УДК 338

Разработка модели уровня цифровой трансформации на основе рисков, связанных с безопасностью организации

Цибулина Екатерина Владимировна

Аспирант,
Московский государственный технологический университет «СТАНКИН»,
127994, Российская Федерация, Москва, Вадковский пер., 1;
e-mail: katsibulina@gmail.com

Попов Дмитрий Владимирович

Кандидат экономических наук, профессор,
Московский государственный технологический университет «СТАНКИН»,
127994, Российская Федерация, Москва, Вадковский пер., 1;
e-mail: d.popov@stankin.ru.

Аннотация

В статье рассматриваются вопросы, связанные с необходимостью цифровой трансформации предприятий с целью повышения их производительности. Проводится анализ бизнес-процессов организации на предмет наличия автоматизированных сервисов и уровня их трансформации. Рассматриваются риски, связанные с уровнем цифровой трансформации в целом и в разрезе уровня автоматизации сервисов, а также влияние этих сервисов на производительность труда. Предлагается модель оценки уровня цифровой трансформации на основе рисков, связанных с безопасностью предприятия. В заключении делается вывод о том, что этапе планирования перехода на цифровую трансформацию необходимо определить, какие решения следует использовать в зависимости от уровня рисков, а также регламентировать правила для предотвращения рисков и последствий утечки или хранения данных. План перехода на цифровую трансформацию следует рассматривать с точки зрения взаимозависимости сервисов, поскольку один функционирующий сервис не обеспечит ожидаемой производительности, а лишь приведет к значительным расходам предприятия. Для плавного перехода необходимо составить график и план взаимозависимых приложений и разрабатывать их поэтапно, начиная с низкого уровня цифровизации и заканчивая высоким уровнем автоматизации, постоянно отслеживая показатели производительности, а следовательно, и прибыльности предприятия.

Для цитирования в научных исследованиях

Цибулина Е.В., Попов Д.В. Разработка модели уровня цифровой трансформации на основе рисков, связанных с безопасностью организации // Экономика: вчера, сегодня, завтра. 2024. Том 14. № 4А. С. 732-738.

Ключевые слова

Цифровая трансформация, цифровизация, риски, безопасность, данные, бизнес-процесс, производительность, утечка, хранение.

Введение

Тенденция последнего столетия, характеризующаяся современной экономической парадигмой, наблюдает устойчивый тренд перехода предприятий к цифровой трансформации. Этот процесс, обусловленный рядом факторов, представляет собой кардинальное изменение в способах ведения бизнеса, что требует внедрения инновационных технологий и пересмотра традиционных подходов к управлению.

Цифровая трансформация предполагает интеграцию информационных технологий во все аспекты деятельности предприятия, начиная от автоматизации производственных процессов и заканчивая оптимизацией бизнес-процессов.

Однако стоит отметить, что успешная реализация цифровой трансформации возможна только при наличии соответствующей инфраструктуры и квалифицированных специалистов. Поэтому многие компании активно инвестируют в развитие своих IT-отделов и создание центров компетенций по работе с новыми технологиями.

Цифровая трансформация становится неотъемлемой частью современного бизнеса. Она позволяет компаниям оставаться конкурентоспособными на рынке и повышать свою эффективность.

На форуме по искусственному интеллекту, Президент РФ, обозначил важную деталь, которая относится к положительному влиянию на развитие производительности в России. Глава государства отметил, что ИИ должен являться помощником для увеличения производительности, для улучшения качества и скорости услуг, а также отметил искусственный интеллект, - как важнейший ключевой ресурс, чтобы добиться суперэффективности. При этом основа трансформации и перехода на использование ИИ, не должна базироваться на замещении рабочих мест. Для роста производительности человек и ИИ должны работать вместе, где на каждого человека, должен быть один робот, что повлечет за собой тот самый рост увеличения показателей.

Таким образом, в связи в связи с уходом с нашего рынка большинства иностранных компаний, существует потребность в увеличении производительности труда.

Анализируя увеличение производительности труда за счёт цифровизации и сопутствующей цифровой трансформации, следует учитывать потенциальные риски для организации. Нормативно-правовая база в данной области находится на начальном этапе развития, особенно это касается регулирования работы с электронными деньгами. В качестве примера можно привести цифровые финансовые активы, представляющие собой новый инструмент для инвестиций на основе технологий блокчейна и смарт-контрактов.

В июле 2020 года был принят Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», регулирующий выпуск и обращение цифровых активов в российских информационных системах, функционирование которых обеспечивают операторы. Операторами могут выступать исключительно российские юридические лица, внесённые Центробанком в специальный реестр. Центральный банк осуществляет надзор за деятельностью всех операторов информационных систем.

