УДК 004.9
DOI: 10.17586/0021-3454-2024-67-2-116-121

ТЕХНИЧЕСКИЕ РИСКИ ПРЕДПРИЯТИЯ, СВЯЗАННЫЕ С ЦИФРОВОЙ ТРАНСФОРМАЦИЕЙ

А. А. Емельянов, И. Л. Коршунов*

Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия
**dept.ait@unecon.ru*

Аннотация. Цифровая трансформация предприятий является обязательным этапом перехода к цифровой экономике. Проанализировано понятие „цифровая трансформация“. Констатирован факт появления новых рисков в деятельности предприятий вследствие значительного увеличения их информационных связей. Предметом исследования являются технические риски предприятия в процессе его цифровой трансформации. Определены три группы рисков: несанкционированный доступ/хищение/искажение информации с использованием средств локального доступа; уязвимость сетевых каналов передачи информации; нечеткое распределение сфер ответственности. Проанализированы особенности каждой группы рисков и предложены мероприятия по снижению их уровня для предприятия.

Ключевые слова: *цифровая трансформация предприятия, киберпространство, кибербезопасность, несанкционированный доступ к информации, уязвимость каналов связи*

Ссылка для цитирования: *Емельянов А. А., Коршунов И. Л.* Технические риски предприятия, связанные с цифровой трансформацией // Изв. вузов. Приборостроение. 2024. Т. 67, № 2. С. 116—121. DOI: 10.17586/0021-3454-2024-67-2-116-121.

ENTERPRISE TECHNICAL RISKS ASSOCIATED WITH DIGITAL TRANSFORMATION

A. A. Emelyanov, I. L. Korshunov*

St. Petersburg State University of Economics, St. Petersburg, Russia
**dept.ait@unecon.ru*

Abstract. Digital transformation of enterprises is a mandatory stage of the transition to digital economy. The concept of “digital transformation” is analyzed. The fact of the emergence of new risks in the activities of enterprises due to a significant increase in their information connections are stated. The subject of the study is the technical risks of an enterprise in the process of its digital transformation. Three groups of risks are identified: unauthorized access/theft/distortion of information using local access means; vulnerability of network information transmission channels; unclear distribution of areas of responsibility. The features of each risk group are analyzed and measures to reduce their level for the enterprise are proposed.

Keywords: digital transformation of enterprise, cyberspace, cybersecurity, unauthorized access to information, vulnerability of communication channels

For citation: Emelyanov A. A., Korshunov I. L. Enterprise technical risks associated with digital transformation. *Journal of Instrument Engineering.* 2024. Vol. 67, N 2. P. 116—121 (in Russian). DOI: 10.17586/0021-3454-2024-67-2-116-121.

Тема цифровой трансформации экономики России остается актуальной. Прошел этап кампанейщины в цифровизации, появился опыт противодействия кибератакам (количество и качество которых резко возросли) на объекты критической информационной инфраструктуры.

Применительно к экономике России термин „цифровая трансформация“ впервые использован в Указе Президента РФ от 21.07.2020 г. № 474 „О национальных целях развития РФ на период до 2030 года“ [1] для обозначения одной из национальных целей развития страны. На сегодняшний день не существует общепринятого определения этого термина, анализ научной литературы [2—4] позволяет выделить обязательные составляющие:

* *© Емельянов А. А., Коршунов И. Л., 2024*

1) кардинальное изменение бизнес-процессов или способов осуществления экономической деятельности;

2) изменения реализуются за счет применения информационных технологий (цифровых инструментов);

3) целью данного процесса является существенное повышение эффективности социально-экономической деятельности.

Суть цифровой трансформации предприятия можно представить следующим образом. Современные информационные технологии и их инструменты (Интернет, мобильные устройства, цифровые сервисы) позволяют существенно расширить возможности взаимодействия предприятия (предприятие—предприятие, предприятие—клиенты, предприятие—государство, клиент—государство и др.). Информационные технологии обеспечивают автоматизацию алгоритмов взаимодействия внутри и вне предприятия — эффективность взаимодействия существенно возрастает (снижается стоимость транзакций, увеличивается скорость информационных процессов, сокращается число ошибок и т.п.) — в результате качественно изменяется функционирование предприятия. Соединение возможностей информационных технологий и традиционных моделей деятельности предприятия приводит к появлению новых продуктов и бизнес-процессов с принципиально иными качествами.

Таким образом, можно констатировать, что одной из основных задач цифровой трансформации предприятия является алгоритмизация и автоматизация его взаимодействий, в настоящее время — с использованием аппаратно-программных комплексов (цифровых платформ). Будем рассматривать аппаратно-программный комплекс (АПК) как сложную информационную систему, обеспечивающую взаимосвязи участников рынка, открытую для использования предприятием, его партнерами и клиентами, включая разработчиков приложений, поставщиков услуг, агентов и регуляторов. Другими словами, АПК — это виртуальная среда, позволяющая интегрировать программные и аппаратные средства для обеспечения взаимодействия сторон. Виртуальная среда, или киберпространство, трактуется как пространство функционирования продуктов инфокоммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей [5].

