

Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора

Н.В. Беспалова¹, С.А. Корчагин², Д.В. Сердечный³, В.В. Селиверстов⁴

^{1,2,3}*Финансовый университет при Правительстве Российской Федерации, Москва*

⁴*Саратовский государственный технический университет им. Гагарина Ю.А., Саратов*

Аннотация: Постоянный рост кибератак на финансовый сектор требует построения современной системы защиты, основанной на использовании искусственного интеллекта или машинного обучения. В работе приведен анализ конкретных продуктов и решений мирового рынка, основанных на технологиях искусственного интеллекта, которые могут быть использованы для защиты критической информационной инфраструктуры.

Ключевые слова: кибератаки, критическая инфраструктура, искусственный интеллект, информационная безопасность, машинное обучение.

Введение

Современный мир характеризуется наличием большого числа кибератак на различные сферы жизни человечества. В рейтинге глобальных рисков Всемирного экономического форума проблема киберпреступности входит в первую пятёрку. Международное экспертное сообщество ставит её даже выше, чем терроризм и экологические проблемы.

Финансовый сектор продолжает оставаться наиболее атакуемым рынком. Аналитики Positive Technologies фиксируют постоянный рост кибератак на финансовый сектор [1]. Так, в третьем квартале 2023 года ими было выявлено вдвое больше уникальных киберинцидентов, чем в тот же период годом ранее, что безусловно говорит о пристальном внимании преступников к данной отрасли.

В качестве актуальных атак, направленных на финансовый сектор, можно считать:

- атаки отказа в обслуживании (DDoS);
- фишинг;
- атаки полного перебора (Brute-force);

- боты;
- атака через посредника (MITM).

Лидером списка актуальных атак, направленных на финансовый сектор, можно считать DDoS-атаки. Согласно данным StormWall, в 2023 году количество DDoS-атак во всем мире увеличилось на 63%. Статистика зафиксированных DDoS-атак по странам мира в 2023 году представлена на рис.1.



Рис. 1. – Статистика DDoS-атак по странам в 2023 году

Лидером по частоте DDoS-атак являются США, на Россию пришлось 7,3% от общего количества нападений, это 7-е место в мире. Кроме усиления мощности атак значительно выросла их продолжительность, вплоть до нескольких суток.

Порядка 26% всех DDoS-атак направлены на финансовый сектор, что составляет рост относительно предыдущего года на 78%.

Действия злоумышленников можно разделить на два основных вида – распределенные и целевые атаки.

Распределенные кибератаки представляют собой использование бот-сети и направлены одновременно на большое количество пользователей и ресурсов компаний.

Целевые атаки (APT advanced persistent threat - APT), отличаются от распределенных тем, что направлены на конкретную отрасль или отдельную систему. В ходе целевой атаки злоумышленник получает несанкционированный доступ к сети, закрепляется в инфраструктуре и надолго остается незамеченным, причем время внедрения может составлять несколько минут, а время обнаружения может измеряться в месяцах [2].

Согласно исследованию Positive Technologies, в IV квартале 2023 года доля целевых атак на организации увеличилась до 78% от общего числа [3]. Основные категории жертв целевых атак — это государственные учреждения, промышленные компании, финансовая отрасль и топливно-энергетический комплекс.

Применение искусственного интеллекта в кибербезопасности

Защита конечных точек становится перспективным инструментом борьбы с кибератаками. Для защиты конечных точек на рынке представлены следующие основные средства:

- классические антивирусы;
 - платформы для защиты конечных точек (Endpoint Protection Platform - EPP), направленные на предотвращение известных атак на основе существующих сигнатур;
 - система выявления киберугроз и реагирование на них для конечных точек (Endpoint Detection and Response – EDR), направленная на мониторинг и сбор информации о конечных точках в режиме реального времени, с целью своевременного реагирования на угрозы [4].
-

Для покрытия большего спектра угроз необходима комбинация всех трех решений. Помимо своевременного обнаружения и предотвращения целевых атак на конечные объекты финансового сектора, необходимо развивать процесс проактивного поиска угроз (threat hunting) [5]. Такой поиск напрямую связан со сбором телеметрии с конечных точек, который осуществляют EDR-решения. В исследовании Sans Institute говорится, что 88,5% компаний используют EDR и системы управления событиями и инцидентами информационной безопасности (Security information and event management - SIEM) в качестве инструментов для проведения threat hunting. Данный подход позволяет получить полную картина инцидентов внутри контура компании. Такая связка дает информацию по развитию инцидентов на каждой отдельной конечной точке [6].

