Электронный научный журнал «Век качества» ISSN 2500-1841 https://www.agequal.ru

2026, №2 https://www.agequal.ru/pdf/2026/AGE_QUALITY_2_2026.pdf

Ссылка для цитирования этой статьи:

Сенина Д.С., Билятдинов К.З. Способ комплексного применения методов оценки рисков в области информационных технологий // Электронный научный журнал «Век качества». 2026. №2. С. 295-310. Режим доступа: https://www.agequal.ru/pdf/2026/226019.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056

Способ комплексного применения методов оценки рисков в области информационных технологий

Сенина Дарья Сергеевна,
студентка кафедры инноватики и интегрированных систем качества,
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП),
190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А
seninadashaserg@gmail.com

Билятдинов Камиль Закирович,
доктор технических наук, доцент,
профессор кафедры инноватики и интегрированных систем качества
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП),
190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А
k74b@mail.ru

В изложенном в статье способе предлагается реализация комплексного и последовательного применения качественных (экспертных) и количественных методов оценки рисков организации (предприятия, учреждения) в области информационных технологий.

Определены предпосылки, нормативно-правовые и методологические основы для разработки способа. Обоснованы область применения, ограничения, допущения и базовые категории активов организации. Составлены этапы экспертной оценки рисков. В качестве количественного метода обоснованно рекомендован метод Монте-Карло, позволяющий моделировать множество возможных сценариев реализации угроз и рассчитывать ожидаемый ущерб при неопределенности исходных параметров. Доказано, что применение имитационного моделирования повышает обоснованность управленческих решений. На практике способ может выступать эффективным инструментом

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

для формирования интеграционного ресурса развития организации (предприятия, учреждения).

Ключевые слова: активы; информационная безопасность; оценка рисков; управление рисками; экспертная оценка; метод Монте-Карло.

Введение

В настоящее время наблюдается динамичное развитие информационных технологий при усилении конкурентной борьбы в условиях неблагоприятных воздействий внешней среды. В связи с этим повышается актуальность своевременной и объективной оценки рисков в области разработки, совершенствования, развития и применения информационных технологий (далее – ИТ) и, соответственно, аппаратно-программных комплексов (далее – АПК), средств связи и автоматизации, реализующих оцениваемые технологии, на всех этапах жизненного цикла.

Результаты анализа нормативно-технической документации и научной литературы [1, 2, 3, 4] в исследуемой предметной области показали следующие тенденции.

1. В основном оценка рисков проводиться в области информационной безопасности ИТ [1, 2, 3, 4 и др.].

2. По сути, отсутствуют методологические решения по комплексному применению методов оценки рисков, предусмотренных ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска».

3. Фактически отсутствуют методология и способы комплексного применения методов оценки рисков в сфере ИТ.

4. Динамика развития ИТ и требования, изложенные в нормативно-технических документах, предопределяют необходимость увеличения объема разнообразной обрабатываемой статистический и экспертной информации.

Таким образом, сегодня становиться актуальным достижение цели исследования, а именно, разработать способ комплексного применения методов оценки рисков в области ИТ (далее – Способ) в интересах обоснованного и

своевременного управления рисками в области ИТ.

Соответственно, научная задача исследования по разработки Способа будет включать в себя последовательное выполнение частных задач исследования:

1) сформулировать предпосылки и нормативно-правовые основы разработки Способа;

2) определить методологические основы разработки Способа;

3) сформулировать назначение, область применения, ограничения и допущения Способа;

4) сформировать содержание Способа в интересах рационального достижения цели исследования;

5) разработать рекомендации по применению Способа как инструмента внедрения риск-ориентированного подхода.

Основная часть

I. Предпосылки и нормативно-правовые основы разработки Способа

Сегодня в различных ведомствах, на промышленных предприятиях и в организациях (далее – организациях) ИТ перестали быть вспомогательной функцией и стали критическим условием обеспечения непрерывности основной деятельности. Нарушение доступности цифровых сервисов, компрометация данных, сбой промышленной автоматизации или появление уязвимостей в корпоративной сети способны привести не только к прямым финансовым потерям, но и к репутационному ущербу, штрафам, простоям, судебным спорам и нарушению обязательств перед контрагентами.

