

7. Управление качеством продукции. Технический регламент, стандартизация и сертификация: Учеб. пособие для вузов. / Б.А. Бузов. М.: издательский центр «Академия», 2006. 176 с.
8. Тартаковский Д. Ф. Метрология, стандартизация и технические средства измерений: Учеб. для вузов / Д. Ф. Тартаковский; Д.Ф. Тартаковский, А.С. Ястребов. М.: Высш. шк., 2002. 205 с.
9. Патент на полезную модель № 3999 U1 Российской Федерации, МПК G01B 13/02. Устройство для измерения линейных размеров : № 95114030/20 : заявл. 03.08.1995 : опубл. 16.04.1997 / В. П. Бондалетов, Р. А. Кукина ; заявитель Ковровский технологический институт. DN QCVYEX.
10. Патент № 2003036 C1 Российская Федерация, МПК G01B 3/28. Устройство для измерения линейных размеров : № 04361383 : заявл. 08.01.1988 : опубл. 15.11.1993 / Н. В. Ухов. EDN AWKQLX.

*Синелюбов Максим Алексеевич, студент, rrr234ttt45@yandex.ru, Россия, Тула, Тульский государственный университет*

#### **ANALYSIS OF PRODUCTION METHODS AND CHARACTERISTICS OF METAL STRUCTURES**

*M.A. Sinelubov*

*This article is devoted to quality control of building metal structures at all stages of their production and installation. The work discusses in detail the importance of quality control of materials, production process, welded joints, geometric parameters and installation. Various control methods are described, such as visual inspection, measurements, laboratory tests, non-destructive testing methods, modern high-tech methods and measuring instruments. In particular, coordinate measuring machines, laser scanners, computed tomography and ultrasound methods are mentioned. The principles of operation of coordinate measuring machines, laser scanners and computed tomography, as well as their application in various industries, are described. It is noted that the use of these technologies can improve the accuracy of measurements and automate the quality control process. Ultrasonic methods are offered as an alternative to expensive equipment. Some new patents are being considered to determine the linear dimensions of semi-finished products and stamped parts.*

*Key words:* metal structures, production technologies, quality control, dimensional characteristics, production control methods, construction.

*Sinelubov Maxim Alekseevich, student, rrr234ttt45@yandex.ru, Russia, Tula, Tula State University*

УДК 004.89

DOI: 10.24412/2071-6168-2024-3-131-132

#### **ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ: СТРАТЕГИИ ОБНАРУЖЕНИЯ АНОМАЛИЙ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ**

*Е.В. Ляпунцова, Арм Ажи Азиз Салих*

*В данной статье исследуется интеграция методов искусственного интеллекта (ИИ), в частности алгоритмов машинного обучения, в системы сетевой безопасности для улучшения стратегий обнаружения аномалий. Рассматриваются реальные примеры и примеры практического использования решений сетевой безопасности с использованием искусственного интеллекта, чтобы продемонстрировать эффективность этих стратегий в укреплении киберзащиты, подчеркивается важность интеграции обнаружения аномалий на базе искусственного интеллекта с существующей инфраструктурой безопасности для обеспечения комплексной защиты от возникающих киберугроз. Обсуждаются направления будущих исследований и соображения по решению проблем сетевой безопасности на базе искусственного интеллекта, которые помогут разработать устойчивые и адаптивные меры безопасности.*

*Ключевые слова:* искусственный интеллект, сетевая безопасность, обнаружение аномалий, алгоритмы машинного обучения, киберугрозы.

**Введение.** В сегодняшнем быстро развивающемся цифровом мире сетевая безопасность приобретает все большее значение. По мере того как организации продолжают оцифровывать свои операции и хранить ценные данные в онлайн, риск киберугроз и атак также растет. С развитием технологий искусственного интеллекта и машинного обучения, предприятия могут внедрять передовые стратегии обнаружения аномалий для повышения сетевой безопасности. Эти стратегии могут помочь выявлять необычные или подозрительные действия в сети и реагировать на них, обеспечивая дополнительный уровень защиты от потенциальных угроз. По мере дальнейшего развития технологий роль сетевой безопасности в защите конфиденциальной информации и поддержании целостности цифровых активов будет только увеличиваться [1].

