Научная статья
УДК 004.056.53
https://doi.org/10.31854/1813-324X-2026-12-2-102-112
EDN:MNHGTS

Модель процесса мониторинга сетевой безопасности сети передачи данных в условиях многоэтапных атак

Александр Александрович Шевченко[1], shevchenko.aa@sut.ru
Вадим Александрович Задбоев[2] ✉, zadboev89@mail.ru
Валерий Алексеевич Липатников[2], lipatnikovanl@mail.ru
Кирилл Витальевич Мелехов[2], kirill_melehov@bk.ru
Павел Игоревич Кузин[3], kuzik78@mail.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Военная академия связи им. Маршала Советского Союза С.М. Буденного, Санкт-Петербург, 194064, Российская Федерация
[3]Санкт-Петербургский государственный лесотехнический университет им. С.М. Кирова, Санкт-Петербург, 194021, Российская Федерация

Аннотация

Постановка задачи. *Развитие современных технологий приводит к тому, что в процессе реализации многоэтапных атак злоумышленники используют интеллектуальные и высокотехнологические инструменты для сокрытия своего воздействия на сетевую инфраструктуру. Противостояние данным атакам является одной из основных задач мониторинга информационной безопасности сети передачи данных. На основе существующей проблемы постоянно требуются новые инструменты противодействия или же оптимизации работы существующих систем обнаружения аномалий, которые позволяют не только эффективнее получать необходимую информацию, но и на ее основе улучшить прогнозирование потенциальных кибератак в будущем.*

Цель исследования: *определить взаимосвязь вероятностно-временны́х характеристик процесса мониторинга сетевой безопасности.*

Результаты. *Предложена структура средства мониторинга сетевой безопасности, в которой используются потоковые двухслойные рекуррентные нейронные сети с управляемыми синапсами для классификации и прогнозирования многоэтапных атак. Проведено моделирование процесса мониторинга сетевой безопасности сети передачи данных с целью определения влияния на него различных факторов. Создано программное обеспечение для расчета вероятностно-временны́х характеристик процесса мониторинга сетевой безопасности сети передачи данных в условиях воздействия злоумышленника.*

Теоретическая значимость: *использование предлагаемой модели и программного обеспечения позволяет сформировать требования к различным подпроцессам мониторинга сетевой безопасности сети передачи данных.*

Практическая значимость: *использование предлагаемой модели возможно в качестве основы при разработке систем по предотвращению многоэтапных атак злоумышленника.*

Ключевые слова: *моделирование, рекуррентные нейронные сети, киберугроза, управляемые синапсы, информационная безопасность, сеть передачи данных, многоэтапная атака, раннее обнаружение*

Ссылка для цитирования: Шевченко А.А., Задбоев В.А., Липатников В.А., Мелехов К.В., Кузин П.И. Модель процесса мониторинга сетевой безопасности сети передачи данных в условиях многоэтапных атак // Труды учебных заведений связи. 2026. Т. 12. № 2. С. 102–112. DOI:10.31854/1813-324X-2026-12-2-102-112. EDN:MNHGTS

Original research
https://doi.org/10.31854/1813-324X-2026-12-2-102-112
EDN:MNHGTS

A Model for the Network Security Monitoring Process in Data Transmission Networks Under Multi-Stage Attack Conditions

Aleksandr A. Shevchenko[1], shevchenko.aa@sut.ru
Vadim A. Zadboev[2] ✉, zadboev89@mail.ru
Valery A. Lipatnikov[2], lipatnikovanl@mail.ru
Kirill V. Melekhov[2], kirill_melehov@bk.ru
Pavel I. Kuzin[3], kuzik78@mail.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Telecommunications Military Academy,
St. Petersburg, 194064, Russian Federation
[3]Saint-Petersburg State Forest Technical University,
St. Petersburg, 194021, Russian Federation

Annotation

Statement of the problem. *The advancement of modern technologies has enabled adversaries to employ intelligent and sophisticated tools during the execution of multi-stage attacks to conceal their activities within the network infrastructure. Countering such attacks constitutes one of the primary objectives of information security monitoring for data transmission networks. Given this persistent challenge, there is a continuous demand for the development of novel countermeasures or the optimization of existing anomaly detection systems. These systems must not only facilitate more efficient acquisition of relevant information but also leverage this information to enhance the prediction of potential cyberattacks.*

Purpose: *to determine the relationship between the probabilistic and temporal characteristics of the network security monitoring process.*

Results. *A network security monitoring tool structure is proposed that utilizes streaming two-layer recurrent neural networks with controlled synapses to classify and predict multi-stage attacks. The network security monitoring process for a data transmission network was modeled to determine the impact of various factors. Software was developed to calculate the probabilistic and temporal characteristics of the network security monitoring process for a data transmission network under attacker attack.*

Theoretical significance. *The model and software used allow for the formulation of requirements for various subprocesses of network security monitoring for a data transmission network.*

Practical Significance: *The proposed model can serve as a foundational framework for the development of systems designed to prevent multi-stage attacks.*

Keywords: *modeling, recurrent neural networks, cyber threat, controlled synapses, information security, data network, multi-stage attack, early detection*

For citation: Shevchenko A.A., Zadboev V.A., Lipatnikov V.A., Melekhov K.V., Kuzin P.I. A Model for the Network Security Monitoring Process in Data Transmission Networks Under Multi-Stage Attack Conditions. *Proceedings of Telecommunication Universities.* 2026;12(2):102–112. (in Russ.) DOI:10.31854/1813-324X-2026-12-2-102-112. EDN:MNHGTS

Введение

Современные сети передачи данных (СПД) часто могут стать объектами воздействия злоумышленников, реализующегося в виде многоэтапных атак (МЭА). МЭА, в отличие от одноэтапных атак, представляют собой последовательно взаимосвязанные этапы, разнесенные во времени и логически зависимые друг от друга образующие единый жизненный

цикл. Жизненный цикл МЭА в основном включает в себя пять ключевых этапов: разведку (OSINT), создание инструментов и выбор методов атаки, проникновение систему через уязвимости, повышение прав в системе и заметание следов для сокрытия своей активности. Благодаря такой особенности МЭА длятся дольше, но имеют высокую степень скрытности и адаптации к защитным мерам.

В процессе реализации МЭА злоумышленники эксплуатируют различные уязвимости в программном, аппаратном и организационном обеспечении сетевой инфраструктуры. Для этого применяются различные инструментарии в зависимости от текущей задачи. На этапах разведки широко используются сканеры портов и уязвимостей, такие как *Nmap, Masscan и OpenVAS*. Для проникновения в систему применяются фреймворки *Metasploit, Cobalt Strike, PowerShell Empire* и аналогичные средства. Для закрепления в системе и повышения прав используются троянские программы, бэкдоры, ботнет-клиенты и средства скрытого удаленного доступа. Для скрытия своей деятельности применяются методы шифрования трафика, прокси-серверы и VPN.

