УДК 338.24

ЦИФРОВИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ КАК НАПРАВЛЕНИЕ УКРЕПЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Екатерина Анатольевна Мягкова
кандидат экономических наук, доцент
eam24@rambler.ru
Алексей Александрович Пузиков
студент
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматриваются теоретические и практические аспекты обеспечения экономической безопасности хозяйствующего субъекта в условиях цифровой трансформации. Обосновывается расширение традиционного контура экономической безопасности за счет включения коммерчески значимой информации, клиентской базы, цифровой инфраструктуры и репутационных активов. Проведен анализ уязвимостей, характерных для поставщиков технически сложной продукции на всех этапах жизненного цикла сделки. Особое внимание уделяется трем ключевым угрозам цифровой эпохи. В результате исследования предложены направления укрепления экономической безопасности компании, позволяющие трансформировать цифровизацию из источника затрат в инструмент повышения устойчивости бизнеса.

Ключевые слова: экономическая безопасность предприятия, цифровизация, риск-менеджмент, конфиденциальная информация, CRM-система, документооборот, S3-объектное хранилище, угрозы информационной безопасности.

В современном понимании экономическая безопасность хозяйствующего субъекта — это не просто совокупность охранных мер, а целостная система, гарантирующая бесперебойность деятельности, сохранность ресурсов и потенциал для развития в турбулентной среде. Ее контур заметно расширился: помимо финансов и физической охраны, критическими объектами стали коммерчески значимая информация, клиентская база, электронные документы, каналы коммуникаций, договорные данные и цифровая инфраструктура [2, 4].

Наиболее остро проблема проявляется у поставщиков технически сложной продукции. Здесь уязвимость возникает на каждом этапе жизненного цикла сделки: при выборе оборудования, переговорах об условиях, закупке, транспортировке, оформлении разрешительной документации, пусконаладочных работах и последующем сервисе [1, 3 ,5]. Цель данной статьи — на примере ООО «КТМ» (дистрибьютора эталонного измерительного оборудования) систематизировать направления повышения экономической безопасности в условиях цифровизации.

Система экономической безопасности предприятия базируется на финансовых, организационных, информационно-правовых, кадровых и процессных элементах. Ее суть не в тотальном устранении всех рисков, а в грамотном риск-менеджменте: компания должна заранее идентифицировать критические активы, сценарии нарушений, возможный масштаб потерь и способы снижения ущерба [2, 7]. Следовательно, безопасность — это интегральная часть операционного управления, а не изолированная формальность.

Оценка уровня безопасности требует комплексного инструментария (рис. 1) [2, 4, 6]. На практике эффективное управление возможно только при синтезе этих подходов и регулярной сверке прогнозных показателей с реальными изменениями в деятельности предприятия.

Компания ООО «КТМ» — это не просто поставщик, а полноценный партнёр в мире эталонного измерительного оборудования. Она берёт на себя пусконаладку, тестирование, сертификацию ПО и техподдержку. В чём

сложность? Продукция высокотехнологичная, поэтому нужны специалисты высокого класса, безупречный подбор техники, жёсткое соблюдение контрактов и образцовый учёт каждой сделки.

Рисунок 1 – Подходы к оценке уровня безопасности предприятия.

Когда говорят об экономической безопасности такой фирмы, то за рамками одних лишь финансов остаётся очень многое. Здесь имеют значение стабильность поставок, качество общения с клиентами, сохранность коммерческих и технических данных, аккуратный документооборот, надёжность партнёров и готовность быстро адаптироваться к переменам. Особо охраняемая информация: кто поставляет, кто покупает, на каких условиях, по каким ценам, с какими характеристиками и обязательствами.

Построена компания по линейно-функциональному принципу. Директор управляет бухгалтерией, экономистами, коммерческим отделом, техподдержкой, юристами и кадровиками. Для среднего бизнеса — самое то: всё под контролем, решения не застревают. Но есть нюанс: нужно чётко разграничить зоны ответственности, прописать регламенты и следить за дисциплиной. Иначе слишком многое замыкается на конкретных людях, а это риск.

Почему ООО «КТМ» держится уверенно? Потому что оборудование, которое они поставляют, реально нужно промышленности и профессионалам. А работа с таким товаром — это длинная история: консультации, согласования, коммерческие предложения, потом постпродажное обслуживание. Получается,

экономическая безопасность прямо привязана к тому, насколько гладко идёт клиентский путь: от первого визита до финальных документов, поставки, наладки и сервиса.

И здесь выходит на сцену репутация. Для продавца сложной техники доверие — это актив, который не купишь за один день. Заказчики смотрят не только на цену, а на то, насколько ты компетентен, есть ли у тебя опыт, выполняешь ли ты обещания, хорошо ли консультируешь и будешь ли рядом после сделки. Поэтому участие в профильных мероприятиях, сайт, экспертные статьи, презентации и общение с рынком — это не просто маркетинг, а прямое укрепление экономической безопасности.

