

Цифровизация как инструмент экономической безопасности современной организации

Свистунов Василий Михайлович

Д-р экон. наук, проф. каф. управления персоналом
ORCID: 0000-0001-8303-9899, e-mail: svistunov@guu.ru

Агеева Ольга Андреевна

Д-р экон. наук, проф. каф. бухгалтерского учета, аудита и налогообложения
ORCID: 0000-0002-8772-1702, e-mail: oa_ageeva@guu.ru

Мацкуляк Иван Дмитриевич

Д-р экон. наук, проф. каф. экономической политики и экономических измерений
ORCID: 0000-0002-2550-0250, e-mail: mid48@mail.ru

Государственный университет управления, г. Москва, Россия

Аннотация

В работе рассматривается роль цифровых технологий и ИТ-инструментов (ИТ – информационные технологии) в обеспечении экономической безопасности современной организации. Анализируется влияние процессов глобализации и усиления конкуренции на необходимость внедрения современных цифровых решений для управления хозяйственной деятельностью и оценки законности бизнес-процессов. Обосновывается важность цифровизации для повышения скорости, точности и надежности работы системы экономической безопасности, а также для противодействия внешним угрозам и реализации корпоративных интересов. Подчеркивается значимость комплексного подхода к внедрению цифровых технологий и создания единой системы цифровой экономической безопасности организации. На основе опроса экспертов из различных промышленных предприятий выявлены наиболее перспективные цифровые инструменты и технологии для ее обеспечения в ближайшие 5 лет. Проблемная область работы – цифровые технологии и ИТ-инструменты, используемые для повышения уровня обеспечения экономической безопасности организации в условиях цифровой трансформации. Цель исследования заключается в определении существующих подходов к практическому использованию последних как важного элемента системы внутреннего контроля, обеспечивающей экономическую безопасность хозяйствующего субъекта. Основные результаты исследования могут быть применены на практике при решении кейсов и управленческих задач на уровне руководителей компании, государственных учреждений, а также включены в программу при изучении курса «Экономическая безопасность».

Ключевые слова

Экономическая безопасность, цифровизация, цифровые технологии, ИТ-инструменты, искусственный интеллект, автоматизация, управление рисками

Для цитирования: Свистунов В.М., Агеева О.А., Мацкуляк И.Д. Цифровизация как инструмент экономической безопасности современной организации // Вестник университета. 2025. № 5. С. 15–27.

© Свистунов В.М., Агеева О.А., Мацкуляк И.Д., 2025.

Статья доступна по лицензии Creative Commons “Attribution” («Атрибуция») 4.0. всемирная (<http://creativecommons.org/licenses/by/4.0/>).



Digitalisation as a tool for economic security of a modern organisation

Vasily M. Svistunov

Dr. Sci. (Econ.), Prof. at the Personnel Management Department
ORCID: 0000-0001-8303-9899, e-mail: svistunov@guu.ru

Olga A. Ageeva

Dr. Sci. (Econ.), Prof. at the Accounting, Audit, and Taxation Department
ORCID: 0000-0002-8772-1702, e-mail: oa_ageeva@guu.ru

Ivan D. Matskulyak

Dr. Sci. (Econ.), Prof. at the Economic Policy and Economic Measurements Department
ORCID: 0000-0002-2550-0250, e-mail: mid48@mail.ru

State University of Management, Moscow, Russia

Abstract

The article examines the role of digital technologies and IT (information technologies) tools in ensuring economic security of a modern organisation. We analyse the impact of globalisation and increased competition on the need to implement modern digital solutions for managing economic activities and assessing the legality of business processes. The authors substantiate the importance of digitalisation for improving the speed, accuracy, and reliability of the economic security system as well as for countering external threats and realising corporate interests. The significance of an integrated approach to the implementation of the digital technologies and creation of a unified digital economic security system for the organisation is emphasised. Based on a survey of experts from various industrial enterprises, the most promising digital tools and technologies for its insurance in the next five years are identified. The problematic area of the article is digital technologies and IT tools used to improve the level of economic security of an organisation in the context of digital transformation. The purpose of the study is to identify the existing approaches to the practical use of them as an important element of the internal control system that ensures the economic security of a business entity. The main results of the can be applied in practice when solving case studies and management tasks at the level of company leaders, government institutions, and can also be included in the programme when studying the course “Economic security”.

Keywords

Economic security, digitalisation, digital technologies, IT-tools, artificial intelligence, automation, risk management

For citation: Svistunov V.M., Ageeva O.A., Matskulyak I.D. (2025) Digitalisation as a tool for economic security of a modern organisation. *Vestnik universiteta*, no. 5, pp. 15–27.

