РАСПОЗНАВАНИЕ КИБЕРУГРОЗ НА АДАПТИВНУЮ СЕТЕВУЮ ТОПОЛОГИЮ КРУПНОМАСШТАБНЫХ СИСТЕМ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

Павленко Е. Ю.[1], Гололобов Н. В.[2], Лаврова Д.С.[3], Козачок А.В.[4]

Цель статьи: *разработка способа распознавания киберугроз в адаптивных сетевых топологиях крупномасштабных систем на основе рекуррентной нейронной сети с долгой краткосрочной памятью.*

Методы исследований: *системный анализ существующих способов распознавания, теоретическая формализация, проведение эксперимента.*

Результат: *подход показал удовлетворительную эффективность распознавания киберугроз, а результаты исследований позволили выдвинуть предложения по дальнейшему развитию данного направления.*

Научная новизна: *сформулирована модель адаптивной сетевой топологии и предложен новый способ распознавания киберугроз на адаптивную сетевую топологию крупномасштабных систем.*

Вклад авторов: *Павленко Е.Ю. – описание модели адаптивной сетевой топологии и определение схемы проведения экспериментальных исследований; Гололобов Н.В. – выбор архитектуры нейронной сети, разработка алгоритмов реализации предложенного метода и проведение экспериментальных исследований; Лаврова Д.С. – постановка задачи исследования и ее формализация; Козачок А.В. – анализ релевантных научных работ и формирование признаков, характеризующих критичность узлов адаптивной сетевой топологии. Все авторы участвовали в написании статьи.*

Ключевые слова: *кибербезопасность, распознавание киберугроз, рекуррентные нейронные сети, выявление аномалий, адаптивная сетевая топология.*

DOI:10.21681/2311-3456-2022-6-93-99

Введение

Информационные технологии значительно оптимизировали управление техническими процессами за счет создания крупномасштабных производственных систем. Количество логических узлов в таких системах может достигать десятков тысяч, что создает необходимость обеспечения их адаптивной сетевой топологией для обеспечения отказоустойчивости и исключения возможности возникновения каскадных нарушений функционирования системы. Использование адаптивной сетевой топологии позволяет при выходе узла из строя оперативно обеспечить перестроение сети так, что уровень функциональности системы не изменится или несущественно снизится в допустимых пределах.

Обеспечение кибербезопасности адаптивных сетевых топологий является основной задачей при проектировании киберустойчивых крупномасштабных систем [1-4]. Использование всех доступных методов защиты от атак на адаптивную топологию зачастую приводит к снижению уровня производительности, что, в свою очередь, неминуемо влечет финансовые издержки. В результате, приоритетным вопросом становится разработка таких методов и способов, которые позволили бы реагировать на киберугрозы на ранних стадиях проведения атаки.

— Сетевая топология в общем случае может быть представлена в виде графа, вершины которого имеют атрибут критичности.

1 Павленко Евгений Юрьевич, кандидат технических наук, доцент Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, Санкт-Петербург, Россия. E-mail:pavlenko_eyu@spbstu.ru, ORCID:0000-0003-1345-1874

2 Гололобов Никита Вячеславович, студент магистратуры Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, Санкт-Петербург, Россия. E-mail:gololobov.nv @spbstu.ru, ORCID:0000-0003-0623-9891

3 Лаврова Дарья Сергеевна, доктор технических наук, профессор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, Санкт-Петербург, Россия. E-mail:lavrova_ds@spbstu.ru, ORCID:0000-0003-2849-4682

4 Козачок Андрей Васильевич, кандидат технических наук, доцент кафедры КБ-4 МИРЭА-Российский технологический университет, Москва, Россия. E-mail:kozachok@mirea.ru, ORCID:0000-0001-6191-8614

Проведение атак отказа в обслуживании при этом может быть смоделировано как удаление вершины и последующая перестройка графа [5].

