УДК 004.056
DOI: 10.26102/2310-6018/2022.39.4.001

Комплексирование механизмов искусственных иммунных систем в составе интегрированной системы обнаружения атак на промышленный Интернет вещей

В.И. Васильев, А.М. Вульфин, В.Е. Гвоздев, Р.Р. Шамсутдинов✉

Уфимский государственный авиационный технический университет,
Уфа, Российская Федерация
shrr2019@yandex.ru✉

Резюме. В статье рассматривается проблема обнаружения сетевых атак на сети и системы промышленного Интернета вещей (Industrial Internet of Things, IIoT). Широкое применение таких систем обусловливает рост уязвимости корпоративных сетей по причине низкой защищенности умных устройств, распределенной архитектуры сетей промышленного Интернета и гетерогенного характера IIoT-устройств. В статье предлагается использование усовершенствованной искусственной иммунной системы, нацеленной на обнаружение вторжений в сети IIoT. Проанализированы основные концепции и механизмы искусственного иммунитета, применяемые в настоящее время для решения различных задач в области информационной безопасности и интеллектуального анализа данных. Рассмотрено использование таких алгоритмов, как алгоритмы отрицательного отбора, клональной селекции, автоматического обновления детекторов, теории опасности, дендритных клеток, идиопатической иммунной сети. Указаны особенности каждого из этих подходов, подчеркиваются преимущества их комбинированного использования в составе интегрированной системы обнаружения атак. Для обучения и оценки эффективности данной системы использован открытый набор тестовых данных относительно сетевого взаимодействия устройств Интернета вещей – Bot-IoT. Результаты вычислительных экспериментов подтверждают высокую эффективность предложенного подхода.

Ключевые слова: информационная безопасность, сетевая атака, датасет Bot-IoT, Интернет вещей, промышленный Интернет вещей, искусственная иммунная система, отрицательный отбор, клональная селекция, дендритные клетки, идиопатическая иммунная сеть.

Благодарности: работа выполнена при поддержке грантов РФФИ №20-37-90024 и №20-08-00668.

Для цитирования: 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. *Моделирование, оптимизация и информационные технологии.* 2022;10(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1240 DOI: 10.26102/2310-6018/2022.39.4.001

Joint application of artificial immune system mechanisms in the integrated system for detecting attacks on Industrial Internet of Things

V.I. Vasilyev, Vulfin A.M., V.E. Gvozdev, R.R. Shamsutdinov✉

Ufa State Aviation Technical University, Ufa, Russian Federation
shrr2019@yandex.ru✉

Abstract. The article considers the issue of detecting network attacks on the Industrial Internet of Things (IIoT) systems. The widespread use of such systems causes an increase in the vulnerability of corporate networks due to the low security of smart devices, the distributed architecture of IIoT networks, and the heterogeneous nature of IIoT devices. The article proposes to employ an advanced artificial immune system aimed at intrusion detection in the IIoT network. The main concepts and mechanisms of artificial immunity currently utilized to solve various kinds of information security and data mining problems are analyzed. Such algorithms as algorithms of negative selection, clonal selection, automatic updating of detectors, danger theory, dendritic cells and idiopathic immune network theory are examined. The features of each approach are regarded; the advantages of their joint application in integrated intrusion detection system are demonstrated. For the purposes of training and evaluating the efficiency of the given system, a set of testing data on the network interaction of Internet of things devices (Bot-IoT) was used. The results of the computational experiments verify the high efficiency of the suggested approach.

Keywords: information security, network attack, dataset Bot-IoT, Internet of Things, Industrial Internet of Things, artificial immune system, negative selection, clonal selection, dendritic cells, idiopathic immune network.

Acknowledgments: the reported research was supported by the RFBR grants No. 20-37-90024 and No. 20-08-00668.

For citation: Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Joint application of artificial immune system mechanisms in the integrated system for detecting attacks on Industrial Internet of Things. *Modeling, Optimization and Information Technology*. 2022;10(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1240 DOI: 10.26102/2310-6018/2022.39.4.001 (In Russ.).