ВВЕДЕНИЕ

Процессы глобализации, наиболее активно протекающие в экономике и политике, сопровождаются быстрой изменчивостью внешней среды хозяйствования и постоянно растущим уровнем конкурентной борьбы, участниками которой являются большинство предприятий и организаций. Важные условия успешной конкурентной борьбы – не только разработка эффективной корпоративной стратегии, но и организация и реализация практических мероприятий, обеспечивающих экономическую безопасность предприятия. В их числе совокупность мер, реализуемых на основе использования современных цифровых технологий как эффективного инструмента управления хозяйственной деятельностью, осуществляемой экономическим субъектом. Данный подход не только позволяет результативно управлять качественной оценкой законности ключевых фактов хозяйственной деятельности и осуществлять ее, но и решает важную задачу – способствует повышению экономической безопасности хозяйствующего субъекта за счет автоматизации широкого спектра выполняемых работ. Использование таких технологий, как искусственный интеллект (англ. artificial intelligence), распределенные базы данных, автоматизированные системы управления аудитом и контролем, интерактивные дашборды, интернет вещей (англ. internet of things), мобильные приложения, криптографические методы защиты данных и др., позволяет снизить экономические и управленческие риски, обеспечить эффективный и результативный контроль по отношению к протекающим и уже реализованным в организации бизнес-процессам.

Цифровизация процессов, обеспечивающих слаженную работу всех элементов системы экономической безопасности современной организации, важна. Выполняемые работы, направленные на соответствие предприятия всей совокупности требований законодательства Российской Федерации (далее – РФ, Россия), реализуемым внутренним политикам (финансовой, организационной, экономической, кадровой, социальной, информационной, научно-технической и т.д.), регламентам и внутренним правилам, требуют высокой скорости сбора и обработки исходной информации; точности и качества формируемых итоговых результатов; надежного информационного обеспечения и сопровождения. Традиционные методы обеспечения эффективности системы экономической безопасности организации (далее – ЭБО) сегодня далеко не всегда результативны. Цифровые инструменты призваны помочь решить указанную задачу за счет:

- существенного увеличения скорости выполнения рабочих процедур и повышения их качества (возможность анализа большого объема исходной и промежуточной информации; выявление потенциальных рисков и проблемных ситуаций и своевременное предупреждение их; подготовка промежуточных и итоговых отчетов в автоматизированном режиме);
- повышения точности и достоверности информационного обеспечения решаемых управленческих и производственно-технологических задач (сбор, обработка, хранение и передача информации в автоматизированном режиме; снижение количества ошибок, имеющих место в случае использования ручного ввода и обработки данных);
- увеличения полноты и точности формируемой информации и повышения наглядности ее представления (визуализация формируемых результирующих данных);
- сокращения внутренних издержек на выполнение работ в автоматизированном режиме (обеспечивается меньшим объемом ручного труда, высвобождением части персонала и снижением затрат на него, возможностью максимально удобного и быстрого доступа к требуемой информации, сокращением общего времени на выполнение рабочих задач);
- ускоренной и адекватной реакции на потенциальные риски и возможные проблемные ситуации, связанные с различными видами нарушений и неэффективными действиями сотрудников;
- улучшения большинства видов внутрикорпоративной коммуникации и взаимодействия с внешней средой (быстрые и надежные каналы обмена информацией и документами; эффективное межличностное и командное взаимодействие).

Среди отечественных и зарубежных ученых и практиков достаточно много трудов, рассматривающих проблемы развития взаимосвязей экономической безопасности и процессов цифровизации экономики, особенностей влияния цифровых технологий и ИИ, среди которых можно выделить научные работы О.А. Агеевой [1], Ю.П. Доронина [2], А.Н. Щапова [3], С.Р. Абрамовой [4], А.И. Юрченко [5], Д.Ю. Десятниченко [6], Т.В. Погодиной [7], А.Д. Шеремет [8], В.А. Шульца [9], Ю.Г. Графова [10],

В.В. Година [11], А.А. Докукиной [12], Р.С. Близкого [13], Т.М. Рогуленко [14] и др. При этом остаются вопросы и проблемы, требующие детализации решений в современных условиях.

Таким образом, цифровые инструменты являются важным элементом ЭБО, поскольку способствуют эффективному решению задач своевременного обнаружения имеющихся текущих и итоговых отклонений от запланированных параметров функционирования организации, их фиксирования и анализа возможных финансовых, экологических, экономических, кадровых, социальных и иных последствий. Приоритет современных цифровых инструментов, по сравнению с другими технологическими инструментами, состоит в том, что они способны обеспечить непосредственное, в режиме реального времени, взаимодействие всех элементов ЭБО, выполняя как функцию информационного обеспечения, так и функцию контроля за эффективностью и результативностью деятельности хозяйствующего субъекта.

ОБЗОР ЛИТЕРАТУРЫ

Термин «безопасность» не следует относить к числу недавно появившихся. По мнению В.И. Даля, это «отсутствие опасности; сохранность, надежность»¹. С.И. Ожегов в «Словаре русского языка» под безопасностью понимает «положение, при котором не угрожает опасность кому-либо или чему-либо»². В Федеральном законе РФ «О безопасности» термин трактуется как «состояние защищенности жизненно принципиальных интересов личности, общества и государства от внутренних и внешних угроз. Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможность прогрессивного развития личности, общества и государства. К основным объектам безопасности относятся личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная целостность»³.

Анализ представленных мнений и положений дает основание сделать вывод о том, что термин используется для описания характеристики состояния защищенности какого-либо субъекта/объекта от воздействия определенных, как правило, внешних и внутренних, угроз или субъекта/объекта. Применяя структурный подход, безопасность следует понимать как инструмент предупреждения или разрешения противоречий интересов, которые потенциально могут возникнуть или возникли в системе отношений «человек – организация – общество – государство». Они значительно реже проявляются в условиях определенности или стабильности развития внешней и внутренней среды. В условиях неопределенности и риска существенно возрастает вероятность возникновения противоречий у двух или более участников системы.

