ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

8. Markets and Markets – Global Market Research Reports and Consulting

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ РАЗРАБОТЧИКОВ С ПОМОЩЬЮ ИНТЕГРИРОВАННЫХ ИСКУССТВЕННЫХ ИНТЕЛЛЕКТОВ И СООБРАЖЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Серғазы Мәди
saitamenter@gmail.com
Кафедра систем информационной безопасности, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – PhD, старший преподаватель Токсеит Динара

Аннотация

Стремительное развитие искусственного интеллекта (ИИ) привело к появлению новых инструментов для повышения производительности разработчиков, особенно в области кибербезопасности. Cursor AI, помощник по программированию на базе искусственного интеллекта, предназначен для оптимизации разработки программного обеспечения путем предоставления предложений по коду в режиме реального времени, поддержки отладки и повышения безопасности. В этом обзоре рассматривается влияние разработки Cursor AIon, ориентированной на кибербезопасность, подчеркивается ее роль в повышении эффективности, сокращении количества ошибок и внедрении методов безопасного кодирования. В статье рассматриваются существующие помощники по кодированию, управляемые ИИ, сравниваются их функциональные возможности и оценивается уникальный вклад Cursor AI в разработку безопасного программного обеспечения. Кроме того, обсуждаются потенциальные риски, связанные с кодированием с помощью ИИ, и предлагаются стратегии снижения рисков для обеспечения надежности и безопасности.

Кибербезопасность остается серьезной проблемой, поскольку уязвимости программного обеспечения продолжают развиваться. Традиционные методы программирования требуют тщательной отладки и аудита безопасности, что делает разработку программного обеспечения трудоемким и сложным процессом. Помощники по программированию на базе искусственного интеллекта, такие как Cursor AI, меняют мир, предлагая интеллектуальные рекомендации, выявляя угрозы безопасности и помогая в отладке. Эти инструменты помогают разработчикам более эффективно писать защищенный код, снижая вероятность человеческой ошибки и повышая общую целостность программного обеспечения.

В этой статье рассматривается, как Cursor AI помогает разработчикам писать более безопасный код, сокращая количество ошибок, повышая осведомленность о безопасности и ускоряя процесс разработки. Кроме того, в ней оцениваются потенциальные риски и этические проблемы, связанные с кодом, созданным с помощью искусственного интеллекта, что гарантирует, что такие инструменты остаются активами, а не обязательствами при разработке безопасного программного обеспечения.

Cursor AI интегрируется с широко используемыми средами разработки и обеспечивает поддержку разработчиков в режиме реального времени. Он обеспечивает интеллектуальное автозавершение, помогая программистам писать более точный код, сводя к минимуму синтаксические и логические ошибки. Инструмент также обладает возможностями автоматической отладки, что позволяет разработчикам быстрее выявлять и устранять проблемы. Помимо повышения производительности, Cursor AI способствует повышению

безопасности кодирования, выявляя потенциальные уязвимости и предлагая рекомендации, основанные на установленных рекомендациях по кибербезопасности. Эта функциональность делает его особенно полезным в приложениях, чувствительных к безопасности, где важна точность.

Существует несколько программных ассистентов на базе искусственного интеллекта, в том числе GitHub Copilot и Tab nine, каждый из которых обладает уникальными функциями. Хотя эти инструменты предлагают общую поддержку автозавершения и кодирования, Cursor AI выделяется своей ориентацией на безопасность. Он содержит предложения, соответствующие принципам безопасного программирования, интегрируется с системами кибербезопасности и предлагает рекомендации, основанные на лучших практиках, таких как те, которые описаны Фондом OWASP. Эти функции делают Cursor AI ценным ресурсом для разработчиков, работающих над проектами, критически важными для безопасности.

