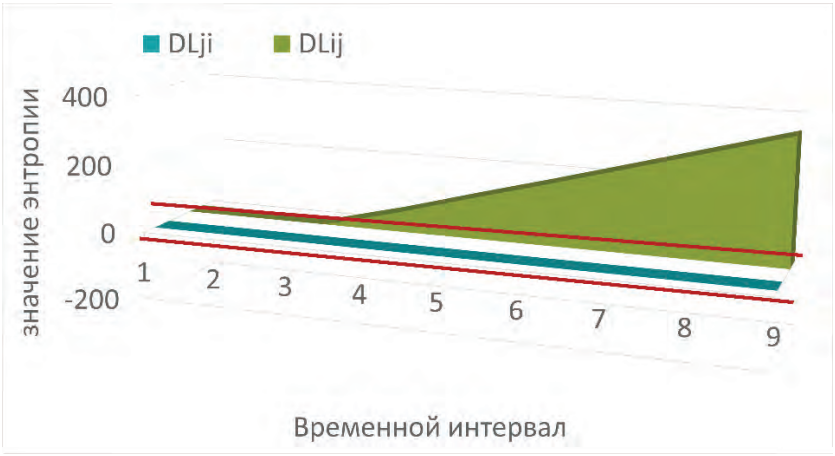
(а)

(б)

Рис. 8. Изменение картины трафика при анализе необработанных данных о: (а) принятых пакетах узла i и (б) отправленных пакетах узла i в условиях атаки SYN-flood



(а)



(б)

Рис. 9. Результат вычисления энтропии для: (а) принятых пакетов и (б) отправленных пакетов узлом i относительно узла j (обозначен зеленым цветом) и узлом j относительно узла i (обозначен синим цветом) в условиях проведения атаки SYN-флуда

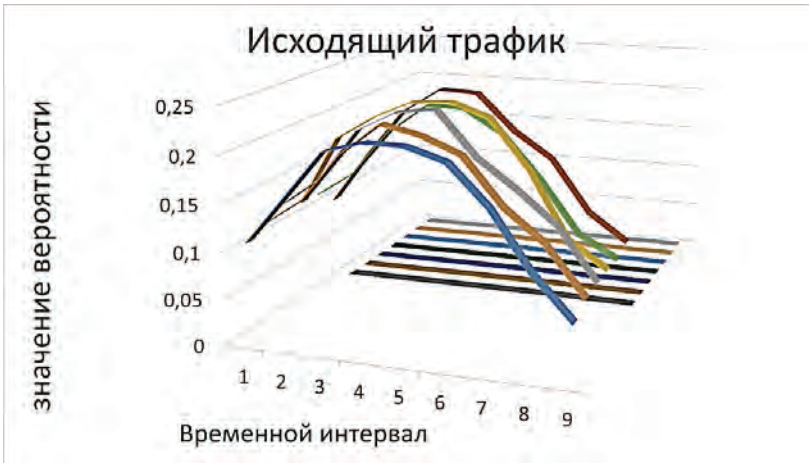


Рис. 10. Результат расчета функции распределения Гаусса для узла i в условиях атаки SYN-flood