Таким образом, формализованная постановка задачи выглядит следующим образом. Сетевая топология есть ориентированный граф $G=(V,E)$, где $V=\{v_1, v_2, \ldots, v_n\}$ – множество узлов сети, $E=\{e_1, e_2, \ldots, e_n\}$ – множество дуг, $E \subseteq (V \times V)$. Поскольку сетевая топология в данном случае характеризуется высокой степенью изменчивости, обозначим начальное состояние сетевой топологии как G^0, а ее состояние в момент времени p – G^p, (этому состоянию предшествует G^{p-1}, $p \in (1, 2, \ldots)$). Тогда для описания адаптивной сетевой топологии целесообразно рассматривать в комплексе серию DG статических графов: $DG=(G^0, G^1, \ldots)$. Любой статический граф G^i ассоциирован с набором следующих атрибутов: предыдущее состояние G^{i-1}, набор графовых операций Op^i, произошедших при преобразовании G^{i-1} в G^i и временная метка t. Графовые операции Op определяются удалением / добавлением вершин и дуг. Состояние сетевой топологии в данном случае во многом определяется параметрами вершин графа, в частности, атрибутом критичности cr: для каждой вершины оператор f задает соответствующее значение критичности – $f: v^i \to \{cr_{v^i}\}$. Значения критичности узла сети определяются его остальными параметрами – пропускной способностью ($bandwidth$), количеством транзитных участков (num) и временной задержкой ($delay$) при передаче данных.

Таким образом, формально решение задачи сводится к обнаружению множества вершин $V' : V' \in V$, таких, что:

- среди прочих вершин показатели критичности этих узлов являются наибольшими, $cr_{V'} \to MAX, cr_{V'} = cr_{v'_1}, \ldots, cr_{v'_m}\}$;
- изменения в характеристиках $bandwidth$, num и $delay$ узлов с высокой критичностью выше допустимых значений. Формально это выражается тем, что применение оператора $\triangle$ к множеству критических узлов V' показывает результат, превышающий некоторую пороговую характеристику $treshold$. При этом, значение $treshold$ может быть превышено как при чрезмерном изменении одного из параметров ($bandwidth$, num и $delay$), так и при чрезмерном изменении их некоторого сочетания. $\triangle(V') > treshold_{V'}$.

Для выявления атак на ранних этапах использованы методы машинного обучения. В частности, рассмотрены методы распознавания киберугроз на основе рекуррентной нейронной сети с долгой краткосрочной памятью. Ее отличительной особенностью является длительное поддержание контекста, что позволяет повысить точность распознавания как при редких, отдельных атаках, так и при реализации серии атак. Более того, точность предсказания будет расти вместе с количеством верно распознанных киберугроз. В контексте выявления серий атак показатели эффективности при использовании данной модели не уступают показателям эффективности при выявлении одиночных атак.

В рамках проведенных исследований использованы методы абстракции и обобщения для создания формализованной и репрезентативной модели адаптивной сетевой топологии. Использование такой модели в ходе эксперимента позволяет получить результаты, справедливые для множества вариаций сетевых топологий в абсолютных значениях.

1. Анализ существующих исследований

В научной работе [1] проведены исследования в части применимости адаптивных нейро-нечетких сетей для выявления угроз кибербезопасности, направленных на защиту сетевых технологий автоматизированной системы. Использованные методы нечеткой логики позволили авторам сделать вывод о высокой эффективности классификатора ANFIS (Adaptive-Network-Based Fuzzy Inference System) в задачах идентификации киберинцидентов. Полученные в статье результаты позволяют использовать разработанные авторами способы для контроля состояния автоматизированных систем управления и производить обработку событий безопасности в режиме реального времени.

В исследовании [6] рассмотрен подход для обнаружения вторжений в сетях Интернета вещей на основе адаптивной сверточной сети оптимизации роя частиц. Под роем частиц в исследовании понимается распределенная сеть клиентского программного обеспечения, функционирующего на устройствах Интернета вещей. Показатели, поступающие от клиентских экземпляров, используются для оценки состояния функционирования сети, в частности, уровня нагрузки, количества активных устройств, задержки и прочих параметров. В результате предложен метод, позволяющий обеспечить удовлетворительную точность выявления вторжений, базирующийся на технологии машинного обучения.

В статье [7] проведен анализ подходов для повышения устойчивости функционирования автомати-

зированных систем с использованием методов обеспечения кибербезопасности на основе машинного обучения. Для рассмотрения авторами выбраны методы, обеспечивающие устойчивость системы камер видеонаблюдения при проведении атак на их сенсоры. Проведенные в ходе исследования эксперименты позволили сравнить эффективность подходов и выдвинуть предложения по их улучшению.