МЭА характеризуются рядом наблюдаемых признаков. На ранних этапах возможна аномальная сетевая активность в виде нетипичных сканирований или попыток подключения к закрытым портам. На более поздних этапах отмечаются множественные неудачные попытки аутентификации, появление неизвестных процессов и служб на узлах, изменения в системных файлах и реестре или аномальные обращения к ресурсам, не соответствующие профилю пользователя.

В противодействие данным атакам требуются инструменты активной защиты, эффективно выявляющие и предотвращающие деятельность злоумышленников в СПД путем вмешательства в этапы жизненного цикла МЭА. Активная защита предусматривает мониторинг информационной безопасности (ИБ) СПД, который включает в себя своевременный анализ киберугроз, определение геолокации источника кибератаки в совокупности с планированием и принятием мер противодействия злоумышленнику путем его нейтрализации. Ввиду того, что геополитическая обстановка в мире остается напряженной, информационная инфраструктура Российской Федерации, которая включает в себя совокупность СПД органов власти и госкорпораций, ежедневно подвергается колоссальному кибервлиянию, поэтому задача организации мониторинга защищенности СПД в условиях МЭА остается актуальной. Для обеспечения защиты СПД от МЭА необходима разработка средств мониторинга сетевой безопасности (СМСБ), которые позволят своевременно обнаруживать, определять параметры вторжений и геолокацию злоумышленника.

В настоящее время решением вышеуказанной задачи занимаются ведущие вендоры программных и аппаратных систем ИБ, основывающие свои разработки на результатах исследований в данной области. В статье [1] предложена концептуальная модель процесса функционирования системы для предупреждения атак, которая обеспечивает сравнение эталонных профилей с текущими профилями процесса функционирования с учетом динамики изменения состояния системы. В [2] авторы предлагают метод повышения защищенности сети, основанный на использовании средств определения геолокации злоумышленника, который позволяет ускорить расследование инцидентов ИБ. Разрабатываются способы анализа и прогнозирования категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интеллекта, один из таких предложен в [3–4]. Способ позволяет прогнозировать категории CVE на основе CPE URI с высокой точностью. В статье [5] рассматривается вопрос разработки моделей оценки процесса подготовки и реализации вторжений в сетях IP-телефонии, который обеспечивает прогнозирование, управление устойчивостью и защищенностью сети VoIP, позволяющий эффективно выбирать необходимые способы нейтрализации атак.

В данных источниках описываются различные модели угроз, способы их прогнозирования и устранения, однако не рассматриваются подходы к разработке СМСБ.

Целью статьи является определение взаимосвязи вероятностно-временны́х характеристик процесса мониторинга сетевой безопасности.

В интересах достижения цели необходимо решить следующие задачи:

– разработать структуру СМСБ, в основе которого используется потоковая двухслойная рекуррентная нейронная сеть (РНС) с управляемыми синапсами, которая будет способна выявлять аномалии на ранних стадиях, а также классифицировать распознанные МЭА;

– провести моделирование процесса мониторинга сетевой безопасности СПД при МЭА с целью определения влияния на него различных факторов.

Разработка структуры средства мониторинга сетевой безопасности

В качестве решения поставленной задачи была разработана структура СМСБ (рисунок 1), способная выявлять аномалии на ранних стадиях, классифицировать и прогнозировать распознанные МЭА.

Далее представлены описания каждого блока СМСБ.

Блок обработки цифрового потока (ЦП) отвечает за аналитическую обработку потока данных, осуществляя над ними различные операции, такие как

классификация, регрессия, сегментация и другие [6–7]. Он адаптирует нейросетевую архитектуру под конкретные задачи обработки входящих данных, обеспечивая их корректное восприятие системой.

Блок формирования синтаксической конструкции ЦП и протокола отвечает за организацию и структурирование информации для последующей передачи, кодируя данные согласно установленным правилам [8–9]. Синтаксическая конструкция определяет формат данных, их структуру и правила обмена информацией, включая заголовки, поля данных, контрольные суммы и другие элементы. Этот блок обеспечивает корректное представление информации как внутри системы, так и при внешней передаче, гарантируя совместимость и безопасность данных.

Блок нормализации и кодирования выполняет предварительную обработку данных, приводя их к единому формату для оптимального восприятия РНС [10]. Он отвечает за нормализацию числовых значений, кодирование категориальных данных с помощью метода one-hot-кодирования, обработку текстовых данных через токены, удаление стоп-слов и преобразование слов в числовые векторы с использованием технологий типа Word2Vec или TF-IDF, а также масштабирование данных для улучшения сходимости модели при обучении.

Блок задержки используется для работы с временны́ми рядами, сохраняющие информацию о предыдущих состояниях системы и передачи ее на следующий временно́й шаг [11–12]. Этот механизм позволяет учитывать долгосрочные зависимости в данных, что особенно важно при решении задач, связанных с анализом речи, видео или других последовательных данных. Блок может быть реализован с помощью различных архитектур, таких как LSTM или GRU.

Блок декодирования генерирует выходные сигналы на основе внутреннего состояния сети и входной информации [13–14]. Этот блок состоит из нескольких слоев, включая рекуррентные слои для передачи информации о предыдущих состояниях и выходные слои для формирования конечного результата. Для повышения качества генерации выходных данных могут использоваться механизмы внимания (*attention*), которые позволяют сфокусироваться на наиболее важных частях входных данных.

Блок управления (БУ) координирует работу всех компонентов системы, организует процессы обучения нейросети, принимает решения на основе полученных результатов и управляет вычислительными ресурсами [15–16]. Он может использовать различные алгоритмы и стратегии, такие как обратное распространение ошибки, градиентный спуск или регуляризация, для оптимизации производительности модели. Помимо этого, БУ анализирует результаты работы системы и отправляет команды другим системам или устройствам для выполнения конкретных действий.

