УДК 33 **DOI: 10.34670/AR.2025.22.28.033**

Количественная оценка информационной безопасности в условиях цифровой экономики: модели и методы

Моденов Анатолий Константинович

Доктор экономических наук, профессор,
Санкт-Петербургский государственный архитектурно-строительный университет,
190005, Российская Федерация,
Санкт-Петербург, 2-я Красноармейская ул., 4;
e-mail: modenov200459@mail.ru

Усков Владислав Владимирович

Кандидат экономических наук, доцент,
Санкт-Петербургский государственный архитектурно-строительный университет,
190005, Российская Федерация,
Санкт-Петербург, 2-я Красноармейская ул., 4;
e-mail: vladuskov@yandex.ru

Статья подготовлена в рамках темы научно-исследовательской работы №33С25 при финансовой поддержке гранта СПбГАСУ.

Аннотация

В условиях цифровой трансформации экономики оценка информационной безопасности становится критически важной для обеспечения экономической безопасности предприятий. В статье рассматриваются различные методы оценки информационной безопасности, включая оценку по эталону, риск-ориентированную оценку и оценку на основе экономических показателей. Особое внимание уделяется риск-ориентированному подходу, который позволяет выявлять и предотвращать потенциальные угрозы до их возникновения. Предлагается математическая модель для количественной оценки информационной безопасности, включающая расчет воздействия риска, потенциального риска и вероятности его возникновения. Модель позволяет определить минимально и максимально допустимые уровни риска, что является важным инструментом для управления информационной безопасностью в условиях нестабильной экономической ситуации. В заключение подчеркивается необходимость комплексного подхода к защите информационных активов и внедрения инновационных технологий.

Для цитирования в научных исследованиях

Моденов А.К., Усков В.В. Количественная оценка информационной безопасности в условиях цифровой экономики: модели и методы // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 8А. С. 318-325. DOI: 10.34670/AR.2025.22.28.033

Ключевые слова

Информационная безопасность, риск-ориентированный подход, цифровая экономика, количественная оценка, управление рисками, кибербезопасность, защита данных, экономическая безопасность.

Введение

В условиях цифровой экономики оценка информационной безопасности становится критически важной составляющей экономической безопасности предприятия. Информационные угрозы могут нанести значительный ущерб, нарушая рабочие процессы, вызывая финансовые и правовые последствия, а также подрывая репутацию компании. Поэтому разработка четких алгоритмов количественной оценки информационной безопасности является необходимым шагом для эффективного управления рисками и обеспечения устойчивого развития предприятия.

Основная часть

Оценка информационной безопасности может проводиться с использованием различных методов, включая оценку по эталону, риск-ориентированную оценку и оценку на основе экономических показателей. Каждый из этих методов имеет свои преимущества и недостатки, и выбор конкретного подхода зависит от специфики предприятия и его бизнес-процессов [Запечников, Милославская, Толстой, Ушаков, 2018] (табл. 1):

Таблица 1 – Методы оценки информационной безопасности предприятия

Метод	Описание	Особенности	Преимущества / недостатки
Оценка ИБ на основе экономических показателей	Оценка стоимости обеспечения системы информационной безопасности (СОИБ) на основе показателей совокупной стоимости владения (ТСО)	Сравнение затрат на СОИБ с аналогичными организациями	Практически не применяется из-за сложности создания актуальной базы данных
Оценка ИБ по эталону	Сравнение требований, реализованных для обеспечения информационной безопасности, с выбранной эталонной моделью	Сравнение процессов управления или элементов системы с аналогичными у эталонного предприятия	Эффективен для выявления лучших практик, но требует наличия актуальной базы данных по эталонным моделям
Риск-ориентированная оценка	Основывается на анализе рисков информационной безопасности и сопоставлении их с мерами по их обработке	Включает идентификацию рисков, определение связанных процессов менеджмента и формирование критериев оценки	Позволяет выявлять и предотвращать потенциальные угрозы до их возникновения

Каждый из указанных методов, безусловно, обладает своими положительными и отрицательными чертами.

Для оценки уровня информационной безопасности будет применена риск-ориентированная

оценка, поскольку, на наш взгляд, в нынешней нестабильной экономической ситуации, подход к анализу систем безопасности стабильно функционирующего предприятия крупного бизнеса должен быть, в первую очередь, основан на предупреждении угроз и проведении мероприятий, устраняющих их до непосредственного возникновения.