Большое количество ученых уделяет внимание изучению проблемы безопасности такого субъекта, как государство, и выделяет следующие виды безопасности: техническая, военная, информационная, продовольственная, экономическая, экологическая. Большинство экспертов считают основополагающим видом экономическую безопасность, являющейся фундаментом, на котором выстроены политический и правовой общественные институты [2; 4].

Структурно экономическая безопасность государства включает в себя следующие основные элементы: контроль, сохранение и преумножение национального благосостояния и ресурсов; экономическую независимость, способствующую взаимовыгодному участию в международных экономических отношениях; устойчивость и стабильность национальной экономики, предполагающие защиту существующих форм собственности; способность к прогрессу и саморазвитию, подтверждаемые созданием необходимых условий для активной модернизации производства, осуществления инновационной и инвестиционной политик и стратегий, для повышения профессионально-образовательного уровня работников.

К числу основных характеристик экономической безопасности государства, по мнению экспертного сообщества, следует отнести наличие технологий и возможностей, обеспечивающих максимально эффективное использование национальных ресурсов и контроль над ними. Указанные технологии призваны предотвратить нерациональное использование природных и иных видов ресурсов, что может нанести непоправимый ущерб национальным интересам. Такой подход призван обеспечить постоянное развитие государства как в настоящем, так и в будущем, а меры экономической безопасности не только служат гарантом государственной независимости, но и обеспечивают стабильность и эффективность жизни общества [5; 7].

¹ Толковый словарь живого великорусского языка В.И. Даля. Безопасный. Режим доступа: <https://gufo.me/dict/dal/безопасный> (дата обращения: 05.03.2025).

² Словарь русского языка С.И. Ожегова. Безопасный. Режим доступа: <https://gufo.me/dict/ozhegov/безопасный> (дата обращения: 05.03.2025).

³ Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности». Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 05.03.2025).

В условиях обострения конкурентной борьбы важным уровнем национальной системы экономической безопасности становится экономическая безопасность отдельных организаций, являющихся экономическими агентами рынка, которая во многом определяет их экономическую состоятельность и успешность.

Проблемам последней уделяет внимание большое количество ученых, делающих акценты на аналитике целей и содержания данного процесса. Все исследователи в общем сходятся во мнении относительно ключевых из них:

- 1) управляемая система, имеющая цель и задачи [3; 9; 10];
- 2) определенное состояние, обеспечивающее достижение конкретных целей [8; 9];
- 3) целевая направленность – обеспечение защиты, устойчивости, выживаемости и развития организации [9–11];
- 4) цели достигаются реализацией совокупности различных мер [6–8];
- 5) выбор реализуемой меры определяется характером внутренней или внешней угрозы, воздействия [9–11];
- 6) меры должны обеспечить устойчивую работу организации на длительный период времени [4; 11].

Анализ авторских мнений дает основание сделать вывод о том, что собой представляет ЭБО. Во-первых, это управляемая система, имеющая конкретные цель и задачи или определенное состояние, характеризующее достигнутый уровень реализации цели, решения ранее сформулированных задач. Во-вторых, указанная система призвана при эффективном использовании всех необходимых видов ресурсов обеспечить защиту, устойчивость, выживаемость и развитие организации в длительной перспективе путем разработки и реализации совокупности практических мер, нейтрализующих или ликвидирующих последствия внутренних и внешних угроз.

На практике должны учитываться уникальность каждой организации и ее отличительные особенности. Такой подход свидетельствует о том, что при относительно общих для большинства предприятий структурах систем корпоративного управления и экономической безопасности в каждом отдельном случае во внимание должны быть приняты специфичные черты и особенности, характерные для конкретного объекта хозяйствования.

Проведенный анализ авторских позиций свидетельствует о том, что экспертное сообщество не уделяет должного внимания анализу роли и специфике использования цифровых инструментов в процессах обеспечения экономической безопасности современной организации. При этом вполне очевидно, что цифровая трансформация экономики уже давно предопределила необходимость перехода от традиционной модели функционирования организации к цифровой. Отличительные особенности последней – цифровой формат разработки и реализации решений, принимаемых на всех уровнях управления, и использование сквозных цифровых технологий для решения задач во всех сферах деятельности предприятия. Переход к цифровой модели делает очень важным параметром экономической безопасности цифровую устойчивость организации [12]. Под цифровой устойчивостью следует понимать совокупность скоординированных практических мер, реализация которых призвана обеспечить внедрение необходимых цифровых инструментов; адаптацию в организационно-производственной корпоративной среде с учетом всего спектра возможных внешних возмущающих воздействий; последующее использование для достижения сформулированных стратегических целей и требуемого уровня экономической безопасности.

Цифровая устойчивость должна быть ориентирована на устойчивое развитие организации за счет реализации:

- уже имеющегося конкурентного преимущества, являющегося следствием его нецифровых возможностей;
- вновь сформированного конкурентного преимущества, выступающего следствием качественной трансформации бизнес-процессов на новой цифровой основе.

В табл. 1 приведены цифровые инструменты и технологии, широко применяемые сегодня при решении задачи повышения ЭБО.