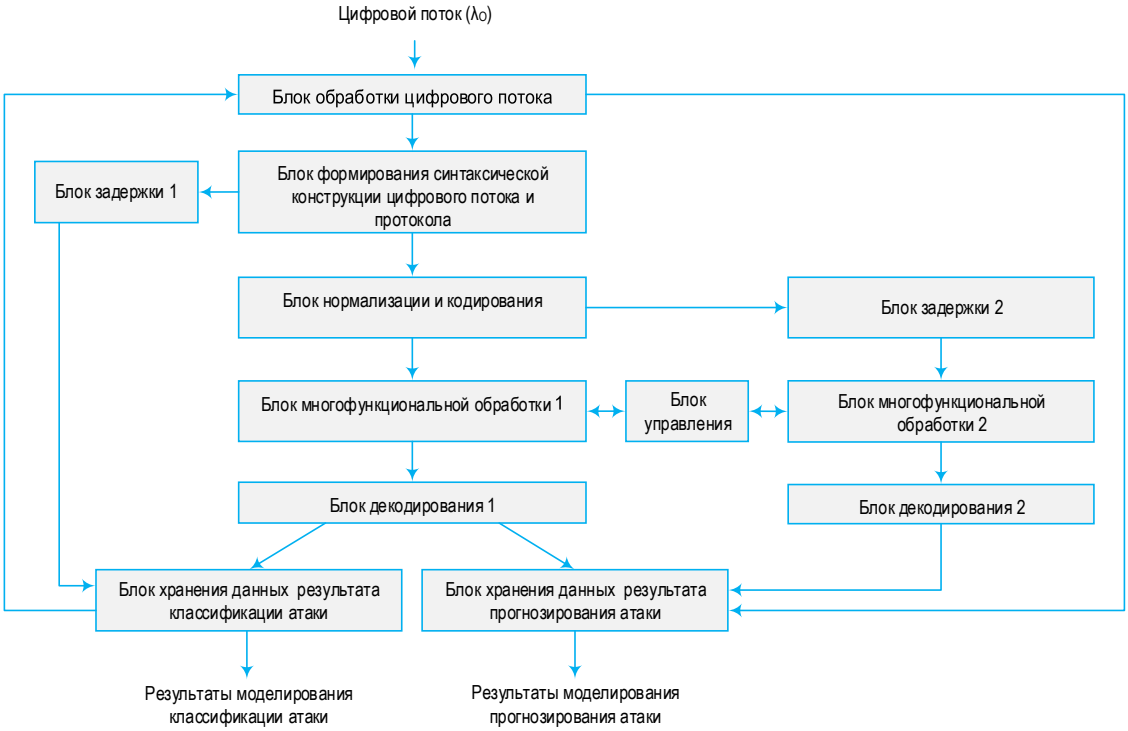

Рис. 1. Структура средства мониторинга сетевой безопасности

Fig. 1. Structure of the Network Security Monitoring Tool

Блок многофункциональной обработки отвечает за обработку последовательных данных. В представленных на рисунках 2 и 3 схемах работает два разных блока, один из которых использует технологии самоорганизующихся карт Кохонена и древовидные модели классификации для анализа зависимостей между элементами данных. Карты Кохонена позволяют выполнять кластеризацию данных и находить скрытые закономерности, а древовидные модели эффективно классифицируют объекты на основе множества признаков. Эти технологии особенно полезны при работе с большими объемами данных, где требуется выявить сложные паттерны и связи.

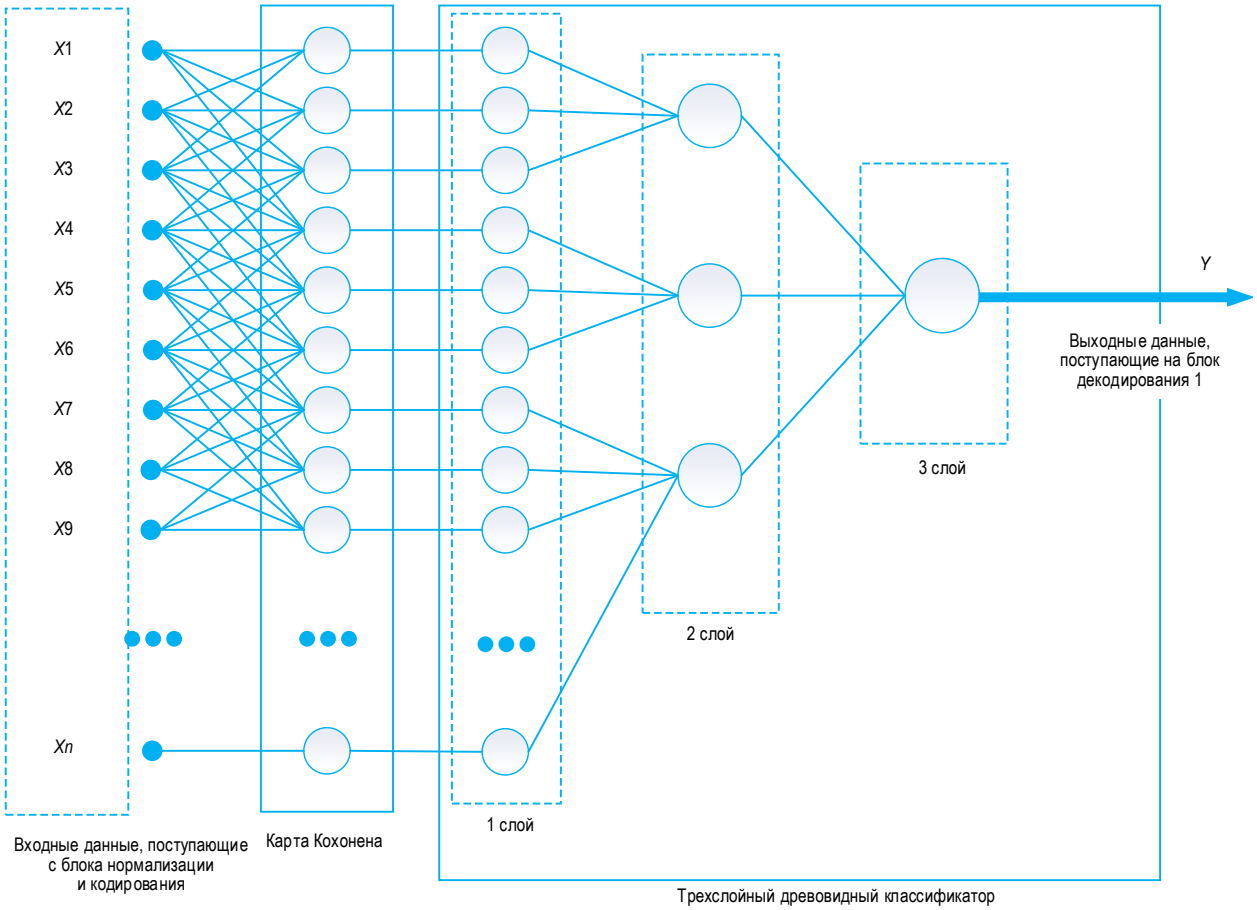

Рис. 2. Схема блока многофункциональной обработки 1

Fig. 2. Multifunctional Processing Unit Diagram 1

Данный блок отвечает за группировку данных (*X1, X2, …, Xn*), включающих в себя результаты анализа сетевого трафика, параметры клиентских приложений и накопленную информацию. Также он отвечает за фильтрацию результатов и выделение целевого класса, характеризующего состояние СПД и обработку значений с помощью древовидного нейронного классификатора, который определяет принадлежность входных значений к заранее заданному классу, описывающему текущее состояние СПД. На основе входных данных модель позволяет однозначно интерпретировать выходное значение как оценку текущего состояния.

На этапе выявления первичных признаков вторжений идентифицируются структурные, неизменные и корреляционные характеристики проводимой атаки, далее обновляются базы данных и уточняются сценарии атак, а после разрабатываются оптимальные меры противодействия и нейтрализации возникшей угрозы.