Введение

Развитие систем Интернета вещей (Internet of Things, IoT) и промышленного Интернета вещей (Industrial Internet of Things, IIoT) значительно увеличивает риски нарушения кибербезопасности. Так, на конференции «RSA Conference 2021» Итцик Фигелевич (Itzik Feiglevitch) и Джастин Шоудер (Justin Sowder) в своем докладе «Into the Mind of an IoT Hacker | How to Protect IoT Networks & Devices» [1] отметили, что зачастую сотрудники компаний даже не имеют представления о том, какое количество IoT-устройств используется в их компаниях. Ими представлена следующая статистика: на типовом предприятии с 10 000 сотрудников сегодня используется около 20 000 IoT-устройств, включая интеллектуальные датчики, камеры безопасности, умные лифты, факсимильные аппараты, принтеры, IP-телевидение и много другое. В больницах, рассчитанных на 500 мест, используется около 10 000 IoT-устройств, таких как инфузионные насосы, мониторы пациентов, рентгеновские аппараты, магнитно-резонансные и компьютерные томографы и др. Заводы с количеством сотрудников около 2 000 характеризуются авторами доклада [1] как использующие около 5 000 IIoT-устройств, включая умные датчики, распределенные системы управления, программируемые логические контроллеры и т. д.

В отчете Лаборатории Касперского [2] отмечается, что нередко IoT-устройства выпадают из внимания подразделений информационной безопасности организаций, а чем чаще сменяются специалисты на рабочих местах, тем больше вероятность того, что никто в компании вообще не представляет, что за IoT-устройства подключены к сети. Часто бывает, что такие устройства доступны из внешних сетей. Конструктивная надежность многих устройств и долгий срок их службы приводит к использованию уже устаревших устройств. К примеру, с целью изучения защищенности устройств исследователи приобрели подержанный аппарат для ультразвукового исследования (УЗИ). На взлом устройства ушло всего 5 минут, так как выяснилось, что оно работает под управлением операционной системы (ОС) Microsoft Windows 2000, которая ни разу не обновлялась. Более того, в ходе эксперимента были обнаружены данные пациентов,

так как их никто не стал удалять перед продажей аппарата. Другой пример – частое использование протоколов Zigbee для подключения различных компонентов умного дома. Эти протоколы были разработаны в 2003 г., и не составляет труда эмулировать Zigbee устройство на ноутбуке, а, находясь в зоне действия этой сети, подключиться к шлюзу и установить вредоносное программное обеспечение (ПО).

По данным [3], в 2022 году компания ABB представила результаты международного исследования компаний, лидирующих в сфере бизнеса и технологий. 72 % респондентов сообщили о том, что они увеличивают расходы на системы IIoT в рамках устойчивого развития, 94 % заявили, что системы промышленного Интернета улучшают качество принимаемых решений и улучшают общие показатели развития. 57 % сообщили о значительном положительном эффекте, оказываемом IIoT на принятие оперативных решений, а в качестве главной преграды использования IIoT отметили их уязвимость.

Целью данного исследования является повышение уровня защищенности промышленного Интернета вещей (IIoT) на основе разработки интегрированной системы обнаружения атак (СОА) с использованием различных механизмов искусственных иммунных систем (ИИС). Рассмотренные ниже задачи проводимого исследования включают в себя анализ основных механизмов ИИС и перспектив их применения, разработку алгоритма их взаимодействия в составе СОА, проведение серии вычислительных экспериментов, анализ полученных результатов с целью оценки эффективности предложенного подхода.

Искусственные иммунные системы

Для обнаружения угроз информационной безопасности в настоящее время все более широкое применение получают интеллектуальные системы. Одно из ключевых мест здесь занимают искусственные иммунные системы (ИИС), характеризующиеся способностью обнаруживать неизвестные угрозы, низким уровнем допускаемых ошибок. Часто они используются совместно с другими интеллектуальными алгоритмами в составе гибридных систем. Существуют различные подходы к реализации искусственного иммунитета.

В [4] проанализированы основные механизмы построения ИИС: отрицательный отбор, положительный отбор, клональная селекция, теория идиотипической иммунной сети, теория опасности, алгоритм дендритных клеток. Рассмотрим их подробнее. В естественной иммунной системе человека в процессе отрицательного отбора созревающим детектирующим агентам (Т-клеткам) предъявляются образцы белков собственного организма. При этом те клетки, которые реагируют на свои белки, уничтожаются, это обеспечивает толерантность Т-клеток к нормальному состоянию организма. С другой стороны, Т-клетки проходят и процедуру так называемого положительного отбора, где погибают те Т-клетки, которые не способны в принципе реагировать с какими-либо белками не своего организма.