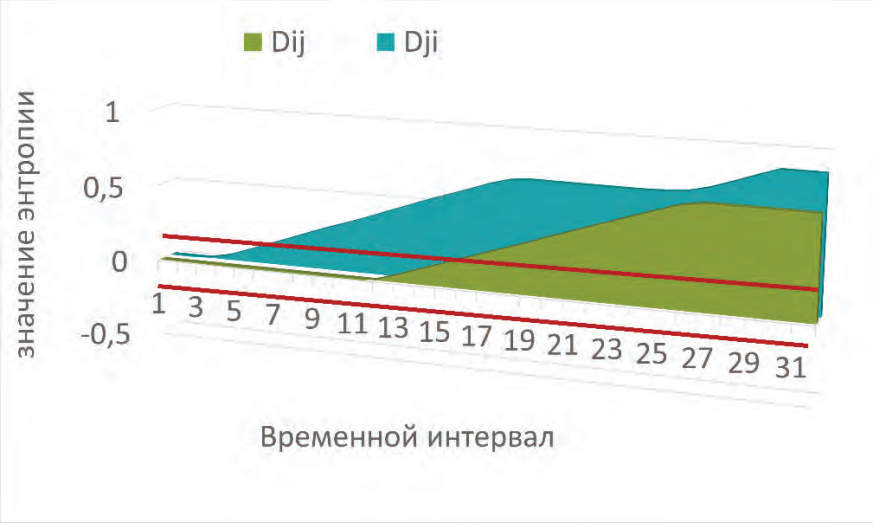
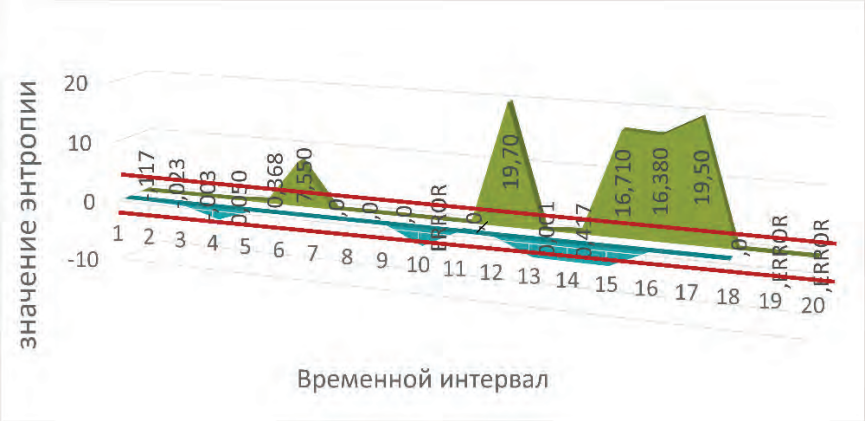
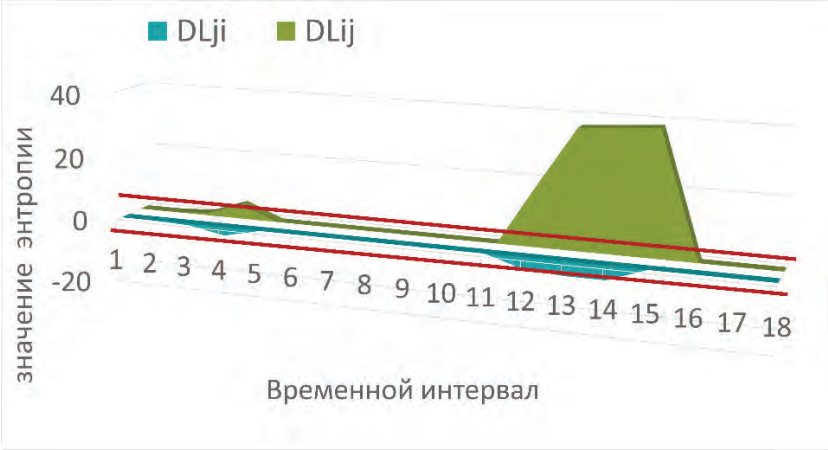


Рис. 11. Результат вычисления энтропии загрузки процессора узлом i относительно узла j (отмечен зеленым цветом) и узлом j относительно узла i (отмечен синим цветом) в условиях атаки SYN-flood



(а)



(б)

Рис. 12. Результат вычисления энтропии для: (а) принятых пакетов и (б) пакетов, отправленных узлом i относительно узла j (отмечено зеленым цветом) и узлом j относительно узла i (отмечено синим цветом) в условиях атаки деаутентификации

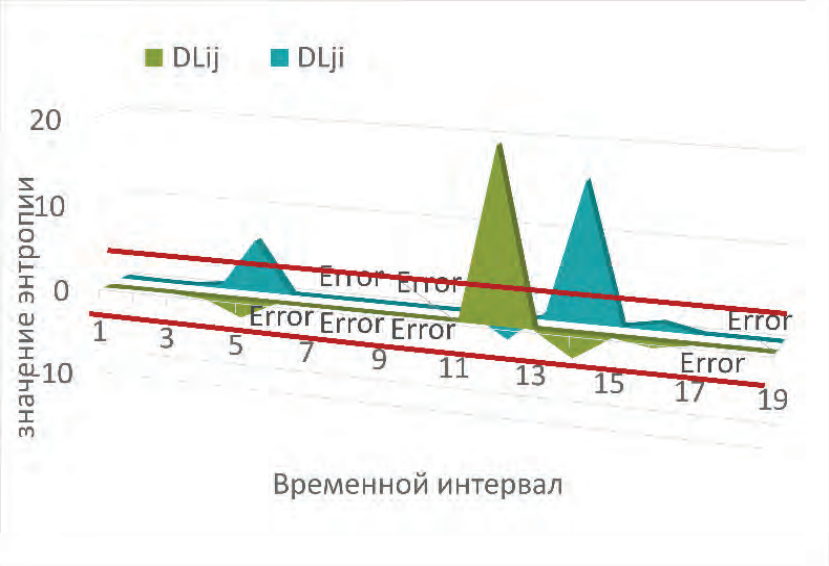


Рис. 13. Результат расчета энтропии для принятых пакетов узлом i относительно узла j (отмечен зеленым) и узлом j относительно узла i (отмечен синим) в условиях атаки деаутентификации

