Оригинальная статья
УДК: 336:004.056
ББК: 32.973-018.2

Математическая модель оценки рисков при совмещении критических бизнес-функций в среде «1С»

Павел Владимирович Ревенков[1], Авдеенко Анна Сергеевна[2]

[1, 2] Финансовый университет при Правительстве Российской Федерации
[1] PVRevenkov@fa.ru, [2] anna.avdeenko2003@gmail.com

Автор, ответственный за переписку: Павел Владимирович Ревенков, PVRevenkov@fa.ru

Аннотация. В статье рассматривается актуальная проблема обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ) в условиях эскалации целенаправленных кибератак. Основное внимание уделяется рискам, возникающим при совмещении критических бизнес-функций пользователями в программной среде «1С». Акцентируется внимание на том, что концентрация полномочий превращает сотрудников в приоритетные цели для социальной инженерии и шантажа, что создает прямую угрозу устойчивости жизненно важных отраслей государства. На базе анализа современных подходов к управлению безопасностью КИИ предложена математическая модель оценки рисков, использующая аппарат теории графов и сценарно-вероятностные методы. В рамках модели вводится интегральный показатель, учитывающий коэффициенты несовместимости функций и потенциальный ущерб от реализации угроз. Представлены результаты анализа матрицы рисков для типовых конфигураций «1С: ERP», доказывающие недопустимость бесконтрольного совмещения административных и операционных ролей. Авторские методы совершенствования защитных механизмов включают внедрение алгоритма динамического взвешивания прав доступа. Данный подход реализует принцип адаптивных разрешений на уровне программного кода, блокируя конфликтные операции в реальном времени на основе статистики действий субъекта. Результаты исследования могут быть использованы руководителями служб безопасности для превентивного предотвращения инцидентов и создания доверенной среды исполнения бизнес-процессов. Интеграция предложенного математического аппарата в архитектуру учетных систем способствует минимизации влияния человеческого фактора на защищенность организации.

Ключевые слова: критическая информационная инфраструктура, оценка рисков, кибербезопасность

Для цитирования: П. В. Ревенков, А. С. Авдеенко Математическая модель оценки рисков при совмещении критических бизнес-функций в среде «1С» // В центре экономики. 2026. № 1. Т. 7. URL: https://vcec.ru/index.php/vcec/article/view/173

Original Paper
JEL Classification:
E59, G21, F65, L86

A mathematical model for assessing risks when combining critical business functions in the environment «1C»

Pavel V. Revenkov[1], Anna Avdeenko Sergeevna[2]

[1, 2] Financial University under the Government of the Russian Federation
[1] PVRevenkov@fa.ru, [2] anna.avdeenko2003@gmail.com

Corresponding author: Pavel V. Revenkov, PVRevenkov@fa.ru

Abstract. This article examines the pressing issue of ensuring information security for critical information infrastructure (CII) facilities in the face of escalating targeted cyberattacks. The focus is on the risks arising when users combine critical business functions in the 1C software environment. It is emphasized that the concentration of authority makes employees prime targets for social engineering and blackmail, posing a direct threat to the stability of vital sectors of the state. Based on an analysis of modern approaches to CII security management, a mathematical risk assessment model is proposed using graph theory and scenario-based probabilistic methods. The model introduces an integral indicator that takes into account the coefficients of incompatibility between functions and the potential damage from the implementation of

threats. The results of a risk matrix analysis for typical 1C: ERP configurations are presented, demonstrating the inadmissibility of uncontrolled combination of administrative and operational roles. The author's methods for improving security mechanisms include the implementation of a dynamic access rights weighting algorithm. This approach implements the principle of adaptive permissions at the program code level, blocking conflicting operations in real time based on subject activity statistics. The results of the study can be used by security managers for proactive incident prevention and the creation of a trusted environment for business process execution. Integration of the proposed mathematical apparatus into the architecture of accounting systems helps minimize the impact of the human factor on organizational security

Keywords: critical information infrastructure, risk assessment, cybersecurity

For citation: P. V. Revenkov, A. S. Avdeenko A mathematical model for assessing risks when combining critical business functions in the environment «1C». *In the Center of Economy*. 2026;1(6). URL: https://vcec.ru/index.php/vcec/article/view/173.

