УДК 519.876.5
DOI 10.17513/snt.40271

КАЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ С ИСПОЛЬЗОВАНИЕМ ЭКСПЕРТНЫХ ОЦЕНОК И ИНТУИТИВНОГО АНАЛИЗА КАК КЛЮЧЕВЫХ ИНСТРУМЕНТОВ УПРАВЛЕНИЯ УГРОЗАМИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Плохута К.Д.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина), Санкт-Петербург, e-mail: klimpl@mail.ru

Целью исследования данной статьи является всестороннее рассмотрение специализированных методик оценки информационных рисков, базирующихся на экспертном анализе и профессиональном опыте специалистов по безопасности, для создания комплексной системы противодействия цифровым угрозам и защиты конфиденциальных данных организации. Современная информационная безопасность требует комплексного подхода к управлению рисками, включающего тщательную оценку и эффективное снижение киберугроз. Стремительная цифровизация бизнес-процессов выдвигает на первый план задачи в области защиты корпоративных данных и информационных систем. Грамотная оценка потенциальных угроз, среди которых особую опасность представляют программы-вымогатели, методы социальной инженерии и распределенные атаки, позволяет существенно снизить вероятность финансовых потерь и сохранить репутацию компании в глазах клиентов. В данной статье автором предпринята попытка анализа применения методов качественной оценки рисков с использованием экспертных оценок и интуитивного анализа для эффективного управления угрозами в информационной безопасности. Применение современных методов научного познания позволило изучить сложившиеся подходы, взгляды на предмет исследования, выработать авторскую позицию и аргументировать ее. Систематизация рисков с применением экспертного анализа, рейтинговых методик и сравнительного подхода способствует принятию обоснованных решений в сфере информационной безопасности. Немаловажную роль в разработке эффективных стратегий играет интуитивный анализ специалистов, дополняющий формализованные методы оценки. Обучение сотрудников компании принципам информационной безопасности является неотъемлемой частью комплексного управления рисками. Беспрерывные тренинги и симуляции реальных атак способствуют формированию у персонала навыков, необходимых для идентификации и эффективного сопротивления кибератакам. Проведенное исследование позволило прийти к выводу о том, что защита цифровых активов и управление рисками становятся неотъемлемыми компонентами успешной стратегии информационной безопасности. В условиях стремительного развития технологий и возрастающей сложности информационных систем интеграция методов качественной оценки рисков позволяет организациям более адекватно реагировать на непредвиденные угрозы и своевременно адаптироваться к изменяющимся условиям. От понимания и тщательного анализа потенциальных рисков зависит не только текущая безопасность бизнеса, но и его устойчивость в долгосрочной перспективе.

Ключевые слова: информационная безопасность, управление рисками, киберугрозы, устойчивость бизнеса, DDoS-атаки, качественная оценка рисков, интуитивный анализ, экспертные оценки, минимизация угроз, цифровая экономика, защита данных, конкурентоспособность

QUALITATIVE RISK ASSESSMENT USING EXPERT ASSESSMENTS AND INTUITIVE ANALYSIS AS KEY INFORMATION SECURITY THREAT MANAGEMENT TOOLS

Plokhuta K.D.

St. Petersburg State Electrotechnical University "LETI" named after V. I. Ulyanov (Lenin), St. Petersburg, e-mail: klimpl@mail.ru