**Цифровые инструменты и технологии, применяемые при решении задачи
повышения экономической безопасности современной организации**

Цифровые инструменты и технологии	Характеристика и особенности практического применения
SIEM-системы	SIEM (англ. security information and event management) – системы сбора информации о безопасности организации и управления ею. Представляют собой системы специализированного ПО, назначением которого являются сбор, агрегирование и систематизация всей информации, что может быть использовано для оценки текущего и перспективного уровней безопасности организации; анализ собранных данных; формирование сообщений об отклонениях, ошибках, несанкционированных попытках проникновения в защищенные информационные массивы
DLP-системы	DLP (англ. data leak prevention) – специализированное ПО, разработанное на основе алгоритмов, призванных обеспечить надежную защиту корпоративной информации от возможных утечек и краж. Дополнительный функционал предоставляет возможность блокировать несанкционированную передачу конфиденциальной или иной информации с использованием корпоративных и иных информационных каналов; проводить мониторинг поведения сотрудников в корпоративном информационном пространстве и др.
Цифровые средства защиты данных	Цифровые средства защиты данных – специальные программные средства шифрования данных в целях защиты конфиденциальной финансово-экономической, управленческой, производственно-технической или иной информации организации от несанкционированного внешнего или внутреннего доступа и использования. Применяемое ПО способно обнаружить сотрудника (рабочее место), предпринимающего попытку несанкционированного доступа к закрытой части корпоративной информационной системы
Корпоративные антивирусы	Специализированное ПО, гарантирующее защиту всех видов корпоративной информации и цифрового оборудования (ресурсов) от вредоносного или шпионского ПО, используемого при вирусных угрозах и кибер-атаках
Системы анализа данных	Назначение систем анализа данных – проведение анализа корпоративных информационных массивов, отличающихся большим объемом данных, с целью поиска и обнаружения явных и скрытых зависимостей и тенденций. Использование цифровых инструментов и технологий способствует повышению качества итоговых данных, включая более точную вероятностную оценку определения потенциальных рисков в сфере экономической безопасности организации
Облачные технологии	Облачные технологии предполагают использование удаленных серверов как физического места хранения соответствующей корпоративной информации. Такой подход позволяет не только упростить доступ к данным, но и существенно ускорить процессы информационного обмена и повысить уровень информационной безопасности
Интерактивные дашборды	Интерактивные дашборды – специализированное ПО, назначением которого является представление по информационному запросу соответствующих результатов данных в режиме реального времени и в максимально удобной и наглядной с точки зрения визуализации форме
Роботизированные процессы	RPA (англ. robotic process automation) – цифровая технология, назначением которой является автоматизация рутинных задач на основе разработки специализированного ПО. Представляет собой цифровую систему, имитирующую действия сотрудника, выполняемые при документационном обслуживании таких процессов, как проверка документов и заполнение отчетов

Цифровые инструменты и технологии	Характеристика и особенности практического применения
Системы ИИ	Использование систем ИИ призвано существенно повысить эффективность и точность выполнения расчетных и аналитических процедур, включая автоматическое выявление отклонений в работе финансово-экономических структурных подразделений организации. Выявление отклонений позволит оперативно реагировать на соответствующую проблемную ситуацию, улучшая качество процесса управления, в частности, ЭБО
Интернет вещей	Интернет вещей – технология, позволяющая собирать данные с различных устройств, которые используются для дальнейшего агрегирования, анализа или контроля
Автоматизированные системы управления аудитом и контролем	Автоматизированные системы управления аудитом и контролем – системы автоматизированного планирования, выполнения расчетных процедур, анализа промежуточных и итоговых результатов, формирования отчетности по итогам проведения мероприятий внутреннего аудита и контроля в организации
Электронные подписи и удостоверение личности	Назначение – упрощение процессов и повышение уровня безопасности документационного обеспечения управленческой деятельности за счет использования специальных программных средств, позволяющих удостоверить личность сотрудника и подписывать документы в электронном виде
Мобильные приложения	Мобильные приложения – цифровые решения, позволяющие ответственному должностному лицу находиться в постоянном контакте с системой безопасности организации, а также получать актуальную информацию в режиме реального времени
Распределенные базы данных	Распределенная база данных, или технология блокчейн, – программно защищенная от несанкционированного внешнего доступа история финансовых транзакций, выполненных участниками системы со своими активами

Примечание: ПО – программное обеспечение

Составлено авторами по материалам источников [4; 6; 8; 11; 12]

Ключевые составляющие цифровой устойчивости организации – возможность управления угрозами экономической безопасности и сокращение негативного влияния всех видов рисков и иных возмущающих воздействий. Данный подход позволяет говорить о том, что уровень цифровой устойчивости во многом определяется широтой использования различных цифровых инструментов, способных существенно повысить ЭБО.

МЕТОДОЛОГИЯ

Отечественными компаниями, несомненно, накоплен опыт практического использования цифровых инструментов и технологий при решении задач повышения ЭБО. Обобщение применения и анализ накопленного опыта представляют как теоретический, так и практический интерес, поскольку позволяют установить перечень наиболее эффективных и перспективных цифровых решений в сфере ЭБО.