В процессе клональной селекции тот детектор, который обнаруживает угрозу, начинает быстро клонировать себя пропорционально степени сродства с обнаруженным образцом, характеризующим угрозу. Механизм клонирования предполагает также наличие некоторых мутаций клонов детектора, расширяющих разнообразие потенциально обнаруживаемых аналогичных образцов угроз всей иммунной системой в целом.

Согласно теории опасности, иммунная система концентрируется не на разделении клеток на «своих» и «чужих», а на определении «опасно» и «безопасно», так что иммунитет, к примеру, должен агрессивно реагировать не на «чужое, но безопасное», а,

скорее, на «свое, но опасное». Теория утверждает, что реакция иммунитета запускается сигналами тревоги, посылаемыми при обнаружении опасности. Сигналы опасности могут формироваться обычными клетками организма, пострадавшими от атаки возбудителя или умирающими по неестественным причинам. Цель систем, построенных на теории опасности, заключается в уменьшении ошибок первого и второго рода.

С теорией опасности тесно связан алгоритм дендритных клеток (ДК), которые также аккумулируют сигналы опасности. На первом этапе незрелые ДК собирают сигналы опасности, затем на более высоком уровне эти сигналы могут быть сопоставлены и определены уровни их опасности. Если обнаруженный ДК сигнал определен как безопасный, то ДК становится полузрелой и, демонстрируя данные детекторам, обеспечивает их толерантность к соответствующим антигенам. Если сигнал определен как опасный, ДК становится зрелой и при демонстрации данных детекторам стимулирует их реакцию на антиген.

В естественной иммунной системе для поддержания активного состояния детекторов необходимо постоянное или периодическое присутствие соответствующего антигена (угрозы). Согласно теории идиотипической иммунной сети, иммунная система способна поддерживать детекторы в активном состоянии даже в отсутствие антигена, определенным образом имитируя его присутствие. Рецепторы некоторых распознающих агентов способны реагировать с подобными рецепторами других распознающих агентов, поддерживая активное состояние последних и так далее по цепочке. Более подробно данный процесс описан в [5].

В работе [6] в комбинации с другими алгоритмами машинного обучения используется искусственная иммунная система, основанная на алгоритмах положительного и отрицательного отбора для обнаружения вредоносных программ мобильных устройств.

В [7] разрабатывается система обнаружения сетевых вторжений на основе анализа аномалий методами искусственных иммунных систем, а именно алгоритмом отрицательного отбора. Предложенная система демонстрирует лучшую эффективность в сравнении с известными системами обнаружения вторжений Snort, Bro, HIDS. В [8] также используется ИИС на основе алгоритма отрицательного отбора в сравнении с классификатором J48.

В [9] для обнаружения сетевых атак используются теория опасности и алгоритм дендритных клеток. Оценка эффективности проводилась на наборах данных UNSW-NB15 [10] и NSL-KDD [11] в сравнении с машиной опорных векторов и искусственной нейронной сетью. Достигнутые показатели точности ИИС: 97,25 % для UNSW-NB15 и 93,28% для NSL-KDD.

В [12] предлагается построение ИИС на основе алгоритма дендритных клеток с использованием датасета UNSW-NB15. Авторы предложили улучшенную версию алгоритма дендритных клеток, достигнувшую точности 90 %. Но, как было отмечено выше, в [9], эталонный алгоритм показал более высокую точность.

В [13] подробно описываются и сравниваются алгоритмы отрицательного отбора, клональной селекции и дендритных клеток. Авторы отмечают, что нет единого алгоритма ИИС, подходящего для решения всех классов задач, рекомендуется выбирать конкретный алгоритм в зависимости от решаемой задачи или комбинировать их.

В [14] реализовано совместное использование алгоритмов отрицательного отбора и клональной селекции для обнаружения распределенных атак. Здесь размерность детектирующей вектор-строки меньше, чем размер анализируемой вектор-строки. Анализ соответствия проводится не на основе расстояния Хэмминга (т. е. по количеству поэлементно совпадающих значений), а по тому факту, является ли строка-детектор подстрокой анализируемого вектора.