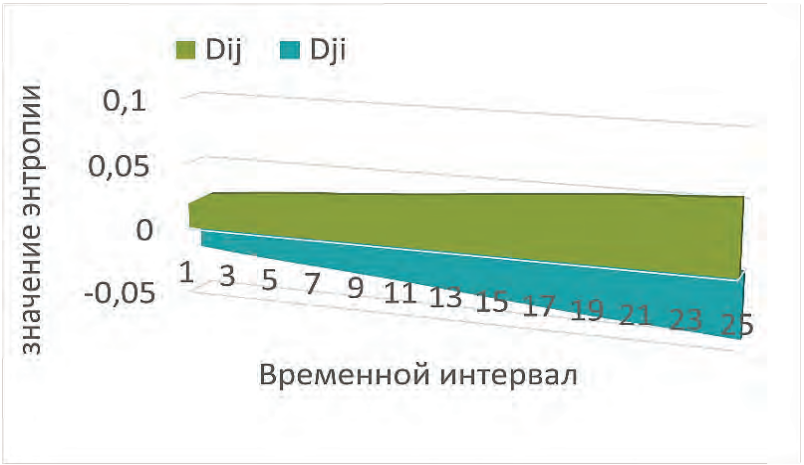


Рис. 14. Результат расчета энтропии загрузки ЦПУ узлом i относительно узла j (отмечен зеленым цветом) и узлом j относительно узла i (отмечен синим цветом) при воздействии атаки деаутентификации

Проанализируем изменение загрузки процессора во время атаки и без нее; узел i находится под атакой, а узел j — нет. Сравним их оценку уровня нагрузки друг с другом (рис. 11). На рис. 11 видно, что сначала происходит увеличение значения энтропии, которое фиксируется обоими узлами, а затем значение остается на одном уровне. Это связано именно с тем, что более резких изменений загрузки ЦПУ не наблюдается.

Этот метод позволяет фиксировать факт изменения состояния и степень этих изменений. Оценить пороги загрузки ЦПУ проще, потому что чем ближе значение к единице, тем выше вероятность атаки. В этом случае значение достигает 0,9. Но увеличение значений до 0,5 также можно рассматривать как изменение состояния.

3.4. Анализ поведения узла при атаке типа «Отказ в обслуживании» – деаутентификация

При проведении атаки деаутентификации соединение разрывается, и сенсорный узел не может полноценно обмениваться данными с соседними узлами. На рис. 12 показан результат расчета энтропии для узла i, подвергшегося атаке. Из рисунков видно, что наблюдается не только рост значения энтропии, но и отсутствие значений для некоторых интервалов времени. Ошибка возникает из-за того, что формула энтропии содержит логарифм частного. Как известно, деление на ноль невозможно, и функция нормального распределения для атакуемого узла может принимать нулевые значения.

В целом можно отметить, что атака фиксируется узлом i; значения энтропии довольно высоки.

Проанализируем ситуацию, когда узел j также находится под влиянием. Такая ситуация может возникнуть, если узлы находятся рядом, и по причине блокировки узла i узел j также не может обмениваться сообщениями, как при атаке Черная дыра (Black Hole). Результат расчета показан на рисунке 13.

На рисунке 13 показано, что хотя оба узла подвержены атакам, они оба обнаруживают аномалию, о чем свидетельствуют высокие значения энтропии. Атака влияет на каждый узел по-разному, поэтому изменение параметров тоже разное, что и фиксируется нашим методом. Когда дело доходит до изменения загрузки процессора, ситуация обратная. Во время атаки снижается загрузка ЦПУ. Это связано с тем, что узел не тратит энергию на пересылку пакетов. Поэтому, как видно из рисунка 14, уровень энтропии для загрузки процессора низкий.

По результатам экспериментального исследования можно резюмировать следующее.

Во-первых, как было сказано ранее, каждая атака по-разному влияет на параметры. В данном исследовании учитываются только три параметра: входящий/исходящий трафик, уровень загрузки процессора. Тем не менее, уже по этим трем параметрам можно определить тип атаки и классифицировать ее.

Во-вторых, метод на основе энтропии позволяет фиксировать разницу между поведением узлов за счет увеличения значений.

В-третьих, в зависимости от типа распределения вероятностей, используемого для нормализации параметра, меняются пороги. Если используется распределение Пуассона, то верхний предел значения равен единице, любое значение от 0,5 до единицы указывает на атаку. Если для нормализации используется нормальное распределение, то верхняя граница отсутствует, при обнаружении атаки значения могут быть очень высокими.

Следовательно, пороговое значение может быть установлено по-разному. Как показали многочисленные эксперименты, некоторые из которых представлены в данной статье, для атаки характерно увеличение значения энтропии более 10. Если значения возрастают до 2, то это может свидетельствовать об изменении активности или незначительные изменения в сенсорной системе. На рисунке 15 показан результат анализа полученных значений.

Таким образом, из рисунка видно, что если происходит резкое увеличение всех трех параметров, которое обнаруживается хотя бы одним из соседних узлов, то проводится атака SYN-flood. Если наблюдается незначительное увеличение одного из параметров, то может произойти изменение режима работы или дополнительная нагрузка на узел. Если происходит увеличение энтропии для трафика, а также наблюдаются ошибочные значения, то проводится атака деаутентификации или обрыв канала связи. Если такая ситуация наблюдается для обоих узлов, то вероятна атака блокировки узлов. При этом загрузка ЦПУ существенно не меняется.

