

Научная статья

<https://doi.org/10.24412/2220-2404-2026-10-19>

УДК 657.6



Attribution

cc by

**ВНУТРЕННИЙ АУДИТ КИБЕРРИСКОВ В СИСТЕМЕ БУХГАЛТЕРСКОГО УЧЕТА
ОРГАНИЗАЦИИ: МЕТОДИЧЕСКИЙ АСПЕКТ**

Щербакова Е.П.

Ростовский государственный экономический университет (РИНХ)

Аннотация. В статье обоснована возрастающая роль внутреннего аудита киберрисков в системе бухгалтерского учета современных организаций в условиях постоянного усложнения угроз информационной безопасности. Раскрыта специфика реализации киберугроз на различных уровнях ИТ-инфраструктуры предприятия. Проведен сравнительный анализ международных методологий управления рисками, в результате которого выявлено отсутствие их интеграции с операционной деятельностью. На примерах реальных масштабных кибератак на крупные российские компании наглядно продемонстрированы критические последствия утечек, данных и простоя учетных систем. Автором предложена пошаговая методика, которая описывает этапы сбора данных, количественного анализа и ранжирования угроз. Практическое внедрение данного подхода позволяет сформировать экономически обоснованную стратегию защиты конфиденциальной информации, трансформируя разрозненные контрольные процедуры в системный управляемый процесс.

Ключевые слова: внутренний аудит, киберриски, информационная безопасность, бухгалтерский учет, оценка рисков, ИТ-инфраструктура, карта рисков, конфиденциальность данных

Финансирование: инициативная работа.

Original article

**INTERNAL AUDIT OF CYBER RISKS IN THE ORGANIZATION'S ACCOUNTING SYSTEM:
METHODOLOGICAL ASPECT**

Ekaterina P. Shcherbakova

Rostov State University of Economics (RINH)

Abstract. The article substantiates the increasing role of internal audit of cyber risks within the accounting system of modern organizations amidst the continuous complication of the information security threat landscape. The study reveals the specifics of cyber threat execution at various levels of enterprise IT infrastructure. A comparative analysis of international risk management methodologies was conducted, exposing their lack of integration with operational activities. Using real-world examples of large-scale cyberattacks on major Russian companies, the critical consequences of data breaches and accounting system downtime are clearly demonstrated. The author proposes a step-by-step methodology, which outlines the stages of data collection, quantitative analysis, and threat ranking. The practical implementation of this approach enables the formation of an economically justified strategy for protecting confidential information, transforming fragmented control procedures into a systematic, manageable process.

Keywords: Internal audit, cyber risks, information security, accounting, risk assessment, IT infrastructure, risk map, data confidentiality

Funding: Independent work.

Введение.

В современной экономической среде предприятия обязаны предоставлять достоверную информацию о своих активах, обязательствах и финансовых результатах как внутренним, так и внешним пользователям. Основным источником таких данных является финансовая отчетность. Защита информационных ресурсов направлена на предотвращение утечки коммерческой тайны, снижение финансовых потерь и увеличение прибыли. Данные из бухгалтерских регистров и корпоративной системы документооборота критически важны для обоснования управленческих решений.

Обсуждение. Результаты.

С ростом внутренних и внешних рисков, связанных с кибербезопасностью, необходимо совершенствовать внутренний аудит как инструмент защиты информации. Эта стратегия основывается на независимой экспертизе защищенности от кибератак и предложениях по устранению уязвимостей в безопасности с последующим контролем их реализации.

Аудит информационной безопасности в организации представляет собой комплекс мероприятий по анализу данных для проверки соответствия корпоративных систем критериям защиты информационных ресурсов и инфраструктуры, обеспечивая конфиденциальность, целостность и доступность данных согласно нормативам. В таблице 1 перечислены способы реализации киберугроз, требующие внимания аудиторов.

Таблица 1 – Перечень способов реализации угроз кибербезопасности.