В Таблице № 1. приведены данные об используемых и планируемых к внедрению средствах защиты конечных точек в компаниях, принявших участие в исследовании CyberRisk Alliance.

Таблица № 1.

	Уже используются	Запланированы на 2024 г.	Не планируются
Технологии на базе искусственного интеллекта или машинного обучения	13%	35%	52%
Выявление киберугроз и реагирование на них для конечных точек (EDR)	72%	20%	9%
Платформы для защиты конечных точек (EPP)	55%	20%	25%
Расширенные возможности обнаружения и реагирования (XDR)	39%	31%	31%
Технология унифицированного управления конечными узлами	39%	27%	35%



(UEM)			
-------	--	--	--

Более трети респондентов нацелены на внедрение технологий на базе искусственного интеллекта или машинного обучения. Определим основные области применения искусственного интеллекта в кибербезопасности:

- **Обнаружение и предотвращение угроз.** Искусственный интеллект может использоваться для анализа трафика в реальном времени, выявляя необычные паттерны поведения, которые могут указывать на наличие угрозы. Искусственный интеллект также может использоваться для разработки алгоритмов машинного обучения, которые могут автоматически обнаруживать и блокировать вредоносные программы и атаки. Кроме этого, машинное обучение способно распознавать скрытые признаки фишинговых и мошеннических писем, не очевидные на первый взгляд.
- **Реагирование на инциденты.** Искусственный интеллект может использоваться для автоматизации процессов реагирования на инциденты, такие как сбор данных, анализ и устранение неполадок. Искусственный интеллект может использоваться для прогнозирования будущих атак на основе текущих тенденций в киберпреступности, автоматически обновлять базы сигнатур вирусов, а также поведенческие модели, используемые для обнаружения аномалий. Искусственный интеллект также может использоваться для разработки алгоритмов машинного обучения, которые могут автоматически определять и классифицировать инциденты.
- **Управление рисками.** Искусственный интеллект может использоваться для оценки рисков, связанных с информационной безопасностью, а также для разработки рекомендаций по снижению рисков [7].

Искусственный интеллект является мощным инструментом, который может использоваться для повышения эффективности и точности

деятельности специалистов по информационной безопасности. Применение искусственного интеллекта в средствах защиты объектов финансового сектора не только повышает эффективность обнаружения и предотвращения потенциальных атак за счет автоматизации задач, но и увеличивает точность информации о потенциальных угрозах.

Современные технологии, использующие искусственный интеллект, помогают защищать данные и информационные системы от угроз, а также способствуют развитию новых методов шифрования и защиты информации.

На мировом рынке существует ряд конкретных продуктов и решений на основе искусственного интеллекта, которые могут быть использованы для защиты критической информационной инфраструктуры. Вот некоторые из них:

1. **Darktrace**

Продукт разработок компании - Darktrace Enterprise Immune System представляет самообучающуюся систему защиты корпоративной среды в двух вариантах: как аппаратное устройство и подключаться в виде виртуальной машины. Darktrace Enterprise Immune System основан не только на анализе ранее произошедших инцидентов, основной акцент делается на всестороннем анализе организации: исследование каждого пользователя, устройства и взаимосвязи между ними. Применение искусственного интеллекта позволяет выявить едва заметные поведенческие отклонения сотрудников, указывающие на потенциальную киберугрозу, даже основанную на применении инструментов и техник, которые никогда ранее не были замечены. В случае выявления аномального поведения формируется уведомление в службу безопасности, а в случае необходимости передача данных блокируется. Технология работает как цифровое антитело, генерируя измеренные и пропорциональные ответы при возникновении

угрожающего инцидента. Эта способность сдерживать угрозы с использованием искусственного интеллекта позволяет избежать значительного ущерба даже в случае масштабных атак [8].