Искусственный интеллект играет ключевую роль в повышении сетевой безопасности, особенно с помощью методов обнаружения аномалий. Используя искусственный интеллект, организации могут анализировать поведение сети в режиме реального времени, чтобы выявлять любые отклонения от обычных моделей и быстро обнаруживать потенциальные нарушения безопасности. Одним из ключевых методов обнаружения аномалий является использование алгоритмов машинного обучения для сравнения поведения сети с нормальным и выявления отклонений (потенциальных аномалий) [2].

Кроме того, система обнаружения аномалий на базе искусственного интеллекта может адаптироваться и учиться на новых угрозах, постоянно совершенствуя свои возможности по выявлению и снижению рисков безопасности. Это не только укрепляет защитные механизмы организации, но и снижает зависимость от ручного мониторинга и реагирования, позволяя отделам безопасности сосредоточиться на более сложных задачах [3].



*Рис. 1. Искусственное применение в сетях*

**Основы сетевой безопасности:** Основы сетевой безопасности включают в себя понимание и снижение рисков для защиты конфиденциальных данных и обеспечения целостности и доступности сетевых ресурсов. В частности, это внедрение многоуровневой защиты, контроль доступа к сети, шифрование данных, установление политик и процедур безопасности, мониторинг подозрительных действий, поддержание современного программного обеспечения, обнаружение и предотвращение вторжений, обучение пользователей и обеспечение физического доступа к сетевой инфраструктуре [4]. Все эти меры необходимы для создания устойчивой системы безопасности, защищающей от широкого спектра киберугроз и уязвимостей.

Традиционные подходы к сетевой безопасности включают брандмауэры, системы обнаружения / предотвращения вторжений (IDS / IPS), виртуальные частные сети (VPN), списки контроля доступа (ACL), сегментацию сети и шифрование. Эти методы направлены на мониторинг и блокировку подозрительного трафика, контроль доступа и защиту данных от несанкционированного доступа или модификации [5]. Однако, они часто имеют ограничения, указанные в таблице 1.

*Таблица 1*

<i>Ограничения традиционных подходов</i>	
<i>Метод</i>	<i>Ограничения</i>
<b>брандмауэры</b>	- Ограниченная способность проверять зашифрованный трафик (только информация заголовка). - Невозможность обнаружить сложные атаки, использующие разрешенные протоколы или службы.
<b>Системы обнаружения вторжений (IDS)</b>	- Вероятность ложных срабатываний, приводящих к перебоям в оповещении. - Ограниченная эффективность против атак нулевого дня или продвинутых постоянных угроз.
<b>Системы предотвращения вторжений (IPS)</b>	- Аналогичные ограничения, что и IDS, включая ложные срабатывания и ограниченную эффективность против атак нулевого дня.
<b>Виртуальные частные сети (VPN)</b>	- Уязвимы для атак "человек посередине", если ключи шифрования скомпрометированы. - Не обеспечивает защиту от внутренних угроз или зараженных вредоносным ПО конечных точек, получающих доступ к сети.
<b>Списки контроля доступа (ACL)</b>	- Статическими правилами может быть сложно управлять в больших сетях с меняющимися требованиями к доступу. - Отсутствие детального контроля над действиями пользователя после предоставления доступа.

**Искусственный интеллект в сетевой безопасности.** Искусственный интеллект (ИИ) в сетевой безопасности предполагает использование машинного обучения, глубокого обучения и других методов ИИ для улучшения возможностей обнаружения, предотвращения и реагирования на киберугрозы. Анализируя огромные объемы сетевых данных и выявляя закономерности или аномалии, системы на базе искусственного интеллекта могут обеспечивать упреждающие меры защиты и снижение количества угроз в режиме реального времени [6].

Например, искусственный интеллект может использоваться следующими способами в сетевой безопасности:

**Обнаружение аномалий:** алгоритмы искусственного интеллекта могут изучать нормальное поведение сетевого трафика и выявлять отклонения, которые могут указывать на вредоносную активность. Например, обнаружение необычных скачков при передаче данных или попыток несанкционированного доступа [6].

