

**Ишкильдина Алия Азатовна**  
Магистрант 2 курс  
ФГБОУ ВО «Башкирский государственный университет»  
ПАО «АК Востокнефтезаводмонтаж»  
г. Уфа, Россия  
aliya.02@yandex.ru

### **Цифровая трансформация бизнеса: риски и перспективы**

*В данной статье рассмотрено развитие бизнеса в цифровом направлении. Цифровой переход начался задолго до коронавируса, но пандемия ускорила этот процесс, в самых разных её направлениях и масштабах. Как у любого другого изменения имеются хорошие стороны и плохие. Цифровизация бизнеса столкнулась с такими проблемами как: киберпреступность и кибермошенничество. Предотвратить данные задачи может цифровой комплаенс, который должен создать для предприятия вспомогательную систему контроля.*

**Ключевые слова:** бизнес-трансформация, киберпреступность, бизнес-процесс, цифровой комплаенс, блокчейн.

**Ishkildina Aliya**  
student  
Bashkir State University  
Ufa, Russia  
aliya.02@yandex.ru

### **Digital Business Transformation: Risks and Prospects**

*This article discusses the development of business in the digital direction. The digital transition began long before the coronavirus, but the pandemic has accelerated this process, in its most diverse directions and scales. Like any other change, there are good sides and bad sides. Digitalization of business has faced such*

*problems as: cybercrime and cybercrime. These tasks can be prevented by digital compliance, which should create an auxiliary control system for the enterprise.*

**Keywords:** business transformation, cybercrime, business process, digital compliance, blockchain.

Пандемия COVID-19 стала ключевой причиной бизнес-трансформаций в 2020 году. Из самых популярных – это и перевод на дистанционный формат, перестройка бизнес-процессов, Zoom-конференции и внедрение в ускоренном режиме цифровых рабочих мест и корпоративных сервисов таких, как CRM, ERP, СЭД и т.д.

Несмотря на все негативные последствия пандемии, она сделала процесс цифровой трансформации ускоренным в самых разных отраслях экономики, повлияла на организации, разные по своему масштабу и профилю. Для наглядности стоит сказать, о глобальных расходах на цифровую трансформацию, которая в 1,3 трлн долларов, по данным исследования Worldwide Digital transformation Guide американской IDC.

Что касается России, речь о цифровой трансформации в научных кругах идет уже давно. При этом существует национальный проект «Цифровая экономика РФ», направленный на развитии России в этом направлении в период 2019-2024 гг. Бюджетное финансирование на эту цель заложено в порядке 1,8 трлн руб.

Пандемия внесла свои коррективы, и сейчас переход на цифровые технологии для всех не выбор, а скорее жизненная необходимость. По данным KMDA, российские компании тратят от 3 до 10 % своей выручки на цифровой переход. Опрос показал, что многие компании довольны такой тенденцией и

отмечают снижение трудозатрат и повышение эффективности бизнес-процессов, следовательно, отсюда и увеличение маржинальности продуктов, и рост капитализации компаний. Раньше внедрение технологий происходило только в отдельные процессы, но сейчас можно говорить о комплексной цифровой трансформации, ведь клиент не будет ждать и бизнесу нужно принимать быстрые решения.

Наиболее популярными направлениями цифровизации являются работа с данными и управление клиентским опытом, технологии интернета вещей, роботизация процессов и искусственного интеллекта. По отраслям наиболее цифровыми можно считать ритейл, банки и страхование, отрасли телекоммуникации и связи. Работа с большими данными и ускорение их обработки в будущем сыграет ключевую роль для аналитики в целом, так как станет реальным переход от ретроспективного к предиктивному анализу технико-экономических показателей компании, а также позволит сыграть на опережение, заняв более выгодную позицию при всех прочих равных рисках на конкурентном рынке.

Рынок технологий стал более гибким и быстрым. Сейчас внедрить новые цифровые решения можно намного легче и со сниженными издержками. Так, например, можно использовать уже готовые облачные решения, а затем уже развить технологию внутри компании. Через пару лет неудивительным будет вообще в целом цифровое производство, где технологические и бизнес-процессы будут объединены при помощи сквозной интегрированной системы управления. [1]

Однако при всех положительных сторонах цифровой трансформации возрастает риски экономической безопасности компаний. При этом именно

цифровая культура – важный фактор успех. Около 73% компаний на сегодняшний день не думают об цифровом образовании своих сотрудников. [1] Но нужно понимать: изменение бизнес-процессов без изменения мышления не приведет к революционным изменениям.