Документооборот — ещё одна точка опоры. В ООО «КТМ» масса операций завязана на договорах, счетах, предложениях, спецификациях и техничке. Одна опечатка в реквизитах, сроках, названии прибора или сумме — и вот уже задержка, спор, потеря денег или недоверие клиента. Поэтому регламент того, как готовить, согласовывать и хранить документы, — это не бюрократия, а защита экономических интересов.

И конечно, информационная безопасность. Когда почти всё уходит в цифру, компания оказывается завязанной на CRM, почту, облачные хранилища, телефонию, бекапы и права доступа. Нет контроля — будут утечки, потеря клиентской истории, подделка документов или срывы сроков. Так что цифровая инфраструктура — это уже не «айтишка», а часть системы экономической безопасности.

В итоге устойчивость ООО «КТМ» складывается из кучи факторов: организация, информация, юриспруденция, репутация, процессы. Чтобы компания была в безопасности, нужно управлять клиентскими циклами, хранить коммерческие тайны, держать документы в идеальном порядке, внедрять цифровой контроль и не допускать, чтобы ключевые операции замыкались на одном человеке. Такой подход укрепляет бизнес без публикации внутренних финансов и при этом не теряет связи с темой экономической безопасности.

Ключевой парадокс цифровой эпохи в том, что автоматизация одновременно гасит старые угрозы и порождает новые. С одной стороны, CRM, телефония, электронный документооборот и централизованные хранилища данных дисциплинируют работу: фиксируют каждый запрос клиента, позволяют отслеживать сделки, ускоряют подготовку бумаг. С другой — чем глубже предприятие погружается в цифру, тем сильнее оно попадает в зависимость от чистоты данных, надёжности систем доступа, стабильности серверов и добросовестности персонала [2, 3, 8].

Применительно к ООО «КТМ» можно выделить три значимые угрозы (рис. 2).

Рисунок 2 – Система основных угроз экономической безопасности ООО «КТМ».

Рассмотрим эти угрозы более детально.

Первая угроза — компрометация конфиденциальной информации. Речь идёт об утечке закупочных цен, условий работы с вендорами, коммерческих предложений, клиентской базы, спецификаций на оборудование, контрактов и сервисной документации. Потеря контроля над этими сведениями оборачивается падением конкурентной силы, ослаблением переговорных позиций и — как следствие — сокращением портфеля заказов [5].

Вторая угроза — нерациональная цифровизация. Лицензии на ПО, серверное оборудование, системы резервного копирования, файловые хранилища, средства защиты информации и техподдержка — всё это стоит денег. Если цифровая инфраструктура строится в отрыве от реальных бизнес-

процессов, затраты начинают обгонять эффект от автоматизации. Отсюда правило: любое цифровое решение нужно оценивать не только по удобству интерфейса, но и по экономической отдаче [6, 8].

Третья угроза — мошенничество через электронные каналы связи. В B2B-секторе сделки завязаны на счета, договоры, банковские реквизиты, электронные письма и подтверждения. Подмена реквизитов, подделка документов или согласование важных условий по непроверенному каналу чреваты прямыми убытками, срывом графиков и судебными спорами с контрагентами. Не стоит сбрасывать со счетов и банальный человеческий фактор: ошибки при заполнении документов, пропущенные входящие обращения, потеря контроля над счетами, выпавшая из переписок информация [7-8].

Укрепление экономической безопасности ООО «КТМ» предлагается выстраивать по пяти ключевым направлениям.

1. Внедрение S3-объектного хранилища. Перемещение части файлов, архивов, записей телефонных разговоров и клиентской документации во внешнее объектное хранилище решает сразу несколько задач: разгружает основной сервер, делает затраты на хранение прогнозируемыми и повышает отказоустойчивость системы. При грамотной настройке шифрования и разграничении прав доступа S3 превращается в дополнительный защищённый контур, существующий отдельно от основной CRM [4].

2. Углублённое использование «Битрикс24». Для ООО «КТМ» CRM-система не должна сводиться к простому справочнику контактов. Она призвана стать полноценным инструментом управления жизненным циклом клиента: фиксация обращений, хранение переписки и звонков, контроль этапов сделки, выставление счетов, анализ результатов. Чем тщательнее заполняются карточки клиентов, компаний и сделок, тем ниже риск утраты информации и выше прозрачность работы каждого сотрудника [1, 6].

3. Автоматизация подготовки документов. Ручное составление договоров, счетов и коммерческих предложений несёт скрытые издержки:

многократные проверки, исправление ошибок, затягивание согласований. Автоматическая подстановка данных из CRM уменьшает зависимость от человеческого фактора, ускоряет документооборот и сводит к минимуму риск некорректного указания реквизитов, сумм, сроков или условий поставки [8].