Введение / Introduction

В соответствии с Федеральным законом № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» критическая информационная инфраструктура (КИИ) определяется как совокупность информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей и сопутствующих цифровых компонентов, обеспечивающих бесперебойную работу жизненно важных отраслей государства. Значимость оценки рисков для объектов КИИ непрерывно возрастает на фоне эскалации целенаправленных кибератак. Злоумышленники постоянно ищут уязвимости в архитектуре управления доступом.

Материалы и методы / Materials and Methods

Совмещение критических бизнес-функций одним сотрудником формирует серьезную брешь в защите. Персонал, наделенный расширенными правами в учетных системах, немедленно становится приоритетной целью для социальной инженерии, шантажа и целевого фишинга. Концентрация полномочий превращает учетную запись отдельного пользователя в орудие потенциального разрушения инфраструктуры предприятия. Доктора технических наук С. Д. Ерохин, А. Н. Петухов и П. Л. Пилюгин акцентируют внимание на необходимости комплексного управления безопасностью КИИ с обязательным учетом человеческого фактора и уязвимостей архитектуры [7, с. 45].

Результаты / Results

Современная практика управления крупными промышленными и коммерческими предприятиями неразрывно связана с эксплуатацией высокотехнологичных систем планирования ресурсов. Программные продукты на платформе «1С» занимают доминирующее положение в секторе автоматизации бизнес-процессов, обеспечивая интеграцию учетных, логистических и финансовых контуров организации. Расширение функциональных возможностей систем 1С: ERP и 1С: Комплексная автоматизация порождает специфические угрозы, вызванные концентрацией прав доступа у ограниченного круга лиц.

На рисунке 1 отражена типовая структура взаимодействия элементов КИИ предприятия, где сервер баз данных обменивается информацией с сервером приложений, а тот, в свою очередь, передает данные на рабочие станции конечных пользователей, подвергающихся прямому риску кибератак.

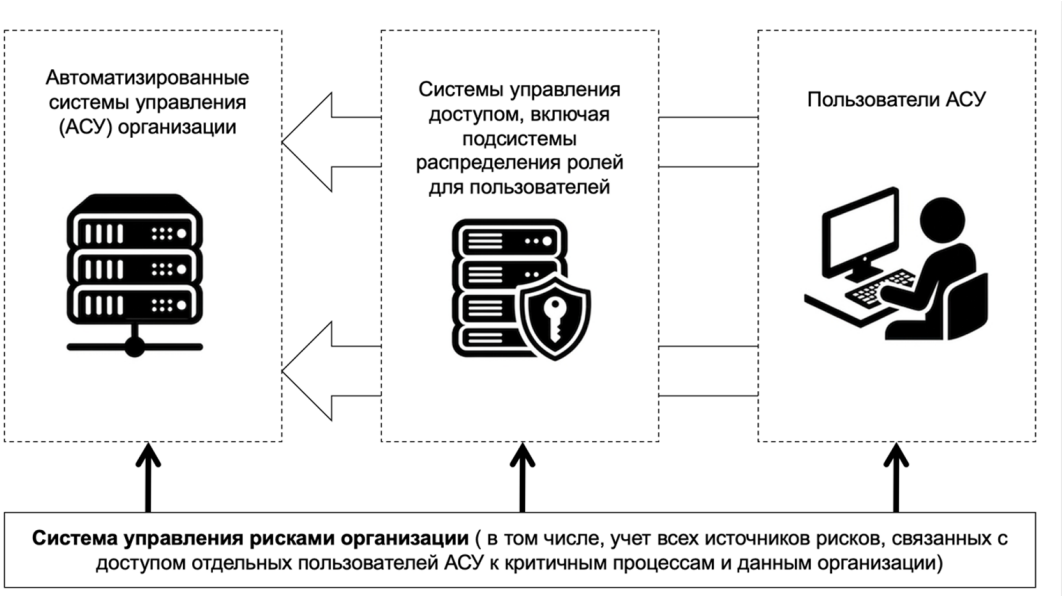

Рис. 1 / Fig. 1. Архитектура взаимодействия элементов КИИ и локализация пользователей / Architecture of interaction between critical information infrastructure elements and user localization