2. Cylance

Американская компания Cylance (с 2018 года функционирует как подразделение канадского производителя программного обеспечения BlackBerry) использует технологии машинного обучения и искусственного интеллекта для проактивного обнаружения и предотвращения вредоносного программного обеспечения и атак на объекты критической информационной инфраструктуры. CylanceOPTICS предлагает подход EDR, ориентированный в первую очередь на предотвращение кибератак, ориентируясь на модули обнаружения угроз с автоматическим машинным обучением, что позволяет выявлять ряд угроз, которые было бы практически невозможно обнаружить при использовании статических правил поведения. Решение EDR, построенное на стратегии предотвращения, намного превосходит традиционные решения EDR, как видно из сравнительной Таблицы № 2.

Таблица № 2.

	Выявление киберугроз и реагирование на них для конечных точек EDR	Выявление киберугроз и реагирование на них для конечных точек CylanceOPTICS	Преимущества подхода CylanceOPTICS
Подход к безопасности	Оперативное обнаружение угроз и реагирование на них	Непрерывное предотвращение угроз и инцидентов	Сокращение общего числа инцидентов, требующих принятия мер/анализа
Требуемые навыки	Продвинутый набор навыков аналитика безопасности	Любой уровень квалификации и опыта	Расширяется круг возможных специалистов, способных управлять решением
Собранные данные	Непрерывно передает всю активность конечных	Собирает и хранит локально только данные, относящиеся к	Снижение ответственности и повышение соответствия требованиям



	точек в облако или отправляет ее на выделенное оборудование	безопасности	
Место хранения данных	Непрерывная передача данных в облако или агрегирование на локальном оборудовании	Хранит данные локально на каждой конечной точке	Локальное хранение данных значительно оптимизирует производительность и масштабируемость
Методы обнаружения угроз	Требует написания индивидуальных правил поведения и их постоянного дополнения	Объединяет правила поведения с обученными модулями обнаружения угроз ML для обеспечения большей и постоянно растущей широты охвата, выполняемой локально на каждой конечной точке	Сокращение числа правил, которые должны создаваться и поддерживаться экспертом по безопасности
Обнаружение угроз	Требуются значительный опыт для настройки и выполнения функций поиска потенциальных угроз.	Оперирует простыми в настройке критериями поиска и оптимизированный сбор оперативных данных с конечных точек	Повышает способность выявлять труднодоступные угрозы без использования дополнительного человеческого ресурсов высокого уровня подготовки.
Определение источника угроз	Анализирует собранные данные, чтобы определить, где активная угроза проникла в среду и как остановить продолжающийся ущерб	Использует данные, собранные при предотвращении угрозы с помощью CylancePROTECT, чтобы понять вектор атаки, выбранный злоумышленником	Автоматизированный подход сокращает время завершения анализа
IR возможности	Требуются обширные знания в области безопасности для использования передовых инструментов, которые выявляют и устраняют проблемы безопасности	Выполняет автоматические действия IR или позволяет выполнять действия вручную, развертывая предварительно настроенные и пользовательские ответные действия, чтобы быстро вернуть	Автоматизация и машинное обучение позволяют большим и малым организациям поддерживать уровень безопасности, который когда-то считался доступным только крупнейшим организациям

		систему в состоянии доверия	
--	--	--------------------------------	--

Решения BlackBerry по предотвращению угроз и реагированию на них на основе искусственного интеллекта осуществляют защиту конечных точек от широкого спектра угроз. Борьба с атаками без файлов требует отхода от традиционных файловых контрмер. BlackBerry использует защиту памяти, управление сценариями и макросами, а также авторский механизм контекстного анализа (CAE) для обеспечения безопасности организации [9].

3. SparkCognition

Американская компания SparkCognition предоставляет AI-powered систему кибербезопасности, которая использует решения в области искусственного интеллекта, основанные на машинном обучении, генеративном искусственном интеллекте, компьютерном зрении, обработке естественного языка для анализа данных с целью обнаружения угроз на объектах критической информационной инфраструктуры. Решения SparkCognition позволяют предотвратить непредвиденные простои, максимизируют производительность активов, реализуют инициативы с нулевым результатом, активно решают вопросы безопасности и предотвращают кибератаки. Используя запатентованную технологию AI/ML, EPP от SparkCognition можно не только защитить ресурсы пользователей, но и свести к минимуму сбои в производительности и уменьшить количество ложных срабатываний, тем самым устраняя помехи в рабочем процессе. Рассмотрим основные решения для различных отраслей и секторов (Таблица № 3).