В ноябре-декабре 2024 г. авторами статьи было проведено исследование, целью которого стало определение приоритетных цифровых инструментов и технологий исходя из анализа практического опыта их внедрения и применения в системах ЭБО, накопленного отечественными компаниями. Под ними авторы понимают совокупность цифровых инструментов и технологий, подлежащих первоочередному приобретению (разработке) и последующему практическому использованию, поскольку именно они способны не только повысить контроль над реализуемыми бизнес-процессами, но и обеспечить существенное повышение ЭБО.

В рамках проведенной работы были собраны исходные данные, представленные мнениями членов экспертной группы, в которую вошли представители предприятий промышленного сектора экономики России из 5 регионов: Москвы, Московской и Калужской областей, Тулы и Казани. В исследовании приняли участие эксперты, представляющие организации, которые активно внедряют или уже используют различные цифровые решения в целях обеспечения экономической безопасности своих предприятий.

В ходе исследования проведено интервьюирование экспертов с постановкой открытых вопросов. Цель проведения интервью – выявление мнений и оценочных суждений каждого из специалистов по отношению к предложенному перечню цифровых инструментов и технологий, которые способны повысить ЭБО и могут быть актуальны для российских организаций в ближайшие 5 лет. Каждый эксперт, представляющий конкретное промышленное предприятие:

- 1) предложил собственный ранжированный перечень перспективных цифровых инструментов и технологий в рамках формулирования ответов на поставленные в исходной анкете вопросы, опираясь на свое видение будущего;
- 2) ранжировал, опираясь на свои профессиональные знания и опыт, данный перечень, сформированный после обобщения мнения всех экспертов, принявших участие в опросе.

Результаты анкетирования содержат открытые высказывания экспертов, обладающих практическим опытом использования цифровых инструментов и технологий в целях обеспечения ЭБО. Большинство специалистов используют цифровой функционал в практике своей повседневной профессиональной деятельности.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ОБСУЖДЕНИЕ

Анализируя причины активного роста цифровых технологий и ИТ-инструментов (ИТ – информационные технологии) следует отметить, что одна из причин состоит в их возможностях обеспечить надлежащий уровень экономической безопасности современных организаций. Все большее число отечественных и зарубежных компаний ощущает активные внешние воздействия, направленные на причинение экономического и информационного ущерба деятельности хозяйствующего субъекта. В этих условиях менеджмент компаний должен обладать надежными инструментами, способными противостоять внешним угрозам путем быстрой и адекватной ответной реакции, обеспечивающей полноценную реализацию корпоративных коммерческих интересов и целей уставной деятельности.

Не только сохранение, но и повышение ЭБО в условиях быстро растущего числа возмущающих воздействий следует отметить как важные особенности, которыми обладают цифровые технологии и ИТ-инструменты. Эксперты все чаще отмечают возможность использования ИИ, который успешно встраивается и дополняет функционал цифровых технологий, уже применяемых при решении задачи повышения ЭБО. ИИ способен обеспечить большую предсказуемость результата решения данной задачи; существенно снизить затраты на ее реализацию; предоставить менеджменту компании возможность оперативной корректировки соответствующих бизнес-процессов в ответ на возмущающее внешнее воздействие.

Технология фрагментарного или несистемного использования цифровых технологий и ИТ-инструментов уже не способна обеспечить надлежащий уровень ЭБО и часто не может сформировать быстрый и адекватный ответ на соответствующую внешнюю угрозу. Сегодня ключевым трендом использования цифровых технологий и ИТ-инструментов экономической безопасности является стремление к созданию единой системы цифровой ЭБО. Единая цифровая система предполагает одновременное применение нескольких технологий и инструментов, функционально дополняющих и расширяющих возможности повышения уровня экономической безопасности хозяйствующего субъекта. Однако следует отметить ее следующие недостатки: высокая стоимость разработки собственной системы или приобретения готового программного решения; существенные эксплуатационные затраты, включая затраты на своевременное обновление программного продукта. Это делает ее доступной, как правило, только для крупных компаний.

Результаты проведенного анализа дают основание сформулировать следующие выводы.

1. Базовые современные тенденции в области использования цифровых технологий и ИТ-инструментов для обеспечения экономической безопасности хозяйствующих субъектов следующие: локальные цифровые решения широко применяются малым и средним бизнесом; многофункциональные цифровые решения с возможностью интеграции в цифровую корпоративную среду доступны для крупных организаций.

2. Активное использование менеджментом отечественных компаний цифровых технологий и ИТ-инструментов свидетельствует о востребованности их информационных, в том числе защитных, и технологических возможностей.

3. Современные цифровые решения с точки зрения разработки и использования все чаще базируются на принципе комплексности. Данный принцип, предполагающий интегрированные варианты разработки и применения цифровых технологий и ИТ-инструментов, способствует растущему к ним интересу со стороны хозяйствующих субъектов, решающих проблему обеспечения собственной экономической безопасности.

Принимая во внимание высокий интерес практиков к возможностям цифровых технологий и инструментов существенно повлиять на эффективность системы ЭБО, отметим, что закономерным является формирование перечня наиболее приоритетных из них. Такой перечень может и должен стать основой цифровой трансформации системы ЭБО, вставших на данный путь или собирающихся это сделать. При проведении исследования была сформулирована следующая задача – опираясь на мнение практикующих экспертов и исходя из пятилетнего стратегического горизонта, определить 5 приоритетных цифровых инструментов и технологий. К участию в исследовании были приглашены эксперты, представляющие 15 отечественных промышленных предприятий.

