Раздел III. Моделирование процессов и систем

УДК 004.896 DOI 10.18522/2311-3103-2022-3-211-222

Р.М. Ауси, Е.В. Заргарян, Ю.А. Заргарян

МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ И ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ СЕТЯХ

Недавние достижения в технологиях беспроводной связи привели к созданию огромного количества данных, которые передаются повсеместно. Большая часть такой информации является частью обширной и общедоступной сети, которая соединяет различные стационарные и мобильные устройства по всему миру. Возможности электронных устройств также увеличиваются день ото дня, что приводит к большему объему генерации данных и обмена информацией через сети. Аналогичным образом, с ростом разнообразия и сложности структур мобильных сетей увеличилась частота возникновения нарушений безопасности в ней. Это препятствует внедрению интеллектуальных мобильных приложений и услуг, о чем свидетельствует большое разнообразие платформ, которые предоставляют услуги хранения данных, вычислений с данными и приложений конечным пользователям. В таких сценариях становится необходимым защитить данные и проверить их использование в сети и приложениях, а также проверить их некорректное использование с целью защиты частной информации. Согласно данному исследованию, модель безопасности на основе искусственного интеллекта должна обеспечивать конфиденциальность, целостность и надежность системы, ее оборудования и протоколов, управляющих сетью, независимо от ее создания, чтобы управлять такой сложной сетью, как мобильная. Открытые трудности, с которыми все еще сталкиваются мобильные сети, такие как несанкционированное сканирование сети, мошеннические ссылки и т.д., были тщательно изучены в данной статье. Также в данном материале обсуждаются несколько технологий машинного и глубокого обучения, которые можно использовать для создания безопасной среды, а также многие угрозы кибербезопасности. Необходимо обратиться к необходимости разработки новых подходов для обеспечения высокого уровня безопасности электронных данных в мобильных сетях, поскольку возможности повышения безопасности мобильных сетей безграничны.

Сеть; информационная безопасность; компьютерная безопасность; искусственный интеллект; машинное обучение; глубокое обучение; угрозы; кибератаки; уязвимости.

R.M. Ausi, E.V. Zargaryan, Yu.A. Zargaryan

MACHINE LEARNING AND DEEP LEARNING MODELS FOR ELECTRONIC INFORMATION SECURITY IN MOBILE NETWORKS

Recent advances in wireless communication technologies have led to the creation of a huge amount of data that is transmitted everywhere. Most of this information is part of an extensive and publicly accessible network that connects various stationary and mobile devices around the world. The capabilities of electronic devices are also increasing day by day, which leads to more data generation and information exchange through networks. Similarly, with the increasing diversity and complexity of mobile network structures, the frequency of security breaches in it has increased. This hinders the introduction of intelligent mobile applications and services, as evidenced by the wide variety of platforms that provide data storage, data computing and application ser-

vices to end users. In such scenarios, it becomes necessary to protect data and check their use in the network and applications, as well as check their incorrect use in order to protect private information. According to this study, a security model based on artificial intelligence should ensure the confidentiality, integrity and reliability of the system, its equipment and protocols that control the network, regardless of its creation, in order to manage such a complex network as a mobile one. The open difficulties that mobile networks still face, such as unauthorized network scanning, fraudulent links, etc., have been thoroughly studied in this article. This article also discusses several ML and DL technologies that can be used to create a secure environment, as well as many cybersecurity threats. It is necessary to address the need to develop new approaches to ensure a high level of electronic data security in mobile networks, since the possibilities for improving the security of mobile networks are limitless.

Network; information security; cyber security; artificial intelligence; machine learning;deep learning; threats; cyber-attacks; vulnerabilities.

Введение. Электронная информация является важным активом для любой организации, и даже в случае использования ее физическим лицом данные могут иметь для них весьма важное значение, и они не могут позволить себе их потерять. Информационная безопасность стала очень важной в современном компьютерном мире, и она требует потенциальных противодействий постоянно меняющимся угрозам. Следовательно, кибербезопасность и управление рисками жизненно важны для задач, связанных с данными или информацией.

Кибербезопасность – это совокупность процедур, действий людей и технологий, которые помогают защитить электронные информационные ресурсы. Киберзлоумышленников явно больше, чем средств защиты, что вызывает опасения по поводу безопасности конфиденциальных цифровых активов [1–4]. Статистика уязвимостей и несанкционированного доступа показывает, что большинство устройств обмена информацией, особенно мобильные сети, подвержены значительному риску безопасности.