По этой причине риск-ориентированный подход в ИТ-сфере рассматривается не как факультативный элемент системы безопасности, а как базовый механизм обоснования управленческих решений.

Российская и международная практики исходят из того, что риск в области информационных технологий должен оцениваться системно, с учетом

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

ценности активов, актуальных угроз, существующих уязвимостей, эффективности уже внедренных защитных мер и допустимого для организации уровня остаточного риска [5, 6, 7].

В ГОСТ Р ИСО/МЭК 27005 [1] менеджмент риска информационной безопасности определяется как непрерывный процесс, включающий в себя установление контекста, оценку риска, обработку риска, принятие риска, обмен информацией о риске и мониторинг риска.

Методические документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России), в свою очередь, устанавливают требования по выявлению угроз, определению нарушителей, описанию сценариев реализации угроз и анализу негативных последствий для информационных систем и объектов критической информационной инфраструктуры.

При этом на практике сохраняются противоречия между требованиями, изложенными в нормативно-технических документах, и прикладной экономической оценкой риска. Наличие этих противоречий выражается в том, что должностные лица (далее – ДЛ) организаций имеют достаточные компетенции по формальному составлению перечней угроз, но испытывают трудности при ответе на вопросы: «какой риск является действительно критичным в заданный период времени?», «какие меры защиты экономически оправданы?» и «насколько уменьшается риск после их внедрения?». Вот почему в научной литературе все чаще подчеркивается необходимость сочетания качественных методов, позволяющих быстро классифицировать риски, с количественными методами, обеспечивающими более точное моделирование последствий и вероятностей.

[1] ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

II. Методологические основы разработки Способа

Под риском в области информационных технологий целесообразно понимать вероятность наступления события, связанного с использованием, отказом, компрометацией или нарушением функционирования ИТ-инфраструктуры, которое способно причинить ущерб активам, процессам или целям организации.

В более узком понимании речь идет об информационном риске, возникающем из сочетания угрозы, уязвимости и значимости затрагиваемого актива.

С точки зрения управления рисками, в ИТ выделяются несколько базовых категорий активов:

1) информационные ресурсы;

2) программное обеспечение;

3) технические средства, ПАК, средства связи и автоматизации;

4) сеть связи;

5) облачные сервисы;

6) персонал (ДЛ и лица, принимающие решения (далее – ЛПР);

7) процессы управления и мероприятия, направленные на достижение цели или функционирование организации;

8) взаимодействующие внешние организации (например, поставщики услуг).

Каждая из этих категорий обладает собственной уязвимостью и различной чувствительностью к нарушениям конфиденциальности, целостности и доступности. Поэтому в Способе оценка риска не может ограничиваться только техническим анализом уязвимостей; она должна учитывать деловой контекст, критичность процесса и возможный масштаб потерь [2].

III. Назначение, область применения, ограничения и допущения Способа

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Назначение Способа комплексного применения методов оценки рисков в области ИТ: организация и выполнение комбинированной оценки ИТ-рисков на основе совместного использования качественных и количественных методов оценки в интересах обоснования управленческих решений ЛПР в области управления рисками.

Область применения: различные организации, разработчики АПК, средств связи и автоматизации, с целью обоснования управленческих решений и технических заданий на разработку и модернизацию АПК.

Ограничения: зависимость от качества исходных данных, субъективность экспертных оценок, ограниченная применимость точных численных результатов.

Допущения: независимость наблюдений и правильный выбор функций распределения.

IV. Содержание Способа

Наиболее распространенная логика анализа предполагает, что риск возрастает при одновременном наличии трех условий: актив обладает ценностью, существует угроза его нарушения, и имеется уязвимость, которая делает реализацию угрозы реальной.