В [15] предложена многоуровневая система обнаружения сетевых атак на системы промышленного Интернета вещей, в частности, на беспроводные сенсорные сети (Wireless Sensor Network, WSN), реализованная на основе теории иммунной сети. Система состоит из ряда блоков: B-клеток, T-клеток, дендритных клеток и базофилов. На начальном этапе генерируются B-клетки, задача которых – осуществление первичного анализа данных. Расстояние между векторами измеряется путем битового сопоставления. Вторичный анализ проводится дендритными клетками, и в случае выявления опасности информация о ней передается блоку T-клеток для изоляции аномального узла. Однако T-клетки не участвуют в анализе. Блок базофилов пока не реализован. B-клетки системы статичны, не изменяются со временем, система не способна самообучаться.

В [16] реализован алгоритм глубокого обучения дендритных клеток. Первичный анализ данных выполняется самоорганизующейся искусственной нейронной сетью, выходом которой является сигнал об опасности или о безопасном состоянии. Вторичный анализ выполняется дендритными клетками. Предложенный подход был сравнен с многослойным персептроном, наивным Байесовским классификатором, машиной опорных векторов и *k*-ближайших соседей. Оценка эффективности проводится на основе данных Bot-IoT [17] – набора данных о сетевом взаимодействии между устройствами Интернета вещей. Предложенный авторами алгоритм продемонстрировал лучший результат. В то же время, необходимо отметить, что здесь речь идет только об обнаружении известных атак.

В [18] используется комбинация алгоритмов отрицательного отбора, клональной селекции и теории опасности для обнаружения аномалий в WSN, совместное использование которых демонстрирует высокую эффективность.

Предлагаемый подход

Рассмотрим преимущества основных механизмов ИИС, сведенных в Таблице 1.

Таблица 1 – Преимущества различных механизмов иммунных систем
Table 1 – Advantages of different immune systems mechanisms

Механизм ИИС	Обеспечиваемое преимущество
Отрицательный отбор	толерантность детекторов к нормальному состоянию контролируемой системы
Клональная селекция	адаптивность, возможность самообучения на основе выявленных атак
Обновление детекторов	возможность обнаружения атак нулевого дня, удаление бесполезных детекторов
Теория опасности	реагирование на опасные события
Дендритные клетки	обеспечение реакции на «опасность», даже если соответствующий паттерн определен как «свой» и бездействия, если «чужой» расценен как «безопасный»
Идиотипическая иммунная сеть	обеспечение поддержания активности детекторов в течение длительного времени даже в условиях отсутствия атак.

Суть предлагаемого в работе подхода заключается в объединении вышеуказанных алгоритмов в составе единой интегрированной системы обнаружения вторжений в сети промышленного Интернета вещей.

В рамках нашей предыдущей работы [19] была спроектирована искусственная иммунная система, основанная на алгоритмах отрицательного отбора, клональной селекции, динамического обновления детекторов. Система продемонстрировала высокую эффективность в обнаружении атак на WSN на основе набора данных WSN-DS [20]. Ниже предлагается адаптация разработанной ранее системы для анализа данных набора Bot-IoT, характерных для сетей Интернета вещей, дополнение ее механизмами теории опасности, ДК, иммунной сети, разработка метода интеграции распределенной ИИС в сети IIoT.

Датасет Bot-IoT представляет собой большой по объему набор данных, поэтому для обучения и тестирования системы была выбрана только 5-процентная его часть. Данные были предварительно обработаны способом, представленным в [21]. Система предварительно была обучена на половине выбранного набора данных следующим образом. Каждый детектор генерировался случайным образом, вычислялось расстояние Хэмминга между вектор-строкой сгенерированного детектора и каждой строкой обучающих данных о нормальной активности. Если хотя бы одно значение расстояния было меньше порогового значения, т. е. если вектор-детектор был слишком близок к вектору-норме, то такой детектор уничтожался в целях сохранения толерантности к нормальному состоянию контролируемой системы. Таким образом, алгоритм отрицательного отбора применяется в процессе обучения системы.