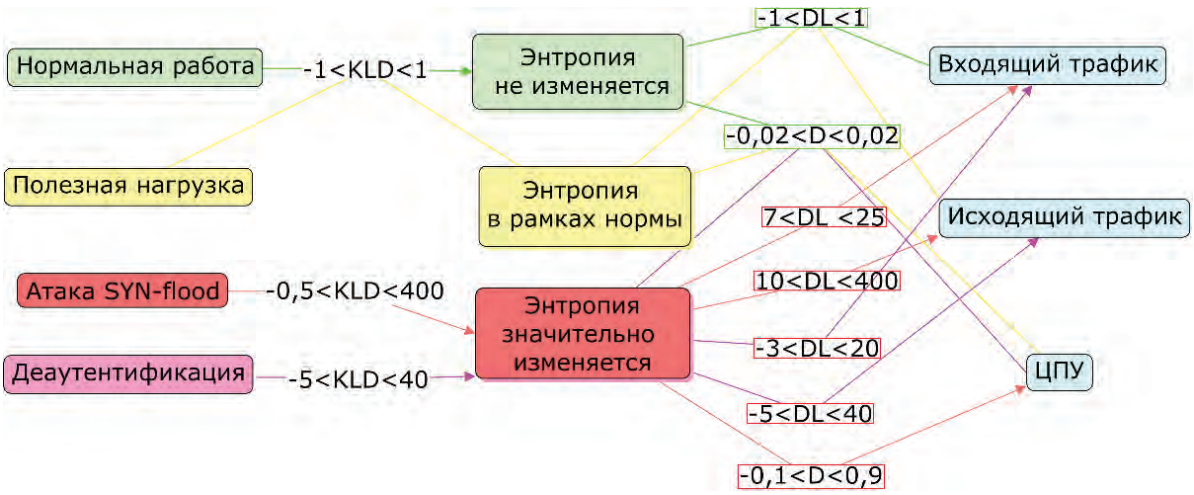


Рис.15. Анализ возможности обнаружения атак разработанным методом

Выводы

В данной статье обсуждались вопросы обнаружения аномалий в киберфизических системах. Существующие системы обнаружения аномалий обычно используют методы машинного обучения. При этом основное внимание авторы уделяют разработке и модификации методов и алгоритмов классификации, доказывая их эффективность. Однако вопросы получения метрик обнаружения часто опускаются и не рассматриваются. Во многих статьях представлено использование готовых наборов сигнатур и наборов данных для классификации и обучения. При этом возникает вопрос о валидности данных для обучения, взятых из открытых источников, а также применимости результатов обучения на них к готовым системам. В некоторых других работах в качестве признаков доверия рассматриваются конкретные сценарии поведения узлов, особенно мобильных узлов сети [36–38].

Данное исследование было сосредоточено на оценке киберфизических параметров и их изменении при различных режимах работы системы. Мера энтропии и нормализация необработанных данных позволяют унифицировать данные и оценивать их с точки зрения обнаружения аномалий. В этом исследовании подробно изучались изменения трех параметров для четырех сценариев. Уже на этом этапе по трем параметрам можно определить разницу между атаками и вариантами нормального поведения. Можно оценить не только факт изменения параметра, но и степень его изменения. При этом узел сенсорной сети сравнивал свои изменения с изменениями соседнего узла.

В качестве расширения метода можно добавить сравнение узла с собственным и оценку изменения его собственных параметров с течением времени. Также планируется увеличить количество оцениваемых киберфизических параметров, на которые может повлиять атака. Кроме того, можно увеличить количество атак для оценки. Уже на этом этапе однозначно выявляется аномальное поведение. Даже если конкретный сценарий атаки неизвестен, можно однозначно установить, на какие свойства и на какие структурные характеристики сенсорной системы она влияет.

Научная новизна данного исследования прежде всего состоит в том, что впервые разработан метод определения аномальной активности киберфизической системы на основе оценки параметров системы с использованием меры энтропии и нормализации необработанных данных, что позволяет достичь высокого уровня обнаружения известных и неизвестных атак. Этот метод может эффективно использоваться в том числе и для автономных систем. Также предложена оригинальная архитектура адаптивной системы защиты киберфизической системы, проработаны ее основные компоненты. При реализации атаки в распределенной системе, данная разработка позволит обнаруживать аномалии узлу не только автономно, но и распределено, то есть обнаруживать воздействие на соседние узлы.

В дальнейших исследованиях планируется использование и сравнение интеллектуальных методов для классификации атак на основе собранного набора данных, тестирование метода на наличие ошибок первого и второго рода, а также тестирование новых сценариев атак и вариантов нормального поведения киберфизической системы.

Работа выполнена при поддержке Совета по грантам Президента Российской Федерации. Стипендия Президента Российской Федерации молодым ученым и аспирантам (Конкурс СП-2022) № СП-858.2022.5.