Уровень кибербезопасности	Способы реализации угроз
Физический уровень	• Утечка информации: кража конфиденциальных носителей • Разрушение / диверсии: уничтожение инфраструктуры • Несанкционированный доступ: физическое проникновение на объект • Хищение / кража: кража оборудования или материальных ценностей
Сетевой уровень	• Атаки DoS / DDoS: отказ в обслуживании • Аппаратные угрозы: внедрение вредоносных модулей • Спуфинг / подмена: подмена доверенного объекта, перехват каналов, отправка сообщений с присвоением прав • Нарушение режимов: сбой и вывод из строя сетевого оборудования
Уровень сетевых приложений и сервисов	• Анализ трафика: перехват и сканирование пакетов данных • Вредоносное ПО: использование спецпрограмм • Сбой приложений: нарушение штатных режимов работы веб-сервисов • Разведка сети: сканирование открытых портов, поиск уязвимых служб и соединений
Уровень операционных систем и СУБД	• Компрометация данных: копирование, модификация, удаление, кража/потеря паролей • Ошибки конфигурации: неправильная или неполная настройка систем защиты • Несанкционированный доступ: логический доступ к ОС и СУБД через спецсофт • Идентификация: подмена ID пользователей, распространение вирусов
Уровень бизнес-процессов	• Саботаж: умышленное деструктивное воздействие сотрудников • Человеческий фактор: халатность, внутренние ошибки, вредительство

Согласно определению стандарта ГОСТ Р ИСО/МЭК 27001-2021 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 30.11.2010 №632-ст), риски информационной безопасности представляют собой потенциальные вероятности, при которых уязвимости определенного актива

или группы активов могут быть использованы конкретной угрозой для нанесения ущерба организации [1].

В сфере информационной безопасности, включая бухгалтерию, выделяют три типа угроз: непреднамеренные, связанные с человеческим фактором, и техногенные (рисунок 1).

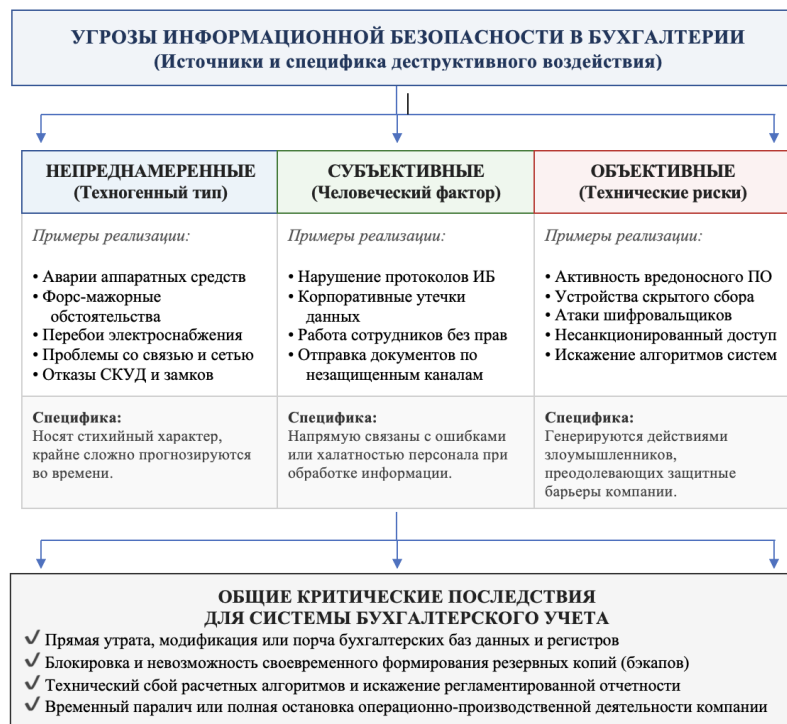


Рисунок 1 – Иерархическая структура и классификация угроз информационной безопасности в системе бухгалтерского учета.

При проектировании систем информационной безопасности (СИБ) критически важен этап обнаружения, изучения и оценки потенциальных рисков, которые могут подорвать безопасность организации. Эффективность работы внедренной системы защиты информации напрямую зависит от точности анализа угроз.

Без формализованной оценки рисков внутренних аудит не может:

- определить приоритетные области проверки;
- обосновать ресурсы на меры защиты;
- доказать руководству, какие угрозы наиболее критичны для бухгалтерской отчетности.

Именно поэтому в рамках реализации функции внутреннего аудита были проанализированы наиболее популярные в настоящее время методики управления рисками информационной безопасности.