В упрощенном виде базовый риск может быть представлен формулой:

$$R_i = P_i \cdot I_i, \quad (1)$$

где R_i – значение риска по i-му сценарию, P_i – вероятность реализации сценария, I_i – величина ущерба.

Данная модель удобна для первичной классификации, но в практических расчетах её обычно дополняют коэффициентами уязвимости, обнаружения, эффективности существующих мер защиты и фактором времени [3].

Если требуется отразить влияние применяемых средств защиты, то может использоваться формула остаточного риска:

$$R_{\text{ост}} = R_{\text{исх}} \cdot (1 - E), \quad (2)$$

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

где $R_{\text{ост}}$ – остаточный риск, $R_{\text{исх}}$ – исходный риск, E – интегральная эффективность набора мер защиты. Чем выше эффективность организационных и технических мер, тем ниже остаточный риск, однако полностью устранить его, как правило, невозможно. Именно поэтому в управлении рисками важны не только меры предотвращения, но и механизмы реагирования, резервирования и восстановления.

В связи с этим в Способе предлагается производить экспертную оценку ИТ-рисков в виде последовательного процесса, а не как разовое экспертное мероприятие.

В Способе данный процесс включает в себя следующие этапы.

Первый этап. Определяется контекст оценки. На этом этапе уточняются цели анализа, границы системы, критерии допустимости риска, перечень заинтересованных сторон и используемая шкала оценки. Без четкого контекста невозможно корректно сопоставить риски различных подразделений, информационных систем и бизнес-процессов.

Второй этап. Проводится идентификация активов. Это обеспечит реализацию комплексного подхода, так как будут оценены не только серверы, рабочие станции и прикладное ПО (традиционный подход), но и учетные записи, технологические регламенты, каналы обмена данными, резервные копии, журналы событий, конфигурации сетевого оборудования и знания специалистов.

В итоге предлагаемый этап позволяет минимизировать потенциальный ущерб посредством комплексной оценки активов, а не отдельных аппаратно-программных комплексов (АПК).

Третий этап. Определяются угрозы и уязвимости. Применяются результаты моделирования угроз, анализ конфигураций, данные сканирования уязвимостей, сведения об инцидентах прошлых периодов, требования, изложенные в правовых актах, и экспертная оценка. Методические документы

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

ФСТЭК ориентируют на описание источников угроз, способов реализации, нарушителей, возможных объектов воздействия и негативных последствий.

Четвертый этап. Выполняется анализ последствий и вероятности. Последствия могут выражаться в финансовых потерях, времени простоя, объеме утечки данных, снижении качества управления, невыполнении договорных обязательств или нарушении требований законодательства. Вероятность оценивается либо экспертно, либо статистически, либо на основе имитационного моделирования. На этом этапе организация может применять простые шкалы «низкий риск – средний риск – высокий риск», либо переходить к численным вероятностным моделям [4].

Пятый этап. Выполняется ранжирование рисков и принятие решения о способе обработки.

В литературе [5] выделяют четыре базовые стратегии: избегание риска, снижение риска, передача риска и принятие риска.

Для ИТ-сферы чаще всего применяется снижение риска путем внедрения дополнительных мер защиты, резервирования, сегментации сети, усиления контроля доступа, обновления ПО, повышения квалификации персонала и совершенствования процедур реагирования на инциденты.

Шестой этап. Результаты подлежат пересмотру. Риск в ИТ-среде не является статичным: меняются архитектура систем, ландшафт угроз, бизнес-модель организации, используемые сервисы и нормативные требования. Следовательно, риск-оценка должна обновляться регулярно, а также после существенных изменений инфраструктуры, инцидентов или выявления критических уязвимостей.

В предлагаемом Способе качественные методы применяются тогда, когда статистических данных недостаточно, либо когда требуется быстрое управленческое решение. Их достоинства состоят в относительной простоте, невысокой стоимости внедрения и возможности использования экспертных оценок. На практике широко применяются матрицы риска, сценарный анализ,

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

опросные листы, сравнительные шкалы критичности, а также методики OCTAVE, CRAMM, FRAP и иные подходы, упоминаемые в профильной литературе [3, 8].