The purpose of the research of this article is a comprehensive review of specialized information risk assessment techniques based on expert analysis and professional experience of security specialists to create a comprehensive system to counter digital threats and protect confidential data of the organization. Modern information security requires a comprehensive approach to risk management, including careful assessment and effective reduction of cyber threats. The rapid digitalization of business processes highlights the challenges of protecting corporate data and information systems. A competent assessment of potential threats, among which ransomware, social engineering methods and distributed attacks are particularly dangerous, can significantly reduce the likelihood of financial losses and preserve the company's reputation in the eyes of customers. In this article, the author attempts to analyze the application of methods of qualitative risk assessment using expert assessments and intuitive analysis for effective threat management in information security. The use of modern methods of scientific cognition allowed us to study the established approaches, views on the subject of research, develop an author's position and argue it. The systematization of risks using expert analysis, rating techniques and a comparative approach contributes to making informed decisions in the field of information security. An important role in the development of effective strategies is played by the intuitive analysis of specialists, which complements the formalized assessment methods. Training of the company's employees in the principles of information security is an integral part of comprehensive risk management. Continuous trainings and simulations of real attacks contribute to the formation of staff skills necessary for identification and effective resistance to cyber attacks. The conducted research led to the conclusion that the protection of digital assets and risk management are becoming integral components of a successful information security strategy. In the context of the rapid development of technologies and the increasing complexity of information systems, the integration of qualitative risk assessment methods allows organizations to respond more adequately to unforeseen threats and adapt to changing conditions in a timely manner. Understanding and careful analysis of potential risks depends not only on the current security of the business, but also on its sustainability in the long term.

Keywords: information security, risk management, cyber threats, phishing attacks, DDoS attacks, qualitative risk assessment, intuitive analysis, expert assessments, threat minimization, digital economy, data protection, business sustainability, competitiveness

Введение

Информационная безопасность – это совокупность мер и методов, направленных на защиту данных, информационных систем и их пользователей от различных угроз. В условиях быстрого роста информационных технологий, а также перехода многих компаний на цифровую основу ведения бизнеса значительно возросли риски, связанные с информационными атаками. Если не управлять потенциальными рисками, то это может привести к потере данных, финансовым убыткам, подрыву доверия клиентов и партнёров, а также к юридическим последствиям.

Управление рисками заключается в выявлении, оценке и контроле различных угроз и уязвимостей, которые могут привести к потере данных или к нарушению работы систем. Этот процесс включает несколько этапов: идентификацию возможных угроз, их оценку с точки зрения вероятности и потенциального ущерба, разработку стратегий по минимизации риска и мониторинг эффективности принимаемых мер. Комплексный подход к управлению рисками требует систематического анализа потенциальных угроз информационной безопасности предприятия.

Организации разрабатывают многоступенчатую методологию защиты, включающую выявление уязвимостей, расчет возможного экономического ущерба, создание превентивных мер безопасности. Грамотное внедрение риск-менеджмента позволяет компаниям существенно снизить вероятность реализации деструктивных сценариев и укрепить общую устойчивость бизнес-процессов к внешним воздействиям.

Цель исследования – всестороннее рассмотрение специализированных методик оценки информационных рисков, базирующихся на экспертном анализе и профессиональном опыте специалистов по безопасности, для создания комплексной системы противодействия цифровым угрозам и защиты конфиденциальных данных организации.

Материалы и методы исследования

Исследования рисков информационной безопасности комплексно базируются на сочетании анализа, профессиональной экспертизы и систематического изучения примеров, взятых из реальной практики.

Базу источников формируют публикации, находящиеся в открытом доступе, и открытые источники, взятые со специализируемых форумов, где представлена информация по отраслевой аналитике, а также материалы реализованных проектов по защите информации, дополненные подробными интервью с ведущими специалистами по кибербезопасности.

Результаты исследования и их обсуждение

Современные организации сталкиваются с растущей необходимостью обеспечения надежной защиты информационных ресурсов от многочисленных сетевых угроз. Масштабная трансформация корпоративных процессов в электронный формат значительно расширила поверхность потенциальных атак злоумышленников. Недостаточное внимание к вопросам управления информационными рисками приводит к масштабным последствиям, включая раскрытие закрытых данных, финансовые убытки, снижение доверия заказчиков и возникновение юридических сложностей.

Грамотное планирование и реализация всесторонних мер информационной защиты становится ключевым фактором сохранения устойчивости бизнеса и предотвращения негативных последствий кибернетических атак в длительной перспективе.

Комплексное управление рисками требует систематического подхода к обнаружению и минимизации потенциальных угроз безопасности информационной инфраструктуры компании. Методология риск-менеджмента предполагает последовательную реализацию взаимосвязанных этапов, начиная с идентификации источников опасности, определения вероятности их возникновения и масштабов возможного ущерба, заканчивая формированием защитных механизмов и регулярной оценкой их результативности. Грамотное применение инструментов риск-менеджмента позволяет организациям выстроить надежную систему защиты от негативных факторов внутренней и внешней среды, минимизируя риски нарушения штатного режима функционирования.