Как с научной, так и с практической точки зрения, оценка риска состоит из двух элементов – качественной его оценки и количественного измерение (вычисления) конкретного риска, а также взаимной связи их последствий. Понятие управления рисками, в свою очередь – это стратегия предотвращения потерь и использования допустимых возможностей, или таких возможностей, которые могут возникнуть в зоне риска [Запечников, Милославская, Толстой, Ушаков, 2018]. Как правило, ни одна стратегия не может покрыть всех рисков информационных и технологических активов, но сбалансированная стратегия обеспечит наилучший порядок решения конкретной ситуации. Когда риск обнаружен, его можно оценить, как приемлемый или неприемлемый. В случае если он приемлем, никаких дальнейших действий не требуется. Если же риск неприемлемый, возникает необходимость контролировать его с помощью специальных разработанных мер по предотвращению или смягчению последствий.

Для количественной оценки информационной безопасности предлагается использовать следующую математическую модель [Андрианов, www]:

$$ВРиск=ПотенцРиск*ВВ, \quad (1)$$

где ВРиск – воздействие риска; ПотенцРиск – потенциальный риск; ВВ – вероятность возникновения.

Под потенциальным риском, в свою очередь, понимается любой тип риска, существующий для конкретного предприятия, или же любой риск, связанный с теоретическим действием при определённых обстоятельствах [1]. Данный риск также способен возникнуть в результате обычного функционирования предприятия, однако чаще всего оно сталкивается с ним при проведении отдельных конкретных мероприятий в определенных отраслях или рынках. Потенциальный риск может быть рассчитан по следующей формуле:

$$ПотенцРиск=ОСА*СУ*СТ, \quad (2)$$

где ОСА – общая стоимость активов; СУ – серьезность уязвимости; СТ – серьезность угрозы.

В данном случае под вероятностью возникновения понимают оценку частоты реализации события, частоты его возникновения. Для определения вероятности возникновения составляется модель определений и соответствующих им оценок уровня угрозы.

Далее, для определения стоимости оценки информационного актива, воспользуемся следующей формулой:

$$ОСА = СА * ВА, \quad (3)$$

где СА – стоимость активов; ВА – вес активов.

Следует уточнить некоторые моменты, касающиеся стоимости оценки активов:

– количественный показатель информации будет имеет минимальное значение 1 для каждого актива;

– значение уровней для информационной безопасности имеет следующий вид: оценка 3 – высокая, 2 – средняя, 1 – низкая;
– стоимость информационного актива определяется суммой трех факторов: конфиденциальность, целостность и доступность.

Далее, согласно модели, должна быть определена стоимость информационных активов, в соответствии с которой производится классификация активов по трём уровням, полученные категории указывают на уровень необходимой защиты для них. Для активов III категории применяется максимальная степень защиты.

Согласно риск-ориентированной оценки, после вышеуказанного следует проанализировать угрозы конкретного предприятия, чтобы с их помощью рассчитать минимальные допустимые риски. С научной точки зрения в данном контексте следует раскрыть следующие понятия [Андрианов, www; Гришина, 2021] (табл. 2):

Таблица 2 – Некоторые показатели риск-ориентированной оценки информационной безопасности предприятия

Показатель	Описание
Уязвимость	Совокупность следующих элементов: уязвимости системы, доступности к уязвимости, возможность использования уязвимости
Чувствительность	Мера усилий, достаточных для эффективного использования уязвимости
Подверженность	Возможность дальнейшего распространения угрозы на остальные элементы системы
Воздействие	Сильнейшее последствие воздействия угрозы для предприятия
Возможности	Мера способности субъекта угрозы успешно атаковать актив, пользуясь его уязвимостями

Согласно составленных моделей возможностей и вероятности риска можно рассчитать минимально допустимый риск, используя следующую формулу:

$$\text{ММДР} = \text{МаксСА} * \text{НизкУ} * \text{НизкВ} * \text{МаксЧВ}, \quad (4)$$

где МДР – минимально допустимый риск; МаксСА – максимальная стоимость активов; НизкУ – низкое значение уязвимости; НизкВ – низкое значение возможностей и влияния; МаксЧВ – максимальная частота вероятности.

Для расчета максимально допустимого риска, в свою очередь, формула будет иметь следующий вид:

$$\text{МДР} = \text{МаксСА} * \text{СредУ} * \text{СредВ} * \text{МаксЧВ}, \quad (5)$$

После установления диапазона допустимого риска составляется таблица оценки рисков, которая может наглядно продемонстрировать долю недопустимых рисков в их общем числе. На её основе исследователи получают возможность разработать необходимые меры для осуществления каких-либо дополнительных мероприятий по защите информационных активов предприятия.

Информационные технологии, которые повсеместно используются предпринимателями во всём мире, являются важнейшей составляющей, обеспечивающей быстрое и эффективное выполнение всех задач предприятия. Однако вместе с их стремительным развитием, всё острее

с каждым годом чувствуется необходимость государства и бизнеса во введении большего количества мер, предупреждающих нанесение ущерба цифровой жизни экономических субъектов.