При выявлении вторичных признаков вторжений проводится анализ корреляционных связей между признаками, далее обновляется база данных со вторичными признаками, уточняется сценарий атаки и на основе обработанной информации разрабатываются эффективные меры противодействия.

Второй блок многофункциональной обработки потока предназначен для прогнозирования МЭА и контроля принятия решений первого блока. Он основан на использовании РНС, имеющие обратную связь между выходным и входным слоями, то есть результат предыдущего шага в потоке является входным сигналом для следующего и так далее [17].

Суть работы второго блока заключается в параллельной обработке разработанных мер противодействия на первом блоке и поиске оптимального решения из предложенных на основе прогнозирования поведения атаки. Результаты прогнозирования предоставляются обратно на первый блок для дальнейшей классификации атаки и принятия решения для ее противодействия.

Так как при прогнозировании МЭА необходимо учитывать состав и последовательность исторических данных для расчета будущих значений, предлагается использовать сети Джордана в виде трехслойной РНС с контекстным слоем (рисунок 3). В сети Джордана контекстные нейроны получают сигнал из выходного слоя и подаются обратно во времени на вход сети. Это позволяет модели использовать контекст прошлых состояний для прогнозирования будущих состояний [18].

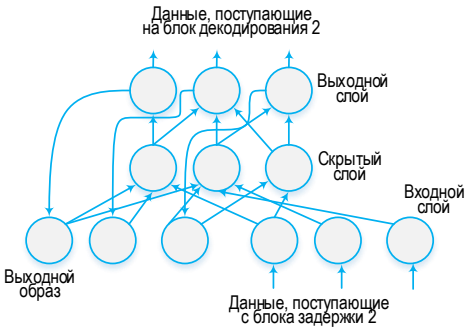

Рис. 3. Схема блока многофункциональной обработки 2

Fig. 3. Multifunctional Processing Unit Diagram 2

Сеть Джордана в виде трехслойной РНС с контекстным слоем имеет полносвязные слои с рекуррентной обратной связью от выходного слоя, позволяющая использовать выходные сигналы на предыдущем шаге для прогнозирования и последующего обучения. Однако следует учитывать одну из ключевых проблем сетей Джордана, связанную с затуханием или взрывом градиентов, что может осложнять процесс обучения и негативно сказываться на производительности модели, особенно при работе с длинными временны́ми последовательностями данных.

По итогу текущего цикла работы СМСБ при параллельной работе двух блоков многофункциональной обработки выводится результат классификации атаки с мерами защиты против нее и прогноз ее возможного поведения. По окончании цикла работы результаты отправляются на входные данные СМСБ для дальнейшего обучения.

Моделирование процесса мониторинга сетевой безопасности передачи данных при многоэтапных атаках

Для корректного описания процесса мониторинга сетевой безопасности СПД при МЭА проведено его преобразование в математическую модель, которая бы учитывала ключевые особенности СМСБ. В качестве возможного подхода используется представление СМСБ как система с переменной структурой, где ее поведение на случайных временны́х интервалах описывается разными режимами работы: наблюдением, обороной и восстановлением; а переходы между этими структурами зависят от текущих параметров системы, например фазовых координат, и подчиняются вероятностным законам. В отличие от точностных характеристик, отражающих корректность классификации сетевых атак, или временны́х показателей, определяющих быстродействие системы обнаружения, вероятностно-временны́е характеристики позволяют оценить вероятность выявления вторжения за заданный промежуток времени. Данные показатели наиболее полно отражают эффективность СМСБ в условиях МЭА. Для такого подхода используется теория марковских процессов, где следующее состояние системы определяется только текущим состоянием, а для анализа динамики вероятностны́х распределений применяется уравнение Фоккера – Планка – Колмогорова, позволяющее прогнозировать эволюцию системы, минимизировать риски и оптимизировать ее работу в условиях неопределенности, как это показано в [19]. На рисунке 4 изображен граф состояний СМСБ в процессе мониторинга сетевой безопасности СПД при МЭА, где $\underline{P_i}$ обозначает вероятность нахождения системы в i-м состоянии. В таблице 1 приведены параметры, характеризующие данный процесс.

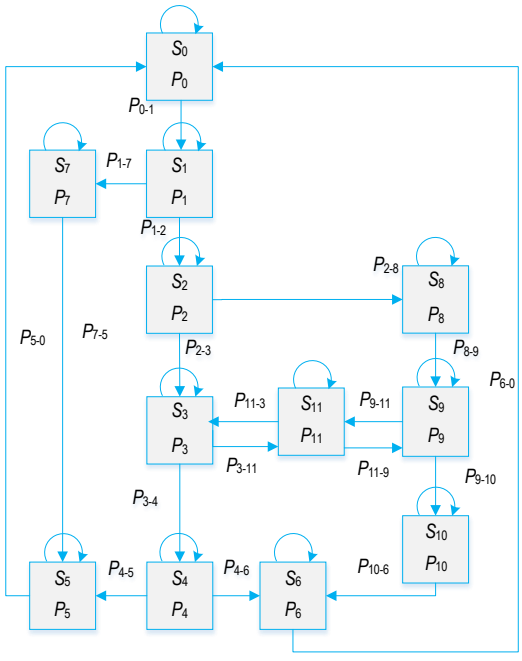

Рис. 4. Граф состояний средства мониторинга сетевой безопасности СПД при МЭА

Fig. 4. State Graph of a Network Security Monitoring Tool for Data Transmission Networks Under a multi-stage attack