Литература

1. Yar H., Imran A.S., Khan Z.A., Sajjad M., Kastrati Z. Towards smart home automation using IoT-enabled edge-computing paradigm // Sensors, 2021. №21, 4932. DOI:10.3390/s21144932.
2. Robles-Durazno A., Moradpoor N., McWhinnie J., Russell G., Porcel-Bustamante J. Implementation and evaluation of physical, hybrid, and virtual testbeds for cybersecurity analysis of industrial control systems // Symmetry, 2021. №13, 519. DOI:10.3390/sym13030519.
3. Choudhary A., Kumar S., Gupta S., Gong M., Mahanti A. FEHCA: A fault-tolerant energy-efficient hierarchical clustering algorithm for wireless sensor networks // Energies, 2021. №14, 3935. DOI:10.3390/en14133935.
4. Bouteraa Y., Ben Abdallah I., Ibrahim A., Ahanger T.A. Development of an IoT-based solution incorporating biofeedback and fuzzy logic control for elbow rehabilitation // Appl. Sci., 2020. №10, 7793. DOI:10.3390/app10217793.
5. Umran S.M., Lu S., Abduljabbar Z.A., Zhu J., Wu J. Secure data of industrial internet of things in a cement factory based on a Blockchain technology. // Appl. Sci., 2021. №11, 6376. DOI:10.3390/app11146376.
6. Barka E., Dahmane,S., Kerrache C.A., Khayat M., Sallabi F. STHM: A secured and trusted healthcare monitoring archi-tecture using SDN and Blockchain. // Electronics, 2021. №10, 1787. DOI:10.3390/electronics10151787.

7. Chang Y.-F., Tai W.-L., Hou P.-L., Lai K.-Y. A secure three-factor anonymous user authentication scheme for internet of things environments // Symmetry, 2021. №13, 1121. DOI:10.3390/sym13071121.
8. Zeng X., Zhang X., Yang S., Shi Z., Chi C. Gait-based implicit authentication using edge computing and deep learning for mobile devices. // Sensors, 2021. №21, 4592. DOI:10.3390/s21134592.
9. Nikolopoulos D., Ostfeld A., Salomons E., Makropoulos C. Resilience assessment of water quality sensor designs under cyber-physical attacks. // Water, 2021. №13, 647. DOI:10.3390/w13050647.
10. Yousefnezhad N., Malhi A., Främling K. Automated IoT device identification based on full packet information using real-time network traffic // Sensors, 2021. №21, 2660. DOI: 10.3390/s21082660.
11. Gluck T., Kravchik M., Chocron S., Elovici Y., Shabtai A. Spoofing attack on ultrasonic distance sensors using a continuous signal // Sensors, 2020. №20, 6157. DOI:10.3390/s20216157.
12. Dodig I., Cafuta D., Kramberger T., Cesar I. A novel software architecture solution with a focus on long-term IoT device security support // Appl. Sci., 2021. №11, 4955. DOI:10.3390/app11114955.
13. Stępień K., Poniszewska-Marańda A. Security measures with enhanced behavior processing and footprint algorithm against sybil and bogus attacks in vehicular Ad Hoc network. // Sensors, 2021. №21, 3538. DOI:10.3390/s21103538.
14. Jiang J.-R., Kao J.-B., Li,Y.-L. Semi-supervised time series anomaly detection based on statistics and deep learning. // Applied Sciences, 2021. №11, 6698. DOI:10.3390/app11156698.
15. Mittal M., de Prado R.P., Kawai Y., Nakajima S., Muñoz-Expósito J.E. Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks. // Energies, 2021. №14, 3125. DOI:10.3390/en14113125.
16. Elsisi M., Mahmoud K., Lehtonen M., Darwish M.M.F. Effective nonlinear model predictive control scheme tuned by im-proved NN for robotic manipulators. // IEEE Access, 2021. №9, 64278–64290. DOI:10.1109/ACCESS.2021.3075581.
17. Robinson Y.H., Julie E.G., Balaji S., Ayyasamy A. Energy aware clustering scheme in wireless sensor network using neu-ro-fuzzy approach. // Wireless Personal Communications, 2017. №95, pp.703–721. DOI:10.1007/s11277-016-3793-8.
18. Schneider T., Helwig N., Schütze A. Automatic feature extraction and selection for classification of cyclical time series data // tm-Technisches Messen, 2017. // 84, pp.198–206. DOI:10.1515/teme-2016-0072.
19. KDD99. KDDCup1999 Data. 2020. URL: http://kddicsuciedu/databases/kddcup99/kddcup99html (дата обращения 15.08.2022).