По своей сути безопасность имеет широкий спектр значений. В рамках нашего исследования мы рассмотрим понятие экономической цифровой безопасности. Вот одно из определений: безопасность – это состояние деятельности, при которой с определенной вероятностью исключаются потенциальные опасности. Если мы говорим о безопасности, значит подразумеваем, что наша компания способна управлять рисками. Уточним понятие экономической безопасности. Экономическая безопасность – это состояние, при котором наблюдается устойчивый и высокий рост экономических показателей, эффективное удовлетворение экономических показателей и соответствующий контроль.

Но что мы имеем, говоря об экономической цифровой безопасности в условиях нынешней экономики? Новый уровень глобализации и трансформации экономического общества дал возможность не только развитию новых отраслей и сфер бизнеса, но и новым угрозам проявлению фактов мошенничества как в деловой, так и в обычной жизни людей. То есть возникает противоречие между цифровой модернизацией экономики и степенью ее безопасности.

На сегодняшний день активно проявляет себя кибермошенничество и киберпреступность. Любые информационные и технологические инновации двигают преступников к повышению эффективности своей деятельности.

Наиболее популярными направлениями на сегодняшний день являются преступления, направленные на:

- нарушение конфиденциальности;
- компьютерные данные;
- кражей контента;
- нарушение авторского права и смежных прав.

Таким образом, помимо трансформации экономики мы получаем и трансформацию самой киберпреступности. Страдают в такой среде больше предприятия малого и среднего бизнеса, так как не имеют достаточно средств и компетенций на обеспечение качественной информационной безопасности. Вторыми жертвами киберпреступлений являются банки. С одной стороны, цифровизация банков позволила снизить издержки и себестоимость оказываемых услуг, но, с другой стороны, повысила риски обеспечения финансовой безопасности своих клиентов. [2]

Предотвратить данные риски способен цифровой комплаенс – внутренняя политика компании, направленная на минимизацию рисков цифровой безопасности и экономического ущерба для компании. Около 50 % МСП не думают об цифровой защите своих данных. Стоит понимать, что комплаенс направлен не только на цифровую безопасность, но и на другие сферы, например, права человека, трудовые права, коррупция, охрана окружающей среды, налоги, конкуренция, наука и технологии, раскрытие информации и защита прав потребителей. Причем решением для экономической цифровой безопасности могут стать, как ни парадоксально, опять же сами технологии. Перевод контрактных отношений в онлайн, а также регистрация контрактов в блокчейне позволяет повысить прозрачность

деятельности компании и цепочек поставок. Кроме того, проведение анализа контрактных отношений с применением технологии искусственного интеллекта позволит выявить финансовые и нефинансовые риски. [3]

Активное освоение цифровых технологий повлияло на быстрое изменение реалий экономики. Свою весомую лепту в развитие внесла пандемия, ставшая ключевой проблемой 2020 года. Несомненно, цифровая трансформация позволила бизнесу открыть для себя новые каналы улучшения своих процессов, снизить издержки и ускорить циклы производства. Но вместе с тем, технологическое развитие повлияло и на экономическую безопасность компаний, увеличились кибератаки, направленные на кражу не только финансов, но и конфиденциальной информации. Таким образом, можно сделать вывод: компании должны прийти к осознанию необходимости внесения изменения в систему управления рисками и свою политику, то есть актуальным на сегодняшний день становится цифровой комплаенс, который должен создать для компании дополнительную цифровую систему контроля.

#### **Список источников и литературы**

1. Пандемия ускорила цифровизацию бизнеса // Информационные технологии. Выпуск №12. URL: <https://plus.rbc.ru/news/5f8f191f7a8aa930ddd3c511> (дата обращения: 07.12.2020)

2. Головинов Олег Николаевич, Погорелов Александр Владимирович Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. №1. URL: <https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya> (дата обращения: 07.12.2020).

3. Левашенко А. // Цифровой бизнес комплаенс – что это? // Инвестиции. Цифровая экономика. URL: <https://oecd-russia.org/analytics/tsifrovoj-biznes-komplaens-eto-cto-.html>

**Выходные данные статьи:**

Ишкильдина А. А. Цифровая трансформация бизнеса: риски и перспективы. // Журнал «У». Экономика. Управление. Финансы., №4. 2020. URL: <https://portal-u.ru/index.php/journal/article/view/443>