ТАБЛИЦА 1. Параметры процесса реализации успешного выявления аномалий

TABLE 1. Parameters of the Process for Implementing Successful Anomaly Detection

S_n	Описание состояния S_n	Интенсивность перехода в состояние S_m	Параметр	Описание параметра	Значение параметра, с
S_0	СМСБ ожидает входной ЦП данных для начала обработки	$\lambda_{0-1} = \frac{1}{\overline{t}_{\text{О}}}$	$\overline{t}_{\text{О}}$	Среднее время обработки входного ЦП данных	2000
S_1	СМСБ производит кодирование и структурирование информации	$\lambda_{1-2/1-7} = \frac{1}{\overline{t}_{\text{ФС}}}$	$\overline{t}_{\text{ФС}}$	Среднее время формирования синтаксической конструкции цифрового потока и протокола	10 20 30
S_2	СМСБ обрабатывает входные данные перед их подачей на РНС	$\lambda_{2-3/2-8} = \frac{1}{\overline{t}_{\text{ОД}}}$	$\overline{t}_{\text{ОД}}$	Среднее время обработки входных данных перед их подачей на РНС	500
$S_{3(9)}$	СМСБ анализирует и моделирует зависимости между элементами последовательности	$\lambda_{3-\frac{4}{3}11\left(9-\frac{10}{9}11\right)} = \frac{1}{\overline{t}_{\text{АМ1(АМ2)}}}$	$\overline{t}_{\text{АМ1(АМ2)}}$	Среднее время анализа и моделирования зависимости между элементами последовательности	110 (115)
$S_{4(10)}$	СМСБ генерирует выходной сигнал или последовательность данных на основе предыдущих скрытых состояний и входных данных	$\lambda_{4-5/4-6(10-6)} = \frac{1}{\overline{t}_{\text{Г1(Г2)}}}$	$\overline{t}_{\text{Г1(Г2)}}$	Среднее время генерации выходного сигнала или последовательности данных на основе предыдущих скрытых состояний и входных данных	1 (130)
S_5	СМСБ классифицирует МЭА	$\lambda_{5-0} = \frac{1}{\overline{t}_{\text{СК}}}$	$\overline{t}_{\text{СК}}$	Среднее время классификации МЭА	100
S_6	СМСБ прогнозирует МЭА	$\lambda_{6-0} = \frac{1}{\overline{t}_{\text{СП}}}$	$\overline{t}_{\text{СП}}$	Среднее время прогнозирования МЭА	300
$S_{7(8)}$	СМСБ сохраняет информацию о предыдущих состояниях и передает ее на следующий временно́й шаг	$\lambda_{7-5(8-9)} = \frac{1}{\overline{t}_{\text{СИ1(СИ2)}}}$	$\overline{t}_{\text{СИ1(СИ2)}}$	Среднее время сохранения информации о предыдущих состояниях и передачи ее на следующий временно́й шаг	100 (120)
S_{11}	СМСБ обучает и использует РНС	$\lambda_{11-3/11-9} = \frac{1}{\overline{t}_{\text{ОП}}}$	$\overline{t}_{\text{ОП}}$	Среднее время обучения и использования РНС	1000

Усл. обозначения: S_n – состояние системы

На основе полученного графа состояний составим систему дифференциальных уравнений:

$$\begin{cases}
\frac{dP_0(t)}{dt} = \lambda_{5-0}P_5(t) + \lambda_{6-0}P_6(t) - \lambda_{0-1}P_0(t);\\
\frac{dP_1(t)}{dt} = \lambda_{0-1}P_0(t) - (\lambda_{1-2} + \lambda_{1-7})P_1(t);\\
\frac{dP_2(t)}{dt} = \lambda_{1-2}P_1(t) - (\lambda_{2-3} + \lambda_{2-8})P_2(t);\\
\frac{dP_3(t)}{dt} = \lambda_{2-3}P_2(t) + \lambda_{11-3}P_{11}(t) - (\lambda_{3-4} + \lambda_{3-11})P_3(t);\\
\frac{dP_4(t)}{dt} = \lambda_{3-4}P_3(t) - (\lambda_{4-5} + \lambda_{4-6})P_4(t);\\
\frac{dP_5(t)}{dt} = \lambda_{4-5}P_4(t) + \lambda_{7-5}P_7(t) - \lambda_{5-0}P_5(t);\\
\frac{dP_6(t)}{dt} = \lambda_{4-6}P_4(t) + \lambda_{10-6}P_{10}(t) - \lambda_{6-0}P_6(t);\\
\frac{dP_7(t)}{dt} = \lambda_{1-7}P_1(t) - \lambda_{7-5}P_7(t);\\
\frac{dP_8(t)}{dt} = \lambda_{2-8}P_2(t) - \lambda_{8-9}P_8(t);\\
\frac{dP_9(t)}{dt} = \lambda_{8-9}P_8(t) + \lambda_{11-9}P_{11}(t) - (\lambda_{9-10} + \lambda_{9-11})P_9(t);\\
\frac{dP_{10}(t)}{dt} = \lambda_{9-10}P_9(t) - \lambda_{10-6}P_{10}(t);\\
\frac{dP_{11}(t)}{dt} = \lambda_{3-11}P_3(t) + \lambda_{9-11}P_9(t) - (\lambda_{11-9} + \lambda_{11-3})P_{11}(t).
\end{cases}$$

Решение системы уравнений представлено выражением:

$$\begin{cases}
P_0 = \alpha;\\
P_1 = a\alpha;\\
P_2 = b\alpha;\\
P_3 = c\alpha;\\
P_4 = d\alpha;\\
P_5 = e\alpha;\\
P_6 = f\alpha;\\
P_7 = g\alpha;\\
P_8 = h\alpha;\\
P_9 = j\alpha;\\
P_{10} = k\alpha;\\
P_{11} = l\alpha,
\end{cases}$$

где:

$$\alpha = \frac{1}{1 + a + b + c + d + e + f + g + h + i + j + k},$$

$$a = \frac{\lambda_{0-1}}{\lambda_{1-2} + \lambda_{1-7}},$$

$$b = \frac{\lambda_{0-1}\lambda_{1-2}}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})},$$

$$c = \frac{\lambda_{0-1}\lambda_{1-2}(\lambda_{2-3} + \lambda_{11-3}b)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})},$$

$$d = \frac{\lambda_{0-1}\lambda_{1-2}\lambda_{3-4}(\lambda_{2-3} + \lambda_{11-3}b)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})},$$

$$e = \frac{\lambda_{0-1}}{\lambda_{5-0}(\lambda_{1-2} + \lambda_{1-7})} \times$$
$$\times \left(\frac{\lambda_{1-2}\lambda_{3-4}\lambda_{4-5}(\lambda_{2-3} + \lambda_{11-3}b)}{(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})} + \lambda_{1-7} \right),$$

$$f = \frac{\lambda_{0-1}\lambda_{1-2}}{\lambda_{6-0}(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})} \times$$
$$\times \left(\frac{\lambda_{3-4}(\lambda_{2-3} + \lambda_{11-3}c)}{(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})} + \frac{\lambda_{9-10}(\lambda_{2-8} + \lambda_{11-9}b)}{\lambda_{9-10} + \lambda_{9-11}} \right),$$

$$g = \frac{\lambda_{0-1}\lambda_{1-7}}{\lambda_{7-5}(\lambda_{1-2} + \lambda_{1-7})},$$

$$h = \frac{\lambda_{0-1}\lambda_{1-2}\lambda_{2-8}}{\lambda_{8-9}(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})},$$

$$i = \frac{\lambda_{0-1}\lambda_{1-2}(\lambda_{2-8} + \lambda_{11-9}b)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{9-10} + \lambda_{9-11})},$$

$$j = \frac{\lambda_{0-1}\lambda_{1-2}\lambda_{9-10}(\lambda_{2-8} + \lambda_{11-9}b)}{\lambda_{10-6}(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{9-10} + \lambda_{9-11})},$$

$$k = \frac{\lambda_{0-1}\lambda_{1-2}b}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})}.$$

Успешное выявление аномалий (P_A) может быть в двух состояниях, а именно при реализации классификации (P_5) или при прогнозировании кибератаки (P_6), где в конечном итоге процесс переходит к выявлению последующей аномалии, то есть система должна быть эффективной в независимости от режима работы или других состояний СМСБ.