Первым этапом оценки безопасности системы или оценки рисков является идентификация ресурсов. Очень важно определить комплексный подход, соответствующий рискованной ситуации. Это помогает внедрять самые передовые методы прогнозирования и смягчения угроз информационной безопасности. Наиболее подходящая модель также может зависеть от сценариев атаки и цели атаки. Следовательно, для решения проблемы электронной информационной безопасности необходимы надлежащие исследования. По мере увеличения числа кибератак, особенно в мобильных сетях, производительность наших систем для борьбы с ними также увеличивается, как описано в следующих частях данной статьи.

На рис. 1 представлена разработанная общая классификация технологий искусственного интеллекта. Существует широкий горизонт междисциплинарной связи между кибербезопасностью и искусственным интеллектом. Такие технологии, как глубокое обучение, можно использовать для создания сложных моделей обнаружения вторжений, классификации вредоносных программ и определения киберугроз в мобильной сети. Модели ИИ требуют специализированных решений в области кибербезопасности и безопасности, чтобы уменьшить уязвимости и обеспечить лучшую конфиденциальность информации, а также обеспечить безопасную унифицированную среду обучения [5–10].

Мобильные программы-вымогатели, крипто-майнинг, мошеннические приложения и банковские трояны являются одними из наиболее распространенных опасностей для мобильных сетей. Мобильные приложения превзошли настольные программы как самый популярный способ доступа к персонализированным услугам, таким как отправка и получение электронной почты, банковские услуги, онлайн-покупки и автоматизированное управление устройствами. Хакеры пользуются системами исправлений для заражения мобильных приложений, что сделало их

идеальными целями для киберпреступников. Существующие решения в области безопасности кажутся недостаточными для будущих мобильных технологий, которые увеличили скорость передачи данных в сетях. Благодаря усовершенствованию технологии искусственного интеллекта сложные модели делают прорыв в безопасности различных критически важных приложений, многие из которых основаны на мобильных сетях. Однако это не означает, что возможности угроз, использующих нашу систему, уменьшились.

Рис. 1. Общая классификация – методы искусственного интеллекта

Обширные достижения в области мобильных сетей помогают новому поколению сетей работать намного быстрее и безопаснее, чем предыдущие версии. Тем не менее, вызов безопасности от идентифицированных и неидентифицированных рисков указывает на необходимость расширения существующих систем управления рисками. В результате, несмотря на обилие структур для защиты ресурсов организации от киберугроз, вариант для лиц, принимающих решения в области кибербезопасности, остается в основном сложным [3].

Методы машинного обучения. Машинное обучение – это основанный на данных подход к разработке искусственного интеллекта. Это подмножество ИИ, обладающее многими сильными сторонами и использующее статистические методы для целей прогнозирования [5]. Он был разработан в 1940-х годах, но только недавно мы смогли использовать его в повседневной жизни. Алгоритмы машинного обучения обычно используют следующие два типа методов обучения: контролируемое и неконтролируемое обучение. Обучение без учителя не требует обратной связи, тогда как обучение с учителем опирается на обратную связь от человека [11–13]. Машинное обучение имеет много сильных сторон, но наиболее важными из них являются его методология и обучение с подкреплением. Методология машинного обучения включает в себя обучение алгоритма набору данных, чтобы он мог идентифицировать закономерности в новых наборах данных. Обучение с подкреплением – это класс машинного обучения, в котором интеллектуальная система учится методом проб и ошибок, получая вознаграждение или наказание за свои действия. В следующем разделе мы рассмотрим модели машинного обучения для электронной информационной безопасности.

Модели машинного обучения для электронной информационной безопасности. Сетевая безопасность – это постоянно меняющаяся область, в которой каждый день появляются новые угрозы. Модели машинного обучения дают возможность быть в курсе последних технологических разработок в этой области, обеспечивая при этом эффективную защиту от этих новых угроз, а также от старых угроз, которые существовали годами. В этой части статья обсудим некоторые модели машинного обучения, которые также можно использовать в кибербезопасности, такие как обнаружение вторжений и обнаружение аномалий. Обнаружение вторжений – это процесс, в котором вторжение обнаруживается и предотвращается до того, как оно причинит какой-либо вред системе, с другой стороны, обнаружение аномалий фокусируется на выявлении аномалий в системе. Эти методы помогают выявлять вредоносные атаки путем поиска необычных шаблонов или поведения. Биологически вдохновленные методы обычно используются в других алгоритмах машинного обучения, но исследования искусственной системы защиты ограничены.

