УДК 004.8:004.056:005.334

Олин Роман Александрович
Самарский государственный экономический университет
Шарипов Рифат Рашатович
Казанский национальный исследовательский технический университет
им. А.Н. Туполева - КАИ
Бондаренко Владимир Владимирович
Самарский национальный исследовательский университет имени академика С.П. Королева

Управление рисками информационной безопасности при внедрении автономных агентов с искусственным интеллектом

Аннотация. В статье рассматриваются риски информационной безопасности, возникающие при внедрении автономных агентов с искусственным интеллектом в деятельность организаций. Показано, что ограниченная самостоятельность агента изменяет характер цифрового действия за счёт способности использования доступных инструментов и интерпретации поставленной цели с учётом контекста. Уделено внимание атакам через внедрение инструкций, риску превышения полномочий, ошибочной постановке задачи и другим угрозам, возникающим при внедрении автономных агентов в корпоративную информационную среду. Предложены меры снижения указанных рисков, основанные на разграничении доверенных и недоверенных фрагментов контекста, принципе минимально необходимых полномочий и закреплении ответственности за агентные сценарии. Сделан вывод о том, что автономные агенты с искусственным интеллектом способны стать значимым фактором роста производительности и конкурентным преимуществом организации только при условии безопасного проектирования и постоянного контроля их действий.

Ключевые слова: автономные агенты, искусственный интеллект, информационная безопасность, агентные системы, риски внедрения, митигация рисков, управление полномочиями, цифровая трансформация.

Olin Roman Alexandrovich
Samara State University of Economics
Sharipov Rifat Rashatovich
Kazan National Research Technical University
Bondarenko Vladimir Vladimirovich
Samara National Research University

Managing information security risks in the implementation of autonomous artificial intelligence agents

Annotation. The article examines information security risks arising from the implementation of autonomous artificial intelligence agents in organizational activities. It is shown that the limited autonomy of an agent changes the nature of digital action through its ability to use available tools and interpret assigned goals with regard to the operational context. Particular attention is paid to prompt injection attacks, excessive privilege risks, incorrect task specification, and other threats associated with the deployment of autonomous agents within corporate information environments. The article proposes risk mitigation measures based on the separation of trusted and untrusted contextual information, the principle of least privilege, and the assignment of responsibility for agent-based operational scenarios. It is concluded that autonomous artificial intelligence agents can become a significant driver of productivity growth and a source of

competitive advantage only under conditions of secure system design and continuous oversight of their actions.

Keywords: autonomous agents, artificial intelligence, information security, agent-based systems, implementation risks, risk mitigation, privilege management, digital transformation.

Инновационная экономика смещает центр технологического роста к созданию программных субъектов, способных самостоятельно поддерживать деловую активность в сложной цифровой среде. Классическая автоматизация строилась вокруг заранее заданных алгоритмов, превращая управленческую задачу в последовательность формализованных команд, исполняемых при совпадении входных условий с описанным сценарием. [1] Такой подход обеспечил значительный прирост скорости, снизив стоимость рутинной обработки сведений и закрепив представление о программе как об исполнительном механизме. [2] По мере увеличения цифровизации предприятий обнаружилась граница прежней модели, большая часть современных процессов опирается на разнородные документы, переписку, внешние базы, нормативные требования и изменяющийся контекст, плохо укладывающийся в жёсткую схему заранее описанные детерминированные алгоритмы. [3] Усложнение организационных процессов, сопровождаемое ростом объёма разнородных данных, расширением цифровых каналов взаимодействия и увеличением числа управленческих ситуаций с неполной формализацией, обусловило переход от традиционных алгоритмических систем к автономным агентам с искусственным интеллектом (ИИ), которые отличаются от чат-бота, экспертной системы и обычного программного модуля характером включения в организационную деятельность. [4] Чат-бот преимущественно поддерживает диалог с пользователем, формируя ответ в пределах заданного коммуникативного сценария. Экспертная система применяет заранее описанную базу правил к формализованной ситуации, сохраняя зависимость от полноты исходной модели предметной области. Прикладной модуль выполняет отдельную функцию внутри информационной системы, получая входные параметры и возвращая результат по определённому алгоритму. В отличие от перечисленных средств, агентная архитектура объединяет интерпретацию цели, анализ контекста, обращение к памяти и выбор инструментов для достижения поставленных задач. [5] Организационная значимость такой схемы возникает из способности самостоятельно определять промежуточные шаги в пределах порученной задачи, сохраняя связь с исходной целью и доступными ресурсами. Самостоятельность остаётся ограниченной, поскольку пределы допустимого поведения задаются полномочиями, политиками доступа, перечнем разрешённых инструментов и регламентом проверки результатов. [6] Агент начинает участвовать в корпоративной среде как цифровой участник, способный инициировать обращения к сервисам, выбирать порядок операций, использовать внешние сведения и влиять на управленческие решения. [7] Предметом регулирования становится траектория делегированного поведения, включающая постановку цели и фиксацию результата. В технической части доступ агента задаётся отдельными разрешениями, связанными с конкретной задачей и уровнем риска, каждое обращение к корпоративным ресурсам фиксируется в проверяемом журнале, что позволяет восстановить происхождение использованных сведений, оценить правомерность выполненной операции и определить момент перехода от аналитической обработки к практическому действию. [8] Расширение самостоятельности агента влияет на проектирование системы безопасности, чем больше принимается промежуточных решений, тем точнее должны быть определены доступ к данным, разрешённые операции и условия, при которых дальнейшее выполнение задачи передаётся человеку. Ограничения закрепляются в архитектуре системы до начала эксплуатации и соотносятся с ролью и допустимыми последствиями операции. [9] Самостоятельный правовой статус у агента отсутствует, однако выполняемые им действия могут создавать экономические и юридические последствия для организации, поскольку совершаются в пределах выданных полномочий и с использованием корпоративных ресурсов. По этой причине безопасность