В исследовании [8] рассмотрен вопрос применимости нейронной сети с долгой краткосрочной памятью для выявления кибератак на веб-приложения. Описываемый авторами метод основан на выявлении аномальной активности со стороны пользователя в отношении веб-приложения. Метод также предполагает дальнейшее реагирование на такую активность в зависимости от ее типа. В результате авторами сделан вывод об удовлетворительном уровне корректного выявления кибератак за счет точного определения и предсказания поведения атакующего.

В работе [9] рассмотрены графоаналитические подходы и их использование при проведении мониторинга состояния информационно-телекоммуникационных сетей, а также для выявления аномальных событий. Авторы предполагают, что одним из признаков аномальной активности является проведение атаки на сеть или выход узла из строя в результате отказа в обслуживании, вызванного внешними причинами. В результате проведения исследований предложен и апробирован подход к выявлению ботнет-атак, позволяющий четко идентифицировать текущее состояние информационно-телекоммуникационной сети.

2. Модель адаптивной сетевой топологии

Предметом исследования данной статьи является свойство адаптивности сети при возникновении неполадок на сетевых узлах [10]. Неполадки могут характеризоваться как аномальными показателями активности сетевых узлов, так и отказом в обслуживании связанных кластеров. В настоящем исследовании в качестве адаптивности рассматривается свойство сети обеспечивать устойчивое функционирование при возникновении негативных факторов, влияющих на функциональность узлов. К таким негативным факторам могут быть отнесены потери связи, снижение производительности, пропускной способности или появление избыточных шумов в канале связи.

Адаптивность является характеристикой топологии и не зависит от типа узлов, что позволяет обобщать множество возможных топологий с механизмами обеспечения надежности [11]. В общем случае любая сетевая топология может быть представлена в виде матрицы смежности размерности N×N, где N – количество узлов в сети. При этом в контексте устойчивости топологии учитывается только наличие связи между функциональными узлами. Такие характеристики сети как средняя пропускная способность, задержки, наличие центров управления не учитываются. Кроме этого, предполагается, что узлы в сети равноправны, но имеют атрибуты приоритета – значение критичности в рамках функциональной нагрузки.

Изначальная матрица связи имеет вид, определяемый в соответствии с текущим состоянием сетевой топологии (1), например:

$$A_0 = \begin{pmatrix} 1 & 0 & \cdots & 1 & 0 \\ & 1 & \cdots & & \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ & & \cdots & & \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix}, \quad (1)$$

где: A_0 – изначальная матрица связи.

При этом значение «1» обозначает наличие связи, значения «0» – ее отсутствие. Таким образом, элементы на главной диагонали исходной матрицы связи всегда имеют значение «1» – считается, что узлы всегда имеют подключение к самим себе, если они не выведены из строя.

Для моделирования реализации киберугроз предлагается использование преобразования d матрицы A (2), такого, что:

$$d : A_{t+1} \rightarrow A_{t+2} + d - 1, \quad (2)$$

где A_{t+1}, A_{t+2} – состояния изначальной матрицы в момент времени t+1 и t+2.

То есть, за одно применение таблица связи может потерять только один узел, при этом адаптационное преобразование – использование резервного маршрута – осуществляется только при нарушении работы основного (наиболее короткого маршрута между целевыми узлами). Если при изменении матрицы связи основной маршрут не затронут адаптационные преобразования не происходят.

3. Предлагаемый подход

Наиболее перспективным направлением в создании автоматизированных средств превентивного реагирования является использование технологий машинного обучения. В частности, для таких целей применяется прогнозирование на основе полученных ранее показателей. Для прогнозирования используют-

ся нейронные сети, позволяющие не только в значительной степени автоматизировать анализ данных, но также сократить вероятность антропогенной ошибки при проведении расчётов и формировании прогнозов.

Одной из современных тенденций развития технологии машинного обучения является сокращение времени обработки данных и повышение точности при минимизации мощностных затрат [12-14]. В данном направлении широкое применение получили нейронные сети с долгой краткосрочной памятью, отличительной особенностью которых является сохранение результатов предыдущих вычислений – накопление опыта [15]. Кроме того, данный вид сетей позволяет отказаться от обратного распространения ошибки до первого слоя без значительных потерь в производительности.