Метод CRAMM, разработанный Insight Consulting Limited, и его программное обеспечение уже более тридцати лет помогают выявлять уязвимости и оценивать риски в информационных системах, и этот подход признан во всем мире. Однако у него есть слабое место: он не связывает выявленные активы, которые нужно защищать, с бизнес-процессами компании. Это ограничение обсуждается в научной работе, где отмечается недостаточное внимание к деловым операциям и документации [2].

Методология FRAP от Peltier and Associates тоже не безупречна. Она основывается на анкетировании, изучении технической документации и автоматизированном анализе сетевых топологий, чтобы определить ключевые объекты инфраструктуры. Но и здесь отсутствует связь между защищаемыми активами и бизнес-процессами организации [3].

CORAS предлагает моделирование рисков и распространяется бесплатно вместе с программным комплексом. Однако у него нет механизма для регулярного пересмотра и обновления оценок рисков, а также средств для расчета рентабельности инвестиций

в защиту. Как и другие методы, он не анализирует внутренние бизнес-процессы для выявления приоритетных активов [4].

Инструмент MSAT от компании Microsoft создан специально для того, чтобы оценивать риски в сфере информационной безопасности. С одной стороны, эта программа реально помогает понять, насколько выгодно и эффективно компания вкладывает деньги в защиту своих данных, а, с другой стороны, у нее есть весомый минус – она вообще не учитывает внутренние бизнес-процессы компании. Из-за этого с ее помощью не получится разобраться, какие именно важные активы и данные нужно защищать в самую первую очередь [5].

В целом анализ существующей практики применения различных методик, применяемого компаниями специализированного программного обеспечения, а также научной литературы по теме работы с киберрисками, позволяет сделать вывод о том, что у ученых и экспертов на сегодня до сих пор нет единого мнения о том, как правильно оценивать риски инфобезопасности. На практике, когда крупные компании создают свои системы защиты, специалисты чаще всего опираются не на теорию, а на личный опыт борьбы с хакерами и угрозами. Исследования показывают, что все понимают слово «риск» по-своему, и методы для его поиска и идентификации у всех абсолютно разные.

Чтобы детально разобраться, как именно искажается информация, эксперты-практики разработали классификацию опасных факторов конкретно для бухгалтерского учета. Такая готовая типология помогает четко увидеть, в каких именно местах и процессах риски максимальны, и когда мы знаем эти слабые зоны уже можно идентифицировать, становится гораздо проще создать надежные инструменты, чтобы эти риски снизить или же вовсе предотвратить.

Рассмотрим пример методологии оценки рисков информационной безопасности в бухгалтерии, предложенной Сафоновым А., техническим директором ООО «ПКИ». Этот подход включает несколько последовательных этапов (рисунок 2).

▼	ЭТАП 1	Сбор информации: Сбор исходных данных перед непосредственной оценкой рисков.
▼	ЭТАП 2	Анализ системы бухгалтерского учета (СБУ): Изучение системы работы предприятия и роли бухгалтерского учета.
▼	ЭТАП 3	Активы и риски: Анализ защищаемых активов и потенциальных рисков в СБУ.
▼	ЭТАП 4	Финансовый аудит: Изучение финансовых показателей компании, сравнение с уровнем ущерба.
▼	ЭТАП 5	Список угроз: Сопоставление рисков с негативными сценариями, актуализация угроз.
▼	ЭТАП 6	Количественная оценка: Оценка вероятности событий и ущерба, расчет числовых характеристик.
▼	ЭТАП 7	Разработка методологии: Комплексная оценка на основе фактов и прогнозов работы организации.
ФИНАЛ (Контроль и внедрение мер): Детальное ранжирование угроз по критичности для управленческих решений. Проверка результативности мер и оценка остаточного риска. Расчет расходов на реализацию, их соответствие прогнозируемому снижению рисков и доступности фондов. При неблагоприятном балансе затрат и эффекта — оперативная разработка альтернативных подходов к минимизации рисков.		

Рисунок 2 – Основные этапы информационной оценки рисков безопасности в ООО «ПКИ».

В процессе учета на каждом этапе возможно появление неполной или искаженной информации. Это обстоятельство заставляет тщательно анализировать каждый шаг при оценке угроз информационной безопасности. Однако ошибки и пробелы, допущенные в начале учетного цикла, обязательно скажутся на точности данных, собранных позже. Вот почему так важно в первую очередь предотвращать подобные недостатки и своевременно их исправлять [6].