**Информация об угрозах:** Искусственный интеллект может обрабатывать и анализировать большие объемы данных об угрозах, выявляя их по мере возникновения и обеспечивая своевременные обновления систем безопасности для усиления защитных механизмов [3].

**Автоматическое реагирование:** решения безопасности на основе искусственного интеллекта могут автономно реагировать на инциденты безопасности, блокируя подозрительный трафик, помешая зараженные устройства в карантин или инициируя оповещения о вмешательстве человека [7].

**Прогностический анализ:** модели искусственного интеллекта могут прогнозировать потенциальные риски безопасности на основе исторических данных и текущих тенденций, позволяя организациям активно внедрять превентивные меры до эскалации угроз [8].

**Анализ поведения пользователей:** Алгоритмы искусственного интеллекта могут анализировать модели поведения пользователей для обнаружения внутренних угроз или несанкционированных действий, таких как необычное время входа в систему или доступ к конфиденциальным данным [7].

**Обнаружение вредоносных программ:** Системы на базе искусственного интеллекта могут идентифицировать известные и неизвестные варианты вредоносных программ путем анализа характеристик файлов, поведения и сетевых коммуникаций, повышая точность обнаружения и блокирования вредоносных программ [7].

**Методы обнаружения аномалий.** Методы обнаружения аномалий можно разделить на несколько категорий в зависимости от их подхода и методологии. К ним относятся:

### 1-Статистические методы:

Z-оценка: определяет аномалии на основе количества стандартных отклонений данных от среднего значения;

Тест Граббса: статистический тест, используемый для обнаружения выбросов в одномерном наборе данных, который получен из нормально распределенной совокупности;

Экспоненциальное сглаживание: присваивает экспоненциально уменьшающиеся веса прошлым наблюдениям с обнаружением аномалий путем сравнения наблюдаемых значений с прогнозируемыми значениями [9].

### 2-Подходы, основанные на машинном обучении:

Машины опорных векторов (SVM): SVM конструирует гиперплоскость в многомерном пространстве, разделяющем классы. Аномалии - это экземпляры, лежащие за пределами границы или на неправильной стороне гиперплоскости;

Случайные леса: метод коллективного обучения, который создает несколько деревьев решений во время обучения и выводит режим занятых в качестве прогноза. Аномалии обнаруживаются на основе неопределенности или несогласия между деревьями [10].

### 3-Глубокое обучение:

Автокодеры: Неконтролируемые нейронные сети, которые обучаются восстанавливать входные данные, могут использоваться для обнаружения аномалий путем измерения ошибки восстановления;

**Рекуррентные нейронные сети (RNN) и долговременная кратковременная память (LSTM):** Эти архитектуры эффективны для анализа последовательных данных и могут использоваться для обнаружения аномалий в данных временных рядов [11].

### 4-Анализ временных рядов:

Скользящие средние: Простые скользящие средние или экспоненциально взвешенные скользящие средние могут использоваться для сглаживания шума и обнаружения аномалий путем сравнения наблюдаемых значений со сглаженными значениями;

**Сезонная декомпозиция:** Методы декомпозиции временных рядов, такие как STL (сезонная и трендовая декомпозиция с использованием LOESS) или классические методы декомпозиции, могут разделять временные ряды на трендовую, сезонную и остаточную компоненты, при этом аномалии часто присутствуют в остаточной компоненте [11].

### 5-Доменно-зависимые методы:

Системы обнаружения вторжений (IDS): IDS используют сигнатуры известных атак или аномальные шаблоны в данных сетевого трафика для выявления подозрительной активности. Например, в Snort IDS записаны правила для обнаружения определенных шаблонов в сетевых пакетах [3].