4. Ужесточение регламентов цифрового взаимодействия. Необходимо чётко прописать порядок выдачи доступов, проверки входящих писем, изменения реквизитов, согласования платежей, хранения файлов и действий при подозрительных сообщениях. Для операций с повышенным риском (особенно при смене банковских реквизитов или одобрении крупных сумм) следует ввести двойное подтверждение через независимый канал связи [4].

5. Систематический мониторинг индикаторов безопасности. Руководству компании стоит отслеживать не только классические финансовые показатели (выручку и прибыль), но и операционные: количество пропущенных обращений, долю ошибок в документах, процент успешно завершённых сделок, затраты на цифровую инфраструктуру, случаи просрочки счетов и регулярность резервного копирования. Такой контроль позволяет обнаруживать источники потерь задолго до того, как ситуация перерастёт в кризис.

Таким образом, устойчивость ООО «КТМ» складывается из четырёх компонентов: финансового надзора, информационной защиты, надёжного документооборота и контролируемой цифровой среды. Анализ показывает, что после спада в 2024 году компания восстанавливает позиции, но остаются уязвимости — неоправданные затраты на цифровизацию, низкое качество данных, риски в электронных коммуникациях и ошибки персонала. В связи с этим ключевыми направления укрепления безопасности для организации может стать переход на S3-хранилище, углублённая работа с CRM «Битрикс24», автоматическая генерация документов, чёткое разграничение прав доступа, формализация цифровых регламентов и системный мониторинг показателей. В этой логике цифровизация перестаёт быть чёрной дырой для бюджета и становится рычагом повышения устойчивости, сокращения операционных потерь и защиты долгосрочных коммерческих интересов.

Список литературы:

1. Акиндинов В.В., Лосева А.С., Мягкова Е.А., Акиндинов К.В. Цифровые технологии в управлении АПК // В сборнике «Аграрная экономика в условиях новых глобальных вызовов» (V Шаляпинские чтения). Материалы Всероссийской (национальной) научно-практической конференции, Мичуринск-наукоград РФ, 25 ноября 2022 года. Мичуринск-наукоград РФ: Мичуринский государственный аграрный университет, 2022. С. 10-15.

2. Бусыгин Д.Ю. Современные тенденции управления рисками в условиях цифровизации // Бухгалтерский учет и анализ. 2025. № 8. С. 51–55.

3. Демидов Александр Реализация мультиоблачной стратегии для Cloud Storage в Битрикс24: технический обзор // Habr – URL: https://habr.com/ru/companies/vk/articles/717940/ (дата обращения: 04.06.2026).

4. Докукина А.А. Экономическая безопасность предприятий в фокусе задач управления в условиях цифровой трансформации: монография. Российский экономический университет имени Г. В. Плеханова. Москва: РЭУ им. Г. В. Плеханова, 2024. 159 с.

5. Ефимова Н.С., Нестеров О.В. Формирование механизмов устойчивого развития высокотехнологичных предприятий в условиях цифровой трансформации // Региональные проблемы преобразования экономики. 2025. № 2.

6. Лопатова Н.Г. Управление экономическими рисками цифрового преобразования организаций // Цифровая трансформация. 2025. Т. 31, № 3. С. 5–13.

7. Ферова И.С., Козлова С.А., Осадченко Е.А., Подтихова Н.Н. Экономическая безопасность в эпоху цифровизации: вызовы, риски и стратегии устойчивого развития: монография. Москва: Русайнс, 2025. 209 с.

8. Хайду Н. Файлы в облаке: как безопасно хранить данные компании // Битрикс24 – URL: https://www.bitrix24.ru/journal/oblachnye-khranilishha-dlya-biznesa.html (дата обращения: 04.06.2026).

UDC 338.24

DIGITALIZATION OF BUSINESS PROCESSES AS A DIRECTION FOR STRENGTHENING THE ECONOMIC SECURITY OF AN ENTERPRISE

Ekaterina An. Myagkova
candidate of economic sciences, associate professor
eam24@rambler.ru
Alexey Al. Puzikov
Student
Michurinsk State Agrarian University
Michurinsk, Russia

Annotation. This article discusses the theoretical and practical aspects of ensuring the economic security of an economic entity during digital transformation. The expansion of the traditional economic security framework is justified by incorporating commercially significant information, client databases, digital infrastructure, and reputational assets. The analysis covers vulnerabilities typical for suppliers of high-tech products at all stages of a transaction's life cycle. Particular attention is paid to three key threats of the digital age. As a result, the study proposes measures to strengthen corporate economic security, transforming digitalization from a cost driver into a lever for improving business resilience.

Keywords: economic security of an enterprise, digitalization, risk management, confidential information, CRM system, document flow, S3 object storage, information security threats.

Статья поступила в редакцию 20.05.2026; одобрена после рецензирования 19.06.2026; принята к публикации 30.06.2026.

The article was submitted 20.05.2026; approved after reviewing 19.06.2026; accepted for publication 30.06.2026.