Общая численность экспертов составила 238 чел., из них 8 % женщин и 92 % мужчин. Средний возраст – 48 лет, возрастной диапазон – от 26 до 64 лет. Эксперты, принявшие участие в исследовании, предварительно были разделены на четыре группы. В первую вошли директора предприятий и их заместители, отвечающие за ИТ- и экономическую сферы; вторая была представлена руководителями функциональных отделов и служб предприятий; третья экспертная группа объединила линейных руководителей; четвертая – специалистов, принимающих участие в процессах цифровой трансформации своих организаций на уровне проектных мероприятий, обеспечивающих автоматизацию соответствующих корпоративных бизнес-процессов. От общего числа количество экспертов первой группы составило 10 % (24 чел.), второй – 25,6 % (61 чел.), третьей – 37,4 % (89 чел.), четвертой – 27 % (64 чел.). В выборке из числа экспертов, вошедших в четвертую группу, 67,2 % (43 чел.) составили люди, принимавшие активное участие в процессах внедрения проектных решений по автоматизации корпоративных бизнес-процессов; 32,8 % (21 чел.) используют в своей повседневной практике цифровые инструменты и технологии, в частности, в целях обеспечения экономической безопасности своих предприятий.

В целях сбора исходной информации в каждой из четырех сформированных групп экспертов было проведено анкетирование, носившее анонимный характер. Каждому из экспертов, принявших участие в анкетировании, было предложено определить три наиболее перспективные цифровые технологии и ИТ-инструменты, способные сыграть ключевую роль в повышении ЭБО в ближайшие 5 лет. При формировании своей точки зрения специалистам полагалось опираться исключительно на собственные критерии, профессиональные знания и практический опыт проектирования, внедрения и эксплуатации цифровых средств при реализации общих и функциональных бизнес-процессов, включая процессы обеспечения экономической безопасности предприятия. После этого эксперты должны были провести ранжирование среди предложенных перспективных цифровых технологий и ИТ-инструментов, расположив их в порядке приоритетности.

Общим итогом проведенного анкетирования экспертов, с учетом значительного числа непосредственных повторений, стал перечень из 27 перспективных цифровых технологий и ИТ-инструментов, практика использования которых способна положительно сказаться на динамике уровня экономической эффективности современной организации на стратегическом горизонте, не превышающем 5 лет. Из указанного перечня отобрано 14 технологий и инструментов, наиболее часто отмечавшихся экспертами. На следующем этапе исследования по отношению к перечню специалистам было предложено провести процедуру итогового ранжирования. В рамках данной процедуры каждый эксперт наиболее перспективную цифровую технологию или ИТ-инструмент располагал на 1-м месте формируемого им ранжированного списка. Те из них, что обладали наименьшим приоритетом, по мнению специалиста, соответственно, располагались на 14-м месте списка. Результаты итоговой экспертизы представлены в табл. 2.

Результаты проведенного исследования свидетельствуют о наличии различных мнений среди групп отечественных экспертов о наиболее перспективных цифровых инструментах и технологиях обеспечения ЭБО. Так, руководители предприятий, входящие в первую группу, отдают предпочтение инструментам и технологиям, способным обеспечить успешное решение поставленной задачи на корпоративном уровне. Эксперты, входящие в другие группы, наиболее перспективными и востребованными из них считают те, что способны гарантировать как качественную автоматизацию осуществляемого бизнес-процесса, так и реализацию цифровых процедур по надежной защите используемых и вновь формируемых данных.

Тенденцию выбора направления автоматизации в пользу цифровых средств защиты данных следует считать современной и оправданной. Эксперты трех из четырех групп поставили этот ИТ-инструмент

на 1-е место в списке своих предпочтений. Только эксперты второй группы, руководители функциональных отделов и служб предприятий, считают более приоритетным использование SIEM-систем, отдав им предпочтение перед цифровыми средствами защиты корпоративных данных.

Таблица 2

Прогнозный результат экспертной оценки перспективных цифровых технологий и ИТ-инструментов, способных влиять на повышение ЭБО

Группа экспертов	Цифровые технологии и ИТ-инструменты													
	SIEM-системы	DLP-системы	Цифровые средства защиты данных	Корпоративные антивирусы	Системы анализа данных	Облачные технологии	Интерактивные дашборды	RPA	Системы ИИ	Интернет вещей	Автоматизированные системы управления аудитом и контролем	Электронные подписи и удостоверения личности	Мобильные приложения	Распределенные базы данных
Первая	3	4	1	7	6	10	9	8	13	14	2	5	11	12
Вторая	3	4	2	7	5	12	6	9	10	14	3	12	11	8
Третья	2	4	1	9	3	8	10	11	7	14	5	13	6	12
Четвертая	2	8	1	7	5	10	12	9	6	13	3	14	4	11
Итоговые приоритеты	2	5	1	6–7	4	6–7	11–12	11–12	9–10	9–10	3	14	8	13

Примечание: количество технологий, которые используются в группах.

Составлено авторами по материалам исследования

В табл. 3 представлены результаты анализа основных преимуществ и недостатков, свойственных цифровым средствам защиты данных, базой которых являются специальные алгоритмы.