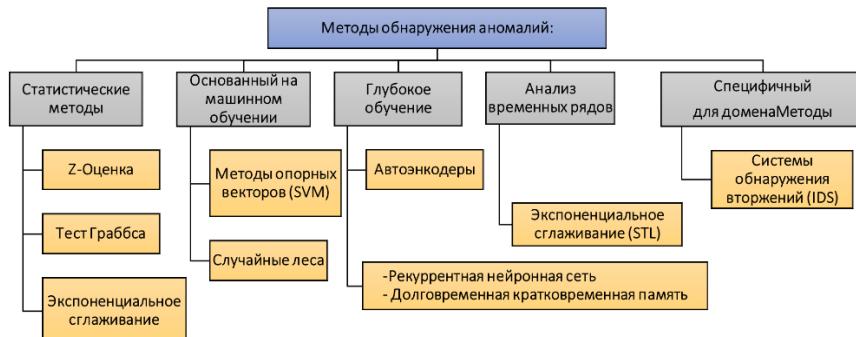


Рис. 2. Различные методы обнаружения аномалий

Вот краткое изложение моделей общего классификационного машинного обучения (ML) для обнаружения сетевых аномалий в сетевой безопасности в таблице 2.

Таблица 2  
Моделей машинного обучения (ML) для обнаружения сетевых аномалий

Название	Описание
Методы опорных векторов (SVM)	Эффективны для задач бинарной классификации, обрабатывают многомерные данные с нелинейными взаимосвязями с помощью функций ядра.
Случайный лес	Использует несколько деревьев принятия решений для классификации, подходящих для несбалансированных наборов данных и больших объемов данных с высокой размерностью.
К-ближайшие соседи (KNN)	Простой и интуитивно понятный метод классификации точек данных на основе большинства голосов их соседей, непараметрический и подходит для различных наборов данных.
Gradient Boosting Machines (GBM)	Последовательно строит деревья решений, исправляя ошибки предшественников, подходит для разнородных данных и фиксирует сложные взаимосвязи.
Логистическая регрессия	Моделирует вероятность двоичного результата, поддается интерпретации и эффективна с точки зрения вычислений, подходит для крупномасштабных наборов данных.
Наивный байесовский	вероятностный классификатор, основанный на теореме Байеса с допущением независимости признаков, простой и быстрый, эффективный для определенных типов данных.
Нейронные сети	Модели глубокого обучения, такие как CNNs и RNNs, могут автоматически извлекать иерархические функции из необработанных данных, что эффективно для захвата сложных шаблонов.

**Тематические исследования и приложения:** Несколько тематических исследований и приложений демонстрируют эффективность методов обнаружения аномалий в выявлении вредоносных программ.

**Тематическое исследование 1:** Повышение безопасности промышленного Интернета Вещей. В промышленном секторе Интернета вещей соединение физической инфраструктуры со взаимосвязанными цифровыми системами создает уникальные проблемы безопасности. Методы обнаружения аномалий, особенно те, которые используют алгоритмы глубокого обучения, сыграли важную роль в повышении уровня безопасности Интернета вещей в промышленности. Путем анализа структуры сетевого трафика и системных показателей с помощью моделей глубокого обучения были эффективно выявлены и устраниены отклонения, указывающие на потенциальные киберугрозы. Такой упреждающий подход значительно повысил устойчивость промышленных сетей Интернета вещей, обеспечив бесперебойную и безопасную работу критически важной инфраструктуры [12].

**Тематическое исследование 2:** Снижение уязвимости Интернета вещей в здравоохранении. В отрасли здравоохранения наблюдается быстрое распространение устройств Интернета вещей, направленных на повышение качества обслуживания пациентов и операционной эффективности. Однако этот приток взаимосвязанных медицинских устройств также привел к появлению уязвимостей, которыми могут воспользоваться киберпреступники. Благодаря внедрению протоколов многофакторной аутентификации и обнаружению аномалий на основе машинного обучения организации здравоохранения успешно устраняют потенциальные уязвимости в устройствах Интернета вещей. Этот повышенный уровень безопасности не только защищает конфиденциальные данные пациентов, но и обеспечивает надежность и целостность медицинских систем Интернета вещей [7].