20. Park P., Marco P.D., Shin H., Bang J. Fault detection and diagnosis using combined autoencoder and long short-term memory network. // Sensors, 2019. №19, 4612. DOI: 10.3390/s19214612.
21. Lu C., Wang Z.-Y., Qin W.-L., Ma, J. Fault diagnosis of rotary machinery components using a stacked denoising autoen-coder-based health state identification // Signal Process, 2017. №130, pp. 377–388. DOI: 10.1016/j.sigpro.2016.07.028.
22. Li Z., Li J., Wang Y., Wang K. A deep learning approach for anomaly detection based on SAE and LSTM in mechanical equipment // International Journal of Advanced Manufacturing Technology, 2019. №103, pp. 499–510. DOI: 10.1007/s00170-019–03557-w.
23. Mallak A., Fathi M. Sensor and component fault detection and diagnosis for hydraulic machinery integrating LSTM auto-encoder detector and diagnostic classifiers // Sensors, 2021. №21, 433. DOI:10.3390/s21020433.
24. Mahdavi A., Amirzadeh V., Jamalizadeh A., Lin T.-I. A Multivariate flexible skew-symmetric-normal distribution: Scale-shape mixtures and parameter estimation via selection representation // Symmetry, 2021. №13, 1343. DOI:10.3390/sym13081343.
25. Aljohani N., Bretas A. A Bi-level model for detecting and correcting parameter cyber-attacks in power system state estimation // Applied Sciences, 2021. №11, 6540. DOI:10.3390/app11146540.
26. Aljohani H.M., Akdoğan Y., Cordeiro G.M., Afify A.Z. The uniform Poisson–Ailamujia distribution: Actuarial measures and applications in biological science // Symmetry, 2021. №13, 1258. DOI:10.3390/sym13071258.
27. Răstoceanu F., Rughiniș R., Ciocîrlan Ș.-D., Enache M. Sensor-based entropy source analysis and validation for use in IoT environments // Electronics, 2021. №10, 1173. DOI:10.3390/electronics10101173.
28. Basan E., Basan A., Nekrasov A., Fidge C., Gamec J., Gamcová M. A self-diagnosis method for detecting UAV cyber-attacks based on analysis of parameter changes // Sensors, 2021. №21, 509. DOI:10.3390/s21020509.
29. Zeng Z., Sun J., Xu C., Wang H. Unknown SAR target identification method based on feature extraction network and KLD–RPA joint discrimination // Remote Sensors, 2021. №13, 2901. DOI:10.3390/rs13152901.
30. Wang, J., Zhang, P., He, Q., Li, Y., Hu, Y. Revisiting label smoothing regularization with knowledge distillation // Appl. Sci., 2021. №11, 4699. DOI:10.3390/app11104699.
31. Basan E., Basan A., Nekrasov A. Method for detecting abnormal activity in a group of mobile robots // Sensors, 2019. №19, 4007. DOI:10.3390/s19184007.
32. Larmo A., Ratilainen A., Saarinen J. Impact of CoAP and MQTT on NB-IoT system performance // Sensors, 2019. №19, 7. DOI:10.3390/s19010007.
33. Guillen-Perez A., Montoya A.-M., Sanchez-Aarnoutse J.-C., Cano M.-D. A comparative performance evaluation of routing protocols for flying Ad-Hoc networks in real conditions // Applied Sciences, 2021. №11, 4363. DOI:10.3390/app11104363.
34. Hsu F.-H., Lee C.-H., Wang C.-Y., Hung R.-Y., Zhuang Y. DDoS flood and destination service changing sensor // Sensors, 2021. №21, 1980. DOI:10.3390/s21061980.
35. Milliken J., Selis V. K., Yap M., Marshall A. Impact of metric selection on wireless deauthentication DoS attack performance // IEEE Wirel. Commun. Le., 2013. №2, pp. 571–574. DOI:10.1109/WCL.2013.072513.130428.
36. Tancev G. Relevance of drift components and unit-to-unit variability in the predictive maintenance of low-cost electrochemical sensor systems in air quality monitoring // Sensors, 2021. №21, 3298. DOI:10.3390/s21093298.
37. Martí L., Sanchez-Pi N., Molina J.M., Garcia A.C.B. Anomaly detection based on sensor data in petroleum industry appli-cations // Sensors, 2015. №15, pp. 2774–2797. DOI:10.3390/s150202774.
38. Okamoto T., Ishida Y. An immunity-based anomaly detection system with sensor agents // Sensors, 2009. №9, pp. 9175–9195. DOI:10.3390/s91109175.