Не стоит упускать из виду и другой факт, что у современной компании имеется множество информационных активов, каждый из которых нуждается в надежной защите. Эффективность систем информационной безопасности зависит от тщательной проработки задач по защите данных и точного определения критически важных информационных активов, подвергающихся угрозам. Устранение существующих пробелов осуществляется с помощью методики «Оценка рисков информационной безопасности для организаций», используемой внутренним аудитом как практический инструмент. Этот анализ позволяет оценить влияние информационных ресурсов на бизнес-процессы компании. Метод помогает определить ценность информационных активов для операционной деятельности и выделить приоритетные объекты для стратегий защиты информации.

Необходимость проработки и применения данной методики подтверждается реальными инцидентами в российских компаниях. В марте 2022 года агрохолдинг «Мираторг» столкнулся с атакой программы-шифровальщика Bitlocker, в результате которой пострадали 18 компаний холдинга. Злоумышленники получили доступ к бухгалтерским информационным ресурсам, что привело к параличу операционной деятельности и остановке отгрузки продукции [7]. В июле 2025 года группа Novabev (сеть «ВинЛаб») подверглась кибератаке, вызвавшей утечку базы данных 9 миллионов клиентов и полный сбой работы розничных точек. Ежедневные потери от простоя составили более 100 млн. рублей, а потенциальные штрафы за утечку персональных данных достигли 860 млн. рублей [8].

При атаке злоумышленника защищаемая инфраструктура рискует потерей различных ресурсов. Критичность воздействия на активы для деловых операций предприятия зависит от интенсивности их использования при работе с секретными данными. Выделяются следующие уровни влияния: высокое влияние (ВВ), среднее влияние (СВ) и низкое влияние (НВ) (рисунк 3).



Рисунок 3 – Уровни влияния рисков безопасности конфиденциальной информации.

На основе собранных данных можно создать матрицу рисков, которая наглядно показывает приоритеты угроз в зависимости от их критичности. Этот инструмент помогает определить, какие потенциальные опасности можно игнорировать без ущерба для деятельности организации. Обновленная карта рисков подтверждает, что все угрозы были выявлены, проанализированы и нейтрализованы. Этот документ может быть представлен контролирующим органам, кредитным учреждениям, рейтинговым агентствам и акционерам как доказательство наличия в компании эффективной системы информационной безопасности. Внутренний аудит использует карту рисков для визуализации

при взаимодействии с руководством и советом директоров. Для ее создания применяются реестр, содержащий полный список бизнес-рисков, и шаблон для фиксации выявленных угроз.

В целом методика «Оценка рисков информационной безопасности для организаций» подходит для двух типов систем: полностью автоматизированных информационных комплексов и тех, где информация обрабатывается вручную без автоматизации. Тем не менее, приоритет стоит отдавать специализированным программам для анализа рисков. При наличии достаточного времени и финансирования они дают возможность управлять рисками оперативно, в режиме реаль-

ного времени. В этом их ключевое отличие от описанного выше метода. Последний можно проводить как разовое мероприятие или же повторять периодически.

Данный метод анализа рисков решает не одну, а несколько задач. Он помогает устранять уязвимости и снижать вероятность угроз информационной безопасности – касающихся как бухгалтерской информации, так и корпоративных данных в целом. Помимо этого, метод повышает уровень знаний сотрудников о том, как правильно защищать информацию.

Заключение.

Таким образом, по результатам проведенного исследования можно сделать вывод о том, что современное киберпространство постоянно меняется, из-за чего растут риски и появляются новые угрозы для компаний. Поэтому бизнесу нужно защищать свою ин-

формацию как от внешних хакеров, так и от внутренних проблем. При этом внутренний аудит не должен выполнять работу IT-специалистов, его задачей являются регулярные и независимые проверки того, как в компании находят, оценивают и снижают цифровые риски, а особенно как это налажено в бухгалтерии.

В условиях постоянных угроз именно внутренний аудит объединяет отдельные защитные меры в понятную для руководства систему.