агентной системы должна рассматриваться как контроль устойчивости связи между целью, разрешёнными средствами и полученным результатом. [10] Нарушение связи приводит к ошибочному исполнению поручений или совершению операции за пределами предоставленных прав.

Наиболее уязвимым местом является рабочий контекст, через который агент получает сведения для анализа и основания для дальнейших действий. В традиционной информационной системе внешние данные обычно отделены от управляющих команд установленным форматом и процедурой обработки. В агентной архитектуре такое разграничение становится менее очевидным, поскольку текст документов, сообщения пользователя или фрагменты веб-страниц поступают в единую область интерпретации. [11] Поэтому угрозы смещаются от повреждения отдельного файла или отказа сервиса к искажению всей исполнительной логики. Если внешний текст воспринимается моделью как часть допустимой инструкции, последующее действие агента выглядит формально связанным с исходной задачей, хотя фактически направляется посторонним указанием. Атаки через внедрение инструкций следует рассматривать как одну из ключевых угроз для агентных систем, поскольку их результат затрагивает выбор инструментов, порядок операций и обращение к внутренним корпоративным данным. [12]

Риск увеличивается при наличии у агента доступа к инструментам, поскольку искажённая инструкция начинает влиять на выбор прикладного программного интерфейса, порядок обращения к сервисам и условия завершения операции. Защита от внедрения инструкций должна рассматриваться как задача разграничения доверенных и недоверенных фрагментов контекста. Входные материалы, полученные из внешних источников, требуют обработки в режиме данных, исключая команды, независимо от формы их представления и степени сходства с внутренними указаниями системы. [13] Без фильтрации агент способен принять текст, созданный третьей стороной, за часть допустимого поручения, после чего нарушение выходит за рамки ответа и влечёт изменения состояния информационной системы.

Превышение полномочий связано с механизмом делегирования, организация передаёт агенту часть полномочий, сохраняя за собой ответственность за результат. [14] Безопасность передачи полномочий зависит от точности настройки прав доступа, ошибки возникают при получении агентом более широкого набора возможностей, чем требуется для конкретной задачи. Избыточные разрешения позволяют использовать несвязанные с поручением инструменты, выполнять операции без согласования с ответственным сотрудником или получать широкий спектр сведений из корпоративной системы. При нормальном ходе работы такие возможности могут оставаться незаметными, поскольку агент применяет лишь часть доступных функций. Опасность проявляется в момент ошибки, атаки через контекст или неоднозначного запроса, когда отклонение в поведении влечёт нежелательные последствия для организации. Методом борьбы с угрозой является принцип предоставления минимально необходимых полномочий, при которых агент должен получать только те данные и инструменты, прямо требующиеся для выполнения порученной функции в заданных условиях. [15] Расширение доступа допустимо лишь при наличии весомого обоснования и процедуры передачи спорных случаев человеку. При таком подходе делегирование задач сохраняет экономический эффект, но снижает вероятность ситуации, при которой агент получит возможность совершить действие вне цели бизнес-процесса.