ARCHITECTURE OF ADAPTIVE PROTECTION SYSTEM FOR SENSOR NETWORK

Basan A.S.[6], Basan E.S.[7], Peskova O.Yu.[8], Sushkin N.A.[9], Shulika M.G.[10]

Purpose: *Development of the adaptive protection system architecture for sensor networks and cyber-physical systems for anomaly detection based on the collection and analysis of cyber-physical parameters.*

Method: *The method is based on the use of probability theory, mathematical statistics, and information theory. The entropy measure and normalization of the raw data make it possible to unify the data and evaluate it in terms of anomaly detection.*

Results: *The existing solutions for the protection of cyber-physical systems from external active attacks were analyzed. The architecture of an adaptive system for a cyber-physical system protection is proposed. As part of the representation of the node data collection and analysis subsystem, a method for estimating cyber-physical parameters to detect intrusions is proposed. Three parameter changes for four behavioral scenarios were analyzed in detail in this study. Even by three parameters, you can determine the difference between attacks and normal behaviors. It is possible to evaluate not only the fact of parameter change, but also the degree of its change. At the same time, the node autonomously compared changes in its parameters with changes in the parameters of the neighboring node and could identify the impact of the attack on the neighboring node.*

The scientific novelty *primarily consists in the fact that for the first time a method for determining the abnormal activity of a cyber-physical system based on the evaluation of system parameters using a measure of entropy and normalization of raw data has been developed, which makes it possible to achieve a high level of detection of known and unknown attacks. This method can be effectively used also for autonomous systems. The original architecture of the adaptive system for protecting the cyber-physical system is also proposed, its main components are worked out. When implementing an attack in a distributed system, this development will allow the node to detect anomalies not only autonomously, but also distributed, that is, to detect the impact on neighboring nodes.*

Keywords: *data analysis, anomaly, statistics, attacks, risks, cyberphysical systems.*

References

1. Yar H., Imran A.S., Khan Z.A., Sajjad M., Kastrati Z. Towards smart home automation using IoT-enabled edge-computing paradigm // Sensors, 2021. №21, 4932. DOI:10.3390/s21144932.
2. Robles-Durazno A., Moradpoor N., McWhinnie J., Russell G., Porcel-Bustamante J. Implementation and evaluation of physical, hybrid, and virtual testbeds for cybersecurity analysis of industrial control systems // Symmetry, 2021. №13, 519. DOI:10.3390/sym13030519.
3. Choudhary A., Kumar S., Gupta S., Gong M., Mahanti A. FEHCA: A fault-tolerant energy-efficient hierarchical clustering algorithm for wireless sensor networks // Energies, 2021. №14, 3935. DOI:10.3390/en14133935.
4. Bouteraa Y., Ben Abdallah I., Ibrahim A., Ahanger T.A. Development of an IoT-based solution incorporating biofeedback and fuzzy logic control for elbow rehabilitation // Appl. Sci., 2020. №10, 7793. DOI:10.3390/app10217793.
5. Umran S.M., Lu S., Abduljabbar Z.A., Zhu J., Wu J. Secure data of industrial internet of things in a cement factory based on a Blockchain technology. // Appl. Sci., 2021. №11, 6376. DOI:10.3390/app11146376.
6. Barka E., Dahmane,S., Kerrache C.A., Khayat M., Sallabi F. STHM: A secured and trusted healthcare monitoring archi-tecture using SDN and Blockchain. // Electronics, 2021. №10, 1787. DOI:10.3390/electronics10151787.

6 Alexandr S. Basan, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: asbasan@sfedu.ru.

7 Elena S. Basan, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

8 Olga Yu. Peskova, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: oyupeskova@sfedu.ru , ORCID 0000-0002-6397-6970.

9 Nikita A. Sushkin, postgraduate student of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: sushkin @sfedu.ru.

10 Maria G. Shulika, postgraduate student of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University «SFedU», Taganrog, Russia. E-mail: mshulika@sfedu.ru.