Таблица № 3.

Решение	Характеристика
Darwin	Платформа машинного обучения и искусственного интеллекта, предназначенная для создания и развертывания моделей машинного обучения и оптимизации бизнес-процессов с использованием данных.
DeepArmor	Продукт, который использует искусственный интеллект для обнаружения и предотвращения атак на компьютеры и сети в реальном времени.
DeepNLP	Библиотека искусственного интеллекта, которая предназначена для обработки естественного языка и автоматического анализа текстов. Она помогает в различных решениях, связанных с текстовыми данными, такими, как анализ эмоциональной тональности или категоризация текста.
DeepArmor Evolve	Решение для разработки, обучения и развертывания моделей машинного обучения для кибербезопасности. Оно позволяет компаниям настраивать и применять интеллектуальные системы для борьбы с актуальными угрозами безопасности.
Ascend	Платформа предиктивного обслуживания, которая использует аналитику данных и искусственный интеллект для оптимизации процессов обслуживания и предотвращения аварий и отказов оборудования.

4. IBM Watson for Cyber Security

IBM Watson использует искусственный интеллект и аналитику данных для обнаружения и предотвращения кибератак на объекты критической информационной инфраструктуры, а также для проведения анализа уязвимостей и прогнозирования рисков. Рассмотрим основные пакеты данной компании.

IBM Security QRadar Suite - модернизированное решение для обнаружения угроз и реагирования на них. В портфолио внедрены средства искусственного интеллекта и автоматизации корпоративного уровня, которые значительно повышают производительность аналитиков и помогают командам безопасности с ограниченными ресурсами работать более эффективно с использованием основных технологий. Решение предлагает интегрированные продукты

для обеспечения безопасности конечных точек (EDR, XDR, MDR), управления журналами, SIEM и SOAR — и все это с общим пользовательским интерфейсом, общими аналитическими данными и связанными рабочими процессами.

IBM QRadar работает на основе сервиса Watson for Cyber Security — IBM QRadar Advisor with Watson, работа ведется круглосуточно и включает в себя этапы, представленные на рис.2.