Сложность в интеграции современных информационных комплексов значительно повышает актуальность риск-менеджмента в сфере защиты данных. Масштабные информационные потери или технические неполадки способны нанести непоправимый ущерб корпоративным структурам, подрывая основы их функционирования. Грамотное управление безопасностью информационных активов выступает ключевым элементом стратегического планирования, гарантируя организациям стабильное развитие и лидирующие рыночные позиции.

Современная практика оценки рисков включает альтернативные способы анализа, позволяющие работать без применения точных математических расчетов вероят-

ностей и последствий рисковых событий. Качественный анализ рисков существенно отличается от традиционных количественных методик, опирающихся на статистические данные и сложные математические модели. Профессиональные эксперты применяют методы сравнительного анализа, рейтингования и специализированных оценочных систем для выявления потенциальных угроз. Главным приоритетом выступает распознавание значимых факторов влияния на бизнес-процессы компании при невозможности их точного количественного определения. Применение качественных методик существенно расширяет возможности риск- менеджмента, позволяя учитывать как легко измеримые параметры, так и сложно формализуемые аспекты деятельности организации.

Методики качественной оценки рисков позволяют систематизировать данные о потенциальных угрозах, определяя наиболее уязвимые аспекты функционирования организации. Аналитики выделяют ряд основополагающих подходов к проведению качественного анализа рисков, каждый из которых имеет свои особенности и сферы применения. Эти методы дают возможность руководителям и специалистам по управлению рисками получить целостное представление о ситуации и принять обоснованные решения по минимизации негативных последствий.

Анализ текущих и потенциальных рисков опирается на историко-ассоциативные методологии, основанные на изучении данных прошлых событий. Такой подход позволяет выявлять закономерности и тенденции, применимые к современным ситуациям. Использование накопленного опыта и исторических прецедентов способствует более точной оценке возможных угроз и разработке эффективных стратегий управления рисками в различных сферах деятельности.

Рейтинговая оценка представляет собой эффективный инструмент для классификации и анализа рисков, учитывающий их потенциальное воздействие и вероятность возникновения. Применение данного метода предполагает присвоение экспертами определенного ранга каждому идентифицированному риску, что способствует выявлению ключевых областей, требующих пристального внимания со стороны руководства. Практическая реализация данного подхода может включать формирование перечня потенциальных угроз для организации с последующим ранжированием их специалистами по степени влияния на деятельность компании. Риски, получившие наивысшие оценки, становятся приоритетными объектами управления для менеджеров, ответственных за минимизацию негативных последствий [1, с. 103].

Метод экспертных оценок занимает лидирующие позиции среди качественных способов анализа рисков. Привлечение компетентных специалистов позволяет получить профессиональное суждение о степени угроз. Экспертиза проходит несколько стадий: формирование группы оценщиков, разработка опросника, аккумулирование информации и обработка полученных данных. Ключевым фактором при выборе экспертов выступает их профессиональный опыт в сфере рискологии, что существенно снижает вероятность неверных выводов. Оценочные процедуры могут осуществляться как отдельными специалистами, так и группой экспертов, обеспечивая многосторонний подход к проблеме и повышая достоверность итоговых заключений.

Один из популярных методов экспертных оценок – метод Дельфи, который предполагает многоэтапное анкетирование экспертов с анонимной обработкой результатов. Такой подход позволяет избежать влияния одного мнения на других участников группы, что способствует более объективной оценке рисков [2, с. 59]. После каждого тура анкетирования эксперты получают результаты предыдущего этапа и могут скорректировать свои оценки на основе новой информации. Обычно после нескольких этапов мнения экспертов стабилизируются, что позволяет сформировать согласованную оценку риска.