Первый оператор был зарегистрирован в феврале 2022 года. В апреле 2022 года закон № 259-ФЗ был дополнен положениями, касающимися организации торгов по цифровым финансовым активам. 1 июля 2022 года компания «ВТБ-факторинг» впервые на платформе оператора информационной системы «Лайтхаус» токенизировала свою коммерческую задолженность. Процедура токенизации позволила компании существенно сократить сроки получения финансирования при низких операционных издержках. В июле 2022 года в России была проведена первая инвестиционная сделка с использованием цифровых финансовых активов и реального товара. Росбанк приобрел цифровой токен, привязанный к стоимости палладия, у глобального палладиевого фонда «Норникеля» на блокчейн-платформе «Атомайз». Впоследствии через различных операторов было выпущено более 50 ЦФА от разных эмитентов, включая иностранную валюту. В конце 2022 года «Метровагонмаш» на платформе «Лайтхаус» выпустил токены на сумму 58 миллионов юаней. Срок обращения ЦФА составил 29 дней, ставка — 4,2% годовых.

В рамках Федерального закона о цифровых финансовых активах рассматриваются вопросы регулирования и обращения данных активов, однако не затрагивается проблема их безопасности. Законодательство подвергается корректировке на основе отдельных случаев с последующими предложениями по его обновлению. Следует отметить, что уровень риска утечки или потери данных крайне высок, поскольку на данный момент отсутствуют подтверждённые факты гарантии сохранности информации.

Уровень автоматизации

При анализе преимуществ и недостатков цифровой трансформации в настоящий момент можно сделать вывод о необходимости соблюдения баланса между стремлением компании к определенному уровню развития и риском, который увеличивается с ее переходом в цифровую среду.

Для достижения этой цели предлагается создать карту направлений деятельности производственного предприятия, которая будет отражать уровень цифровой трансформации на основе бизнес-процессов, выполняемых сотрудниками компании. Для каждого процесса должен быть предусмотрен специализированный сервис выполнения. При анализе предприятия возможно определение уровня автоматизации сервисов. Полностью «ручной процесс» соответствует отсутствию цифровой трансформации, тогда как наличие сервиса и интегрированного решения с автоматизацией и выполнением преобразующих функций с помощью автоматизированных алгоритмов свидетельствует о высоком уровне автоматизации.

Автоматизированный процесс включает алгоритмы, которые на основе входных данных преобразуют и выполняют определенный результат. Интеграция сервиса с источником данных и происходящие в нем преобразования данных свидетельствуют о высоком уровне автоматизации. Если сервис выполняет преобразования внутри себя, но не получает исходные данные через интеграцию, то процесс является частично ручным, то есть обладает низким уровнем автоматизации.

Если в сервисе не происходит преобразований, а данные загружаются извне вручную и только хранятся, то процесс оцифрован, но имеет низкий уровень автоматизированной цифровизации. Если в сервисе не происходит преобразований, а данные загружаются извне через интеграцию, то процесс оцифрован и обладает высоким уровнем автоматизированной цифровизации. Оценка уровня автоматизации бизнес-процессов позволяет определить степень трансформации компании в целом, оценить увеличение производительности и эффективность трансформации, а также выявить риски в области безопасности данных.

Архитектурные решения взаимодействия с внешними источниками и влияние на риски

безопасности предприятия

Ранее мы определили уровни автоматизации бизнес-процессов, для автоматизированных сервисов и для дальнейшего определения рисков безопасности необходимо учитывать архитектурные решения каждого сервиса и его взаимодействие с внешними источниками, тем самым определить зону рисковых сервисов на предмет безопасности.

Влияние на выбранное архитектурное решение и наличие интеграций напрямую влияет на риски предприятия в части безопасности данных.

Определение соотношения рисков безопасности данных и уровнем цифровой трансформации. Рассмотрим прямую влияния на риски безопасности данных в таблице 1, в соотношении уровня цифровой трансформации. Не рассматривая уровень цифровой трансформации равный уровню - отсутствует.

Таблица 1 Соотношение уровня цифровой трансформации к уровню риска безопасности данных