**Тематическое исследование 3:** Усиление безопасности "умного дома". Внедрение устройств Интернета вещей в среде "умного дома" изменило то, как люди взаимодействуют со своими жилыми помещениями. Интеграция методов обнаружения аномалий на основе искусственного интеллекта - от интеллектуальных терmostатов до подключенных камер видеонаблюдения - доказала свою важную роль в повышении безопасности сетей "умного дома". Благодаря выявлению статистических аномалий и анализу временных рядов были оперативно выявлены и устраниены аномальные закономерности, указывающие на попытки несанкционированного доступа или вредоносные действия. Такой упреждающий подход к обеспечению безопасности вселял уверенность в домовладельцев, гарантируя конфиденциальность и защиту их подключенных устройств и личного пространства [13].

Благодаря этим тематическим исследованиям становится очевидным, что интеграция методов обнаружения аномалий, основанных на искусственном интеллекте, играет ключевую роль в защите среды Интернета вещей в различных отраслях промышленности. Постоянное развитие этих стратегий обещает дальнейшее укрепление сетей Интернета вещей и расширение возможностей организаций ориентироваться в сложном и меняющемся ландшафте киберугроз.

**Включение статистических данных и контрольных показателей эффективности искусственного интеллекта в повышении сетевой безопасности.** В таблице 3. представлена четкая разбивка организаций, их соответствующих алгоритмов, основанных на ИИ, показатели эффективности, демонстрирующие его влияние на сетевую безопасность, и результирующее влияние на кибербезопасность [14].

**Таблица 3**  
**Контрольные показатели эффективности искусственного интеллекта в различных компаниях**

Организация	ИИ-управляемый алгоритм	показатели эффективности	результаты
Дарктрейс	Иммунная система предприятия	- 46% быстрее обнаружение угроз - 33% более эффективного реагирования на инциденты	значительное снижение киберугроз
Сплайнк	Сплайнк Аналитическая информация об инфраструктуре	- 40% сокращение среднего времени обнаружения инцидентов безопасности - 35% уменьшение среднего времени ответа	улучшенная безопасность и реагирование на инциденты
компания Циско	Циско стелс-дозор	- 90% улучшение точности обнаружения угроз - 70% уменьшение ложных срабатываний	расширение обнаружения угроз и снижение ложных тревог
Банк Америки	алгоритм обнаружения мошенничества с помощью системы ИИ	- 40% снижение мошеннических операций - 60% увеличение обнаружения изощренного мошенничества	существенному сокращению потерь при финансовых операциях
Нетфликс	Управляемые ИИ системы обнаружения аномалий	- 30% снижение инцидентов нарушения безопасности - 25% увеличение удовлетворенности клиентов	повышенная безопасность и надежность потоковой платформы

**Ограничения, сложности и направления будущих исследований.** Современные технологии искусственного интеллекта для повышения сетевой безопасности сталкиваются с различными ограничениями и проблемами. Во-первых, существует проблема обобщения, когда моделям искусственного интеллекта может быть трудно расширить свои знания за пределы конкретных данных, на которых они обучались, что приводит к трудностям в обнаружении новых угроз или адаптации к различным средам [15]. Во-вторых, возникают опасения, связанные с конфиденциальностью данных, поскольку модели искусственного интеллекта часто требуют доступа к большим наборам данных, что вызывает вопросы о безопасности и приватности конфиденциальной информации. Кроме того, искажения, присутствующие в обучающих данных, могут непреднамеренно просачиваться в модели искусственного интеллекта, что приводит к несправедливым или дискриминационным результатам при принятии решений в области безопасности. Кроме того, модели искусственного интеллекта не поддаются интерпретации, что затрудняет понимание обоснования их решений и препятствует доверию и принятию. Более того, уязвимость моделей искусственного интеллекта возникает из-за состязательных атак, при которых злоумышленники манипулируют входными данными, что представляет серьезную проблему для сетевой безопасности [16]. Вычислительные ресурсы, необходимые для обучения и развертывания этих систем, также создают ограничения, влияющие на устойчивость масштабируемости. Наконец, этические проблемы, связанные с последствиями для общества, вызывают опасения по поводу сокращения числа рабочих мест, также алгоритмическая подотчетность еще больше усложняет развертывание. Устранение этих недостатков важно для реализации потенциала, обеспечивая при этом этическое, ответственное развертывание и широкое внедрение методов обнаружения аномалий на основе искусственного интеллекта для сетевой безопасности в будущем [2].