С учетом вышесказанного вероятность успешного выявления аномалии примет вид:

$$\begin{cases} P_A = \alpha(1 + e), \text{если кибератака неизвестная;} \\ P_A = \alpha(1 + f), \text{если кибератака известна.} \end{cases}$$

На основе системы уравнений с исходными данными из таблицы 1 была проведена верификация разработанной модели. В целях автоматизации будущих расчетов зависимостей было разработано программное обеспечение [20–21], интерфейсы которого представлены на рисунке 5. Программное обеспечение в консольном окне (рисунок 5a) получает на вход все требуемые значения параметров и проводит расчет вероятностей на основе заранее подготовленных формул. По окончании вычислений для наглядного представления выводятся графики (рисунок 5b) полученных зависимостей.

В результате успешных расчетов получены зависимости вероятности успешного выявления аномалий (P_A) от времени обработки входных данных ($t_{ОД}$) в виде закодированной и структурированной информации перед их подачей на РНС в случаях, когда обнаружена:

1) неизвестная кибератака и необходима ее дальнейшая классификация (рисунок 6a);

2) известная кибератака и необходимо прогнозировать ход ее возможной реализации (рисунок 6b).

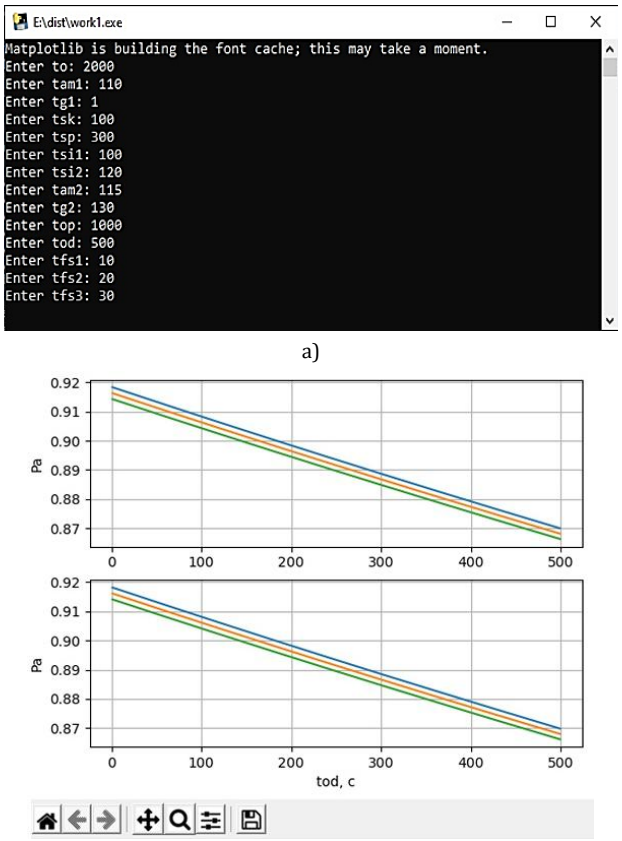

Рис. 5. Интерфейс программного продукта «Программа расчета вероятностно-временных характеристик средств сетевого контроля в условиях многоэтапных атак»: a) консоль ввода исходных данных; b) поле вывода графиков

Fig. 5. Interface of the Software Product «Program for Calculating the Probabilistic-Temporal Characteristics of Network Control Tools Under Conditions of Multi-Stage Attacks»: a) Console for Inputting Initial Data; b) Field for Outputting Graphs

Анализ зависимостей, представленных на рисунке 6, позволяет сделать следующие выводы:

– вероятность выявления аномалии (P_A) зависит от времени кодирования и структурирования информации ($t_{ФС}$), в связи с этим при разработке СМСБ необходимо использовать оптимальные по времени методы реализации данного подпроцесса;

– на обработку данных процесса выявления аномалий в случае реализации злоумышленником неизвестной МЭА тратиться больше на 5 %, чем при реализации известной МЭА, следовательно, необходимо при разработке СМСБ также использовать оптимальный по времени метод кодирования и структурирования информации, либо наиболее быстродействующие методы обработки данных.

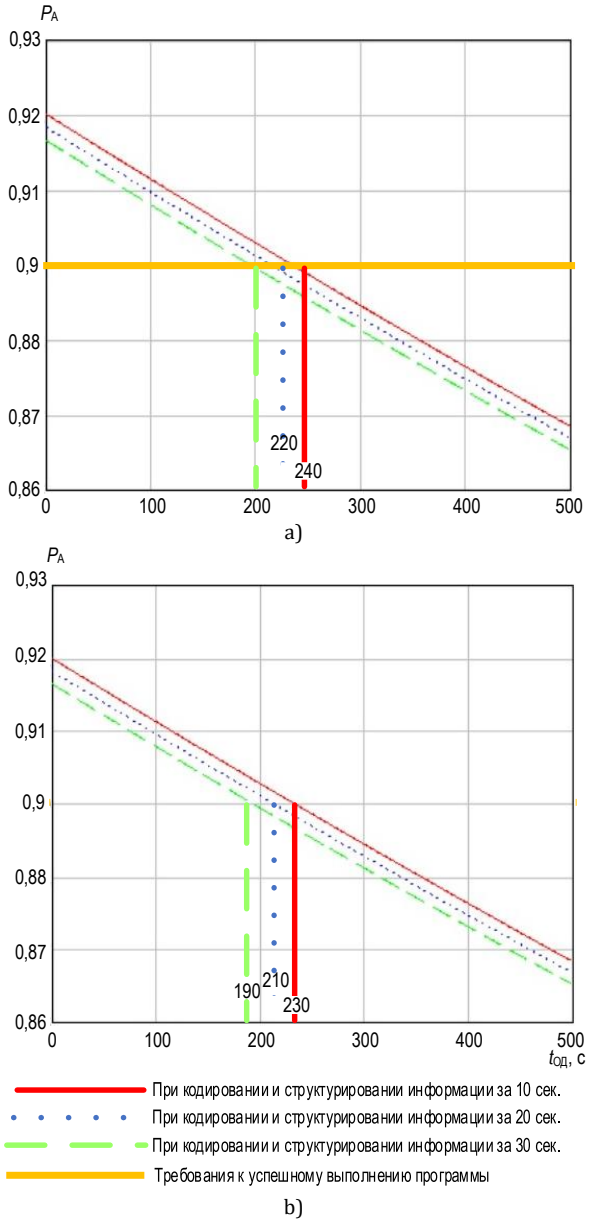

Рис. 6. Изменение вероятности P_A успешного выявления аномалий в случае реализации злоумышленником: а) неизвестной МЭА; b) известной МЭА

Fig. 6. Change in the Probability of P_A Successful Detection of Anomalies: a) in the Case of an Unknown Multi-Stage Attack by an Intruder; b) in the Case of an Attacker Implementing a Known Multi-Stage Attack

Заключение

В рамках исследования была предложена структура СМСБ, в которой используются потоковые двухслойные РНС с управляемыми синапсами для классификации и прогнозирования МЭА.