Уровень цифровой трансформации	Уровень риска безопасности данных	Комментарии
-высоко-автоматизирована (1)	Критичный-контурное решение/критичный-облачное решение	Критичный уровень безопасности данных, связан с тем, что данные преобразовываются и не имеют дубликатов на ином носителе, а также интегрированы с внешними источниками, что приводит к высокой вероятности утечки данных. Если решение является облачным, то вероятность вырастает в геометрической прогрессии.
-высоко-оцифрована (2)	Высокий-контурное решение/критичный-облачное решение	Высокий уровень безопасности данных, связан с тем, что данные оцифровываются и имеют дубликат на ином носителе, но данные также интегрированы с внешними источниками, что соответственно приводит у высокой вероятности утечки данных. Также, определяем, если данные находятся в облачном решении, то уровень риска -критичный
-низко-автоматизированная (3)	Средний-контурное решение/высокий-облачное решение	Средний уровень безопасности данных, связан с тем, что данные преобразовываются и не интегрированы с внешними источниками, соответственно, присутствует риск потери преобразованных данных, так как дубликатов, но ином носителе нет. Также, определяем, если данные находятся в облачном решении, то уровень риска - высокий
-низко-оцифрована (4)	Низкий - контурное решение/высокий-облачные решения	Низкий уровень безопасности данных, связан с тем, что данные извне грузятся вручную, соответственно присутствует их дубликат. Отсутствует интеграция с внешними источниками, соответственно утечка данных возможна, но крайне низка. И тут мы определяем еще один критерий с точки зрения безопасности — это наличие сервисов в облаке или в контуре. Облачные решения всегда равны высокому уровню риска в части утечки данных.

Таким образом, можно оценить на сколько компания трансформирована в целом, оценить уровень увеличения производительности и соответственно, эффективность трансформации. А также, определить риск в части безопасности данных. Также необходимо учитывать, что

уровень трансформации напрямую связан с необходимостью регламентирования хранения и шифрования данных, прежде чем переходить на новый уровень трансформации.

Заключение

В рамках Федерального закона о цифровых финансовых активах рассматриваются аспекты регулирования и оборота этих активов, однако вопросы их безопасности остаются без внимания. Законодательная база подвергается модификациям на основе конкретных прецедентов с последующими предложениями по ее модернизации. Важно подчеркнуть, что риск утраты или утечки данных чрезвычайно высок, поскольку на текущий момент нет подтвержденных гарантий сохранности информации. Кроме того, необходимость повышения производительности труда подчеркивается руководством страны. Инвестирование в ИТ-отделы становится все более популярным. Необходимость пересмотра подходов к управлению и инвестированию в развитие сервисов в контексте цифровой трансформации становится очевидной.

Оценка уровня автоматизации бизнес-процессов позволяет определить степень преобразования компании в целом, оценить рост производительности и эффективность трансформации, а также выявить потенциальные риски в области безопасности данных.

Влияние выбранного архитектурного решения и наличие интеграций непосредственно влияет на риски предприятия в сфере безопасности данных.

При оценке предприятия на основе оценки уровня автоматизации бизнес-процессов можно определить, насколько компания претерпела преобразования в целом, оценить рост производительности и, соответственно, эффективность трансформации. Также можно определить риск в области безопасности данных. Необходимо учесть, что уровень преобразования напрямую связан с необходимостью регламентации хранения и шифрования данных перед переходом на новый уровень трансформации.

Разрабатывая план перехода на трансформацию с целью повышения производительности, сервисы можно разделить на прямые (которые непосредственно влияют на производительность) и косвенные (которые не влияют на производительность или влияют косвенно). К трансформации косвенных сервисов следует подходить в последнюю очередь.

На основании проведенного анализа можно сделать вывод, что на этапе планирования перехода на цифровую трансформацию необходимо определить, какие решения следует использовать в зависимости от уровня рисков, а также регламентировать правила для предотвращения рисков и последствий утечки или хранения данных.

План перехода на цифровую трансформацию следует рассматривать с точки зрения взаимозависимости сервисов, поскольку один функционирующий сервис не обеспечит ожидаемой производительности, а лишь приведет к значительным расходам предприятия.

Для плавного перехода необходимо составить график и план взаимозависимых приложений и разрабатывать их поэтапно, начиная с низкого уровня цифровизации и заканчивая высоким уровнем автоматизации, постоянно отслеживая показатели производительности, а следовательно, и прибыльности предприятия. Таким образом, предприятие сможет избежать высоких затрат на автоматизацию.

Библиография

1. Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» — URL: http://www.kremlin.ru/acts/bank/45766 (дата обращения: 04.05.2024). -Текст : электронный.
2. Оценка уровня цифровой трансформации организации на основе управленческой документации/ Попов Д.В., Ральникова К.В., Кутикова С.П. // Цифровая экономика. 2023. - №3(24). С.65-75. - URL: http://digital-economy.ru/images/easyblog_articles/1135/DE-2023-03-08.pdf (дата обращения: 04.05.2024). -
3. Stewart H. Digital transformation security challenges //Journal of Computer Information Systems. – 2023. – Т. 63. – №. 4. – С. 919-936.
4. Di Z., Liu Y., Li S. Networked organizational structure of enterprise information security management based on digital transformation and genetic algorithm //Frontiers in Public Health. – 2022. – Т. 10. – С. 921632.
5. Schwertner K. Digital transformation of business //Trakia Journal of Sciences. – 2017. – Т. 15. – №. 1. – С. 388-393.
6. Chouaibi S. et al. The risky impact of digital transformation on organizational performance–evidence from Tunisia //Technological Forecasting and Social Change. – 2022. – Т. 178. – С. 121571.
7. Karpunina E. K. et al. Economic security of businesses as the determinant of digital transformation strategy //Digital Economy: Complexity and Variety vs. Rationality 9. – Springer International Publishing, 2020. – С. 251-260.
8. Möller D. Guide to Cyber security in Digital Transformation //Trends, Methods, Technologies, Applications and Best Practices. Cham, Switzerland: Springer Verlag. – 2023.
9. Lambropoulos G., Mitropoulos S., Douligeris C. A review on cloud computing services, concerns, and security risk awareness in the context of digital transformation //2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – С. 1-6.
10. Lambropoulos G., Mitropoulos S., Douligeris C. A review on cloud computing services, concerns, and security risk awareness in the context of digital transformation //2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – С. 1-6.