Обсуждение / Discussion

Проблема разделения обязанностей приобретает особую актуальность при цифровой трансформации, когда традиционные методы контроля сменяются автоматизированными алгоритмами мониторинга. Доктор экономических наук Л. Р. Магомаева и кандидат экономических наук Ш. С. Кадыров указывают на наличие существенных различий в архитектуре решений 1С, влияющих на методику реализации бизнес-логики и профиль возникающих рисков [4, с. 284].

Эффективное моделирование бизнес-процессов в среде «1С» требует детального понимания взаимосвязей между различными объектами метаданных, такими как справочники, документы и регистры. Кандидат педагогических наук Н. Л. Ивинская подчеркивает необходимость тщательной проработки структуры информационных потоков на этапе проектирования системы, поскольку ошибки в архитектуре прав доступа неизбежно ведут к несанкционированным операциям [2, с. 60]. Математическое описание подобных систем осложняется высокой динамичностью программной среды и вариативностью пользовательских сценариев. Применение интегрированных сред разработки, таких как 1С: EDT, дает шанс частично автоматизировать проверку корректности настройки бизнес-логики, о чем упоминает исследователь В. В. Сорокина, рассматривая вопросы повышения качества программного кода и снижения вероятности возникновения логических коллизий [6, с. 126].

Кандидат технических наук А. С. Римша предлагает применять сценарно-вероятностные подходы к оценке рисков информационной безопасности при анализе уязвимостей автоматизированных систем управления [8, с. 112]. Адаптация данных подходов к среде «1С» дает возможность строго формализовать процесс выявления конфликтов интересов при назначении ролей.

В рамках построения математической модели оценки рисков целесообразно использовать аппарат теории графов и вероятностный анализ. Пусть G = (V,E) представляет собой ориентированный граф, где множество вершин V соответствует отдельным бизнес-функциям, реализуемым в среде «1С», а ребра E отражают логические связи и последовательность выполнения операций. Каждой вершине v_i $v_i \in V$ V сопоставляется коэффициент критичности Ci, определяемый потенциальным ущербом для организации в случае компрометации функции. Риск совмещения функций i и j выражается через вероятность возникновения конфликта интересов Pij и величину ожидаемых потерь. Кандидат технических наук А. В. Быкасов и исследователь А. Н. Соколов предлагают рассматривать аналогичные задачи через призму активного сканирования уязвимостей, что отлично применимо к анализу конфигураций прав доступа в учетных системах [1, с. 251].

Предложенная модель базируется на вычислении интегрального показателя риска R, который суммирует потенциальные угрозы от всех парных совмещений полномочий. Формула для расчета принимает вид:

$$R=\sum_{i=1}^{n} \sum_{j=i+1}^{n} (Ci * Cj * Kij * Wij)$$

Здесь Kij выступает коэффициентом несовместимости функций, принимающим значение от 0 до 1, а Wij представляет собой весовой множитель, учитывающий специфику конкретной базы данных и наличие компенсирующих контролей. Мурашев рассматривает возможности имитационного моделирования в среде «1С», проводя параллели между распространением эпидемий и передачей ошибочных данных внутри системы, что подтверждает применимость стохастических методов для оценки масштабных сбоев [5, с. 1111].