Информационная безопасность существует для разработки и реализации инструментов и мероприятий, которые впоследствии будут использованы для защиты информационных активов предприятия. Её главная цель - обеспечить безопасность и конфиденциальность важных для предприятия данных, отвечающих ряду критериев. Безусловно, инциденты безопасности с утечкой таких данных могут повлечь тяжкие финансовые и правовые последствия для предприятия, нарушить его рабочие процессы, нанести репутационный ущерб.

Говоря о рисках информационной и экономической безопасности, стоит указать, что поскольку потенциальные угрозы информации в организации могут быть крайне разнообразными и сложными, а также учитывая сам факт участия человека в технологическом процессе обработки информации, цели защиты могут быть достигнуты путем создания системы защиты информации на базе комплексного подхода. Сами же риски делятся на две основные категории:

1. Риски, связанные с утечкой информации, которая может быть использована конкурентами организации с целью нанести ущерб последней.

2. Риски, связанные с техническим сбоем функционирования непосредственно каналов передачи информации, способным приостановить нормальную деятельность предприятия на срок его устранения.

Главная же задача специалиста, осуществляющего деятельность в области противодействия угрозам информационной и экономической безопасности, является предупреждение информационных рисков путём ликвидации уязвимостей в цифровых системах предприятия.

Поскольку в 2023 году вопросы цифровизации экономической жизни бизнеса являются крайне актуальными для предпринимателей любых уровней, современная наука предлагает ряд методик управления рисками информационной безопасности, основанных на инновационных программных продуктах, применяющих средства построения и анализа бизнес-процессов. Предложенная в рамках исследования модель оценки уровня информационной безопасности конкретного предприятия, основанная на анализе рисков в данной сфере деятельности, представляет из себя процесс качественного и количественного измерения рисков, результатом которого является определение ряда наиболее опасных из них для организации.

Проблема информационной безопасности приобретает критическое значение в контексте современной цифровой экономики ввиду увеличения объемов циркулирующей информации, роста числа потенциальных угроз и повышения чувствительности данных. Надежность информационно-коммуникационных инфраструктур оказывает непосредственное влияние на экономическую устойчивость предприятий, уровень доверия контрагентов и потребителей, финансовое благополучие организаций и их конкурентные преимущества на рынках.

Применение риск-ориентированного подхода представляется наиболее эффективным инструментом снижения негативных последствий современных киберугроз. Данный подход основывается на комплексном анализе вероятностных характеристик возникновения угроз, прогнозировании возможного ущерба и выработке превентивных мер по минимизации рисков. Особенную значимость такой подход обретает в периоды повышенной нестабильности, обусловленной изменением внешней среды и кризисными явлениями в экономике [Моденов, Белякова, Власов, Лелявина, 2019].

Для точной оценки текущей ситуации в сфере информационной безопасности

рекомендуется применение специализированной математической модели. Данная модель позволяет проводить расчет интегральных показателей защищенности путем формализации факторов риска и формирования алгоритмов анализа. Полученные данные позволяют принимать рациональные управленческие решения касательно оптимизации инвестиций в средства защиты информации и распределять финансовые ресурсы в соответствии с установленными приоритетами. Итоговая интерпретация результатов моделирования отражает уровни риска и устанавливает предельные границы, превышение которых сигнализирует о необходимости экстренных корректирующих мероприятий.

Обеспечение надежной защиты корпоративных информационных активов возможно лишь посредством реализации комплексного подхода, охватывающего ряд направлений:

Интеграция новейших аппаратных и программных решений, направленных на предотвращение несанкционированного доступа, нейтрализацию попыток хищения данных и отражению хакерских атак.

Совершенствование процедур управления рисками через внедрение систем постоянного мониторинга угроз, своевременного выявления инцидентов, регулярного обновления элементов защитной инфраструктуры и проведения тренингов среди персонала по вопросам соблюдения норм цифровой гигиены [Усков, Харченко, 2025].

Периодический аудит действующих инструментов защиты и их модификация с учетом появления новых типов угроз, что способствует формированию многослойной защиты информационных ресурсов от широкого спектра рисков.

Заключение

Предприятия сталкиваются с необходимостью постоянной модернизации стратегии информационной безопасности вследствие трансформации цифровизированных экосистем и сопутствующих изменений ландшафта угроз. Возникающие технологические инновации открывают перспективные направления развития бизнеса, однако сопровождаются появлением специфичных рисков, связанных с недостаточно эффективной защитой используемых технологий и процессов. Следовательно, необходимым условием успешного функционирования является постоянное совершенствование стандартов информационной безопасности, адаптация регламентов и активизация внедрения актуальных методов контроля и защиты, обеспечивающих соответствие динамично развивающимся требованиям высокотехнологичного рынка и снижение вероятности наступления неблагоприятных событий.