В сфере сетевой безопасности будущие достижения в области технологий искусственного интеллекта способны революционизировать стратегии защиты. Ключевые области внимания включают совершенствование ал-

горитмов искусственного интеллекта для расширения возможностей обобщения и обеспечения того, чтобы модели могли эффективно адаптироваться к развивающимся угрозам. Кроме того, предпринимаются согласованные усилия по разработке методов сохранения конфиденциальности для защиты данных при одновременном использовании возможностей искусственного интеллекта. Устранение предубеждений в моделях искусственного интеллекта и обеспечение справедливости при принятии решений в области безопасности остается приоритетом наряду с усилиями по улучшению интерпретируемости и прозрачности. Важно отметить, что защита систем искусственного интеллекта от атак противника и оптимизация их энергоэффективности необходимы для долгосрочной устойчивости. Более того, учет этических соображений при разработке и внедрении искусственного интеллекта имеет первостепенное значение для обеспечения ответственного и справедливого использования в обеспечении безопасности цифровых инфраструктур. Благодаря этим направлениям прогресса технологии искусственного интеллекта способны значительно повысить стандарты сетевой безопасности в будущем.

**Интеграция с существующей инфраструктурой безопасности.** Одним из важных аспектов внедрения обнаружения аномалий на базе искусственного интеллекта в сетевую безопасность является интеграция с существующей инфраструктурой безопасности. Такая интеграция обеспечивает комплексный подход к сетевой безопасности, при котором системы обнаружения аномалий на основе искусственного интеллекта работают в сочетании с другими мерами безопасности, такими как брандмауэры, системы обнаружения вторжений и инструменты мониторинга безопасности. Это сотрудничество гарантирует, что алгоритмы искусственного интеллекта смогут использовать существующую инфраструктуру безопасности и дополнять ее возможности для обеспечения более комплексной защиты от сетевых угроз. Более того, интеграция системы обнаружения аномалий на базе искусственного интеллекта с существующей инфраструктурой безопасности позволяет обмениваться информацией и совместно принимать решения. Такой подход повышает общую ситуационную осведомленность и возможности реагирования при операциях сетевой безопасности, поскольку алгоритмы искусственного интеллекта могут анализировать данные из нескольких источников и принимать решения в режиме реального времени на основе коллективного разума интегрированной системы.

**Вывод.** В заключение, интеграция искусственного интеллекта для обнаружения аномалий в сетевой безопасности представляет собой многообещающий путь повышения киберзащиты в современном цифровом ландшафте. Используя алгоритмы машинного обучения, организации могут анализировать поведение сети в режиме реального времени, выявлять аномалии и активно реагировать на потенциальные нарушения безопасности. Сотрудничество между системами обнаружения аномалий на базе искусственного интеллекта и существующей инфраструктурой безопасности обеспечивает комплексный механизм защиты от возникающих киберугроз. Хотя необходимо решать такие проблемы, как качество данных, масштабируемость, враждебные атаки и этические соображения, непрерывные исследования и разработки в области обнаружения аномалий на основе искусственного интеллекта имеют решающее значение для того, чтобы предупреждать киберугрозы. Синергия между экспертами по кибербезопасности, специалистами по обработке данных и исследователями искусственного интеллекта сыграет ключевую роль в преодолении этих проблем и формировании будущего сетевой безопасности.