Особое внимание следует уделить компетенциям персонала. Кандидат педагогических наук Н. Г. Куфтинова отмечает значимость интеграции вопросов информационной безопасности в методику преподавания инструментов «1С» для минимизации угроз, вызванных непреднамеренными действиями сотрудников [3, с. 81]. Процесс обучения и последующей аттестации пользователей становится неразрывным элементом системы защиты, снижая вероятность активации опасных комбинаций прав.

Для наглядного представления зависимости уровня риска от типа совмещаемых функций разработана таблица, отражающая коэффициенты взаимного влияния критических операций.

Таблица 1. / Table 1. Матрица коэффициентов риска совмещения бизнес-функций в «1С» / Matrix of risk coefficients for combining business functions in «1С»

Бизнес-функция	Бизнес-функция	Коэффициент несовместимости (K_ij)	Потенциальный ущерб (баллы)	Рекомендуемый уровень контроля
Ведение справочника контрагентов	Формирование платежных поручений	0,95	92	Двойное подтверждение
Складской учет (приход)	Списание материальных ценностей	0,88	85	Инвентаризационный аудит
Настройка прав доступа	Проведение финансовых документов	0,98	98	Мониторинг в реальном времени
Утверждение заявок на закупку	Акцептование счетов на оплату	0,75	70	Коллегиальное решение
Редактирование цен в заказах	Оформление документов реализации	0,82	78	Блокировка отклонений
Всего НДС	31 117	38 439	52 189	57 885,3

Анализ данных, представленных в таблице, позволяет сделать вывод о критическом характере совмещения административных функций с операционным управлением денежными средствами. Коэффициент несовместимости 0,98 указывает на недопустимость обладания правами на изменение конфигурации и одновременное проведение платежей без жесткого внешнего контроля. Средний уровень риска наблюдается в логистических цепочках, где возможности для злоупотреблений ограничиваются процедурами физического контроля остатков на складах.

Собственные методы совершенствования системы оценки рисков в среде «1С» предполагают внедрение алгоритма динамического взвешивания прав доступа на базе графовых нейронных сетей. Разработанный метод инициирует расчет текущего уровня риска в момент запуска сеанса пользователя, опираясь на непрерывный анализ накопленной статистики предшествующих транзакций. Вместо статического назначения ролей применяется механизм адаптивных разрешений, временно блокирующий возможность совершения второй части конфликтной операции при условии успешной инициации первой тем же субъектом. Подобная реализация принципа «четырех глаз» на уровне исходного кода программной платформы существенно снижает вероятность реализации киберугроз без раздувания штата контролирующих подразделений. Дополнительный мониторинг отклонений в поведении пользователей происходит мгновенно, фиксируя нетипичные запросы к таблицам базы данных.

Дальнейшее развитие предложенной математической модели связывается с применением методов машинного обучения для идентификации аномального поведения пользователей. Программная среда «1С» предоставляет широкие возможности для сбора логов и журналов регистрации, которые служат базой для обучения нейронных сетей. Выявление паттернов, предшествующих совершению рискованных операций, позволит перейти от реактивного исправления последствий к превентивному предотвращению инцидентов. Интеграция математического аппарата оценки рисков непосредственно в ядро конфигурации обеспечит создание доверенной среды исполнения критических бизнес-функций.

Рассматривая архитектурные особенности 1С: ERP, необходимо отметить важность использования механизма «Области данных» для разделения полномочий в распределенных информационных системах. Доктор экономических наук Л. Р. Магомаева и кандидат экономических наук Ш. С. Кадыров справедливо подчеркивают прямую зависимость сложности управления доступом от масштабности системы [4, с. 287]. Введение дополнительных измерений в математическую модель, учитывающих территориальную распределенность и специфику филиальной сети, даст шанс точнее прогнозировать возможные финансовые потери. Применение инструментов 1С: EDT, описанных исследователем В. В. Сорокиной, помогает внедрять автоматизированные тесты на проверку соблюдения правил разделения обязанностей на раннем этапе разработки новых функциональных блоков [6, с. 130].