Однако качественная оценка имеет и ограничения. Она зависит от субъективности экспертов, может искажать приоритеты при большом количестве сравниваемых рисков и не всегда позволяет убедительно обосновать экономическую эффективность мер защиты. Например, два риска, получившие одинаковую категорию «высокий», могут принципиально различаться по ожидаемому ущербу: один приведет к часовому простою, другой – к длительной остановке производства или крупной утечке данных.

Количественные методы, напротив, ориентированы на численное выражение риска. В этом случае оцениваются вероятности реализации сценариев, распределения возможного ущерба, ожидаемые потери, доверительные интервалы и показатели чувствительности. В современных исследованиях подчеркивается, что именно количественный анализ позволяет более обоснованно выбирать приоритетные меры защиты, особенно для критически важных систем и объектов промышленной автоматизации [6].

Вместе с тем количественная оценка требует исходных данных и методической дисциплины. Необходимо корректно описывать сценарии атак, источники данных, интервалы неопределенности и допущения модели. Иначе возникает ложная точность: формально риск выражен числом, но само число неустойчиво и не отражает реальную ситуацию [7].

Таким образом, Способ основывается на комбинированном подходе.

При этом вначале проводиться качественная оценка рисков (например, с помощью экспертного оценивания [9, 10, 11], позволяющая своевременно отобрать наиболее значимые риски и определить перечень сценариев, требующих углубленного анализа. Затем для этой ограниченной группы наиболее значимых рисков применяется количественное моделирование, которое дает более точные показатели и помогает сопоставить риск с затратами

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

на его обработку. Такой подход соответствует современной тенденции развития риск-менеджмента в информационной безопасности [4, 8].

Для количественной оценки рисков в Способе предлагается применять метод Монте-Карло.

Обоснование: метод Монте-Карло относится к инструментам статистического моделирования и особенно полезен в тех случаях, когда параметры риска заданы не точными значениями, а распределениями вероятностей.

Для ИТ-сферы это типичная ситуация: невозможно заранее знать точную частоту инцидента, точный объем ущерба, точное время восстановления или точную эффективность каждой меры защиты. Но можно задать вероятностные интервалы и выполнить многократное моделирование возможных исходов [12].

В Способе сущность применения метода Монте-Карло заключается в следующем. Для выбранного экспертами сценария риска задаются случайные переменные: вероятность эксплуатации уязвимости, вероятность успешного развития атаки после первичного проникновения, длительность простоя, объем утечки данных, стоимость восстановления, размер регуляторных и репутационных потерь. Затем выполняется большое количество итераций моделирования.

На каждой итерации случайным образом генерируются значения входных параметров в пределах заданных распределений, после чего рассчитывается итоговый ущерб по сценарию. Множество таких итераций формирует эмпирическое распределение потерь.

Математически ожидаемый ущерб по результатам моделирования может быть представлен так [13]:

$$\hat{E}(L) = \frac{1}{N}\sum_{k=1}^{N} L^{(k)}, \qquad (3)$$

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

где $\hat{E}(L)$ – оценка ожидаемого ущерба, N – число итераций моделирования, $L^{(k)}$ – ущерб в k -й итерации. Дополнительно может рассчитываться квантиль распределения потерь [13], например, уровень потерь, не превышаемый с вероятностью 0,95:

$$VaR_{0.95} = \inf\{x \in \mathbb{R}: P(L \leq x) \geq 0.95\}. \quad (4)$$

Для управленческой практики это особенно важно, поскольку руководителя интересует не только средний ущерб, но и риск редких, но крайне тяжелых последствий. Если, например, средний ущерб умеренный, а верхние 5% распределения показывают катастрофические потери, это означает необходимость отдельного внимания к мерам устойчивости и планам аварийного восстановления.

В научных публикациях метод Монте-Карло рассматривается как применимый инструмент оценки устойчивости объектов информатизации при редких и трудно предсказуемых атаках, а также как средство моделирования киберугроз в сложных сетевых и критических инфраструктурах [14].