Попарное сравнение представляет собой эффективный инструмент для качественной оценки рисков в организациях. Данный подход предполагает систематическое сопоставление различных угроз с целью определения их относительной значимости для компании. В ходе анализа каждый фактор риска оценивается относительно других по установленным параметрам, включая вероятность возникновения и потенциальный масштаб негативных последствий. Результаты такого сравнительного анализа позволяют сформировать ранжированный перечень рисков, служащий основой для разработки комплексных стратегий по минимизации и контролю выявленных угроз.

Методология качественной оценки рисков, подобно иным аналитическим инструментам, обладает рядом сильных и слабых сторон. Ключевым достоинством данного подхода выступает его адаптивность и применимость в условиях дефицита информации. При отсутствии или недостаточности количественных показателей для всестороннего анализа качественный метод позволяет

идентифицировать основные уязвимости и разработать стратегии их нивелирования. Тем не менее субъективность качественного анализа и его зависимость от компетенций специалистов и применяемых методик могут привести к неточным заключениям и рекомендациям.

В процессе управления рисками экспертные оценки приобретают особую значимость, когда сведения о потенциальных опасностях и их последствиях характеризуются неопределенностью. Применение данного метода способствует принятию аргументированных решений, основанных на суждениях и практическом опыте профессионалов, обладающих глубокими познаниями в специфической сфере. Компенсируя недостаточность количественных показателей, экспертные оценки обеспечивают всесторонний подход к анализу и контролю рисков, что позволяет организациям эффективно справляться с неопределенностями в различных областях деятельности.

Экспертные оценки представляют собой комплексный процесс аккумулирования, обработки и применения профессиональных суждений для анализа рисков и формирования управленческих решений. В ситуациях, характеризующихся высокой степенью неопределенности, когда использование точных количественных методов становится затруднительным или невозможным, экспертные оценки приобретают особую значимость. Данный инструментарий позволяет выявлять потенциальные угрозы и разрабатывать эффективные стратегии по их минимизации. Основываясь на глубоких профессиональных знаниях и интуитивном понимании предметной области, эксперты способны учитывать многочисленные факторы, оказывающие влияние на вероятность реализации рисковых событий [3, с. 100].

Экспертное мнение играет ключевую роль на разных стадиях риск-менеджмента. При выявлении потенциальных угроз специалисты, опираясь на накопленные знания и практический опыт, способны обнаружить ранее не учтенные факторы риска, характерные для аналогичных ситуаций в других компаниях. Анализируя риски, профессионалы предоставляют более точную оценку вероятности наступления различных событий и их возможного влияния на деятельность организации. Кроме того, ранжирование рисков экспертами по степени значимости позволяет руководству сосредоточиться на наиболее приоритетных направлениях для снижения потенциальных угроз бизнесу.

Организация экспертных опросов представляет собой комплексный процесс, требующий детальной проработки и последовательного выполнения определенных стадий. Ключевым этапом выступает формирование группы специалистов, обладающих глубокими познаниями и практическим опытом в сфере, непосредственно связанной с анализируемыми рисками. При отборе экспертов учитываются различные параметры, характеризующие их профессиональную компетентность: значимые достижения в карьере, продолжительность работы в данной области, вовлеченность в реализацию масштабных проектов и иные показатели, свидетельствующие о высоком уровне квалификации. Достоверность и обоснованность результатов оценки напрямую зависят от уровня профессионализма привлекаемых специалистов.

Разработка опросного инструментария для экспертной оценки рисков требует тщательного подхода. Формулировка вопросов играет ключевую роль в получении информативных и обоснованных ответов от специалистов. Грамотно составленные анкеты позволяют всесторонне рассмотреть различные аспекты потенциальных угроз, включая вероятность их возникновения и возможные способы минимизации негативных последствий. Предоставление экспертам возможности предложить собственные варианты решений способствует выявлению нестандартных подходов к управлению рисками, которые могли быть упущены при первоначальном анализе ситуации. Успешность всего процесса оценки во многом определяется качеством разработанных опросных материалов.