Еще одним растущим направлением в машинном обучении является полууправляемое обучение, которое определяется как комбинация обучения с учителем и без учителя [14–18]. Модели обучения с подкреплением для сетевой безопасности были разработаны, чтобы помочь в обнаружении и предотвращении кибератак. Эти модели основаны на идее, что система должна иметь возможность учиться на своем прошлом опыте, а затем использовать эти знания для принятия решений в будущем. Его можно обучить обнаруживать определенные шаблоны или поведение, которые являются индикаторами атаки. Затем модель обучения будет отправлять оповещения, когда обнаружит что-то подозрительное, чтобы люди могли при необходимости взять на себя управление и продолжить расследование. На рис. 2 показана разработанная номенклатура современных моделей машинного обучения для электронной информационной безопасности.

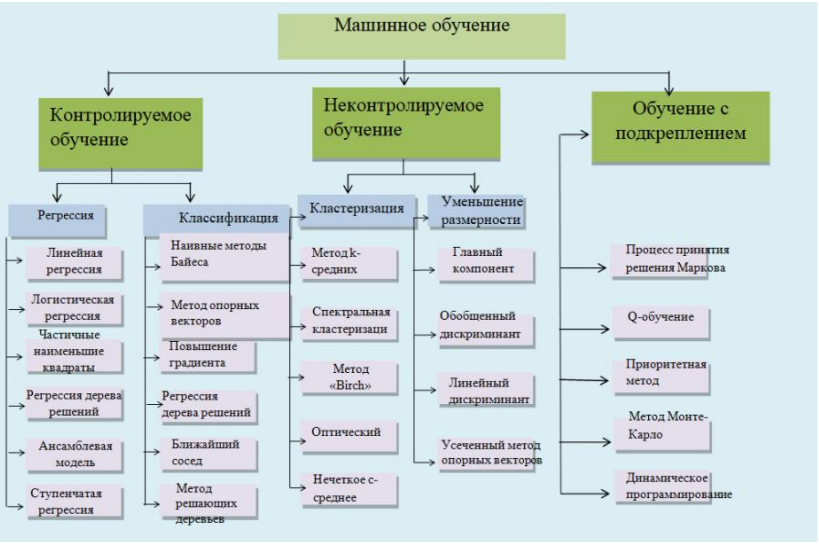

Рис. 2. Разработанная номенклатура современных моделей машинного обучения для электронной информационной безопасности

В табл. 1 представлен разработанный анализ подходов к методам машинного обучения для использования в электронной информационной безопасности в мобильной сети.

Таблица 1

Анализ подходов к методам машинного обучения для использования в электронной информационной безопасности

Категория безопасности	Машинное обучение. Используемые подходы	Ключевой вклад	Ограничения
Схемы сетевых атак	C4.5 Решающее дерево; Байесовская сеть; Наивный байесовский алгоритм	Подход с использованием машинного обучения для определения правил безопасности на контроллере, Влияние незначительных угроз безопасности на безопасность программно-определяемой сети	Подход генерирует переменные результаты для разных наборов данных. Более высокая дисперсия данных приведет к более высоким шансам ложного прогноза
Обнаружение сетевых аномалий	Генетический алгоритм; машины опорных векторов	Выберите более подходящие поля пакета через генетический алгоритм, используя метод выбора основных признаков. Использование усовершенствованного метода машины опорных векторов наряду с возможностью обнаружения новинок машины опорных векторов одного класса обеспечивает высокую производительность машины опорных векторов с мягкой маржой	Для применения структуры в реальной среде трафика TCP/IP потребуется более реалистичный метод профилирования
Классификация трафика	Метод Лапласа машины опорных векторов	Адаптивная классификация потока трафика в режиме реального времени по категории QoS без необходимости точного определения приложения, создающего поток трафика	Маркировка должна выполняться явно для наборов данных в полуконтролируемых алгоритмах, поскольку неконтролируемые алгоритмы на основе машинного обучения не могут быть непосредственно применены в сети
Обнаружение вторжений в реальном времени	Метод роя части; машины опорных векторов	Для построения системы обнаружения вторжений вводится алгоритм, аналогичный подходу выбора на основе метода роя частиц	Требуется улучшение алгоритма выбора признаков по стратегии поиска и критерию оценки
Глушение атак	Искусственные нейронные сети; машины опорных векторов; логистическая регрессия; K-ближайший сосед; древо решений; Наивный байесовский алгоритм	Обнаружение, локализация и предотвращение атак Отключения питания в оптических сетях с использованием различных решений на основе машинного обучения. Снижение вероятности успешного блокирования световых путей с помощью схемы перераспределения ресурсов, использующей статистическую информацию о точности обнаружения атак	Исследуемая локализация ограничена закупоренным каналом