Для определения киберугрозы посредством предлагаемого метода достаточно, чтобы предсказанное значение отличалось от фактического на некоторую величину, определяемую в ходе функционирования алгоритма. Для распознавания киберугроз на адаптивную сетевую топологию предлагается использование следующего подхода:

1. Каждому узлу в топологии присваивается метка критичности, значение которой определяется количеством соседних узлов. Большее количество смежных узлов означает больший показатель критичности.
2. Для всех доступных маршрутов из узла А в узел В определяются критичные узлы.
3. При изменении состояния узлов в маршруте определяется степень влияния изменений на метрики топологии (пропускную способность, количество транзитных участков и временную задержку).
4. В случае, если метрики для маршрута не удовлетворяют минимально допустимым значениям, определяемым в соответствии с возможностями топологии, считается, что изменения вызваны вследствие попытки реализации киберугрозы
5. В противном случае считается, что изменения выполняются штатно.

Использование нейронной сети с долгой краткосрочной памятью за счет поддержания контекста позволяет классифицировать изменения топологии с большей точностью, поскольку предыдущие состояния узлов фиксируются. В случае реализации киберугрозы адаптация топологии может приобретать каскадный характер, в отличие от штатной адаптации, при которой изменение состояние узлов будет более растянуто во времени.

4. Эксперимент

Перед началом эксперимента подготовлен набор данных, описывающих топологию сети за 15 000 тактов. На каждом такте может быть произведена штатная адаптация или адаптация в результате попытки реализации киберугрозы, а также адаптация может отсутствовать. В обучающем наборе явно размечены штатные и аварийные адаптации. При формировании набора также установлено правило, что критические узлы с меньшей вероятностью могут быть подвержены штатным изменениям, и в большинстве случаев адаптация после изменения критических узлов является аварийной. Набор содержит следующие поля:

- такт времени;
- идентификатор изменившегося узла (если изменений нет, данное поле имеет значение 0);
- метка критичности;
- метрики топологий для маршрутов изменившегося узла (если изменений нет, данное поле имеет значение 0);

Эксперимент состоит из трех этапов:

1. Построение модели адаптивной крупномасштабной сетевой топологии.
2. Обучение нейронной сети на наборе данных, содержащем сведения о топологии на каждом такте времени.
3. Моделирование киберугроз, вызывающих отказ узла в обслуживании и штатных адаптаций топологии сети с фиксированием результатов работы нейронной сети.

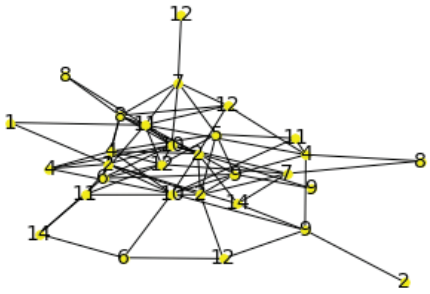

Рис. 1. Пример модели адаптивной крупномасштабной сетевой топологии

Модель адаптивной крупномасштабной сетевой топологии представляет собой граф, ребра которого обозначают наличие связей между узлами, а вершины – сами узлы. Вес вершины при этом означает степень критичности узла в соответствии с исходным состояни-

ем сети (Рис. 1). Для наглядности в примере изображены 30 узлов. Эксперимент проводится с моделью, количество узлов в которой составляет 3500 штук.

В качестве киберугроз рассмотрены единичный и каскадный отказ в обслуживании. Реализация единичного отказа в обслуживании ведет к удалению только одного узла, в то время как каскадный отказ ведет к удалению произвольного участка топологии. Оба сценария в итоге приводят к изменениям в топологии.

Для обучения нейронной сети использованы неразмеченные наборы данных, сгенерированные по определённым правилам:

- обучающий набор содержит 130 000 записей, единичный отказ в обслуживании возникает каждые 100 записей, каскадный – каждые 1000;
- тестовый набор содержит 370 000 записей, единичные и каскадные отказы возникают псевдослучайно с вероятностью появления 0.2.

В ходе анализа результатов сопоставлены выявленные киберугрозы с фактическими киберугрозами в тестовом наборе данных. Точность определения составила 87,2%. Потери точности, полученные в первой десятой части, связаны с использованием определенного паттерна при обучении. При обработке последующих записей из тестового набора точность увеличивалась. Это объясняется особенностями работы рекуррентной нейронной сети с долгой краткосрочной памятью. Архитектура такой сети позволяет запоминать предыдущие результаты и корректировать свое поведение в зависимости от их корректности.