### **Список литературы**

1. Аббаси М., Шахраки А., Тахеркорди А. Глубокое обучение для мониторинга и анализа сетевого трафика (NTMA): обзор // Компьютерные коммуникации, 2021. Том 170. С. 19-41. DOI: 10.1016/j.comcom.2021.01.021.
2. Олдвиш А., Дерхаб А., Эмам А.З. Подходы к глубокому обучению для систем обнаружения вторжений на основе аномалий: обзор, таксономия и открытые проблемы // Системы, основанные на знаниях, 2019. Том 189. С. 105124. DOI: 10.1016/j.knosys.2019.105124.
3. Стампар М., Ферталдж К. Искусственный интеллект в обнаружении сетевых вторжений // 38-я Международная конвенция по информационно-коммуникационным технологиям, электронике и микроэлектронике (MIPRO), 2015.С. 1318-1323. DOI: 10.1109/MIPRO.2015.7160479.
4. Ю Е., Ян Л., Жэнь С., Чжан К. Исследование стратегии защиты сетевой безопасности // Международной конференции по роботам и интеллектуальным системам, 2019. С. 152-154. DOI: 10.1109/ICRIS.2019.00047.
5. Рустам Ф., Раза А., Касим М., Поза С.К., Юркут А.Д. Новый подход к обнаружению серверных атак в реальном времени с использованием метаобучения // IEEE Access, 2024. Том 12. С. 39614-39627. DOI: 10.1109/ACCESS.2024.3375878.
6. Труонг Т.К., Дип К.Б., Зелинка И. Искусственный интеллект в киберпространстве: нападение и защита // Symmetry. Том 12. № 3. DOI: 10.3390/sym12030410.
7. Рафик С.Х., Абдалла А., Муса Н.С., Муруган Т. Машинное обучение и методы глубокого обучения для обнаружения сетевых аномалий Интернета вещей — текущие тенденции исследований // Sensors. Том 24, № 6, DOI: 10.3390/s24061968.
8. Саркер И.Х., Фурхад М.Х., Новрози Р. Кибербезопасность, основанная на искусственном интеллекте: обзор, интеллектуальное моделирование безопасности и направления исследований // SN Computer Science, 2021. Том 2, № 3. С. 173. DOI: 10.1007/s42979-021-00557-0.
9. Чандола В., Банерджи А., Кумар В. Обнаружение аномалий: обзор // ACM Comput. 2009. Том 41, № 3. С. Статья 15, 2009. DOI: 10.1145/1541880.1541882.
10. Ресенде П.А.А., Драммонд А.К. Обзор методов, основанных на случайных лесах, для систем обнаружения вторжений // ACM Computut. 2018. Том 51. № 3. С. 48. DOI: 10.1145/3178582.
11. Чжоу К., Паффенрот Р.К. Обнаружение аномалий с помощью надежных глубоких автоэнкодеров // 23-я Международная конференция ACM SIGKDD по обнаружению знаний и интеллектуальному анализу данных, Галифакс, Северная Каролина, Канада, 2017. DOI: 10.1145/3097983.3098052.
12. Менахем Д., Суджата Дж., Арулможи К. Обнаружение аномалий в IoT: последние достижения, перспективы и приложения искусственного интеллекта и ОД в обнаружении аномалий. Изд-во Риека: IntechOpen, 2023. С. 3.
13. Баталла Дж.М., Василакос А., Гаевски М. Безопасные умные дома: возможности и вызовы // ACM Computut, 2017. Том 50, № 5. С. Статья 75. DOI: 10.1145/3122816.

14. Юань Тан, Тан Х. Исследование применения искусственного интеллекта в защите сетевой безопасности // Журнал физики: серия конференций, 2021. Том 2033, № 1. С. 012149. DOI: 10.1088/1742-6596/2033/1/012149.
15. Нгуен Т.Н. Проблемы безопасности SDN на основе ML // 2-я конференция по кибербезопасности в се-тях 2018 года (CSNet), 2018. С. 1-9. DOI: 10.1109/CSNET.2018.8602680.
16. Цю С., Лю К., Чжоу С., Ву К. Обзор технологий состязательной атаки и защиты искусственного ин-теллекта // Прикладные науки. Том 9. № 5. DOI: 10.3390/app9050909.