Обнаружение вредоносных программ	Древо решений; Наивный байесовский алгоритм; обучение с подкрепление	Предоставление централизованного решения для обеспечения безопасности предприятия, которое работает на уровне брандмауэра в сети. Для создания модуля обнаружения вредоносных программ используются современные и усовершенствованные методы машинного обучения и интеллектуального анализа данных	Предложенное решение непригодно для домашних пользователей, так как для машины общего назначения требуется слишком большой процессор
Сетевые анамалии (DoS Flooding)	AdaboostM1; обучение с подкреплениеv; Многослойный персептон	Методы, связанные с машинным обучением, используются для обнаружения и классификации сетевых вторжений с использованием подхода на основе информационной базы управления. Для классификации и обнаружения атак типа «отказ в обслуживании» и «грубой силы» используются различные классификаторы. Использование алгоритмов машинного обучения для данных - очень успешная стратегия для обнаружения DoS-атак и атак методом грубой силы	Ни одному из классификаторов не удалось обнаружить атаку грубой силы в наборе данных TCP. Производительность результатов менее эффективна для классификаторов AdaboostM1 в атаках TCP-SYN и UDP по сравнению с другими атаками
Обнаружение атак интернет-магазинов	Метод k-средних; Многослойный персептон; Наивный байесовский алгоритм; древо решений; машины опорных векторов; K-ближайший сосед	Для экспериментов с безопасностью серверов Интернета вещей был составлен новый набор данных, включающий 1551 вредоносный веб-шелл PHP и 2593 обычных скрипта PHP. Для предварительной обработки данных были изучены подходы к извлечению признаков частоты термина, обратной частоте документа, код операции и комбинированный подход к извлечению признаков кода операции и принципу «частота слова - обратная частота документа». Набор данных анализируется с использованием метода кластеризации признаков, основанного на анализе основных компонентов. Оцениваются функции, важные для обнаружения веб-оболочки	Тесты, проведенные на моделях машинного обучения для обнаружения веб-оболочки только в PHP-скриптах. Для получения более точных результатов требуются серверы IoT с надежной вычислительной мощностью
Помехи на основе атаки типа «Отказ в обслуживании» и «прослушки»	Многослойный персептон; машины опорных векторов; K-ближайший сосед; древо решений	Предложение уникального подхода к защите беспроводной связи в беспроводной сети на кристаллах от внешних и внутренних злоумышленников с использованием атак типа «отказ в обслуживании» (DoS)	При наличии внутренней DoS-атаки производительность не столь адекватна и лишь немного лучше, чем у проводной сети на кристалле

		на основе постоянных помех и подслушивания (ED). Защита связи по беспроводным каналам с помощью легкого механизма скремблирования данных с малой задержкой.	
Отравляющие атаки (ненадежные обновления модели)	Стохастический градиентный спуск	Решение проблем ненадежных обновлений модели путем введения репутации в качестве надежной меры для выбора надежных работников для надежного федеративного обучения. Эффективная методика расчета репутации разработана с использованием многовесовой субъективной логической модели.	Каждая обученная локальная рабочая модель должна регулярно отправлять обновления на центральный сервер. Недостаточно надежный метод для мониторинга рабочих показателей.

Изучение и анализ проблем в электронной информационной безопасности в мобильных сетях. В последние годы наблюдается значительный рост сложности и проблем электронного управления данными. Сложность связана с кросс-функциональным характером, который пытается защитить достоверность информации и зависимость для защиты ценных активов организации, улучшая деловое взаимодействие путем создания доверия, деловых союзов и платформ для совместной работы [19–22]. В данной статье определено три следующие проблемы управления, которые необходимо решить, чтобы полностью решить эту проблему: (1) поставить под угрозу безопасность системы путем устранения рисков после создания всей системы; (2) Системы безопасности и информационные системы разрабатываются параллельно; (3) Неадекватное мышление используется для формирования решений [14].

В статье был проведен анализ и составлена схема (рис. 3), иллюстрирующая открытые вопросы, связанные с электронной информационной безопасностью для мобильных сетей.

Рис. 3. Электронная информационная безопасность в мобильных сетях – открытые проблемы

Большинство инцидентов за последние два-три года были связаны с несанкционированным сканированием сети, проверкой, скомпрометированными сервисами, вирусами, вредоносным кодом и аномалиями веб-сайтов. С каждым годом количество аварий увеличивается, как и количество новых уязвимостей. Тем не менее, они определенно разделяют определенный шаблон, с помощью которого они изощренно атакуют систему, оставляя пользователя в неведении. Многие из этих атак даже не требуют создания новой технологии для борьбы с ними. Кроме того, в этой ситуации могут помочь изменения в существующих технологиях. Однако время на борьбу с угрозой настолько ограничено, что иногда мы не можем вмешаться.