Основной функцией предлагаемого СМСБ является мониторинг сетевой безопасности, который является сложным технологическим процессом, зависящим от множества внутренних и внешних факторов. В связи с этим проведено моделирование данного процесса при МЭА с целью определения влияния на него различных факторов. На основе разработанной модели создано программное обеспечение для расчета вероятностно-временны́х характеристик процесса мониторинга сетевой безопасности СПД в условиях воздействия злоумышленника. Использование модели и программного обеспечения позволяет сформировать требования к различным подпроцессам мониторинга сетевой безопасности СПД, которые возможно будет использовать как критерии выбора технологий, методов и способов при разработке СМСБ.

Результаты моделирования процесса мониторинга сетевой безопасности СПД при МЭА позволяют сформулировать логичные корректные выводы по взаимосвязи вероятностно-временны́х характеристик данного процесса, что говорит об адекватности предлагаемых решений.

Научная новизна приведенных исследований заключается в том, что представленный подход к мониторингу и прогнозированию сетевой безопасности СПД при МЭА отличается использованием двухслойных РНС с управляемыми синапсами.

Теоретическая значимость заключается в использовании основных положений теорий массового обслуживания, вероятности, марковских цепей для развития методологических положений теории управления защищенностью систем.

Практическая значимость определяется возможностью использования предложенной модели в качестве основы при разработке систем по предотвращению МЭА злоумышленника.

Список источников

1. Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. Динамическая модель контроля функционирования для предупреждения компьютерных атак // Правовая информатика. 2024. № 2. С. 35–43. DOI:10.21681/1994-1404-2024-2-35-43. EDN:OGOTEF

2. Липатников В.А., Задбоев В.А., Мелехов К.В., Шевченко А.А. Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя // Труды учебных заведений связи. 2023. Т. 9. № 4. С. 86–96. DOI:10.31854/1813-324X-2023-9-4-86-96. EDN:FWQHUC

3. Левшун Д.С., Веснин Д.В., Котенко И.В. Прогнозирование категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интеллекта // Вопросы кибербезопасности. 2024. № 3(61). С. 33–39. DOI:10.21681/2311-3456-2024-3-33-39. EDN:FTORLR

4. Kim S., Park K.J., Lu C.A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design // IEEE Communications Surveys & Tutorials. 2022. Vol. 24. Iss. 3. PP. 1534–1573. DOI:10.1109/COMST.2022.3187531. EDN:ZEUEHY

5. Липатников В.А., Косолапов В.С., Шевченко А.А., Сокол Д.С. Модель оценки процесса подготовки и реализации

вторжений в сетях IP-телефонии // Информация и космос. 2021. № 4. С. 55–69. EDN:FRPUPC

6. Zhou P., Zhou G., Wu D., Fei M. Detecting multi-stage attacks using sequence-to-sequence model // Computers & Security. 2021. Vol. 105. P. 102203. DOI:10.1016/j.cose.2021.102203. EDN:KUKUOO

7. Mishra S., Alotaibi W.B., Alshehri M., Saxena S. Cyber-attacks visualisation and prediction in complex multi-stage network // International Journal of Computer Applications in Technology. 2022. Vol. 68. Iss. 4. PP. 345–356. DOI:10.1504/IJCAT.2022.125180. EDN:CQPVYR

8. Weerakody P.B., Wong K.W., Wang G., Ela W. A review of irregular time series data handling with gated recurrent neural networks // Neurocomputing. 2021. Vol. 441. PP. 161–178. DOI:10.1016/j.neucom.2021.02.046. EDN:JKFTCG

9. Olszewski D. A data-scattering-preserving adaptive self-organizing map // Engineering Applications of Artificial Intelligence. 2021. Vol. 105. P. 104420. DOI:10.1016/j.engappai.2021.104420. EDN:EGGQEI

10. Осипов В.Ю., Никифоров В.В. Кодирование и устойчивость обработки сигналов в потоковых рекуррентных нейронных сетях // Информационно-управляющие системы. 2021. № 3(112). С. 9–18. DOI:10.31799/1684-8853-2021-3-9-18. EDN:TMUFQK

11. Al-Turaiki I., Altwaijry N. A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection // Big Data. 2021. Vol. 9. Iss. 3. PP. 233–252. DOI:10.1089/big.2020.0263. EDN:BINXTC

12. Sarker I.H. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective // SN Computer Science. 2021. Vol. 2. Iss. 3. P. 154. DOI:10.1007/s42979-021-00535-6. EDN:EKIIIP

13. Gong J. Network Information Security Pipeline Based on Grey Relational Cluster and Neural Networks // Proceedings of the 5th International Conference on Computing Methodologies and Communication (Erode, India, 08–10 April 2021). IEEE, 2021. PP. 971–975. DOI:10.1109/ICCMC51019.2021.9418311

14. Khan M.A. HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System // Processes. 2021. Vol. 9. Iss. 5. P. 834. DOI:10.3390/pr9050834. EDN:BBATMC

15. Долгачев М.В., Москвичев А.Д., Москвичева К.С. Обнаружение атак на веб-приложение с помощью самоорганизующихся карт Кохонена // Вопросы кибербезопасности. 2024. № 1(59). С. 38–44. DOI:10.21681/2311-3456-2024-1-38-44. EDN:KHTKXR

16. Плетенкова А.Д., Соколов А.Н. Применение двухэтапного метода кластеризации на основе самоорганизующейся карты Кохонена для обнаружения аномалий в синтетических наборах данных // Вестник УрФО. Безопасность в информационной сфере. 2024. Т. 4(54). С. 49–60. DOI:10.14529/secur240406. EDN:ZLGTJQ

17. Pinto A., Herrera L.-C., Donoso Y., Gutierrez J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure // Sensors. 2023. Vol. 23. Iss. 5. P. 2415. DOI:10.3390/s23052415. EDN:GBGCLV

18. Yang H., Li X., Qiang W., Zhao Y., Zhang W., Tang C. A network traffic forecasting method based on SA optimized ARIMA–BP neural network // Computer Networks. 2021. Vol. 193. P. 108102. DOI:10.1016/j.comnet.2021.108102. EDN:NKGPOO

19. Липатников В.А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121–130. EDN:KSBCGK

20. Робак В.А., Липатников В.А., Парфиров В.А., Задбоев В.А., Шевченко А.А., Петренко М.И. и др. Программа расчета вероятностно-временных характеристик средств сетевого контроля в условиях многоэтапных атак. Свидетельство о регистрации программы для ЭВМ № RU 2024661259 от 11.04.24. Опубл. 16.05.24. EDN:WTNJLT