Таблица 3

Преимущества и недостатки цифровых средств защиты корпоративных данных

Преимущества	Характеристика базовых алгоритмов	Недостатки	Ключевые особенности
Обеспечение надлежащего уровня конфиденциальности	Алгоритмы кодирования данных; алгоритмы обеспечения доступа к данным только авторизованных пользователей с использованием индивидуального ключа	Высокая стоимость автоматизации средств защиты информации	Чем выше уровень защиты корпоративных данных, тем более высоки затраты на приобретение (разработку) средств защиты и их эксплуатацию
Обеспечение целостности данных	Алгоритмы защиты данных от несанкционированного изменения	Сложность алгоритмов кодирования данных	У компании есть вычислительные ресурсы большой мощности

Преимущества	Характеристика базовых алгоритмов	Недостатки	Ключевые особенности
Персонализация	Алгоритмы адаптации мер безопасности с учетом потребностей конкретного пользователя	Высокая вероятность ошибки в базовом алгоритме или использовании ПО	Ошибка кодирования способна сделать информацию уязвимой с точки зрения безопасности
Прогнозная аналитика	Алгоритмы выявления потенциальных угроз безопасности данных; алгоритмы предотвращения утечек данных	Сложность управления ключами доступа	Следствием ошибки управления ключами доступа является повышение уровня уязвимости к внешним атакам
Репликация	Алгоритм непрерывного копирования данных, поддерживающий и сохраняющий их актуальную копию	Автоматизированный контроль	Наличие ошибки в исходном алгоритме повышает уровень уязвимости к внешним атакам
Очистка данных	Алгоритм удаления данных, потерявших свою актуальность	Проблемы с обновлением ПО	Своевременное обновление ПО – гарантия требуемого уровня защиты и сохранения корпоративных данных

Составлено авторами по материалам источников [11; 13; 14]

Защита данных с помощью цифровых средств в любой отрасли и сфере сегодня весьма актуальна. При этом чем больше сотрудников работает в компании, тем сложнее и важнее отслеживать их действия. В этом случае работает следующее правило: чем крупнее предприятие, тем более важно и трудно решить задачу обеспечения ЭБО. Средства защиты данных базируются на использовании специальных программных средств, обеспечивающих требуемый уровень защиты информации, имеющей коммерческую ценность или являющейся конфиденциальной.

ЗАКЛЮЧЕНИЕ

Результатом проведенного исследования явилось формирование перечня наиболее перспективных цифровых технологий и ИТ-инструментов, которые способны выполнять ключевую роль в решении проблемы повышения ЭБО в ближайшие 5 лет в отечественных компаниях. Разработанный на основе мнения экспертов, принявших участие в проведенном исследовании, перечень цифровых технологий и ИТ-инструментов следующий: приоритет 1 – цифровые средства защиты данных, приоритет 2 – SIEM-системы, приоритет 3 – автоматизированные системы управления аудитом, приоритет 4 – системы анализа данных и приоритет 5 – DLP-системы.

Перечень, приведенный в табл. 4, может быть полезен руководителям и специалистам, которые разрабатывают стратегию внедрения и практического использования цифровых технологий и ИТ-инструментов, решая задачу повышения уровня ЭБО. Результаты, полученные в ходе проведенного исследования, дают основание сделать вывод, что эксперты склоняются к мнению о необходимости первоочередного внимания к внедрению цифровых технологий и ИТ-инструментов, обеспечивающих надежную защиту корпоративных данных в реальном масштабе времени в рамках взаимодействия участников системы «бизнес-процесс – ЭБО». Они, по мнению экспертов, способны в пятилетней перспективе обеспечить не только сохранение уже достигнутого уровня экономической безопасности отечественных организаций, но и способствовать его значительному росту.

Цифровые технологии и ИТ-инструменты находят все большее распространение при решении всего комплекса задач, стоящего перед менеджментом современной организации, и не наблюдается каких-либо факторов, способных остановить или изменить данную тенденцию. Для решения задачи обеспечения надлежащего уровня своей экономической безопасности данные технологии и инструменты

сегодня наиболее активно используют преимущественно крупные компании. Однако нет сомнений в том, что в ближайшей перспективе к их возможностям будет привлечено внимание большего числа отечественных организаций.