Одной из самых известных и сложных проблем с моделями машинного обучения является их уязвимость для атак противника. Эти атаки предназначены для того, чтобы обманным путем классификаторы ошибочно классифицировали входную выборку как принадлежащую одному классу, хотя на самом деле она принадлежит другому. Текущие исследования состязательного ИИ сосредоточены на методах, при которых небольшие модификации входных данных машинного обучения могут обмануть классификатор машинного обучения, заставив его реагировать неправильно.

На рис. 4 показана разработанная схема будущих направлений исследований, связанных с электронной информационной безопасностью для мобильных сетей.

Рис. 4. Будущие направления исследований – электронная информационная безопасность в мобильных сетях

Вывод. Раннее обнаружение и устранение киберугроз приобрели первостепенное значение в современном мире, будь то отдельные лица или мегаорганизации, имеющие дело с электронной информацией и данными. Противники больше не полагаются только на обычные стратегии нападения и со временем развиваются, что вызывает необходимость в разработке и развитии ранее существовавших планов защитных действий [11]. В этой статье мы стремимся объединить различные подходы, предложенные в недавних исследованиях, с помощью методов с поддержкой ИИ, таких как машинное и глубокое обучение, для повышения чувства безопасности

в мобильных сетях [12–15]. На основе рассмотренных статей представлен краткий обзор популярных алгоритмов машинного обучения, за которым следует обзор предложений, направленных на борьбу с многочисленными категориями угроз безопасности. соответствующие статьи были оценены, чтобы определить влияние различных поворотов, внесенных в общие алгоритмы машинного и глубокого обучения, на уязвимости, с которыми сталкиваются электронные информационные системы и мобильные сети. Предоставляя краткий обзор наиболее известных наборов данных, которые используются для обучения и тестирования моделей, была проведена качественная разбивка наборов данных о кибератаках. Наконец, чтобы поощрить будущих исследователей и энтузиастов, были изложены краткие обзоры текущих открытых проблем и потенциальных областей исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кейт А. Смит, Джатиндер Н.Д. Гупта.* Нейронные сети в бизнесе: методы и приложения для исследователя операций // Computers & Operations Research. – 2000. – 27. – С. 1023-1044.
2. *Заргарян Е.В., Акопджанян Ж.Ж.* Исследование автоматизации коллаборативных роботов и способы их применения // Технологии разработки информационных систем ТРИС-2020: Матер. X Международной научно-технической конференции. "Технологии разработки информационных систем". – 2020. – С. 218-223.
3. *Заргарян Ю.А.* Задача управляемости в адаптивной автоматной обучаемой системе управления // Технологии разработки информационных систем ТРИС-2020: Матер. X Международной научно-технической конференции. "Технологии разработки информационных систем". – 2020.
4. *Zargaryan E.V., Zargaryan Y.A., Dmitrieva I.A., Sakharova O.N. and Pushnina I.V.* Modeling design information systems with many criteria. Information Technologies and Engineering – APITECH - 2020 // Journal of Physics: Conference Series. – 2020. – Vol. 2085 (3). – P. 032057(1-7). – DOI:10.1088/1742-6596/1679/3/032057.
5. *Джордж Боджадзиев, Мария Боджадзиев.* Нечеткая логика для бизнеса, финансов и управления. – 2-е изд, Достижения в области нечетких систем - Приложения и теория. – Т. 23.
6. *Zargaryan E.V., Zargaryan Y.A., Карс I.V., Sakharova O.N., Kalyakina I.M and Dmitrieva I.A.* Method of estimating the Pareto-optimal solutions based on the usefulness // International Conference on Advances in Material Science and Technology - CAMSTech-2020. IOP Conf. Series: Materials Science and Engineering. – 2020. – Vol. 919 (2). – P. 022027 (1-8). – DOI: 10.1088/1757-899X/919/2/022027.
7. *Аламир Х.С., Заргарян Е.В., Заргарян Ю.А*. Модель прогнозирования транспортного потока на основе нейронных сетей для предсказания трафика на дорогах // Известия ЮФУ. Технические науки. – 2021. – № 6 (223). – С. 124-132.
8. *Soomro Z.A., Shah M.H., & Ahmed J.* Information security management needs more holistic approach: A literature review // International Journal of Information Management. – 2016. – Vol. 36 (2). – P. 215-225.
9. *Beloglazov D., Shapovalov I., Soloviev V., Zargaryan E.* The hybrid method of path planning in non-determined environments based on potential fields // ARPN Journal of Engineering and Applied Sciences. – 2017. – Т. 12, No. 23. – P. 6762-6772.
10. *Zargarjan E.V., Zargarjan Ju.A., Finaev V.I.* Information support for the training of fuzzy production account balance in the conditions of incomplete data // Innovative technologies and didactics in teaching (ITDT-2016): Collected papers. – 2016. – P. 128-138.
11. *Лаптев А.С., Шестова Е.А.* Недостатки нейро-экспертных систем управления и способы их решения // Наука и современность: Матер. Всероссийской научно-практической конференции студентов и молодых ученых. – Таганрог, 2021. – С. 104-106.
12. *Финаев В.И., Заргарян Ю.А., Заргарян Е.В., Соловьев В.В.* Формализация групп подвижных объектов в условиях неопределённости для выбора управляющих решений // Информатизация и связь. – 2016. – № 3. – С. 56-62.
13. *Slimani I., Farissi I. El, et Achchab S.* Artificial Neural Networks for Demand Forecasting: Application Using Moroccan Supermarket Data. – 2015.