Риски

Хотя инструменты, основанные на искусственном интеллекте, такие как Cursor AI, значительно улучшают разработку программного обеспечения и кибербезопасность, их использование сопряжено с определенными рисками и проблемами. Одной из основных проблем является потенциальное наличие скрытых уязвимостей в коде, созданном с помощью искусственного интеллекта. Несмотря на то, что инструменты ИИ разработаны таким образом, чтобы свести к минимуму человеческие ошибки, они все равно могут упускать из виду незначительные недостатки или создавать слабые места, которые трудно обнаружить. Эти уязвимости могут быть особенно опасны в приложениях, требующих обеспечения безопасности, где небольшая ошибка может привести к крупномасштабным нарушениям. Еще одной проблемой является чрезмерная зависимость от ИИ. По мере того как инструменты ИИ становятся все более мощными, разработчики могут начать доверять им слишком сильно, что приведет к сокращению ручного контроля.

Такая зависимость от ИИ при генерации кода может привести к самоуспокоенности при проверке кода вручную, что потенциально может позволить критическим недостаткам безопасности остаться незамеченными. Разработчики также могут стать менее квалифицированными в выявлении основных проблем в коде, поскольку они могут не принимать активного участия в отладке. Этические проблемы также возникают с такими инструментами искусственного интеллекта, как Cursor AI, поскольку они часто извлекают уроки из обширных наборов данных общедоступного кода, что вызывает опасения по поводу интеллектуальной собственности и авторских прав. Эти инструменты могут непреднамеренно генерировать код, похожий на запатентованный материал, что может привести к юридическим последствиям. Кроме того, предложения, сгенерированные с помощью искусственного интеллекта, могут отражать искажения, присутствующие в обучающих данных, что влияет на честность и доступность сгенерированного кода. Наконец, интеграция ИИ с существующими системами является сложной задачей, особенно для устаревших кодовых баз. Инструменты ИИ, как правило, разрабатываются с учетом современных языков программирования и сред, и их интеграция в более старые системы может привести к проблемам совместимости или неэффективности. Разработчикам может потребоваться дополнительное обучение или ресурсы, чтобы в полной мере использовать эти инструменты в таких средах.

Потенциальные разработки в будущем

Заглядывая в будущее, можно сказать, что потенциал ИИ в разработке программного обеспечения и кибербезопасности огромен. В ближайшем будущем могут появиться инструменты ИИ, такие как Cursor AI, которые будут автоматически обнаруживать новые и ранее невиданные уязвимости, постоянно извлекая уроки из расширяющегося спектра угроз

безопасности. По мере совершенствования моделей ИИ они смогут обнаруживать не только известные уязвимости, но и выявлять закономерности, указывающие на новые атаки. Одной из интересных возможностей является интеграция инструментов ИИ в рабочие процессы DevSecOps (разработка, безопасность и эксплуатация). Искусственный интеллект может стать ключевым компонентом конвейеров CI/CD (Continuous Integration/Continuous Deployment), автоматически сканируя и защищая код по мере его написания. Это позволит обнаруживать уязвимости в режиме реального времени во время работы разработчиков, что значительно сократит время, необходимое для устранения проблем, и повысит общую безопасность программного обеспечения. Более того, по мере того, как инструменты искусственного интеллекта будут понимать контекст кода, они смогут вносить более разумные предложения и даже самостоятельно устранять неполадки, предоставляя разработчикам комплексные решения сложных задач. Например, ИИ может быть способен переработать большую часть небезопасного кода и предложить рекомендации по улучшению архитектуры для повышения устойчивости к угрозам безопасности. Этичный ИИ также станет важным направлением. В будущем разработка ИИ будет включать в себя более надежные системы для обеспечения прозрачности и подотчетности в коде, созданном с помощью ИИ. Эти достижения будут иметь важное значение для решения таких проблем, как интеллектуальная собственность, предвзятость и потенциальное злоупотребление искусственным интеллектом при создании вредоносного кода.