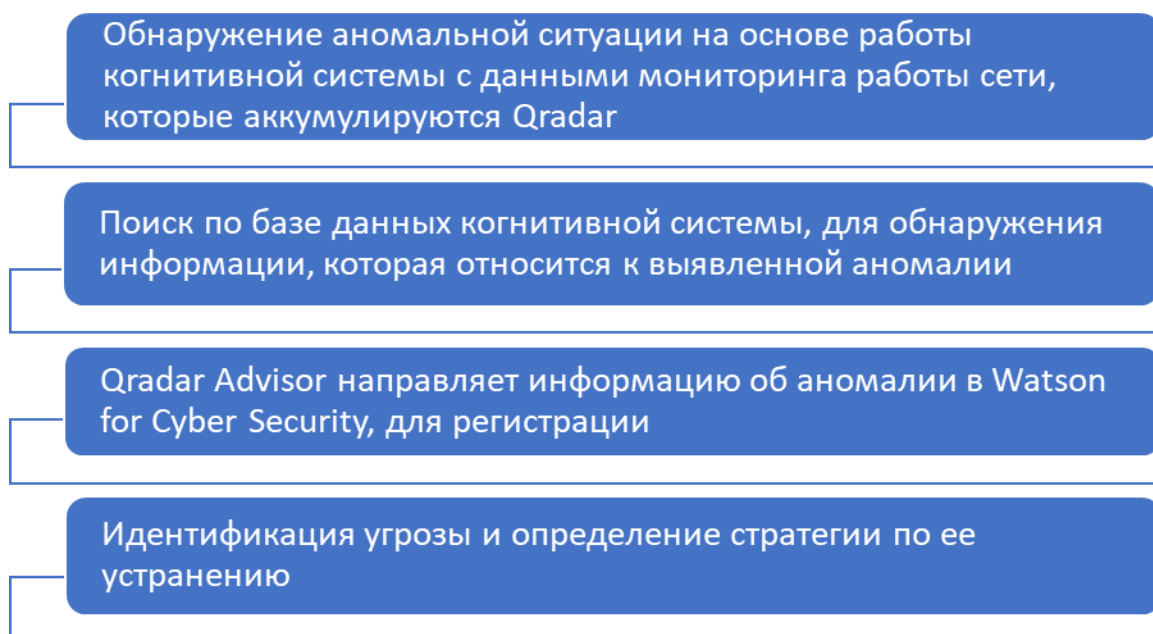


Рис. 2. Этапы работы IBM QRadar

К достоинствам QRadar можно отнести единую архитектуру анализа сетевых потоков, уязвимостей, данных о пользователях и ресурсах; анализ корреляции в реальном времени с использованием Sense Analytics для диагностики наиболее серьезных угроз; расстановку приоритетов и автоматическое реагирование на инциденты.

IBM Security Guardium — это решение для защиты данных, которое может адаптироваться к изменениям среды угроз, обеспечивая полную

видимость, соответствие требованиям и защиту на протяжении всего жизненного цикла безопасности данных.

IBM Security Guardium современная масштабируемая платформа безопасности данных, которая оснащена встроенным искусственным интеллектом, направленным на обнаружение выбросов. Непрерывный мониторинг с помощью Guardium DSPM помогает организациям повысить уровень безопасности. Решение Plug-and-Play подключается к облачным хранилищам данных и приложениям SaaS и оперативно дает информацию по безопасности облачных данных. IBM Security Guardium Data Protection поддерживает современный подход к безопасности данных, основанный на нулевой доверии, обеспечивая обнаружение и классификацию данных в основных хранилищах данных, комплексный мониторинг активности и гибкие варианты развертывания для быстрого и интеллектуального реагирования на сложные угрозы, автоматизацию рабочих процессов используя готовые шаблоны для нормативных документов, включая PCI DSS, SOX, HIPAA, GDPR, CCPA и многих других [10].

IBM Security Guardium включает модульные решения, которые обеспечивают шифрование данных, токенизацию, маскирование данных и возможности управления ключами, чтобы помочь защитить и контролировать доступ к данным в гибридной мультиоблачной среде.

Семейство *IBM Security Verify* предоставляет автоматизированные, облачные и локальные возможности для администрирования управления идентификацией и доступом сотрудников и потребителей, а также управления привилегированными учетными записями [11].

В качестве интересных решений, можно также предложить к рассмотрению CryptoMove, систему, использующую децентрализованное

шифрования и перемещение данных, что позволяет снизить криптоатаки. А также системы, основанные на использовании квантовых технологий: система Quantum Computing and Cryptography: разрабатывает квантово-устойчивые алгоритмы шифрования, где искусственный интеллект используется при тестировании эффективности и криптостойкости методов шифрования и Post-Quantum Cryptography, включающие в себя алгоритмы, устойчивые к атакам с использованием квантовых компьютеров.

Можно также выделить ряд российских компаний в области кибербезопасности:

- Kaspersky Lab активно использует машинное обучение и искусственный интеллект для обнаружения и предотвращения киберугроз. Их технологии помогают в анализе поведения программ и файлов в реальном времени, что позволяет выявлять и блокировать вредоносные действия даже от ранее неизвестного вредоносного ПО.
- Ростелеком-Солар дочерняя компания "Ростелекома", которая разрабатывает продукты и решения для обеспечения безопасности информационных систем предприятий и государственных органов.
- VI.ZONE компания, принадлежащая Сбербанку, занимается разработкой решений для анализа угроз и защиты от кибератак. VI.ZONE активно сотрудничает с российскими и международными организациями для повышения уровня кибербезопасности.

Заключение

Поскольку финансовый сектор находится под пристальным вниманием киберпреступников, повышение безопасности остается актуальной проблемой, требующей своевременных и эффективных решений.