Его достоинствами являются учет неопределенности, возможность анализа чувствительности факторов и наглядность результатов. Недостатки состоят в зависимости от качества входных распределений и в том, что моделирование не заменяет полноценного анализа архитектуры системы и процессов управления в организации.

V. Рекомендации по применению Способа как инструмента внедрения риск-ориентированного подхода в организации

1. В качестве организационной основы для рационального применения Способа целесообразно сформировать группу внутренних и внешних экспертов из высококвалифицированных и мотивированных технических специалистов.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

2. Необходимо рассчитывать нормированный показатель важности эксперта в зависимости от достигнутых результатов (достоверности) в оценке рисков.

3. На основе требований, изложенных в правовых актах, специфики деятельности организации, условий и экспертных мнений (мнений ЛПР и ДЛ) вести и корректировать базу данных значений показателей, влияющих на объективную оценку риска.

4. Осуществлять обратную связь в виде оценки эффективности управленческих решений (соотношение затраченных ресурсов и достигнутого результата), принятых по результатам оценки риска предлагаемым Способом.

5. Применять Способ на всех этапах изменения ИТ-архитектуры предприятия.

Заключение

Предлагаемый Способ комплексного применения методов оценки рисков в области ИТ представляет собой методологическое решение в области оценки рисков ИТ, основанное на оригинальном авторском подходе к комплексному и последовательному применению качественных и количественных методов оценки рисков организации в области ИТ.

На практике Способ позволяет ЛПР и ДЛ организаций при оценке рисков учитывать ценности активов, особенности процессов управления, наличие ресурсов, квалификацию и мотивацию персонала, анализ угроз и возможный ущерб, динамику результатов оценки в отчётные периоды времени, взаимосвязь технических показателей эксплуатируемых (модернизируемых) АПК и средств связи с экономическими и организационными последствиями.

Таким образом, Способ может выступать эффективным инструментом для формирования интеграционного ресурса и компонентом методологической основы для научно обоснованного изменения (корректировки) стратегии развития организации.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Список литературы

1. Аникин И.В., Емалетдинова Л.Ю., Кирпичников А.П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях // Вестник технологического университета. – 2015. – Т. 18, № 21. – URL: https://cyberleninka.ru/article/n/metody-otsenki-i-upravleniya-riskami-informatsionnoy-bezopasnosti-v-korporativnyh-informatsionnyh-setyah (дата обращения: 27.03.2026).
2. Каналиев А.С. Риски информационной безопасности // Colloquium-journal. - 2022. – URL: https://cyberleninka.ru/article/n/riski-informatsionnoy-bezopasnosti (дата обращения: 25.03.2026).
3. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа. – 2012. – № 1(25), ч. 2. – С. 83-88. – URL: https://journal.tusur.ru/storage/45721/083.pdf (дата обращения: 25.03.2026).
4. Ожгибесова А.С., Шабуров А.С., Южаков А.А. Об оценке рисков информационной безопасности на основе применения нечетких когнитивных карт в интеллектуальных транспортных системах управления дорожным движением // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 2(52). – С. 56-67. – DOI: 10.14529/secur240206. – URL: https://ojstest.susu.ru/index.php/ojs_test/article/download/124/117 (дата обращения: 26.03.2026).
5. Ян Лу. Стратегии риск менеджмента в современной организации // Экономика и социум. – 2024. – № 5(120)-1. – С. 1897-1901. – URL: https://cyberleninka.ru/article/n/strategii-risk-menedzhmenta-v-sovremennoy-organizatsii (дата обращения: 26.03.2026)
6. Иваненко В.Г., Иванова Н.Д. Оценка рисков информационной безопасности автоматизированных систем управления технологическим процессом // Вопросы кибербезопасности. – 2024. – № 1. – С. 116-123. – DOI: 10.21681/2311-3456-2024-1-116-123. – URL: https://cyberrus.info/wp-

content/uploads/2024/02/vokib-2024-1-st13-s116-123.pdf (дата обращения: 27.03.2026).