14. *Singh A.N., Gupta M.P., & Ojha A*. Identifying factors of "organizational information security management" // Journal of Enterprise Information Management. – 2014.
15. *Пушнина И.В.* Система управления подвижным объектом в условиях неопределенности // Наука и образование на рубеже тысячелетий. сборник научно-исследовательских работ. – Кисловодск: Кисловодский гуманитарно-технический институт, ЮФУ, 2018. – С. 65-74.
16. *Wang X., Wang C.* Time series data cleaning: A survey // IEEE Access. – 2020. – Vol. 8. – P. 1866-1881. – DOI: 10.1109/ACCESS.2019.2962152.
17. Data-driven smart cities: Big Data, analytics, and security. – 2018. – URL: https://skelia.com/articles/data-driven-smart-cities-big-data-analytics-and-security/.
18. *Kim J., Tae D., Seok J.* A survey of missing data imputation using generative adversarial networks // Proc. of the 2020 Int. Conf. on Artificial Intelligence in Information and Communication, ICAIIC 2020. – P. 454-456. – DOI: 10.1109/ICAIIC48513.2020.9065044.
19. *Dmitrieva I.A., Mileshko L.P., Begun O.V., Berezhnaya A.V.* Information Modernization of the General Theory of Environmental Safety Ensuring // IOP Conference Series: Materials Science and Engineering. III International Scientific Conference. – Krasnoyarsk, 2021. – P. 12072.
20. *Ma Q., Johnston A.C., & Pearson J.M*. Information security management objectives and practices: a parsimonious framework // Information Management & Computer Security. – 2008.
21. *Шестова Е.А., Шадрина В.В.* Исследование построения видов операций над нечеткими множествами и нечеткой аппроксимирующей системы в среде MATLAB: учеб. пособие. – Таганрог, 2019.
22. *Бабенко Л.К., Шумилин А.С., Алексеев Д.М.* Алгоритм обеспечения безопасности конфиденциальных данных медицинской информационной системы хранения и обработки результатов обследований // Известия ЮФУ. Технические науки. – 2020. – № 5 (215). –С. 6-16.

REFERENCES

1. *Keyt A. Smit, Dzhatinder N.D. Gupta.* Neyronnye seti v biznese: metody i prilozheniya dlya issledovatelya operatsiy [Neural Networks in Business: Methods and Applications for the Operations Researcher], *Computers & Operations Research,* 2000, 27, pp. 1023-1044.
2. *Zargaryan E.V., Akopdzhanyan Zh.Zh.* Issledovanie avtomatizatsii kollaborativnykh robotov i sposoby ikh primeneniya [Research of automation of collaborative robots and methods of their application], *Tekhnologii razrabotki informatsionnykh sistem TRIS-2020: Mater. X Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. "Tekhnologii razrabotki informatsionnykh sistem"* [Technologies for the development of information systems TRIS-2020. Materials of the X International Scientific and Technical Conference "Technologies for the Development of Information Systems"], 2020, pp. 218-223.
3. *Zargaryan Yu.A*. Zadacha upravlyaemosti v adaptivnoy avtomatnoy obuchaemoy sisteme upravleniya [The problem of controllability in an adaptive automaton learning control system], *Tekhnologii razrabotki informatsionnykh sistem TRIS-2020: Mater. X Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. "Tekhnologii razrabotki informatsionnykh sistem"* [Technologies for the development of information systems TRIS-2020. Materials of the X International Scientific and Technical Conference. "Technologies for the Development of Information Systems"], 2020.
4. *Zargaryan E.V., Zargaryan Y.A., Dmitrieva I.A., Sakharova O.N. and Pushnina I.V.* Modeling design information systems with many criteria. Information Technologies and Engineering – APITECH – 2020, *Journal of Physics: Conference Series,* 2020, Vol. 2085 (3), pp. 032057(1-7). DOI:10.1088/1742-6596/1679/3/032057.
5. *Dzhordzh Bodzhadziev, Mariya Bodzhadziev*. Nechetkaya logika dlya biznesa, finansov i upravleniya [Fuzzy Logic for Business, Finance and Management]. 2nd ed, Dostizheniya v oblasti nechetkikh sistem - Prilozheniya i teoriya [Advances in Fuzzy Systems - Applications and Theory], Vol. 23.
6. *Zargaryan E.V., Zargaryan Y.A., Kapc I.V., Sakharova O.N., Kalyakina I.M and Dmitrieva I.A.* Method of estimating the Pareto-optimal solutions based on the usefulness, *International Conference on Advances in Material Science and Technology - CAMSTech-2020. IOP Conf. Series: Materials Science and Engineering,* 2020, Vol. 919 (2), pp. 022027 (1-8). DOI: 10.1088/1757-899X/919/2/022027.