Для снижения риска ошибочной постановки задачи поручение должно превращаться в проверяемый сценарий с заранее определённым допустимым результатом и условием для обращения за помощью к человеку. Внедрение агента становится безопаснее, когда критическая операция начинается с подтверждения интерпретации цели, позволяющего сопоставить машинную декомпозицию с фактическим намерением владельца процесса. [16]

Вероятность некорректного применения инструмента сохраняется даже при правомерно выданном доступе. Агент, обладая разрешением на работу с корпоративным сервисом, может выбрать неподходящий режим операции, неверно заполнить параметр, обратиться к устаревшей версии объекта или применить функцию записи вместо предварительной проверки. Опасность возникает при расхождении между технической возможностью использовать инструмент и обоснованностью его применения в конкретной управленческой задаче. Митигация риска требует описания инструментов как управляемых действий с заранее заданными последствиями, перед изменением состояния информационной системы агент должен проходить через режим предварительного расчёта последствий, при котором результат операции сначала отображается как проект действия и только после проверки переводится в исполнение. [17]

Риск вторичного раскрытия конфиденциальных данных появляется после надлежащего получения сведений агентом. [18] Доступ к документу или записи может быть предоставлен обоснованно, однако последующее использование результата создаёт самостоятельную угрозу, если служебная информация включается в ответ, пересылается внешнему сервису или объединяется с другими материалами и используется за пределами исходного поручения. Ситуация опасна в процессах, в рамках которых один и тот же агент анализирует документы, формирует отчёт и взаимодействует с внешними каналами. Ограничение риска должно строиться на раздельных строгих политиках чтения и вывода данных, корпоративная система должна оценивать возможность дальнейшего распространения подготовленного результата. [19]

Угроза, связанная с долговременной памятью агента, имеет отложенный характер. Сохранённое предпочтение пользователя, промежуточный вывод, или фрагмент служебного документа способны повлиять на будущую задачу, не имеющую прямой связи с первоначальным запросом. В отличие от краткосрочного контекста, память создаёт устойчивую зависимость последующих действий от ранее накопленных сведений. [20] Уменьшение угрозы предполагает отношение к памяти как к контролируемому хранилищу, запись нового элемента должна сопровождаться указанием источника, срока действия и допустимой области повторного применения, а сведения с признаками служебной тайны или высокой чувствительности должны сохраняться только после отдельного разрешения ответственного лица.

Риск недостаточной проверяемости результата возникает при получении организацией итога действия агента без возможности восстановить историю действий. Обычный журнал событий фиксирует факт обращения к сервису, но не всегда отображает, какие версии документов были сопоставлены, какие допущения приняты моделью и каким образом промежуточный вывод повлиял на следующий шаг. В следствие чего результат трудно оспорить, исправить или использовать как доказательство некорректного исполнения. Меры митигации состоят в формировании проверяемого следа как в ходе выполнения операций, так и после их завершения. Для чувствительных сценариев агент должен сохранять связку между входными материалами, промежуточными решениями и конечным действием в форме, пригодной для последующего аудита. [21]

Неконтролируемое масштабирование ошибки обусловлено способностью агента выполнять однотипные действия с высокой скоростью. Неверная интерпретация поручения или сбой в параметрах запроса могут затронуть массив документов и цепочку связанных операций. В отличие от единичной ошибки пользователя, агентное отклонение распространяется быстрее и дольше остаётся незамеченным при пакетной обработке. Снижение вероятности масштабирования ошибки достигается поэтапным исполнением операции, корректность первых результатов проверяются до расширения сценария на весь набор объектов. [22] Продолжение работы агента должно зависеть от отсутствия аномальных признаков и соответствия последующих действий установленным ограничениям безопасности.

Организационная неопределённость возникает при отсутствии согласованного распределения ответственности между техническим администратором агента, владельцем бизнес-процесса и подразделением информационной безопасности компании. В случае отсутствия установленного порядка взаимодействия между участниками, отклонение в работе агента может остаться без выявления продолжительное время. В ситуации неопределённости техническая ошибка постепенно переходит в управленческую проблему, поскольку становится неясно, кто должен изменить сценарий, ограничить доступ или остановить выполнение задачи. Снижение риска требует закрепления ответственности за каждый агентный сценарий до промышленного запуска за конкретным работником. [23] Владелец процесса должен отвечать за допустимый результат, техническая служба за корректность интеграции, а подразделение информационной безопасности за режим допуска и порядок реагирования, что позволяет рассматривать автономного агента как управляемый элемент организационной системы организации.