Дальнейший порядок работы системы заключается в следующем. Агентами ИИС, распределенными по сети IIoT на уровне периферийных устройств, собираются данные о сетевом взаимодействии. Вычисляются расстояния Хэмминга между анализируемой строкой и каждой строкой-детектором. Если хотя бы одно значение расстояния оказывается меньше порогового, то считается, что обнаружена аномалия. Соответствующий вектор подлежит клональной селекции. Для этого, в зависимости от того, насколько он близок с обнаруженным аномальным вектором, создается определенное количество клонов. Количество создаваемых клонов обратно пропорционально расстоянию между векторами. Каждый клон претерпевает некоторую мутацию и проходит процедуру негативной селекции, чтобы сохранить толерантность к нормальному состоянию контролируемой системы.

Информация о выявленной аномалии отправляется всем агентам уровня периферийных устройств для самообучения на основе обнаруженной аномалии. Также эта информация отправляется на уровень центра обработки данных (ЦОД), где сигнал передается одному из агентов ДК, после чего в соответствии с теорией опасности определяется опасность данной аномалии. Оценивается количество подобных аномалий, количество любых аномалий за тот же временной промежуток, наличие связи с возможно скомпрометированным узлом и т. д. Принимается решение об опасности или безопасности подобной аномалии. Если аномалия безопасна, передается сигнал периферийным агентам ИИС о снижении реакции на подобные аномалии. Если аномалия опасна, стимулируется дополнительная клональная селекция обнаружившего детектора, возможно, изоляция сегмента сети и пр.

Следует отметить, что обучение ИИС, как описано выше, осуществлялось только на основе данных о нормальном состоянии контролируемой системы. То есть все атаки, обнаруживаемые ИИС, являются для нее неизвестными, что обусловливает потенциальную возможность обнаружения иммунной системой атак нулевого дня.

Детекторы ИИС обновляются постоянно. Каждый из них имеет свой период существования. Если за него детектор так и не обнаружил ни одну аномалию, он

уничтожается как ненужный. Вместо него случайным образом генерируется новый, который, как и все другие, при создании подвергается негативной селекции. Если за срок своего существования детектор обнаруживает аномалию, он считается активированным, и срок его существования значительно увеличивается, однако также не становится вечным. Если детектор обнаружил аномалию, которая была определена как опасная, то целесообразно постоянно держать этот и другие подобные детекторы активными в соответствии с теорией идиопатической сети. В искусственной иммунной системе, в отличие от естественной, нет необходимости для этого имитировать присутствие опасной аномалии, достаточно передать детекторам информацию о необходимости поддержания детектора в активном состоянии, сохранить информацию о критичной аномалии в базе данных ЦОД.

Была проведена серия вычислительных экспериментов с агентами, распределенными на различных компьютерах, взаимодействующих друг с другом, анализирующих выбранный набор данных.

Обсуждение результатов вычислительных экспериментов

В результате проведенного тестирования системы были получены следующие результаты, сведенные в Таблице 2. При оценке эффективности системы были использованы показатели, подробно описанные в [22].

Таблица 2 – Показатели эффективности ИИС
Table 2 – Artificial immune system efficiency indicators

Показатели	$Precision$	$Recall$	$Accuracy$	F_1score
Значения	0,996	0,994	0,995	0,995

Как видно из Таблицы 2, первичный анализ данных с помощью искусственной иммунной системы демонстрирует высокие показатели ее эффективности. Далее, по теории опасности, часть атак была определена как безопасная, другая часть – как опасная. Различия обусловлены неравномерным количеством каждого вида атак в используемом наборе данных, а также количеством атак в единицу времени, кроме того, вычисления выполнялись одновременно различными хостами.

Стоит отметить, что часть атак, оцененная системой в качестве безопасных, выглядит как недостаток системы, поскольку фактически система не обнаружила атаку, однако рассмотренные наборы данных зачастую все же слишком идеализированы, и датасет Bot-IoT – не исключение. Здесь данные могут быть либо нормой, либо атакой, но в реальных условиях могут возникать и просто безвредные аномалии. ИИС без использования теории опасности и дендритных клеток обеспечивает параноидальный уровень точности обнаружения «не я». Предположим, мы обнаружим 100 % «не я», но не являющихся атаками. Это нельзя назвать ошибками первого рода, так как данные паттерны, действительно, не соответствуют норме, но и их игнорирование нельзя назвать ошибками второго рода, так как они не являются атаками. Предлагаемый подход потенциально позволит отсеять незначительные аномалии и выделить среди большого их числа действительно критически важные инциденты безопасности.