После формирования анкет начинается взаимодействие с экспертами. Процесс сбора данных может осуществляться различными способами, включая персональные беседы, групповые дискуссии или письменные ответы на вопросы, представленные в анкете. Каждый метод имеет свои преимущества и применяется в зависимости от специфики исследования и доступности экспертов. Выбор оптимального формата способствует получению наиболее полной и достоверной информации от специалистов в изучаемой области.

Анализ экспертных оценок начинается после завершения сбора мнений специалистов. Ключевым аспектом обработки полученных данных выступает оценка согласованности суждений экспертов относительно различных рисков. Для определения степени единства во взглядах профессионалов применяются специальные методики, среди которых выделяется расчет коэффициента конкордации. Данный показатель позволяет количественно измерить уровень

согласия между участниками экспертной группы. Высокое значение коэффициента свидетельствует о значительной согласованности мнений, что повышает надежность полученных оценок и обосновывает их использование в качестве фундамента для последующего принятия управленческих решений.

Отсюда прослеживается один из недостатков этого метода, а именно сложность организации процесса экспертных опросов. Сбор мнений экспертов требует значительных ресурсов, как временных, так и финансовых. Кроме того, если группа экспертов слишком велика, могут возникнуть трудности с обработкой и анализом данных. Напротив, если экспертов недостаточно, это может привести к тому, что результаты будут неполными и не отражающими реальную ситуацию. Оптимальный размер группы экспертов и правильно организованный процесс опроса являются ключевыми факторами для успеха метода.

Интуитивный анализ представляет собой незаменимый инструментарий для оценки рисков в условиях ограниченности данных или невозможности применения строгих количественных методик. Специалисты, опираясь на накопленный опыт, профессиональные знания и развитое чутье, способны принимать обоснованные решения даже при высокой степени неопределенности. В сфере управления рисками, включая область информационной безопасности, интуитивный подход приобретает особую значимость в ситуациях, требующих молниеносной реакции на возникающие угрозы без возможности проведения детального анализа.

Интуитивный анализ в информационной безопасности основывается на способности специалистов принимать оперативные решения, базируясь на подсознательных механизмах, накопленных знаниях и ассоциативных связях. Данный подход позволяет оценивать ситуацию без детального рассмотрения всех аспектов, что приобретает особую значимость в условиях постоянно меняющейся среды киберугроз. Динамичность рисков и внезапное появление новых опасностей требуют от экспертов быстрой реакции, даже при отсутствии полной информации для проведения традиционного анализа. Интуитивный метод оценки рисков дает возможность специалистам эффективно противодействовать возникающим вызовам в сфере информационной безопасности, опираясь на свой профессиональный опыт и интуицию.

Профессионалы в сфере информационной безопасности регулярно применяют интуитивный анализ для выявления потенциальных угроз. Специалисты по кибербезопасности, опираясь на многолетний опыт работы с вредоносными программами, способны обнаруживать признаки опасности задолго до ее полного проявления. Нередко эксперты, сталкиваясь с нестандартной активностью в сетевом пространстве или нетипичным функционированием системы, интуитивно ощущают наличие угрозы даже при отсутствии конкретных доказательств. Такой подход позволяет своевременно принимать предупредительные меры для предотвращения атак.

Интуитивное определение уязвимостей в системах безопасности также широко распространено среди специалистов. Эксперты, обладающие глубокими познаниями в области информационной безопасности и знакомые с историей предыдущих инцидентов, способны выявлять слабые места в инфраструктуре до того, как они будут обнаружены и использованы злоумышленниками [4].

Интуитивный подход обладает рядом значительных преимуществ в процессе принятия решений. Главное достоинство заключается в возможности оперативного реагирования на возникающие ситуации. При ограниченном времени и потенциально серьезных последствиях промедления интуитивный анализ позволяет действовать без глубокого изучения всех доступных данных. Особую ценность такой метод приобретает в условиях дефицита информации, когда необходимо немедленно отреагировать на возникшую угрозу.

Интуитивный анализ также даёт возможность специалистам принимать решения, опираясь на свой профессиональный опыт и интуицию, что особенно ценно в условиях отсутствия шаблонных решений. Многие риски в сфере информационной безопасности являются новыми и неизвестными, и применение стандартных методик может быть неэффективным. Интуиция, развитая на основе многолетнего опыта работы в данной сфере, помогает специалистам учитывать множество неявных факторов, которые не могут быть учтены в рамках формального анализа [5].