*Ляпунцова Елена Вячеславовна, д-р техн. наук, профессор, lev86@bmstu.ru, Россия, Москва, Московский государственный технический университет им. Н.Э. Баумана,*

*Арм Ажи Азиз Салих, аспирант, arm.azhi@yandex.com, Россия, Москва, Национальный исследователь-ский университет «МИСиС»*

**USING ARTIFICIAL INTELLIGENCE TO ENHANCE NETWORK SECURITY: ANOMALY DETECTION STRATEGIES AND IMPLEMENTATION PROSPECTS**

*E.V. Lyapuntsova, Arm Azhi Aziz Salih*

*This article explores the integration of artificial intelligence (AI) methods, in particular machine learning algorithms, into network security systems to improve anomaly detection strategies. Real-world examples and examples of practical use of network security solutions using artificial intelligence are considered to demonstrate the effectiveness of these strategies in strengthening cyber defense, and the importance of integrating artificial intelligence-based anomaly detection with existing security infrastructure to provide comprehensive protection against emerging cyber threats is emphasized. The directions of future research and considerations for solving the problems of network security based on artificial intelligence are discussed, which will help to develop sustainable and adaptive security measures.*

*Key words:* *artificial intelligence, network security, anomaly detection, machine learning algorithms, cyber threats.*

*Lyapuntsova Elena Vyacheslavovna, doctor of technical sciences, professor, lev86@bmstu.ru, Russia, Moscow, Bauman Moscow State Technical University,*

*Arm Azhi Aziz Salih, postgraduate, arm.azhi@yandex.com, Russia, Moscow, National University of Science and Technology «MISiS»*

УДК 621.3.09  
DOI: 10.24412/2071-6168-2024-3-136-137

**АЛГОРИТМ ВОССТАНОВЛЕНИЯ АМПЛИТУДНО-ЧАСТОТНОЙ ХАРАКТЕРИСТИКИ ПРИЕМНИКА ПО АРХИВНЫМ ДАННЫМ ПАНОРАМНОГО ИЗМЕРЕНИЯ РАДИОПОМЕХ**

А.О. Щирый

*Предложен алгоритм восстановления амплитудно-частотной характеристики радиоприемного устройства по архивным данным панорамного измерения радиопомех декаметрового диапазона. Полученная характеристика необходима для корректной обработки и интерпретации указанных данных, которые после коррекции амплитудно-частотной характеристики будут использоваться для построения статистических предиктивных моделей радиопомех методами машинного обучения. Актуальность задачи обусловлена наличием архивных данных измерения радиопомех, полученных много лет назад, причем без измерения амплитудно-частотной характеристики радиоприемного устройства, и в настоящий момент применявшаяся измерительная аппаратура уже недоступна для непосредственного изучения. Основная идея предложенного алгоритма заключается в поиске периодической составляющей в панораме спектра помех, с периодом примерно равным полосе приемника и/или шагу его пере-стройки; полученные периодические составляющие разбиваются по интервалам (равным размерам периода) и усредняются, полученная характеристика принимается за оценку амплитудно-частотной характеристики радио-приемного устройства.*

*Ключевые слова:* *радиопомехи декаметрового диапазона, измерение помех, калибровка измерительной аппаратуры.*

Работа радиотехнических систем (РТС) декаметрового (ДКМ) диапазона основана на способности коротких волн (КВ) многократно отражаться от ионосфера и земной поверхности, поэтому адаптация таких РТС к ионо-сферным условиям является важнейшим условием обеспечения их корректной работы. Для указанной адаптации проводят оперативную диагностику ионосферы [1-6], состояние которой зависит от времени суток и сезона года, солнечной и геомагнитной активности, и других факторов, как правило, носящих случайный характер. Традиционно для диагностики среды распространения в интересах радиолокации используется возвратно-наклонное зондирование (ВНЗ) ионосферы, а в интересах систем связи – наклонное зондирование ионосферы (НЗИ); целесообразно дополнять средства диагностики также средствами вертикального (ВЗ) зондирования ионосферы, особенно в точках отражения лучей наклонных трасс от ионосферы [1-4]. Наиболее перспективным является выбор сигнала с линейно-частотной модуляцией (ЛЧМ) в качестве зондирующего [1].