7. *Alamir Kh.S., Zargaryan E.V., Zargaryan Yu.A.* Model' prognozirovaniya transportnogo potoka na osnove neyronnykh setey dlya predskazaniya trafika na dorogakh [A traffic flow prediction model based on neural networks for predicting traffic on the roads], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2021, No. 6 (223), pp. 124-132.
8. *Soomro Z.A., Shah M.H., & Ahmed J.* Information security management needs more holistic approach: A literature review, *International Journal of Information Management,* 2016, Vol. 36 (2), pp. 215-225.
9. *Beloglazov D., Shapovalov I., Soloviev V., Zargaryan E.* The hybrid method of path planning in non-determined environments based on potential fields, *ARPN Journal of Engineering and Applied Sciences*, 2017, Vol. 12, No. 23, pp. 6762-6772.
10. *Zargarjan E.V., Zargarjan Ju.A., Finaev V.I.* Information support for the training of fuzzy production account balance in the conditions of incomplete data, *Innovative technologies and didactics in teaching (ITDT-2016): Collected papers*, 2016, pp. 128-138.
11. *Laptev A.S., Shestova E.A*. Nedostatki neyro-ekspertnykh sistem upravleniya i sposoby ikh resheniya [Disadvantages of neuroexpert control systems and ways to solve them], *Nauka i sovremennost': Mater. Vserossiyskoy nauchno-prakticheskoy konferentsii studentov i molodykh uchenykh* [Science and Modernity. Materials of the All-Russian scientific and practical conference of students and young scientists]. Taganrog, 2021, pp. 104-106.
12. *Finaev V.I., Zargaryan Yu.A., Zargaryan E.V., Solov'ev V.V.* Formalizatsiya grupp podvizhnykh ob"ektov v usloviyakh neopredelennosti dlya vybora upravlyayushchikh resheniy [Formalization of groups of mobile objects in conditions of uncertainty for the choice of control solutions], *Informatizatsiya i svyaz'* [Informatization and communication], 2016, No. 3, pp. 56-62.
13. *Slimani I., Farissi I. El, et Achchab S.* Artificial Neural Networks for Demand Forecasting: Application Using Moroccan Supermarket Data, 2015.
14. *Singh A.N., Gupta M.P., & Ojha A*. Identifying factors of "organizational information security management", *Journal of Enterprise Information Management,* 2014.
15. *Pushnina I.V*. Sistema upravleniya podvizhnym ob"ektom v usloviyakh neopredelennosti [Control system of a moving object under conditions of uncertainty. In the collection], *Nauka i obrazovanie na rubezhe tysyacheletiy. sbornik nauchno-issledovatel'skikh rabot* [Science and education at the turn of the millennium. collection of research papers]. Kislovodsk: Kislovodskiy gumanitarno-tekhnicheskiy institut, YuFU, 2018, pp. 65-74.
16. *Wang X., Wang C.* Time series data cleaning: A survey, *IEEE Access,* 2020, Vol. 8, pp. 1866-1881. DOI: 10.1109/ACCESS.2019.2962152.
17. Data-driven smart cities: Big Data, analytics, and security, 2018. Available at: https://skelia.com/ articles/data-driven-smart-cities-big-data-analytics-and-security/.
18. *Kim J., Tae D., Seok J.* A survey of missing data imputation using generative adversarial networks, *Proc. of the 2020 Int. Conf. on Artificial Intelligence in Information and Communication, ICAIIC 2020,* pp. 454-456. DOI: 10.1109/ICAIIC48513.2020.9065044.
19. *Dmitrieva I.A., Mileshko L.P., Begun O.V., Berezhnaya A.V.* Information Modernization of the General Theory of Environmental Safety Ensuring, *IOP Conference Series: Materials Science and Engineering. III International Scientific Conference*. Krasnoyarsk, 2021, pp. 12072.
20. *Ma Q., Johnston A.C., & Pearson J.M*. Information security management objectives and practices: a parsimonious framework, *Information Management & Computer Security,* 2008.
21. *Shestova E.A., SHadrina V.V.* Issledovanie postroeniya vidov operatsiy nad nechetkimi mnozhestvami i nechetkoy approksimiruyushchey sistemy v srede MATLAB: ucheb. posobie [Investigation of the construction of types of operations on fuzzy sets and a fuzzy approximating system in MATLAB: textbook]. Taganrog, 2019.
22. *Babenko L.K., Shumilin A.S., Alekseev D.M.* Algoritm obespecheniya bezopasnosti konfidentsial'nykh dannykh meditsinskoy informatsionnoy sistemy khraneniya i obrabotki rezul'tatov obsledovaniy [Algorithm for ensuring the security of confidential data of the medical information system for storing and processing survey results], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 5 (215), pp. 6-16.