Для экспериментальной проверки последнего утверждения необходимо применение набора данных, содержащих, кроме нормы и атак, еще и безобидные аномалии. Либо необходимо проведение эксперимента в функционирующей сети IIoT с поочередной эмуляцией атак, распределенных во времени, чтобы между атаками

успевало возникнуть достаточное количество аномалий, и система могла бы отделять аномалии от атак.

Следующая серия экспериментов заключалась в оставлении обученной ИИС с отключенными механизмами идиотипической взаимной активации в функционирующем состоянии на период, достаточный для инактивации некоторых детекторов, в том числе, обнаруживших опасность. Затем был повторен анализ данных, и система справилась хуже. Далее точно так же обученная ИИС была оставлена в функционирующем состоянии с включенными механизмами идиотипической иммунной сети. Повторение вычислительного эксперимента показало, что в последнем случае паттерны, определенные в качестве опасных, были обнаружены с тем же высоким уровнем эффективности.

Заключение

Развитие систем Интернета вещей (Internet of Things, IoT) и промышленного Интернета вещей (Industrial Internet of Things, IIoT) значительно увеличивает риски нарушения кибербезопасности. Одним из наиболее перспективных подходов к построению интеллектуальных систем обнаружения как известных, так и неизвестных сетевых атак является применение искусственных иммунных систем (ИИС). ИИС при этом включают в себя множество различных механизмов реализации, таких как алгоритмы отрицательного отбора, клональной селекции, дендритных клеток, идиотипической иммунной сети и т. д. Предлагаемый авторами подход заключается в интеграции основных механизмов ИИС в составе единой интегрированной системы обнаружения атак на системы промышленного Интернета вещей. Проведенные вычислительные эксперименты на основе набора данных Bot-IoT продемонстрировали высокую точность первичной классификации детекторами ИИС, обученными с помощью алгоритмов отрицательного отбора и клональной селекции, а также функциональность теории опасности, дендритных клеток и идиотипической сети.

СПИСОК ИСТОЧНИКОВ

1. Into the Mind of an IoT Hacker | How to Protect IoT Networks & Devices. *RSA Conference*. 2021. Доступно по: https://www.rsaconference.com/Library/presentation/USA/2021/Into%20the%20Mind%20of%20an%20IoT%20Hacker%20%20How%20to%20Protect%20IoT%20Networks%20%20Devices (дата обращения 10.09.2022).
2. Защищать IoT в сети или защищать сеть от IoT. *Лаборатория Касперского*. Доступно по: https://www.kaspersky.ru/blog/rsa2021-dangerous-iot/30870/ (дата обращения 10.09.2022).
3. Industrial Internet of Things – IIoT. Промышленный интернет вещей. TADVISER. Доступно по: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IIoT_-_Industrial_Internet_of_Things_(%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9) (дата обращения 10.09.2022).
4. Protic D.D. Intrusion detection based on the artificial immune system. *Vojnoteh. glas*. 2020;4. Доступно по: https://cyberleninka.ru/article/n/intrusion-detection-based-on-the-artificial-immune-system (дата обращения: 23.09.2022).
5. Частикова В.А., Картамышев Д.А. Искусственные иммунные системы: основные подходы и особенности их реализации. *Научные труды КубГТУ*. 2016;8:193–208.