Субъективность представляет собой основной недостаток интуитивного анализа. Личный опыт и индивидуальное восприятие, лежащие в основе интуитивных решений, могут приводить к ошибочным выводам. Различные специалисты нередко дают несовпадающие интерпретации идентичных ситуаций, что потенциально влечет за собой разнородные заключения и последующие действия. Особую акту-

альность данная проблема приобретает при недостаточной компетентности аналитика или искажении его восприятия предшествующим опытом. Подобные обстоятельства способны повлечь за собой некорректную оценку рисков и принятие ошибочных решений на основе интуитивного подхода к анализу.

Недостаточная надежность интуитивного анализа проявляется в его ограниченной способности предвидеть весь спектр потенциальных исходов и траекторий развития ситуации. Данный подход демонстрирует наибольшую эффективность при оперативном принятии решений в условиях временных ограничений. Однако его применимость существенно снижается в контексте долгосрочного планирования и комплексной оценки стратегических рисков, требующих более систематического и всестороннего рассмотрения.

Качественные и количественные методы оценки рисков представляют собой два разных подхода к анализу рисков, каждый из которых имеет свои преимущества и ограничения. Основное различие между ними заключается в том, что качественные методы основываются на субъективных данных, мнениях экспертов и аналогиях, в то время как количественные методы предполагают использование числовых данных, статистики и математических моделей для определения вероятности возникновения риска и его потенциального воздействия [6].

Сравнительный анализ качественных и количественных методов оценки рисков позволяет глубже понять их специфику и области применения. Каждый подход обладает уникальными преимуществами и ограничениями, эффективность которых зависит от имеющихся данных и задач исследования. Представленная ниже таблица систематизирует основные различия между рассматриваемыми методами, способствуя выбору оптимальной стратегии оценки рисков в конкретных обстоятельствах. Детальное изучение характеристик обоих подходов позволяет более рационально использовать их в практике управления рисками.

Сравнение качественных и количественных методов оценки рисков

Критерий	Качественные методы	Количественные методы
Основные характеристики	Основаны на субъективных данных, экспертных мнениях и аналогиях	Основаны на объективных числовых данных, статистике и математических моделях
Использование данных	Требуют ограниченного объема данных или могут применяться при их отсутствии	Требуют большого объема достоверных данных для точного анализа
Гибкость	Высокая. Применяются в условиях неопределенности или недостаточной информации	Низкая. Ограничены в применении, если отсутствует достаточное количество данных
Примеры методов	Историко-ассоциативные методы, рейтинги, экспертные оценки, метод Дельфи, попарное сравнение	Вероятностный анализ, статистические методы, методы на основе моделирования (например, Монте-Карло), количественные опросы
Основные преимущества	- Гибкость применения в условиях неопределенности - Подходит для выявления скрытых и новых рисков - Быстрое применение	- Точные и объективные результаты - Позволяют прогнозировать вероятности и возможные убытки - Применимы для стратегий
Основные недостатки	- Субъективность - Зависимость от квалификации экспертов - Неточность и отсутствие конкретных числовых данных	- Необходимость больших объемов данных - Высокие затраты времени и ресурсов - Ограниченное применение при новых рисках
Когда использовать	- На начальных этапах анализа - При ограниченной информации - При оценке новых, уникальных рисков	- При наличии точных данных - Для долгосрочного планирования - Для стратегического анализа
Точность	Относительно низкая, зависит от квалификации и опыта экспертов	Высокая, поскольку основывается на количественных данных
Примеры применения	Идентификация новых угроз, экспертные опросы, предварительная оценка рисков	Прогнозирование последствий рисков, расчет вероятностей наступления событий

Выбор между качественным и количественным подходом к анализу рисков определяется спецификой задачи и доступностью информации. На начальных стадиях, при ограниченных или неизвестных данных, качественные методики демонстрируют наибольшую эффективность. Многоаспектные и трудноизмеримые риски также поддаются оценке с помощью качественных инструментов. Напротив, количественный анализ целесообразно применять при наличии достаточного объема данных для углубленного изучения рисков. Данный метод особенно ценен в ситуациях, требующих точного определения вероятности возникновения рисковых событий и масштаба их последствий.