По результатам обучения установлено, что нейронной сетью достигнуты удовлетворительные показатели метрики средней похожести объектов внутри кластера, при этом среднее расстояние между кластерами выше, чем расстояние между объектами внутри кластера.

Выводы

Выявление киберугроз на адаптивные сетевые топологии является комплексной задачей, которая должна решаться в несколько этапов. На каждом из таких этапов должны быть реализованы меры, направленные на контроль соответствующих уровней абстракции топологии. Так, на уровне архитектуры должны быть определены критерии, по которым можно отличать штатное изменение топологии от изменений, вызванных реализацией киберугрозы. На уровне реализации, в свою очередь, определяется способ выявления нештатных изменений в соответствии с определёнными ранее критериями.

В рамках настоящей статьи предложен один из возможных подходов к решению данной задачи на этапе обработки поведения узлов в сети. В ходе эксперимента подход показал удовлетворительную эффективность выявления киберугроз, реализуемых в отношении модели адаптивной сетевой топологии.

В результате проведенных исследований установлено, что рекуррентная нейронная сеть с долгой краткосрочной памятью может быть применена при выявлении киберугроз с точностью, достаточно высокой для апробации на реальных адаптивных топологиях.

Таким образом, авторами статьи достигнут положительный эффект в области обеспечения кибербезопасности сложных систем, базирующихся на адаптивной сетевой инфраструктуре. Специфика таких сетей требует разработки новых подходов к выявлению киберугроз, адаптированных к особенностям предметной области. Достоверность предложенного подхода подтверждена на практике – в ходе экспериментальных исследований была достигнута точность определения киберугроз свыше 87%, и следует отметить, что данный показатель может быть значительно улучшен путем более длительного обучения, в связи со свойством выбранного типа нейронных сетей запоминать предыдущие результаты анализа.

Научная новизна предложенного подхода состоит в описании графовой модели, описывающей функционирование адаптивной сетевой топологии, и в разработке нового способа распознавания киберугроз на адаптивную сетевую топологию крупномасштабных систем, учитывающего специфику таких систем.

Дальнейшие исследования должны быть направлены на определение возможности использования рекуррентной нейронной сети с долгой краткосрочной памятью для выявления киберугроз в масштабируемых сетевых топологиях и Ad-hoc сетях.

Исследование выполнено за счет гранта Российского научного фонда № 22-21-20008, https://rscf.ru/project/22-21-20008/