Development of a model of the level of digital transformation based on the risks associated with the security of the organization

Ekaterina V. Tsibulina

Postgraduate student
Moscow State University of Technology «STANKIN»,
127994, 1, Vadkovskii lane, Moscow, Russian Federation;
e-mail: katsibulina@gmail.com

Dmitrii V. Popov

PhD in Economics, Professor,
Moscow State University of Technology «STANKIN»,
127994, 1, Vadkovskii lane, Moscow, Russian Federation;
e-mail: d.popov@stankin.ru

Abstract

The article discusses issues related to the need for digital transformation of enterprises in order to increase their productivity. An analysis of the organization's business processes is carried out to determine the availability of automated services and the level of their transformation. The risks associated with the level of digital transformation in general and in terms of the level of automation of services, as well as the impact of these services on labor productivity, are considered. A model for assessing the level of digital transformation based on risks associated with enterprise security is

proposed. In conclusion, it is concluded that the planning stage for the transition to digital transformation needs to determine which solutions should be used depending on the level of risks, as well as regulate rules to prevent the risks and consequences of data leakage or storage. The digital transformation plan should be considered from the point of view of the interdependence of services, since one functioning service will not provide the expected performance, but will only lead to significant costs for the enterprise. For a smooth transition, it is necessary to create a schedule and plan for interdependent applications and develop them in stages, starting with a low level of digitalization and ending with a high level of automation, constantly monitoring performance indicators, and therefore the profitability of the enterprise.

For citation

Tsibulina E.V. Popov D.V. (2024) Razrabotka modeli urovnya tsifrovoy transformatsii na osnove riskov, svyazannykh s bezopasnost'yu organizatsii [Development of a model of the level of digital transformation based on risks associated with the security of an organization]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 14 (4A), pp. 732-738.

Keywords

Digital transformation, digitalization, risks, security, data, business process, productivity, leakage, storage.

References

1. Federal Law No. 259-FZ “On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation” - URL: http://www.kremlin.ru/acts/bank/45766 (access date: 05/04/2024). -Text: electronic.
2. Assessing the level of digital transformation of an organization based on management documentation / Popov D.V., Ralnikova K.V., Kutikova S.P. // Digital economy. 2023. - No. 3(24). P.65-75. - URL: http://digital-economy.ru/images/easyblog_articles/1135/DE-2023-03-08.pdf (access date: 05/04/2024). -
3. Stewart H. Digital transformation security challenges // Journal of Computer Information Systems. – 2023. – T. 63. – No. 4. – pp. 919-936.
4. Di Z., Liu Y., Li S. Networked organizational structure of enterprise information security management based on digital transformation and genetic algorithm //Frontiers in Public Health. – 2022. – T. 10. – P. 921632.
5. Schwertner K. Digital transformation of business //Trakia Journal of Sciences. – 2017. – T. 15. – No. 1. – pp. 388-393.
6. Chouaibi S. et al. The risky impact of digital transformation on organizational performance–evidence from Tunisia // Technological Forecasting and Social Change. – 2022. – T. 178. – P. 121571.
7. Karpunina E. K. et al. Economic security of businesses as the determinant of digital transformation strategy //Digital Economy: Complexity and Variety vs. Rationality 9. – Springer International Publishing, 2020. – pp. 251-260.
8. Möller D. Guide to Cyber security in Digital Transformation //Trends, Methods, Technologies, Applications and Best Practices. Cham, Switzerland: Springer Verlag. – 2023.
9. Lambropoulos G., Mitropoulos S., Douligeris C. A review on cloud computing services, concerns, and security risk awareness in the context of digital transformation //2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – pp. 1-6.
10. Lambropoulos G., Mitropoulos S., Douligeris C. A review on cloud computing services, concerns, and security risk awareness in the context of digital transformation //2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – pp. 1-6.