Оптимальной стратегией управления рисками часто является использование комбинированного подхода, который включает как качественные, так и количественные методы. Такой подход позволяет учесть как субъективные мнения экспертов, так и объективные данные, что обеспечивает более полное и точное понимание рисков и позволяет разрабатывать более эффективные стратегии по их управлению [7].

Развитие методов качественной оценки рисков играет ключевую роль в современной модели управлении рисками, особенно в условиях цифровой экономики и информационной безопасности. Качественные методы позволяют проводить оценку рисков в условиях недостатка данных, что делает их незаменимыми на ранних этапах анализа или в ситуациях, когда количественные методы невозможно применить из-за отсутствия точных показателей. Качественная оценка рисков предоставляет гибкость и вариативность, позволяя использовать экспертные знания и интуитивный подход для идентификации потенциальных угроз.

Заключение

Будущее экспертных оценок и интуитивного анализа напрямую связано с повышением их точности и эффективности путем использования новых инструментов и технологий. Профессиональная аналитика, подкрепленная многолетним практическим опытом и глубоким пониманием рыночных механизмов, сохраняет фундаментальную значимость в принятии стратегических решений.

Современные методологические подходы направлены на создание инструментария, позволяющего специалистам максимально нивелировать субъективные факторы при формировании экспертных заключений. Субъективность интуитивных методов анализа создает существенные методологические ограничения, несмотря на внедрение передовых технологических решений.

Личностные предпочтения и эмоциональные аспекты продолжают оказывать значительное влияние на результаты исследований. Совершенствование процедур сбора экспертной информации и внедрение усовершенствованных алгоритмов обработки данных позволяют минимизировать субъективные искажения. Повышение профессиональных требований к специалистам-экспертам дополняется внедрением образовательных программ, направленных на развитие когнитивно-аналитического потенциала.

Комплексный подход к управлению информационными рисками выходит далеко за пределы технических решений, создавая прочный базис конкурентного преимущества и долгосрочного развития компаний. Внедрение многоуровневого анализа, объединяющего экспертную оценку с вычислительными моделями, значительно укрепляет защитные механизмы корпоративной инфраструктуры, позволяя организациям эффективно противостоять современным киберугрозам. Построение многогранной системы управления рисками становится ключевым фактором сохранения цифровых активов, помогая компаниям защищать корпоративные данные, поддерживать деловую репутацию и предотвращать возможные финансовые убытки.

Динамичное развитие методологии качественного анализа рисков открывает широкие возможности для совершенствования систем управления в условиях технологической трансформации бизнес-процессов.

Список литературы

1. Грачев С.А. Оценка и управление рисками. Владимир: Издво ВлГУ, 2020. 287 с.

2. Орлов А.И. Организационно-экономическое моделирование. М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. 486 с.

3. Раскатова М.И. Оценка рисков. Челябинск: ИЦ ЮУрГУ, 2021. 125 с.

4. Рыленков Д. А. Алгоритм ранжирования угроз информационной безопасности на основе метода анализа иерархий // Инженерный вестник Дона. 2024. № 8 (116). С. 123-134

5. Гурбандурдыева А., Шохрадов А., Розыев Э., Язбердыев Я. Исследование проблем и решений в области кибербезопасности на основе анализа угроз и уязвимостей // CETERIS PARIBUS. 2024. № 3. С. 13-16.

6. Беззатеев С.В., Елина Т.Н., Мыльников В.А., Лившиц И.И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 4. С. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561.

7. Зубкова Т.М., Тагирова Л.Ф., Тагиров В.К. Прототипирование адаптивных пользовательских интерфейсов прикладных программ с использованием методов искусственного интеллекта // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19, № 4. С. 680–688. DOI: 10.17586/2226-1494-2019-19-4-680-688.