Литература

1. Исследование алгоритмов адаптивных нейро-нечетких сетей ANFIS для решения задачи идентификации сетевых атак / Д. И. Парфенов, И. П. Болодурина, Л. С. Забродина, А. Ю. Жигалов // Современные информационные технологии и ИТ-образование. 2020. Т. 16. № 3. С. 533-542. – DOI 10.25559/SITITO.16.202003.533-542. EDN RGBMIK.
2. Воропай Н. И., Колосок И. Н., Коркина Е. С. Проблемы повышения киберустой-чивости цифровой подстанции // Релейная защита и автоматизация. 2019. № 1(34). С. 78-83. – EDN ELLPYX.
3. Петренко, С. А. Киберустойчивость систем Индустрии 4.0 / С. А. Петренко // Защита информации. Инсайд. 2019. № 3(87). С. 6-15. – EDN QWWFXU.
4. Лаврова, Д. С. Обеспечение киберустойчивости промышленных систем на основе Концепции молекулярно-генетических систем управления // Проблемы информационной безопасности. Компьютерные системы. 2019. № 4. С. 67-71. – EDN DAGWGN.
5. Павленко, Е. Ю. Модель функционирования адаптивной сетевой топологии крупномасштабных систем на основе динамической теории графов // Проблемы информационной безопасности. Компьютерные системы. 2022. № 3. С. 68-79. – DOI: 10.48612/jisp/tn56-xvah-7tf1. – EDN WUDQXX.
6. A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network / X. Kan, Y. Fan, Z. Fang [et al.] // Information Sciences. 2021. Vol. 568. P. 147-162. – DOI 10.1016/j.ins.2021.03.060. – EDN KTZZXY.
7. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks / C. Kyrkou, A. Papachristodoulou, T. Theocharides [et al.] // Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI : 19, Limassol, 06–08 июля 2020 года. Limassol, 2020. P. 476-481. – DOI 10.1109/ISVLSI49217.2020.00-11.
8. LSTM neural networks for detecting anomalies caused by web application cyber-attacks / I. Kotenko, I. Saenko, O. Lauta, K. Kribel // Frontiers in Artificial Intelligence and Applications. 2021. Vol. 337. P. 127-140. – DOI 10.3233/FAIA210014. – EDN DBNPSR.
9. Будко Н. П., Васильев Н. В. Обзор графо-аналитических подходов к мониторингу информационно-телекоммуникационных сетей и их применение для выявления аномальных состояний // Системы управления, связи и безопасности. 2021. № 6. С. 53-75. – DOI 10.24412/2410-9916-2021-6-53-75. – EDN KVLWCE.
10. Масленников О. В., Некоркин В. И. Адаптивные динамические сети // Успехи физических наук. 2017. Т. 187. № 7. С. 745-756. – DOI 10.3367/UFNr.2016.10.037902. – EDN YTNSJV.
11. Павленко, Е. Ю. Модель функционирования адаптивной сетевой топологии крупномасштабных систем на основе динамической теории графов // Проблемы информационной безопасности. Компьютерные системы. 2022. № 3. С. 68-79. – DOI: 10.48612/jisp/tn56-xvah-7tf1. – EDN WUDQXX.
12. Астапов Р. Л., Мухамадеева Р. М. Автоматизация подбора параметров машинного обучения и обучение модели машинного обучения // Актуальные научные исследования в современном мире. 2021. № 5-2(73). С. 34-37. – EDN GJEUNW.
13. Тормозов В. С., Золкин А. Л., Василенко К. А. Настройка, обучение и тестирование нейронной сети долгой краткосрочной памяти для задачи распознавания образов // Промышленные АСУ и контроллеры. 2020. № 3. С. 52-57. – DOI 10.25791/asu.3.2020.1171.
14. Пустынный, Я. Н. Решение проблемы исчезающего градиента с помощью нейронных сетей долгой краткосрочной памяти // Инновации и инвестиции. 2020. № 2. С. 130-132. – EDN MRQIHM.
15. Multihead Self-attention and LSTM for Spacecraft Telemetry Anomaly Detection / S. Gundawar, N. Kumar, P. Yash [et al.] // Communications in Computer and Information Science. 2022. Vol. 1528. P. 463-479. – DOI: 10.1007/978-3-030-95502-1_35. – EDN PYVPLX.

RECOGNITION OF CYBER THREATS ON THE ADAPTIVE NETWORK TOPOLOGY OF LARGE-SCALE SYSTEMS BASED ON A RECURRENT NEURAL NETWORK

Pavlenko E.Y.[5], Gololobov N.V.[6], Lavrova D.S.[7], Kozachok A.V.[8]

The purpose of the article: *the development of a method for recognizing cyber threats in adaptive network topologies of large-scale systems based on a recurrent neural network with a long short-term memory.*

Main research methods: *system analysis of existing recognition methods, theoretical formalization, experiment.*

5 Evgeny Yu. Pavlenko, Ph.D., Associate Professor of the Institute of Cybersecurity and Information Protection of Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: pavlenko_eyu@spbstu.ru, ORCID:0000-0003-1345-1874

6 Nikita V. Gololobov, Master's student at the Institute of Cybersecurity and Information Protection of Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: gololobov. nv @spbstu.ru, ORCID:0000-0003-0623-9891

7 Daria S. Lavrova, Dr. Sc. (in Tech.), Professor of the Institute of Cybersecurity and Information Protection of Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: lavrova_ds@spbstu.ru, ORCID:0000-0003-2849-4682

8 Andrey V. Kozachok, Ph.D., Associate Professor of the Department KB-4, MIREA-Russian Technological University, Moscow, Russia. E-mail: kozachok@mirea.ru, ORCID:0000-0001-6191-8614

Result: *The approach showed a satisfactory efficiency of cyber threat recognition, and the results of the research made it possible to put forward proposals for the further development of this area.*

Scientific novelty: *A model of adaptive network topology is formulated and a new way of recognizing cyber threats on the adaptive network topology of large-scale systems is proposed.*

Keywords: *Cyber security, cyber threat detection, recurrent neural networks, anomaly detection, adaptive network topology.*