Статью рекомендовала к опубликованию к.т.н., доцент Н.А. Иванова.

Ауси Рим Мохаммед Худхейр – Южный федеральный университет; e-mail: ausi@sfedu.ru; г. Таганрог, Россия; кафедра систем автоматического управления; аспирант.

Заргарян Елена Валерьевна – e-mail: ezargaryan@sfedu.ru; кафедра систем автоматического управления; к.т.н.; доцент.

Заргарян Юрий Артурович – e-mail: yazargaryan@sfedu.ru; кафедра систем автоматического управления; к.т.н.; доцент.

Aussi Rim Mohammed Hedhair – Southern Federal University; e-mail: ausi@sfedu.ru; Taganrog, Russia; the department of automatic control systems; postgraduate student.

Zargaryan Elena Valerevna – e-mail: ezargaryan@sfedu.ru; the department of automatic control systems; cand. of eng. sc.; associate professor.

Zargaryan Yuri Arturovich – e-mail: yazargaryan@sfedu.ru; the department of automatic control systems; cand. of eng. sc.; associate professor.

УДК 681.2.089 DOI 10.18522/2311-3103-2022-3-222-234

С.И. Клевцов

ВЫБОР МОДЕЛИ ХАРАКТЕРИСТИКИ ПРЕОБРАЗОВАНИЯ ДАТЧИКА ДЛЯ УПРАВЛЕНИЯ ПОГРЕШНОСТЬЮ ПРИ ИЗМЕРЕНИИ ФИЗИЧЕСКИХ ВЕЛИЧИН

На примере датчика давления рассматривается проблема подбора модели и параметров функции преобразования микропроцессорного датчика. Функция преобразования базируется на математической модели, которая ставит в соответствие электрическому сигналу, поступающему с измерительного преобразователя датчика, значение физической величины. Модель функции преобразования микропроцессорного датчика должна повторять реальную пространственную зависимость электрического сигнала от измеряемой величины и учитывать влияние дестабилизирующих факторов, таких как температура. Микропроцессорные датчики используют для измерения параметров объекта с заданной точностью. Основной вклад в погрешность измерений вносит неточность аппроксимации реальной функции преобразования ее моделью. Необходимость достижения оптимального уровня погрешности измерения параметра в системе с учетом сложности и стоимости измерений требует управления погрешностью датчика. С этой целью представлены различные модели и методы аппроксимации. Для эффективного управления погрешностью предлагается метод мультисегментной пространственной аппроксимации, в основе которого лежат модели линейных или нелинейных пространственных элементов. Сформулирована процедура управления погрешностью. Порядок использования модели мультисегментной пространственной аппроксимации характеристики преобразования для вычислений давления с учетом влияния температуры основан на комбинированном применении линейных и нелинейных пространственных элементов в рамках одной модели. Процедура подбора типа сегмента должна начинаться с оценки возможности использования сначала линейного пространственного элемента, а в случае невозможности выполнения требований по точности, анализа использования нелинейного элемента. Метод позволяет изменять типы и конфигурацию пространственных элементов и таким способом влиять на погрешность измерений. Преимущества данного подхода подтверждаются результатами моделирования.

Модель; микропроцессорный датчик; характеристика преобразования; погрешность; аппроксимация.