Библиография

1. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х т. Угрозы, уязвимости, атаки и подходы к защите. — М.: Горячая линия-Телеком, 2018. — 536 с.
2. Андрианов, В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов. URL: https://econ.wikireading.ru/25722 (дата обращения: 18.05.2023).
3. Симонов С. Современные технологии анализа рисков в информа Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. – Москва : Общество с ограниченной ответственностью «Научно-издательский центр ИНФРА-М», 2021. – 216 с.
4. Кияев, В. Безопасность информационных систем : курс лекций / В. Кияев, О. Граничин. – Москва : Национальный открытый университет "ИНТУИТ", 2016. – 192 с.ционных системах. — М.: PCWEEK, – 2019. – С. 37.
5. Экономическая безопасность предприятия / А. К. Моденов, Е. И. Белякова, М. П. Власов, Т. А. Лелявина ; Министерство науки и высшего образования Российской Федерации, Санкт-Петербургский государственный

архитектурно-строительный университет. – Санкт-Петербург : Санкт- Петербургский государственный архитектурно-строительный университет, 2019. – 550 с.
6. Усков, В. В. Теоретические и правовые основы информационной безопасности как составной части системы экономической безопасности / В. В. Усков, О. В. Харченко // Право и государство: теория и практика. – 2025. – No 3. – С. 31-34.

Quantitative Assessment of Information Security in the Context of Digital Economy: Models and Methods

Anatolii K. Modenov

Doctor of Economic Sciences, Professor,
Saint Petersburg State University of Architecture and Civil Engineering,
190005, 4 2-ya Krasnoarmeyskaya str., Saint Petersburg, Russian Federation;
e-mail: modenov200459@mail.ru

Vladislav V. Uskov

PhD in Economic Sciences, Associate Professor,
Saint Petersburg State University of Architecture and Civil Engineering,
190005, 4 2-ya Krasnoarmeyskaya str., Saint Petersburg, Russian Federation;
e-mail: vladuskov@yandex.ru

Abstract

In the context of digital transformation of the economy, information security assessment becomes critically important for ensuring economic security of enterprises. The article examines various methods of information security assessment, including benchmark assessment, risk-oriented assessment, and assessment based on economic indicators. Special attention is paid to the risk-oriented approach, which allows identifying and preventing potential threats before they occur. A mathematical model for quantitative assessment of information security is proposed, including calculation of risk impact, potential risk, and probability of its occurrence. The model allows determining minimum and maximum acceptable risk levels, which is an important tool for managing information security in conditions of unstable economic situation. In conclusion, the necessity of a comprehensive approach to protecting information assets and implementing innovative technologies is emphasized.

For citation

Modenov A.K., Uskov V.V. (2025) Kolichestvennaya otsenka informatsionnoy bezopasnosti v usloviyakh tsifrovoy ekonomiki: modeli i metody [Quantitative Assessment of Information Security in the Context of Digital Economy: Models and Methods]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (8A), pp. 318-325. DOI: 10.34670/AR.2025.22.28.033

Keywords

Information security, risk-oriented approach, digital economy, quantitative assessment, risk management, cybersecurity, data protection, economic security.

References

1. Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I., Ushakov D. V. Information security of open systems. In 2 volumes. Threats, vulnerabilities, attacks and approaches to protection. Moscow: Hotline-Telecom, 2018. 536 p.
2. Andrianov, V. V. Ensuring information security of business / V. V. Andrianov. URL: https://econ.wikireading.ru/25722 (date of request: 05/18/2023).
3. Simonov S. Modern technologies of risk analysis in information Grishina, N. V. Fundamentals of enterprise information security : a textbook / N. V. Grishina. – Moscow : Limited Liability Company "Scientific Publishing Center INFRA-M", 2021. – 216 p.
4. Kiyaev, V. Information systems security : a course of lectures / V. Kiyaev, O. Borichin. Moscow : National Open University "INTUIT", 2016. 192 p. in systems. Moscow: PCWEEK, 2019. p. 37.
5. Economic security of the enterprise / A. K. Modenov, E. I. Belyakova, M. P. Vlasov, T. A. Lelyavina ; Ministry of Science and Higher Education of the Russian Federation, St. Petersburg State University of Architecture and Civil Engineering. Saint Petersburg : Saint Petersburg State University of Architecture and Civil Engineering, 2019. 550 p.
6. Uskov, V. V. Theoretical and legal foundations of information security as an integral part of the economic security system / V. V. Uskov, O. V. Kharchenko // Law and the State: theory and practice. - 2025. – No. 3. – pp. 31-34.