6. Brown J., Anwar M., Dozier G. An artificial immunity approach to malware detection in a mobile platform. *URASIP Journal on Information Security*. 2017:7. Доступно по: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-017-0059-2 (дата обращения: 20.09.2022).
7. Kumaravel H.V. An anomaly-based intrusion detection system based on artificial immune system (AIS) techniques. *Open Access Theses*. 2016:964. Доступно по: https://docs.lib.purdue.edu/open_access_theses/964 (дата обращения: 25.08.2022).
8. Бурлаков М.Е., Ивкин А.Н. Система обнаружения вторжения на основе искусственной иммунной системы. *Вестник ПНИПУ*. 2019;29:209–224.
9. Limon-Cantu D., Alarcon-Aquino V. Network intrusion detection using dendritic cells and danger theory. *Technology, Science and Culture: A Global Vision*. 2020;23:89–106.
10. The UNSW-NB15 Dataset, *University of New South Wales*. Доступно по: https://research.unsw.edu.au/projects/unsw-nb15-dataset (дата обращения: 25.09.2022).
11. NSL-KDD. *University of New Brunswick.* Доступно по: https://www.unb.ca/cic/datasets/nsl.html (дата обращения: 25.09.2022).
12. Farzadnia E., Shirazia H., Nowroozi A. A New Intrusion Detection System using the Improved DendriticCell Algorithm. *The Computer Journal*. 2021;8(64):1193–1214.
13. Duru C., Ladeji-Osias J., Wandji K., Otily T., Kone R. A review of human immune inspired algorithms for intrusion detection systems. *2022 IEEE World AI IoT Congress (AIIoT)*. 2022:364–371.
14. Селеменев А.В., Астахова И.Ф., Трофименко Е.В. Применение искусственных иммунных систем для обнаружения сетевых вторжений. *Вестник ВГУ*. 2019;2:49–56.
15. Alaparthy V., Morgera S. A multi level intrusion detection system for wirel ess sensor networks based on immune theory. *IEEE Access*. 2018;6:47364–47373.
16. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al Barakat A. DeepDCA: Novel network based detection of iot attacks using artificial immune system. *Applied sciences*. 2020;10:1909–1932.
17. The Bot-IoT Dataset. *University of New South Wales*. Доступно по: https://research.unsw.edu.au/projects/bot-iot-dataset (дата обращения: 25.09.2022).
18. Xiao X., Zhang R. A danger theory inspired protection approach for hierarchical wireless sensor networks. *KSII Transactions on Internet and Information Systems*. 2019;5(13):2732–2753.
19. Васильев В.И., Гвоздев В.Е., Шамсутдинов Р.Р. Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы. *Доклады ТУСУР*. 2021;4(21):40–45.
20. Almomani I., Al-Kasasbeh B., AL-Akhras M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. *Journal of Sensors*. 2016. Доступно по: https://www.hindawi.com/journals/js/2016/4731953/ (дата обращения: 25.09.2022).
21. Васильев В.И., Шамсутдинов Р.Р. Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной иммунной системы. *Моделирование, оптимизация и информационные технологии.* 2019;1(7):521–535.
22. Васильев В.И., Вульфин А.М., Гвоздев В.Е., Шамсутдинов Р.Р. Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения. *Моделирование, оптимизация и информационные технологии.* 2021;9(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1032. DOI: 10.26102/2310-6018/2021.34.3.019.

REFERENCES

1. Into the mind of an IoT hacker | how to protect IoT networks & devices. *RSA Conference*. 2021. Available by: https://www.rsaconference.com/Library/presentation/USA/2021/Into%20the%20Mind%20of%20an%20IoT%20Hacker%20%20How%20to%20Protect%20IoT%20Networks%20%20Devices (accessed on 10.09.2022).
2. Zashchishchat' IoT v seti ili zashchishchat' set' ot IoT. *Laboratoriya Kasperskogo = Kaspersky Lab.* Available by: https://www.kaspersky.ru/blog/rsa2021-dangerous-iot/30870/ (accessed on 10.09.2022) (In Russ.).
3. Industrial Internet of Things – IIoT. Промышленный интернет вещей. TADVISER. Available by: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IIoT_-_Industrial_Internet_of_Things_(%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9) (accessed on 10.09.2022).
4. Protic D.D. Intrusion detection based on the artificial immune system. *Vojnoteh. glas*. 2020;4. Available by: https://cyberleninka.ru/article/n/intrusion-detection-based-on-the-artificial-immune-system (accessed on 23.09.2022).
5. Chastikova V.A., Kartamyshev D.A. Artificial immune system: basic approaches and feature of their realization. *Nauchnye trudy KubGTU = Scientific Works of the Kuban State Technological University*. 2016;8:193–208. (In Russ.).
6. Brown J., Anwar M., Dozier G. An artificial immunity approach to malware detection in a mobile platform. *URASIP Journal on Information Security*. 2017:7. Available by: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-017-0059-2 (accessed on 20.09.2022).
7. Kumaravel H.V. An anomaly-based intrusion detection system based on artificial immune system (AIS) techniques. *Open Access Theses*. 2016:964. Available by: https://docs.lib.purdue.edu/open_access_theses/964 (accessed on 25.08.2022).
8. Burlakov M.E., Ivkin A.N. Intrusion detection system based on the artificial immune system. *Vestnik PNIPU = PNRPU Bulletin.* 2019;29:209–224. (In Russ.).
9. Limon-Cantu D., Alarcon-Aquino V. Network intrusion detection using dendritic cells and danger theory. *Technology, Science and Culture: A Global Vision*. 2020;23:89–106.
10. The UNSW-NB15 Dataset, *University of New South Wales.* Available by: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed on 25.09.2022).
11. NSL-KDD. *University of New Brunswick.* Available by: https://www.unb.ca/cic/datasets/nsl.html. (accessed on 25.09.2022).
12. Farzadnia E., Shirazia H., Nowroozi A. A New Intrusion Detection System using the Improved DendriticCell Algorithm. *The Computer Journal*. 2021;8(64):1193–1214.
13. Duru C., Ladeji-Osias J., Wandji K., Otily T., Kone R. A review of human immune inspired algorithms for intrusion detection systems. *2022 IEEE World AI IoT Congress (AIIoT)*. 2022:364–371.
14. Selemenev A.V., Astakhova I.F. Application of artificial immune systems for detection of network inclusions. *Vestnik VGU = Proceedings of Voronezh State University*. 2019;2:49–56. (In Russ.).
15. Alaparthy V., Morgera S. A multi level intrusion detection system for wirel ess sensor networks based on immune theory. *IEEE Access.* 2018;6:47364–47373.
16. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al Barakat A. DeepDCA: Novel network based detection of IoT attacks using artificial immune syste. *Applied sciences*. 2020;10:1909–1932.