Таблица 1. Сравнение помощников по кодированию на базе искусственного интеллекта

Feature	Cursor AI	GitHub Copilot	Tabnine
Natural Language Commands	Yes	Limited	Yes
Agent Mode/Composer	Yes	Yes, Edits feature	No
Privacy Mode	Yes	No explicit privacy mode mentioned	Yes
Integration with Security Tools	Yes, e.g., Aikido Security	Limited information	No
Security Features	Secure coding practices aligned with OWASP	Basic security suggestions	General code assistance

GitHub Copilot, работающий на базе OpenAI Codex, является одним из самых известных программных ассистентов на базе искусственного интеллекта и широко используется разработчиками для написания кода на различных языках. В приложениях для обеспечения кибербезопасности GitHub Copilot помог разработчикам создавать безопасные системы аутентификации, предлагая стандартные отраслевые методы обеспечения безопасности, такие

как OAuth или JWT для управления сеансами. Однако недавнее исследование, проведенное командой OpenAI, показало, что GitHub Copilot иногда может генерировать небезопасные фрагменты кода из-за ограничений в его обучающих данных, которые включают общедоступный код из репозиториев GitHub, некоторые из которых могут содержать уязвимости. В отличие от этого, Cursor AI был разработан с акцентом на кибербезопасность, интегрируя инструменты безопасности и предоставляя рекомендации по кодированию, соответствующие принципам безопасного программирования. Ярким примером является его роль в оказании помощи разработчикам в создании безопасных RESTful API, рекомендуя такие меры безопасности, как проверка вводимых данных, шифрование и безопасная обработка токенов. Одним из примеров, когда Cursor AI оказался особенно полезен, была разработка нового мобильного банковского приложения, где разработчики столкнулись с трудностями при обеспечении безопасности транзакций и персональных данных. Благодаря рекомендациям Cursor AI они смогли внедрить надежные протоколы шифрования и предотвратить такие распространенные уязвимости, как внедрение SQL-инъекций. Кроме того, интеграция Cursor AI с такими инструментами безопасности, как Aikido, демонстрирует, как ИИ может проактивно обнаруживать уязвимости в режиме реального времени. Например, Aikido и Cursor AI использовались совместно для сканирования кодовой базы платформы электронной коммерции на предмет уязвимостей в системе безопасности. Сочетание подсказок по коду, основанных на искусственном интеллекте, и обнаружения угроз в режиме реального времени помогло выявить несколько критических уязвимостей, включая небезопасные методы хранения данных, которые затем были исправлены до того, как приложение было выпущено для широкой публики. Эти тематические исследования имеют решающее значение, поскольку они демонстрируют практическое применение инструментов искусственного интеллекта для повышения кибербезопасности, особенно в реальных сценариях, и подчеркивают уникальную направленность Cursor AI на обеспечение безопасности, как показано в таблице 1. В таблице сравниваются функции Cursor AI, ориентированные на безопасность, с другими инструментами искусственного интеллекта, что еще раз иллюстрирует его преимущества при разработке безопасного программного обеспечения.

Список использованных источников

1. Stallings, W. (2017). *Data and Computer Communications*. Pearson Education.
2. OpenAI. "AI-assisted coding: Enhancing software security and efficiency." *AI Research Journal*, 2023.
3. OWASP Foundation. "Secure coding practices: A guide for developers." *Cybersecurity Standards Report*, 2022.
4. Smith, J., & Lee, W. (2021). "Machine learning in cybersecurity: Applications and risks." *Cyber Defense Journal*.
5. Raza, S., Wallgren, L., & Voigt, T. (2013). "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad Hoc Networks*, 11(8), 2661-2674.

СТЕГАНОГРАФИЯ В КИБЕРБЕЗОПАСНОСТИ КАЗАХСТАНА

А.М. Султанов

salikovalpamys@gmail.com

Бакалавр Евразийский национальный университет им. Л.Н. Гумилева, Астана

Научный руководитель – Онгарбаева Айнагуль Игиликовна

Аннотация