Автономные агенты с ИИ следует рассматривать как один из ключевых механизмов будущего развития корпоративных информационных систем. Их ценность определяется способностью быстро и качественно связывать разрозненные данные, управленческие цели и организационные процедуры в единую комплексную последовательность действий, сокращая время выполнения сложных операций и снижая нагрузку на сотрудников, занятых рутинной аналитической и административной работой. При корректном внедрении агентные системы способны существенно повысить производительность компании за счёт ускорения обработки документов, координации процессов и более рационального использования накопленных данных. Объединяя автономность с ограничениями и проверяемыми действиями, достигается существенное расширение возможностей. Компании, способные раньше других выстроить безопасную модель применения ИИ-агентов, получают прирост операционной эффективности и долгосрочное конкурентное преимущество, поскольку быстрее адаптируют внутренние процессы к изменяющейся деловой среде и формируют более высокий уровень управляемости цифровой инфраструктуры.

Массовое внедрение автономных агентов с ИИ требует зрелой инженерной и управленческой культуры, при которой каждый источник угрозы получает соразмерный механизм митигации, что отображено в Таблице 1. Ошибочная постановка задачи устраняется через проверяемый сценарий и подтверждение цели, а проверяемость результата обеспечивается сохранением связи между исходными материалами, промежуточными выводами и конечным действием.

Таблица 1. Риски внедрения автономных агентов и меры их смягчения

№	Риск	Неочевидный механизм	Возможное последствие	Митигация
1.	Ошибочная операционализация цели	Естественно-языковое поручение превращается в машинный маршрут без проверки смысла конечного результата.	Агент формально завершает задачу, но создаёт управленчески неверный результат.	Вводится контракт задачи с критерием завершения и обязательным подтверждением трактовки для критичных сценариев.
2.	Некорректное применение разрешённого инструмента	Разрешение на доступ к сервису не определяет безопасный режим вызова и допустимые	Правомерный инструмент используется способом, меняющим данные вне	Инструменты оформляются как управляемые действия с предварительным расчётом

		параметры операции.	делового смысла поручения.	последствий и режимом проектного исполнения.
3.	Вторичное раскрытие данных	Данные получены законно, но затем включаются в ответ, отчёт или внешний запрос вне первоначальной цели.	Конфиденциальная информация покидает допустимый контур после корректного этапа чтения.	Политика вывода отделяется от политики доступа, а результат проверяется по адресату, каналу и категории сведений.
4.	Инерция долговременной памяти	Сохранённый фрагмент прошлого контекста влияет на будущие решения без повторной проверки применимости.	Ошибочная или чувствительная запись становится скрытым основанием для серии последующих действий.	Память получает источник, срок действия и область применения, а сохранение чувствительных сведений требует отдельного разрешения.
5.	Непроверяемость результата	Журнал фиксирует факт операции, но не восстанавливает содержание промежуточных решений.	Результат трудно оспорить, воспроизвести или использовать для внутреннего расследования.	В ходе исполнения формируется доказательная связка входных материалов, промежуточных выводов и конечного действия.
6.	Масштабирование ошибки	Единичное неверное решение автоматически распространяется на множество объектов или связанных операций.	Локальное отклонение быстро превращается в массовое изменение корпоративных данных.	Исполнение расширяется поэтапно, а переход к следующему объёму зависит от отсутствия аномальных признаков.
7.	Организационная неопределённость	Ответственность распределена между бизнесом, ИТ и безопасностью без единого владельца сценария.	Инцидент задерживается на стыке функций и теряет управляемость.	Для каждого сценария заранее закрепляется владелец делового результата, технической интеграции и режима безопасности.

Будущее автономных агентов связано с переходом от экспериментального применения к широкому повсеместному внедрению с предоставлением достаточной свободы для обработки сложных задач. При таком подходе агентные системы способны существенно повысить производительность компаний и снизить нагрузку на сотрудников. Наибольшее конкурентное преимущество получат организации, способные соединить техническую автономию с дисциплиной безопасного внедрения, такая модель позволит расширить

масштабы применения инноваций без утраты контроля над последствиями принимаемых решений.