7. Кириллова А.Д., Килин В.Ю. Оценка рисков информационной безопасности промышленных объектов на основе метода дерева атак // Системная инженерия и информационные технологии. – 2023. – URL: https://siit.ugatu.su/index.php/journal/article/download/147/170 (дата обращения: 27.03.2026).
8. Шинаков К.Е., Голембиовская О.М. Формализация процесса оценки рисков информационной безопасности на основе методики OCTAVE // Вестник Брянского государственного технического университета. – 2015. –№ 3(47). – С. 175-181. – URL: https://auspublishers.com.au/temp/ e0b93da39979c0eed34265521591a22f.pdf (дата обращения: 26.03.2026).
9. Билятдинов К.З. Усовершенствованный метод парных сравнений для оценки качества технических систем в процессе эксплуатации // Вестник воздушно-космической обороны. – 2021. – № 3 (31). – С. 39-44.
10. Билятдинов К.З. Методика оценки качества технических систем на основе усовершенствованного метода парных сравнений // Вестник воздушно-космической обороны. – 2021. – № 4 (32). – С. 102-107.
11. Biliatdinov K.Z., Dosikov V.S., Meniailo V.V. Improvement of the paired comparison method for implementation in computer programs used in assessment of technical systems' quality // Computer Research and Modeling. – 2021. – Т. 13, № 6. – С. 1125-1135.
12. Воеводин В.А., Писаренко А.Ю. Метод Монте-Карло для оценки устойчивости функционирования объекта информатизации в условиях массированных компьютерных атак // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2022. – № 4. – URL: https://www.mathnet.ru/php/

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

getFT.phtml?jrnid=vagtu&paperid=719&what=fullt (дата обращения: 28.03.2026).

13. Брызгалов А.А. Экономико-математическое моделирование рисков в сервисной бизнес-модели сетевого предприятия // Статистика и экономика. – 2025. – Т. 22, № 4. – С. 36-51. – URL: https://cyberleninka.ru/article/n/ekonomiko-matematicheskoe-modelirovanie-riskov-v-servisnoy-biznes-modeli-setevogo-predpriyatiya (дата обращения: 28.03.2026).
14. Краснов А.Е., Федоров А.В., Абушкин Х.Х. Оценивание устойчивости критических инфраструктур // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – URL: https://bit.spels.ru/index.php/bit/article/view/1328 (дата обращения: 28.03.2026).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

A Method for the Integrated Application of Risk Assessment Methods in Information Technology

Senina Daria Sergeevna,
Student of the Department of Innovation and Integrated Quality Systems
Federal State Autonomous Educational Institution of Higher Education "Saint Petersburg State University of Aerospace Instrumentation" (SUAI),
190000, Saint Petersburg, Bolshaya Morskaya St., Bldg. 67, Lit. A
seninadashaserg@gmail.com

Bilyatdinov Kamil Zakirovich,
Doctor of Engineering Sciences, Associate Professor
Professor, Department of Innovation and Integrated Quality Systems
Federal State Autonomous Educational Institution of Higher Education "Saint Petersburg State University of Aerospace Instrumentation" (SUAI),
190000, Saint Petersburg, Bolshaya Morskaya St., Bldg. 67, Lit. A
k74b@mail.ru

This method proposes the integrated and consistent application of qualitative (expert) and quantitative methods for assessing the risks of an organization (enterprise, institution) in the field of information technology.

The prerequisites, regulatory, and methodological foundations for the method's development are defined. The scope of application, limitations, assumptions, and basic categories of the organization's assets are substantiated. The stages of expert risk assessment are outlined. The Monte Carlo method is justifiably recommended as a quantitative method, allowing for the modeling of multiple possible threat scenarios and the calculation of expected damage under uncertainty of initial parameters. It has been proven that the use of simulation modeling improves the validity of management decisions. In practice, the method can serve as an effective tool for developing an integrated resource for the development of an organization (enterprise, institution).

Keywords: assets; information security; risk assessment; risk management; expert assessment; Monte Carlo method.