Таким образом, математическая модель оценки рисков при совмещении критических бизнес-функций выступает действенным инструментом поддержки принятия решений для руководителей служб безопасности и ИТ-директоров. Систематический анализ коэффициентов несовместимости и внедрение адаптивных механизмов контроля способствуют повышению устойчивости бизнеса к внутренним угрозам и внешним атакам на КИИ. Комплексный подход, сочетающий математическое моделирование, современные программные инструменты и методическую подготовку персонала, формирует надежную основу для безопасного функционирования информационных систем на платформе «1С» в условиях высокой неопределенности внешней среды.

Список источников

1. Быкасов, А. В. Математическая модель оценки рисков информационной безопасности сети АСУ ТП при использовании методов активного сканирования / А. В. Быкасов, А. Н. Соколов // Безопасность информационного пространства - 2024 : Сборник материалов XXIII всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, Курган, 04 декабря 2024 года. – Курган: Курганский государственный университет, 2025. – С. 251-258.

2. Ивинская, Н. Л. Моделирование бизнес-процессов организации в среде 1С:предприятие при подготовке выпускной квалификационной работы / Н. Л. Ивинская // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : сборник научных трудов. – Челябинск : Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, 2025. – С. 60-67.

3. Куфтинова, Н. Г. Методика преподавания инструментов среды «1С» для решения практических бизнес-задач в выпускной работе студентов / Н. Г. Куфтинова // Преподавание информационных технологий в Российской Федерации : сборник научных трудов Двадцать третьей открытой Всероссийской конференции, Омск, 15–16 мая 2025 года. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2025. – С. 81-84.

4. Магомаева, Л. Р. Автоматизация бизнес-процессов на крупных предприятиях: сравнительный анализ 1С:ERP и 1С:КА / Л. Р. Магомаева, Ш. С. Кадыров // Механизм реализации стратегии социально-экономического развития государства : Сборник материалов XV Международной научно-практической конференции, Дагестанский государственный технический университет, 20–21 сентября 2023 года. – Махачкала: Дагестанский государственный технический университет, 2023. – С. 284-288.

5. Мурашев, Д. Е. Разработка математической модели эпидемии в программной среде 1С / Д. Е. Мурашев

// Мечниковские чтения-2024 : Материалы 97-й Всероссийской научно-практической конференции студенческого научного общества с международным участием, Санкт-Петербург, 24–26 апреля 2024 года. – Санкт-Петербург: Северо-Западный государственный медицинский университет им. И.И. Мечникова, 2024. – С. 1111-1112.

6. Сорокина, В. В. Применение интегрированной среды разработки 1С:EDT для автоматизации бизнес-процессов / В. В. Сорокина // Современные научные исследования: исторический опыт и инновации : Сборник материалов XX Международной (политематической) научно-практической конференции, Краснодар, 08–09 февраля 2024 года. – Краснодар: Академия маркетинга и социально-информационных технологий - ИМСИТ (г. Краснодар), 2024. – С. 126-131.

7. Ерохин С. Д., Петухов А. Н., Пилюгин П. Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2024. – 240 с.:ил.

8. Римша, А. С. Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур : специальность 23.60.00 : диссертация на соискание ученой степени кандидата технических наук / Римша Андрей Сергеевич, 2022. – 234 с.

Reference

1. Bykasov, A. V. Mathematical model for assessing the information security risks of an automated process control system network using active scanning methods / A. V. Bykasov, A. N. Sokolov // Information space security - 2024: Collection of materials from the XXIII All-Russian scientific and practical conference of students, graduate students and young scientists, Kurgan, December 4, 2024. - Kurgan: Kurgan State University, 2025. - Pp. 251-258.

2. Ivinskaya, N. L. Modeling of an organization's business processes in the 1C: enterprise environment in preparing a final qualifying work / N. L. Ivinskaya // Innovative technologies in the training of modern professional personnel: experience, problems: collection of scientific papers. - Chelyabinsk: Russian Presidential Academy of National Economy and Public Administration, 2025. - Pp. 60-67.