Список источников

1. Воропаева, Н. В. Декомпозиция разнотемповых дискретных систем управления / Н. В. Воропаева, В. А. Соболев // Мехатроника, автоматизация, управление. – 2004. – № 8. – С. 2-6. – EDN KMMQPJ.

2. Воропаева, Н. В. Декомпозиция задач управления для разнотемповых систем с дискретным временем / Н. В. Воропаева // XII всероссийское совещание по проблемам управления ВСПУ-2014, Москва, 16–19 июля 2014 года / Институт проблем управления им. В.А. Трапезникова РАН. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2014. – С. 842-848. – EDN SSIATB.

3. Влияние стандартизации процессов разработки ПО на достижимость конечного результата / К. В. Портнов, Б. Э. Забержинский, Г. В. Аванесян [и др.] // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник материалов XX Международной научно-практической конференции., Москва, 17 мая 2023 года. Том Часть 2. – Санкт-Петербург: Печатный цех, 2023. – С. 19-23. – EDN MHRKKY.

4. A survey on large language model based autonomous agents / L. Wang, Ch. Ma, X. Feng [et al.] // Frontiers of Computer Science. – 2024. – Vol. 18, No. 6. – P. 186345. – DOI 10.1007/s11704-024-40231-1. – EDN XTFUTO.

5. Федина, М. Е. Использование автономных интеллектуальных агентов для персонализации образовательных траекторий / М. Е. Федина, В. Ю. Живцов, Е. О. Манякова // Математика и математическое моделирование : материалы III Всероссийской научной конференции, Самара, 20–21 ноября 2025 года. – Самара: Самарама, 2026. – С. 170-174. – EDN ZRKZXK.

6. Шиверов, П. К. Доверие в контексте анализа стойкости протоколов аутентификации / П. К. Шиверов, Т. Г. Новосад, М. Н. Осипов // Ползуновский вестник. – 2014. – № 2. – С. 248-250. – EDN SYNZJZ.

7. Анализ методов эмерджентного искусственного интеллекта / К. В. Портнов, Б. Э. Забержинский, Р. Р. Габбасов, К. А. Агафонов // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник материалов XX Международной научно-практической конференции., Москва, 17 мая 2023 года. Том Часть 2. – Санкт-Петербург: Печатный цех, 2023. – С. 30-36. – EDN GVVLER.

8. Бондаренко, В. В. Применение методов математического и функционального анализа для исследования смарт-контрактов / В. В. Бондаренко, В. Ю. Живцов, Е. О. Манякова // Математика и математическое моделирование : материалы III Всероссийской научной конференции, Самара, 20–21 ноября 2025 года. – Самара: Самарама, 2026. – С. 44-48. – EDN NYMOFM.

9. Артамонов, В. А. Обеспечение доверия при децентрализованном взаимодействии автономных агентов / В. А. Артамонов, В. Ю. Живцов // Кибернетика и информационная безопасность "КИБ-2025" : Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 114-115. – EDN GXSYSR.

10. Харитонов, Е. В. Детектирование уязвимостей на основе графовых нейронных сетей / Е. В. Харитонов, В. Ю. Живцов // Кибернетика и информационная безопасность "КИБ-2025" : Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 72-73. – EDN IJSVEQ.

11. Awasthi, A. Beyond pre-training: the critical role of contextual data in real-world LLM applications / A. Awasthi // International Journal of Information Technology and Management

Information Systems. – 2025. – Vol. 16, No. 2. – P. 1595-1608. – DOI 10.34218/ijitmis_16_02_100. – EDN EIVUWE.

12. Елисеев, Е. Э. Разработка адаптивного алгоритма оценки эффективности систем обнаружения вторжений для предотвращения web-угроз / Е. Э. Елисеев, М. Е. Бурлаков, М. Н. Осипов // Математическое и компьютерное моделирование : Сборник материалов IX Международной научной конференции, посвященной 85-летию профессора В.И. Потапова, Омск, 19 ноября 2021 года. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2021. – С. 285-287. – EDN IQCIIN.

13. Бурлаков, М. Е. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум / М. Е. Бурлаков, М. Н. Осипов. – Самара : Самарский национальный исследовательский университет им. акад. С.П. Королева, 2021. – 96 с. – ISBN 978-5-7883-1659-8. – EDN FJVXUU.