21. Савина А.Г., Малявкина Л.И., Герасимова Ю.Я., Жилина Д.Е. Язык программирования Python в научных вычислениях // Национальная научно-практическая конференция «Инфраструктура цифрового развития образования и бизнеса» (Орел, Российская Федерация, 01–30 апреля 2021 г.). Орёл: Орловский государственный университет экономики и торговли, 2021. С. 64-69. EDN:CPPPGG

References

1. Kotenko I., Saenko I., Zakharchenko R., Velichko D. A Dynamic Functioning Control Model for Preventing Computer Attacks. *Legal Informatics.* 2024;2:35–43. (in Russ.) DOI:10.21681/1994-1404-2024-2-35-43. EDN:OGOTEF

2. Lipatnikov V., Zadboev V., Melekhov K., Shevchenko A. A Method of Improving the Security of Information and Telecommunications Network Using the Means of Determining Intruder's Geolocation. *Proceedings Telecommunication Universities.* 2023;9(4):86–96. (in Russ.) DOI:10.31854/1813-324X-2023-9-4-86-96. EDN:FWQHUC

3. Levshun D.S., Vesnin D.V., Kotenko I.V. Prediction of Vulnerability Categories in Configurations of Devices Using Artificial Intelligence Methods. *Cybersecurity Issues.* 2024;3(61):33–39. (in Russ.) DOI:10.21681/2311-3456-2024-3-33-39. EDN:FTORLR

4. Kim S., Park K.J., Lu C. A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design. *IEEE Communications Surveys & Tutorials.* 2022;24(3):1534–1573. DOI:10.1109/COMST.2022.3187531. EDN:ZEUEHY

5. Lipatnikov V.A., Kosolapov V.S., Shevchenko A.A., Sokol D.S. A Model for Evaluating the Process of Preparing and Implementing Intrusions in IP Telephony Networks. *Information and Space.* 2021;4:55–69. (in Russ.) EDN:FRPUPC

6. Zhou P., Zhou G., Wu D., Fei M. Detecting multi-stage attacks using sequence-to-sequence model. *Computers & Security*. 2021;105:102203. DOI:10.1016/j.cose.2021.102203. EDN:KUKUOO

7. Mishra S., Alotaibi W.B., Alshehri M., Saxena S. Cyber-attacks visualisation and prediction in complex multi-stage network. *International Journal of Computer Applications in Technology.* 2022;68(4):345–356. DOI:10.1504/IJCAT.2022.125180. EDN:CQPVYR

8. Weerakody P.B., Wong K.W., Wang G., Ela W. A review of irregular time series data handling with gated recurrent neural networks. *Neurocomputing*, 2021;441:161–178. DOI:10.1016/j.neucom.2021.02.046. EDN:JKFTCG

9. Olszewski D. A data-scattering-preserving adaptive self-organizing map. *Engineering Applications of Artificial Intelligence*. 2021;105:104420. DOI:10.1016/j.engappai.2021.104420. EDN:EGGQEI

10. Osipov V.Yu., Nikiforov V.V. Coding and stability of signal processing in streaming recurrent neural networks. *Information and Control Systems.* 2021;3(112):9–18. (in Russ.) DOI:10.31799/1684-8853-2021-3-9-18. EDN:TMUFQK

11. Al-Turaiki I., Altwaijry N. A convolutional neural network for improved anomaly-based network intrusion detection. *Big Data*. 2021;9(3):233–252. DOI:10.1089/big.2020.0263. EDN:BINXTC
12. Sarker I.H. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. *SN Computer Science.* 2021;2(3):154. DOI:10.1007/s42979-021-00535-6. EDN:EKIIIP
13. Gong J. Network Information Security Pipeline Based on Grey Relational Cluster and Neural Networks // Proceedings of the 5th International Conference on Computing Methodologies and Communication, 08–10 April 2021, Erode, India. IEEE, 2021. p.971–975. DOI:10.1109/ICCMC51019.2021.9418311
14. Khan M.A. HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*. 2021;9(5):834. DOI:10.3390/pr9050834. EDN:BBATMC
15. Dolgachev M.V., Moskvichev A.D., Moskvicheva K.S. Detection of attacks on a web application using self-organizing Kohonen maps. *Cybersecurity Issues.* 2024;1(59):38–44. (in Russ.) DOI:10.21681/2311-3456-2024-1-38-44. EDN:KHTKXR
16. Pletenkova A.D., Sokolov A.N. Application of a two-stage clustering method based on the Kohonen self-organizing map for detecting anomalies in synthetic data sets. *Journal of the Ural Federal District. Information security.* 2024;4(54):49–60. (in Russ.) DOI:10.14529/secur240406. EDN:ZLGTJQ
17. Pinto A., Herrera L.-C., Donoso Y., Gutierrez J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors.* 2023;23(5):2415. DOI:10.3390/s23052415. EDN:GBGCLV
18. Yang H., Li X., Qiang W., Zhao Y., Zhang W., Tang C. A network traffic forecasting method based on SA optimized ARIMA–BP neural network. *Computer Networks.* 2021;193:108102. DOI:10.1016/j.comnet.2021.108102. EDN:NKGPOO
19. Lipatnikov V.A., Shevchenko A.A. Mathematical Model of Information Security Management Process for a Distributed Information System Under Conditions of Unauthorized Attacker Impact. *Information systems and technologies.* 2022;3(131): 121–130. (in Russ.) EDN:KSBCGK
20. Robak V.A., Lipatnikov V.A., Parfirov V.A., Zadboev V.A., Shevchenko A.A., Petrenko M.I., et al. *Program for Calculating Probabilistic-Temporal Characteristics of Network Control Tools Under Conditions of Multi-Stage Attacks*. Patent RF, no. 2024661259, 11.04.2024. (in Russ.) EDN:WTNJLT
21. Savina A.G., Malyavkina L.I., Gerasimova Yu.Ya., Zhilina D.E. Python Programming Language in Scientific Computing. *Proceedings of the National Scientific and Practical Conference on Infrastructure for Digital Development of Education and Business, 1–30 April 2021, Orel, Russian Federation*. Orel: Oryol State University of Economics and Trade Publ.; 2021. p.64–69 (in Russ.) EDN:CPPPGG

Статья поступила в редакцию 08.12.2025; одобрена после рецензирования 03.02.2026; принята к публикации 09.02.2026
The article was submitted 08.12.2025; approved after reviewing 03.02.2026; accepted for publication 09.02.2026

Информация об авторах:

ШЕВЧЕНКО Александр Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0001-9113-1089

ЗАДБОЕВ Вадим Александрович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. С.М. Буденного
https://orcid.org/0009-0003-9362-1307

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0000-0002-3736-4743

МЕЛЕХОВ Кирилл Витальевич — кандидат технических наук, преподаватель кафедры организации боевой подготовки и повседневной деятельности войск связи Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0009-0007-3474-412X

КУЗИН Павел Игоревич — кандидат технических наук, доцент, доцент кафедры информационных систем и технологий Санкт-Петербургского государственного лесотехнического университета им. С.М. Кирова
https://orcid.org/0000-0003-0880-6204

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.