3. Kuftinova, N. G. Methodology of Teaching the Tools of the 1C Environment for Solving Practical Business Problems in Students' Graduation Work / N. G. Kuftinova // Teaching Information Technology in the Russian Federation: Collection of Scientific Papers of the Twenty-Third Open All-Russian Conference, Omsk, May 15-16, 2025. - Omsk: F.M. Dostoevsky Omsk State University, 2025. - Pp. 81-84.

4. Magomaeva, L. R. Automation of Business Processes in Large Enterprises: A Comparative Analysis of 1C:ERP and 1C:KA / L. R. Magomaeva, Sh. S. Kadyrov // Mechanism for Implementing the Strategy of Socio-Economic Development of the State: Collection of Materials of the XV International Scientific and Practical Conference, Dagestan State Technical University, September 20-21, 2023. – Makhachkala: Dagestan State Technical University, 2023. – Pp. 284-288.

5. Murashev, D. E. Development of a mathematical model of an epidemic in the 1C software environment / D. E. Murashev // Mechnikov Readings-2024: Proceedings of the 97th All-Russian Scientific and Practical Conference of the Student Scientific Society with International Participation, St. Petersburg, April 24–26, 2024. – St. Petersburg: North-Western State Medical University named after I.I. Mechnikov, 2024. – Pp. 1111-1112.

6. Sorokina, V. V. Application of the 1C:EDT integrated development environment for business process automation / V. V. Sorokina // Modern scientific research: historical experience and innovation: Collection of materials of the XX International (polythematic) scientific and practical conference, Krasnodar, February 8–9, 2024. – Krasnodar: Academy of Marketing and Social and Information Technologies - IMSIT (Krasnodar), 2024. – Pp. 126–131.

7. Erokhin S. D., Petukhov A. N., Pilyugin P. L. Security management of critical information infrastructures. – Moscow: Goryachaya Liniya – Telecom, 2024. – 240 p.: ill.

8. Rimsha, A. S. Method and algorithms for managing information security risks of automated process control systems of critical infrastructures: specialty 23.60.00: dissertation for the degree of candidate of technical sciences / Rimsha Andrey Sergeevich, 2022. - 234 p.

Информация об авторах

П. В. Ревенков – доктор экономических наук, профессор кафедры информационной безопасности,
Финансовый университет при Правительстве Российской Федерации
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия
E-mail: PVRevenkov@fa.ru
https://orcid.org/0000-0002-0354-0665

А. С. Авдеенко – студент 1-го года обучения магистратуры направления
«Управление информационной безопасностью»,
Финансовый университет при Правительстве Российской Федерации
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия
E-mail: anna.avdeenko2003@gmail.com
https://orcid.org/0009-0007-3391-2208

Information about the authors

P. V. Revenkov – Doctor of Economics, Professor of the Information Security Department,
Financial University under the Government of the Russian Federation,
Address: 4th Veshnyakovsky Proezd, 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: PVRevenkov@fa.ru
https://orcid.org/0000-0002-0354-0665

A. S. Avdeenko – First-year Master's student in Information Security Management,
Financial University under the Government of the Russian Federation,
Address: 4th Veshnyakovsky Proezd, 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: anna.avdeenko2003@gmail.com
https://orcid.org/0009-0007-3391-2208

Вклад авторов

Ревенков П. В. – научное руководство; концепция исследования; развитие методологии; написание и доработка текста; итоговые выводы.

Авдеенко А. С. – участие в написании исходного текста, оформление статьи.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors

Revenkov P. V. – scientific guidance; research concept; development of methodology; writing and revision of the text; final conclusions.

Avdeenko A. S. – participation in the writing of the source text; design of the article.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Статья поступила в редакцию: 10.02.2026;
одобрена после рецензирования: 21.02.2026;
принята к публикации: 24.03.2026.

The article was submitted: 10.02.2026;
approved after reviewing: 21.02.2026;
accepted for publication: 24.03.2026.