14. Автоматизированный комплекс определения форм и частотных характеристик собственных колебаний / М. Н. Осипов, Н. А. Шарафутдинов, Ю. Д. Щеглов [и др.] // Известия Самарского научного центра Российской академии наук. – 2015. – Т. 17, № 2-5. – С. 1072-1075. – EDN VOCBZL.

15. Новиков, С. Я. Полные системы в задачах восстановления сигнала / С. Я. Новиков, М. Е. Федина // Перспективные информационные технологии (ПИТ 2015) : труды Международной научно-технической конференции, Самара, 28–30 апреля 2015 года / СГАУ. Том 1. – Самара: Самарский научный центр РАН, 2015. – С. 280-284. – EDN TZIJDP.

16. Новиков, С. Я. Полные системы в задачах восстановления сигнала / С. Я. Новиков, М. Е. Федина // Известия Самарского научного центра Российской академии наук. – 2015. – Т. 17, № 2-5. – С. 1069-1071. – EDN VOCBYR.

17. Воропаева, Н. В. Декомпозиция разнотемповых динамических систем со слабой диссипацией / Н. В. Воропаева // Вестник Самарского государственного университета. Естественнонаучная серия. – 2013. – № 9-2(110). – С. 5-10. – EDN RXWIDB.

18. Novikov, S. Y. Boundary spaces for inclusion map between rearrangement invariant spaces / S. Y. Novikov // Collectanea Mathematica. – 1993. – Vol. 44, No. 1-3. – P. 211-216. – EDN XJBRTG.

19. Novikov, S. Y. Singularities of embedding operators between symmetric function spaces on [0, 1] / S. Y. Novikov // Mathematical Notes. – 1997. – Vol. 62, No. 4. – P. 457-468. – DOI 10.1007/bf02358979. – EDN RQJYMB.

20. Новиков, С. Я. Котип и тип функциональных пространств Лоренца / С. Я. Новиков // Математические заметки. – 1982. – Т. 32, № 2. – С. 213-221. – EDN MYFHMD.

21. Степанова, Л. В. О геометрии области полностью поврежденного материала у вершины трещины антиплоского сдвига в связанной постановке задачи (связка "ползучесть - поврежденность") / Л. В. Степанова, М. Е. Федина // Вестник Самарского государственного университета. Естественнонаучная серия. – 2001. – № 2(20). – С. 87-114. – EDN TISNND.

22. Об одной модели динамического управления потоком данных в радиоканале / В. П. Цветов, Г. И. Леонович, С. Я. Новиков [и др.] // Перспективные информационные технологии (ПИТ 2015) : труды Международной научно-технической конференции, Самара, 28–30 апреля 2015 года / СГАУ. Том 1. – Самара: Самарский научный центр РАН, 2015. – С. 299-302. – EDN TZIJFN.

23. Каримов, Б. Ф. Проблемы адаптации генетических алгоритмов к решению задач структурно-параметрической оптимизации / Б. Ф. Каримов, К. В. Портнов // Современные исследования: теория, практика, результаты : Сборник материалов Международной научно-практической конференции, Москва, 29 декабря 2023 года. – Москва: Центр развития образования и науки, ООО "Издательство АЛЕФ", 2023. – С. 443-448. – DOI 10.26118/1590.2023.63.10.010. – EDN PUGPKI.

Сведения об авторах

Олин Роман Александрович, старший преподаватель кафедры прикладной информатики, ФГАОУ ВО «Самарский государственный экономический университет», г. Самара, Россия

Шарипов Рифат Рашатович, к.т.н., доцент кафедры систем информационной безопасности, ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», г. Казань, Россия

Бондаренко Владимир Владимирович, к.ф.-м.н., доцент кафедры безопасности информационных систем, ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева» (Самарский университет), г. Самара, Россия

Information about the authors

Olin Roman Alexandrovich, Senior lecturer of the Department of Applied Informatics, Samara State University of Economics, Samara, Russia

Sharipov Rifat Rashatovich, Candidate of Technical Sciences, Associate Professor at the Department of Information Security Systems, Kazan National Research Technical University, Kazan, Russia

Bondarenko Vladimir Vladimirovich, Candidate of Physical and Mathematical Sciences, Associate Professor at the Department of Information Systems Security, Samara National Research University, Samara,Russia