References

1. Issledovanie algoritmov adaptivnyh nejro-nechetkih setej ANFIS dlja reshenija zadachi identifikacii setevyh atak / D. I. Parfenov, I. P. Bolodurina, L. S. Zabrodina, A. Ju. Zhigalov // Sovremennye informacionnye tehnologii i IT-obrazovanie. 2020. T. 16. № 3. S. 533-542. – DOI: 10.25559/SITITO.16.202003.533-542. EDN RGBMIK.
2. Voropaj N. I., Kolosok I. N., Korkina E. S. Problemy povyshenija kiberustoj-chivosti cifrovoj podstancii // Relejnaja zashhita i avtomatizacija. 2019. № 1(34). S. 78-83. – EDN ELLPYX.
3. Petrenko, S. A. Kiberustojchivost' sistem Industrii 4.0 / S. A. Petrenko // Zashhita informacii. Insajd. 2019. № 3(87). S. 6-15. – EDN QWWFXU.
4. Lavrova, D. S. Obespechenie kiberustojchivosti promyshlennyh sistem na osnove Koncepcii molekuljarno-geneticheskih sistem upravlenija // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2019. № 4. S. 67-71. – EDN DAGWGN.
5. Pavlenko, E. Ju. Model' funkcionirovanija adaptivnoj setevoj topologii krupnomasshtabnyh sistem na osnove dinamicheskoj teorii grafov // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2022. № 3. S. 68-79. – DOI: 10.48612/jisp/tn56-xvah-7tf1. – EDN WUDQXX.
6. A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network / X. Kan, Y. Fan, Z. Fang [et al.] // Information Sciences. 2021. Vol. 568. P. 147-162. – DOI 10.1016/j.ins.2021.03.060. – EDN KTZZXY.
7. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks / C. Kyrkou, A. Papachristodoulou, T. Theocharides [et al.] // Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI : 19, Limassol, 06–08 ijulja 2020 goda. Limassol, 2020. P. 476-481. – DOI 10.1109/ISVLSI49217.2020.00-11.
8. LSTM neural networks for detecting anomalies caused by web application cyber-attacks / I. Kotenko, I. Saenko, O. Lauta, K. Kribel // Frontiers in Artificial Intelligence and Applications. 2021. Vol. 337. P. 127-140. – DOI 10.3233/FAIA210014. – EDN DBNPSR.
9. Budko N. P., Vasil'ev N. V. Obzor grafo-analiticheskih podhodov k monitoringu informacionno-telekommunikacionnyh setej i ih primenenie dlja vyjavlenija anomal'nyh sostojanij // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 6. S. 53-75. – DOI 10.24412/2410-9916-2021-6-53-75. – EDN KVLWCE.
10. Maslennikov O. V., Nekorkin V. I. Adaptivnye dinamicheskie seti // Uspehi fizicheskih nauk. 2017. T. 187. № 7. S. 745-756. – DOI 10.3367/UFNr.2016.10.037902. – EDN YTNSJV.
11. Pavlenko, E. Ju. Model' funkcionirovanija adaptivnoj setevoj topologii krupnomasshtabnyh sistem na osnove dinamicheskoj teorii grafov // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2022. № 3. S. 68-79. – DOI: 10.48612/jisp/tn56-xvah-7tf1. – EDN WUDQXX.
12. Astapov R. L., Muhamadeeva R. M. Avtomatizacija podbora parametrov mashinnogo obuchenija i obuchenie modeli mashinnogo obuchenija // Aktual'nye nauchnye issledovanija v sovremennom mire. 2021. № 5-2(73). S. 34-37. – EDN GJEUNW.
13. Tormozov V. S., Zolkin A. L., Vasilenko K. A. Nastrojka, obuchenie i testirovanie nejronnoj seti dolgoj kratkosrochnoj pamjati dlja zadachi raspoznavanija obrazov // Promyshlennye ASU i kontrollery. 2020. № 3. S. 52-57. – DOI 10.25791/asu.3.2020.1171.
14. Pustynnyj, Ja. N. Reshenie problemy ischezajushhego gradienta s pomoshh'ju nejronnyh setej dolgoj kratkosrochnoj pamjati // Innovacii i investicii. 2020. № 2. S. 130-132. – EDN MRQIHM.
15. Multihead Self-attention and LSTM for Spacecraft Telemetry Anomaly Detection / S. Gundawar, N. Kumar, P. Yash [et al.] // Communications in Computer and Information Science. 2022. Vol. 1528. P. 463-479. – DOI: 10.1007/978-3-030-95502-1_35. – EDN PYVPLX.