Список литературы

1. Агеева О.А., Матыцына Ю.Д. Мониторинг эффективности системы внутреннего контроля и экономической безопасности организации. Вестник университета. 2022;1:70–77. <https://doi.org/10.26425/1816-4277-2022-1-70-77>
2. Доронин Ю.П. Экономическая безопасность как один из стратегических национальных приоритетов Российской Федерации. Евразийский юридический журнал. 2023;4(179):498–500.
3. Щапов А.Н. Система показателей экономической безопасности предприятия и их пороговые значения. Вестник Московского финансово-юридического университета. 2022;1:134–143. https://doi.org/10.52210/2224669X_2021_4_134
4. Абрамова С.Р., Баширина Е.Н., Хакимов Р.М., Абрамов И.Р. Экономическая безопасность и социальная устойчивость российского общества. Евразийский юридический журнал. 2023;3(178):415–416. <https://doi.org/10.46320/2073-4506-2023-3-178-415-416>
5. Юрченко А.И., Мамателашвили О.В. Концепция мониторинга эффективности системы экономической безопасности на предприятии. Экономика и управление: научно-практический журнал. 2023;5(173):124–129. <https://doi.org/10.34773/EU.2023.5.23>
6. Десятниченко Д.Ю., Десятниченко О.Ю., Остапенко В.В. Угрозы финансовой безопасности устойчивого функционирования предприятия. Экономика и бизнес: теория и практика. 2018;4:75–81.
7. Погодина Т.В. Финансовый менеджмент: учебник и практикум. М.: Юрайт; 2018. 351 с.
8. Шеремет А.Д. Анализ и диагностика финансово-хозяйственной деятельности предприятия: учебник. 2^е изд., перераб. и доп. М.: Инфра-М; 2022. 374 с.
9. Шульц В.А. (ред.) Безопасность предпринимательской деятельности: учебник для вузов. 2^е изд., перераб. и доп. М.: Юрайт; 2020. 585 с.
10. Графов Ю.Г. Цифровая устойчивость как условие обеспечения экономической безопасности цифрового предприятия при конкретизации целей национального развития. Индустриальная экономика. 2022;5(2):466–471.
11. Годин В.В., Терехова А.Е. Блокчейн: философия, технология, приложения и риски. Вестник университета. 2019;9:54–61. <https://doi.org/10.26425/1816-4277-2019-9-54-61>
12. Докукина А.А., Пименов В.В. Экономическая безопасность предприятий в условиях цифровой трансформации. Вестник Российского экономического университета имени Г.В. Плеханова. 2022;3:16–30. <https://doi.org/10.21686/2413-2829-2022-3-16-30>
13. Близкий Р.С., Хмелевской А.С. Актуализация цифровых форматов администрирования информационных систем в органах Федерального казначейства. Учет. Анализ. Аудит. 2024;4(11):35–46. <https://doi.org/10.26794/2408-9303-2024-11-4-35-46>
14. Розуленко Т.М., Близкий Р.С., Гун И. Экономика цифрового контакта в условиях трансформации георынков. Вестник университета. 2023;11:227–237. <https://doi.org/10.26425/1816-4277-2023-11-227-237>

References

1. Ageeva O.A., Matytsyna Yu.D. Monitoring the efficiency of organisation's internal control and economic security system. Vestnik universiteta. 2022;1:70–77. (In Russian). <https://doi.org/10.26425/1816-4277-2022-1-70-77>
2. Doronin Yu.P. Economic security as one of the strategic national priorities of the Russian Federation. Eurasian Law Journal. 2023;4(179):498–500. (In Russian).
3. Shchapov A.N. The system of indicators of the economic security of the enterprise and their thresholds. Herald of the Moscow University of Finance and Law. 2022;1:134–143. (In Russian). https://doi.org/10.52210/2224669X_2021_4_134
4. Abramova S.R., Bashirina E.N., Khakimov R.M., Abramov I.R. Economic security and social stability of Russian society. Eurasian Law Journal. 2023;3(178):415–416. (In Russian). <https://doi.org/10.46320/2073-4506-2023-3-178-415-416>
5. Yurchenko A.I., Mamatelashvili O.V. The concept of monitoring the effectiveness of the economic security system at the enterprise. Economics and Management: Scientific and Practical Journal. 2023;5(173):124–129. (In Russian). <https://doi.org/10.34773/EU.2023.5.23>
6. Desyatnichenko D.Yu., Desyatnichenko O.Yu., Ostapenko V.V. Threats of financial safety steady functioning of the enterprise. Economy and business: theory and practice. 2018;4:75–81. (In Russian).

7. *Pogodina T.V.* Financial management: textbook and practicum. Moscow: Urait; 2018. 351 p. (In Russian).
8. *Sheremet A.D.* Analysis and diagnostics of financial and economic activity of the enterprise: textbook. 2nd ed., revised and enlarged. Moscow: Infra-M; 2022. 374 p. (In Russian).
9. *Shults V.L. (ed.)* Safety of entrepreneurial activity: textbook for universities. 2nd ed., revised and enlarged. Moscow: Urait; 2020. 585 p. (In Russian).
10. *Grafov Yu.G.* Digital sustainability as a condition for ensuring the economic security of a digital enterprise when specifying the goals of national development. *Industrial economy*. 2022;5(2):466–471. (In Russian).
11. *Godin V.V., Terekhova A.E.* Blockchain: philosophy, technology, applications and risks. *Vestnik universiteta*. 2019;9:54–61. (In Russian). <https://doi.org/10.26425/1816-4277-2019-9-54-61>
12. *Dokukina A.A., Pimenov V.V.* Enterprise economic security in time of digital transformation. *Vestnik of the Plekhanov Russian University of Economics*. 2022;3:16–30. (In Russian). <https://doi.org/10.21686/2413-2829-2022-3-16-30>
13. *Blizkiy R.S., Khmelevskoy A.S.* Updating digital formats for administering info-systems in the treasury of Russia. *Accounting. Analysis. Auditing*. 2024;4(11):35–46. (In Russian). <https://doi.org/10.26794/2408-9303-2024-11-4-35-46>
14. *Rogulenko T.M., Blizkiy R.S., Gong Z.* The economy of digital contact in the conditions of geomarkets transformation. *Vestnik universiteta*. 2023;11:227–237. (In Russian). <https://doi.org/10.26425/1816-4277-2023-11-227-237>