17. The Bot-IoT Dataset, *University of New South Wales.* Available by: https://research.unsw.edu.au/projects/bot-iot-dataset (accessed on 25.09.2022).
18. Xiao X., Zhang R. A danger theory inspired protection approach for hierarchical wireless sensor networks. *KSII Transactions on Internet and Information Systems.* 2019;5(13):2732–2753.
19. Vasilyev V.I., Gvozdev V.E., Shamsutdinov R.R. Network Anomaly Detection Based on Artificial Immune System for Industrial Internet of Things. *Doklady TUSUR = Proceedings of TUSUR University.* 2021;4(21):40–45. (In Russ.).
20. Almomani I., Al-Kasasbeh B., AL-Akhras M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. *Journal of Sensors.* 2016. Available by: https://www.hindawi.com/journals/js/2016/4731953/ (accessed on 25.09.2022).
21. Vasilyev V.I., Shamsutdinov R.R. Intelligent network intrusion detection system based on artificial immune system mechanisms. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii. = Modeling, Optimization and Information Technology.* 2019;1(7):521–535. (In Russ.).
22. Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Hybrid intelligent intrusion detection system based on combining machine learning methods. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii. = Modeling, Optimization and Information Technology.* 2021;9(3). Available by: https://moitvivt.ru/ru/journal/pdf?id=1032 (accessed on 25.09.2022). DOI: 10.26102/2310-6018/2021.34.3.019. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Васильев Владимир Иванович, доктор технических наук, профессор Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: vas0015@yandex.ru

Vladimir Ivanovich Vasilyev, Doctor of Technical Sciences, Professor at Ufa State Aviation Technical University, Ufa, Russian Federation.

Вульфин Алексей Михайлович, кандидат технических наук, доцент Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Alexey Mikhailovich Vulfin, Candidate of Technical Sciences, Associate Professor at Ufa State Aviation Technical University, Ufa, Russian Federation.

Гвоздев Владимир Ефимович, доктор технических наук, профессор Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: wega55@mail.ru

Vladimir Efimovich Gvozdev, Doctor of Technical Sciences, Professor at Ufa State Aviation Technical University, Ufa, Russian Federation.

Шамсутдинов Ринат Рустемович, аспирант Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: shrr2019@yandex.ru
ORCID: 0000-0002-4178-5284

Rinat Rustemovich Shamsutdinov, Postgraduate Student, Ufa State Aviation Technical University, Ufa, Russian Federation.

Статья поступила в редакцию 04.10.2022; одобрена после рецензирования 03.11.2022; принята к публикации 09.11.2022.

The article was submitted 04.10.2022; approved after reviewing 03.11.2022; accepted for publication 09.11.2022.