Предложенная методика оценки рисков может способствовать четкому и точному обнаружению и фиксации угрозы для бухгалтерских данных, когда пользователей много и обрабатывается большой объем учетной информации. На практике же такой подход помогает компании самой понять, какие активы нужно защищать в первую очередь, а также вовремя усилить их безопасность.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (Переиздание). [Электронный ресурс]. - Режим доступа: <https://docs.cntd.ru/document/1200181890>.
2. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. 2015. № 1. С. 73-79. EDN: TNDTUP
3. Сухаревская Е.В., Михальченко С.В., Шамин И.М., Никитинова А.В. Анализ методов оценки рисков при применении ERP-систем [Электрон. ресурс] // Современные научные исследования и инновации. 2016. № 9. Режим доступа: <http://web.snauka.ru/issues/2016/09/72016>. EDN: WVNIOL
4. Файзулаев Д. Ф., Морозов Б. Б. Методы и средства анализа рисков информационной безопасности предприятия // Безопасность информационных технологий. 2017. Т. 24. № 3. С. 72-77. EDN: ZEMPKN
5. Абрамов А.С., Писарев В.Д., Шилов А.К. Применение методологии MSAT для оценки защищенности предприятия // Аллея науки. 2017. Т. 3. № 13. С. 961-965. EDN: ZMIOHN
6. Лазичный, И. А. Анализ рисков информационной безопасности / И. А. Лазичный // Обществознание и социальная психология. - 2023. - № 10-3(53). - С. 13-18. EDN: WCRKEE
7. Хакеры заблокировали данные огромного российского агрохолдинга [Электронный ресурс]. - Режим доступа: <https://tass.ru/ekonomika/14113029>.
8. Novabev Group сообщила о кибератаке на "Винлаб" с требованием выкупа [Электронный ресурс]. - Режим доступа: <https://www.rbc.ru/rbcfreenews/6877c05c9a79472e3f1a8d68>.

References:

1. GOST R ISO/IEC 27001-2021 Information technology (IT). Methods and means of ensuring security. Information security management systems. Requirements (Reissue). [electronic resource]. - Access mode: <https://docs.cntd.ru/document/1200181890>
2. Baranova E.K. Methods of information security risk analysis and assessment // Bulletin of the S.Y. Witte Moscow University. 2015. No. 1. pp. 73-79. EDN: TNDTUP
3. Sukharevskaya E.V., Mikhailchenko S.V., Shamin I.M., Nikishova A.V. Analysis of risk assessment methods in the application of ERP systems [Electron. resource] // Modern scientific research and innovation. 2016. № 9. Access mode: <http://web.snauka.ru/issues/2016/09/72016>. EDN: WVNIOL
4. Fayzulaev D. F., Morozov B. B. Methods and tools of enterprise information security risk analysis // Information technology security. 2017. Vol. 24. No. 3. pp. 72-77. EDN: ZEMPKN
5. Abramov A.S., Pisarev V.D., Shilov A.K. Application of the MSAT methodology to assess the security of an enterprise. Alley of Science. 2017. Vol. 3. No. 13. pp. 961-965. EDN: ZMIOHN
6. Lazichny, I. A. Information security risk analysis / I. A. Lazichny // Social studies and social psychology. - 2023. - № 10-3(53). - Pp. 13-18. EDN: WCRKEE
7. Hackers blocked the data of a huge Russian agricultural holding [Electronic resource]. - Access mode: <https://tass.ru/ekonomika/14113029>.
8. Novabev Group reported a cyberattack on Vinlab demanding a ransom [Electronic resource]. - Access mode: <https://www.rbc.ru/rbcfreenews/6877c05c9a79472e3f1a8d68>.

Информация об авторе:

Щербакова Екатерина Павловна, кандидат экономических наук, доцент, доцент кафедры бухгалтерского учета, ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)», ID ORCID: 0000-0002-1871-9027, E-mail: nauka.509@bk.ru

Ekaterina P. Shcherbakova, PhD in Economics, Associate Professor, Associate Professor of Accounting, Rostov State University of Economics (RINH)

Статья поступила в редакцию / The article was submitted 02.10.2026;

Одобрена после рецензирования / Approved after reviewing 19.10.2026;

Принята к публикации / Accepted for publication 20.10.2026.

Автором окончательный вариант рукописи одобрен.