7. Chang Y.-F., Tai W.-L., Hou P.-L., Lai K.-Y. A secure three-factor anonymous user authentication scheme for internet of things environments // Symmetry, 2021. №13, 1121. DOI:10.3390/sym13071121.
8. Zeng X., Zhang X., Yang S., Shi Z., Chi C. Gait-based implicit authentication using edge computing and deep learning for mobile devices. // Sensors, 2021. №21, 4592. DOI:10.3390/s21134592.
9. Nikolopoulos D., Ostfeld A., Salomons E., Makropoulos C. Resilience assessment of water quality sensor designs under cyber-physical attacks. // Water, 2021. №13, 647. DOI:10.3390/w13050647.
10. Yousefnezhad N., Malhi A., Främling K. Automated IoT device identification based on full packet information using real-time network traffic // Sensors, 2021. №21, 2660. DOI: 10.3390/s21082660.
11. Gluck T., Kravchik M., Chocron S., Elovici Y., Shabtai A. Spoofing attack on ultrasonic distance sensors using a continuous signal // Sensors, 2020. №20, 6157. DOI:10.3390/s20216157.
12. Dodig I., Cafuta D., Kramberger T., Cesar I. A novel software architecture solution with a focus on long-term IoT device security support // Appl. Sci., 2021. №11, 4955. DOI:10.3390/app11114955.
13. Stępień K., Poniszewska-Marańda A. Security measures with enhanced behavior processing and footprint algorithm against sybil and bogus attacks in vehicular Ad Hoc network. // Sensors, 2021. №21, 3538. DOI:10.3390/s21103538.
14. Jiang J.-R., Kao J.-B., Li,Y.-L. Semi-supervised time series anomaly detection based on statistics and deep learning. // Applied Sciences, 2021. №11, 6698. DOI:10.3390/app11156698.
15. Mittal M., de Prado R.P., Kawai Y., Nakajima S., Muñoz-Expósito J.E. Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks. // Energies, 2021. №14, 3125. DOI:10.3390/en14113125.
16. Elsisi M., Mahmoud K., Lehtonen M., Darwish M.M.F. Effective nonlinear model predictive control scheme tuned by im-proved NN for robotic manipulators. // IEEE Access, 2021. №9, 64278–64290. DOI:10.1109/ACCESS.2021.3075581.
17. Robinson Y.H., Julie E.G., Balaji S., Ayyasamy A. Energy aware clustering scheme in wireless sensor network using neu-ro-fuzzy approach. // Wireless Personal Communications, 2017. №95, pp.703–721. DOI:10.1007/s11277-016-3793-8.
18. Schneider T., Helwig N., Schütze A. Automatic feature extraction and selection for classification of cyclical time series data // tm-Technisches Messen, 2017. // 84, pp.198–206. DOI:10.1515/teme-2016-0072.
19. KDD99. KDDCup1999 Data. 2020. URL: http://kddicsuciedu/databases/kddcup99/kddcup99html (data obrashhenija 15.08.2022).
20. Park P., Marco P.D., Shin H., Bang J. Fault detection and diagnosis using combined autoencoder and long short-term memory network. // Sensors, 2019. №19, 4612. DOI: 10.3390/s19214612.
21. Lu C., Wang Z.-Y., Qin W.-L., Ma, J. Fault diagnosis of rotary machinery components using a stacked denoising autoen-coder-based health state identification // Signal Process, 2017. №130, pp. 377–388. DOI: 10.1016/j.sigpro.2016.07.028.
22. Li Z., Li J., Wang Y., Wang K. A deep learning approach for anomaly detection based on SAE and LSTM in mechanical equipment // International Journal of Advanced Manufacturing Technology, 2019. №103, pp. 499–510. DOI: 10.1007/s00170-019–03557-w.
23. Mallak A., Fathi M. Sensor and component fault detection and diagnosis for hydraulic machinery integrating LSTM auto-encoder detector and diagnostic classifiers // Sensors, 2021. №21, 433. DOI:10.3390/s21020433.
24. Mahdavi A., Amirzadeh V., Jamalizadeh A., Lin T.-I. A Multivariate flexible skew-symmetric-normal distribution: Scale-shape mixtures and parameter estimation via selection representation // Symmetry, 2021. №13, 1343. DOI:10.3390/sym13081343.
25. Aljohani N., Bretas A. A Bi-level model for detecting and correcting parameter cyber-attacks in power system state estimation // Applied Sciences, 2021. №11, 6540. DOI:10.3390/app11146540.
26. Aljohani H.M., Akdoğan Y., Cordeiro G.M., Afify A.Z. The uniform Poisson–Ailamujia distribution: Actuarial measures and applications in biological science // Symmetry, 2021. №13, 1258. DOI:10.3390/sym13071258.
27. Răstoceanu F., Rughiniș R., Ciocîrlan Ș.-D., Enache M. Sensor-based entropy source analysis and validation for use in IoT environments // Electronics, 2021. №10, 1173. DOI:10.3390/electronics10101173.
28. Basan E., Basan A., Nekrasov A., Fidge C., Gamec J., Gamcová M. A self-diagnosis method for detecting UAV cyber-attacks based on analysis of parameter changes // Sensors, 2021. №21, 509. DOI:10.3390/s21020509.
29. Zeng Z., Sun J., Xu C., Wang H. Unknown SAR target identification method based on feature extraction network and KLD–RPA joint discrimination // Remote Sensors, 2021. №13, 2901. DOI:10.3390/rs13152901.
30. Wang, J., Zhang, P., He, Q., Li, Y., Hu, Y. Revisiting label smoothing regularization with knowledge distillation // Appl. Sci., 2021. №11, 4699. DOI:10.3390/app11104699.
31. Basan E., Basan A., Nekrasov A. Method for detecting abnormal activity in a group of mobile robots // Sensors, 2019. №19, 4007. DOI:10.3390/s19184007.
32. Larmo A., Ratilainen A., Saarinen J. Impact of CoAP and MQTT on NB-IoT system performance // Sensors, 2019. №19, 7. DOI:10.3390/s19010007.
33. Guillen-Perez A., Montoya A.-M., Sanchez-Aarnoutse J.-C., Cano M.-D. A comparative performance evaluation of routing protocols for flying Ad-Hoc networks in real conditions // Applied Sciences, 2021. №11, 4363. DOI:10.3390/app11104363.
34. Hsu F.-H., Lee C.-H., Wang C.-Y., Hung R.-Y., Zhuang Y. DDoS flood and destination service changing sensor // Sensors, 2021. №21, 1980. DOI:10.3390/s21061980.
35. Milliken J., Selis V. K., Yap M., Marshall A. Impact of metric selection on wireless deauthentication DoS attack performance // IEEE Wirel. Commun. Le., 2013. №2, pp. 571–574. DOI:10.1109/WCL.2013.072513.130428.
36. Tancev G. Relevance of drift components and unit-to-unit variability in the predictive maintenance of low-cost electrochemical sensor systems in air quality monitoring // Sensors, 2021. №21, 3298. DOI:10.3390/s21093298.
37. Martí L., Sanchez-Pi N., Molina J.M., Garcia A.C.B. Anomaly detection based on sensor data in petroleum industry appli-cations // Sensors, 2015. №15, pp. 2774–2797. DOI:10.3390/s150202774.
38. Okamoto T., Ishida Y. An immunity-based anomaly detection system with sensor agents // Sensors, 2009. №9, pp. 9175–9195. DOI:10.3390/s91109175.