Повышение киберустойчивости возможно за счет разработок, адаптирующихся в режиме реального времени и направленных на

опережение действий киберприступников. Применение искусственного интеллекта в таких разработках позволяет сократить затраты и оптимизировать ресурсы для решения задач детектирования аномалий, выявления внутренних нарушителей и др.

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Литература

1. Positive Technologies Киберугрозы финансовой отрасли: промежуточные итоги 2023 года. ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения 01.02.2024)

2. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – №1. – С. 77-96.

3. Positive Technologies Актуальные киберугрозы: III квартал 2023 года ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения 04.02.2024)

4. Парфений Н. А., Скворцова Н. В. Киберпреступность в финансовом секторе экономики // Инновационные, финансовые и экономические аспекты информационной экономики XXI века. – 2020. – С. 145-151.

5. Александрович С. А. Анализ влияния компьютерных атак на банковскую систему Российской Федерации // Вестник Российского экономического университета им. ГВ Плеханова. – 2019. – №. 6 (108). – С. 202-210.

6. Феклин В.Г., Соловьев В.И., Корчагин С.А., Царегородцев А.В. Методы машинного обучения в задачах контроля криптовалютных транзакций // Вопросы кибербезопасности. - 2023. № 4 (56). С. 2-11.

7. Беспалова Н.В., Нечаев С.В. Обеспечение информационной безопасности облачных хранилищ // Вопросы безопасности. - 2023. № 2. С. 19-26.

8. Filkins.B SANS 2019 State of OT/ICS Cybersecurity Survey. sans.org/reading-room/whitepapers/analyst (дата обращения: 11.02.2024).

9. Vamrara A. Evaluating database security and cyber-attacks: A relational approach //Journal of Internet Banking and Commerce. – 2015. vol. 20. № 2. p. 1-17.

10. Castillo D.P., Regidor F.M., Higuera J.B., Higuera J.R., Montalvo J.A. A new mail system for secure data transmission in cyber physical systems. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2020. vol. 28(2). pp. 23-48. DOI: 10.1142/ S0218488520400127.

11. Zobal L., Kolar D., Kroustek J. Exploring current e-mail cyber threats authenticated SMTP honeypot. 17-th International Conference on Security and Cryptography. Paris. 2020. pp.253-262.

References

1. Positive Technologies Kiberugrozy` finansovoj otrasli: promezhutochny`e itogi 2023 goda [Cyber threats to the financial industry: interim results of 2023]. ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (date assesed 01.02.2024).

2. Semeko G.V. Social`ny`e novacii i social`ny`e nauki. Moskva: INION RAN, 2020. №1. p. 77-96.

3. Positive Technologies Aktual`ny`e kiberugrozy`: III kvartal 2023 goda [Current cyber threats: The third quarter of 2023]. ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (date assesed 04.02.2024)

4. Parfenij N. A., Skvorczova N. V. Innovacionny`e, finansovy`e i e`konomicheskie aspekty` informacionnoj e`konomiki XXI veka. 2020. pp. 145-151.



5. Aleksandrovich C. A. Vestnik Rossijskogo e`konomicheskogo universiteta im. GV Plexanova. 2019. №. 6 (108). pp. 202-210.
6. Feklin V.G., Solov`ev V.I., Korchagin S.A., Czaregorodcev A.V. Voprosy` kiberbezopasnosti. 2023. № 4 (56).pp. 2-11.
7. Bepalova N.V., Nechaev S.V. Voprosy` bezopasnosti. 2023. № 2. pp. 19-26.
8. Filkins.B, SANS 2019 State of OT/ICS Cybersecurity Survey. sans.org/reading-room/whitepapers/analyst (date assesed: 11.02.2024).
9. Bamrara A. J. Internet Bank. Commer. 2015. vol. 20. № 2. pp. 1-17.
10. Castillo D.P., Regidor F.M., Higuera J.B., Higuera J.R., International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2020. vol. 28(2). pp. 23-48.
11. Zobal L., Kolar D., Kroustek J. 17-th International Conference on Security and Cryptography. Paris. 2020. pp.253-262.

Дата поступления: 13.03.2024

Дата публикации: 26.04.2024