Существенное увеличение связей предприятия, особенно внешних, ведет к появлению новых экономических (новая модель бизнес-процессов) и технических рисков (использование киберпространства). Экономические риски, как правило, связаны с угрозой цифровому суверенитету предприятия и с изменением роли государства, а также с ростом сложности бизнес-моделей и схем взаимодействия. Отмечаемые специалистами социальные риски цифровой трансформации определяются человеческим фактором: утечки персональных данных; отсутствие достаточного количества специалистов, обладающих требуемыми компетенциями; значительное сокращение персонала из-за автоматизации деятельности и др.

Одним из важнейших требований эффективной и безопасной реализации различного рода бизнес-процессов на предприятиях является корректный анализ и сведение к минимуму технических рисков. Вследствие того что данная сфера затрагивает практически все области деятельности, становится очевидной необходимость инвестирования ресурсов (в частности, финансово-экономических) для корректного формирования модели потенциальных угроз безопасности с последующим принятием мер по их устранению [6].

Можно выделить несколько видов технического риска:

1) несанкционированный доступ к информации, ее хищение/искажение с использованием средств локального доступа. Подобные ситуации возникают, когда имеется возможность использования уязвимостей внутри защищаемого периметра (некорректно реализованные политики безопасности, разрешение сотрудникам выполнять действия, не входящие в их функциональные обязанности и т.д.);

2) уязвимость сетевых каналов передачи информации, что может приводить к перехвату/анализу/подмене межсетевого трафика на транзитных узлах;

3) неоднозначное распределение сфер ответственности, приводящее к тому, что ряд действий либо бездействие привели к утечке/повреждению данных. Например, использование организацией как локальных, так и облачных вычислительных ресурсов/хранилищ данных в гибридной модели IT-инфраструктуры зачастую размывает границы ответственности лиц за каждый из аспектов деятельности.

Для снижения вероятности возникновения рисков, связанных с информационной безопасностью, цифровая трансформация должна быть постепенной, поэтапной. Переход на использование любых технологий без тщательного анализа целесообразности часто приводит к значительным проблемам в функционировании предприятий. Например, внедрение технологий виртуализации с применением гипервизоров вместо изолированных серверных систем порождает потенциальные уязвимости, связанные с несанкционированным доступом одной операционной системы, работающей в рамках единого АПК, к процессам другой. В качестве примера можно привести АПК Meltdown, Spectre, TLBleed, связанные со специфическими особенностями исполнения микрокоманд в рамках различных центральных процессоров. Устранение ряда аппаратных уязвимостей (используемых методами несанкционированного доступа с общим названием side-channel) для снижения их влияния на всю систему в целом является весьма сложным и затратным процессом. Ситуация осложняется тем, что в программном и аппаратном обеспечении регулярно обнаруживаются новые, еще не учтенные уязвимости (называемые в технической литературе „уязвимости нулевого дня“), которые в ряде случаев позволяют без существенных усилий вредоносно воздействовать на IT-инфраструктуру. Для устранения таких уязвимостей требуется оперативная разработка обновлений безопасности и их внедрение. Зачастую при проектировании и поддержке работы серверной и сетевой подсистем предприятия данный аспект либо не учитывается, либо реализуется не в полной мере из-за существенных затрат времени и других ресурсов.

Также немаловажным фактором в рамках разработки локальной политики безопасности предприятия является корректное разграничение полномочий сотрудников. С одной стороны, жесткие меры, позволяющие в значительной степени снизить риски информационной безопасности, порой весьма эффективно защищают IT-активы предприятия; с другой — при этом могут возникать ситуации, когда для выполнения сотрудником функциональных обязанностей требуется привлечение специалистов отдела информационной безопасности, технической поддержки, получение разрешений от руководства и т.д. В этом случае временные и организационные затраты могут нивелировать преимущества жесткой модели разграничения прав и сфер ответственности. Данный аспект приобретает особенную значимость при организации работы в рамках IT-отделов предприятия. Наиболее рационален, с точки зрения авторов, сбалансированный вариант, при котором сотрудники без существенных сложностей выполняют свои рутинные задачи, имея возможность преодолевать технические проблемы, не затрачивая время профильных специалистов. В качестве меры контроля может применяться система мониторинга, включающая запись любых действий каждого сотрудника с последующим анализом в режиме реального времени. Если действие является потенциально недопустимым либо имеется высокая вероятность того, что оно может оказаться вредоносным, информация передается руководителю структурного подразделения и специалистам отдела информационной безопасности.

Как уже было отмечено, использование сетевых каналов передачи информации порождает опасность ее перехвата. Однако в процессе цифровой трансформации локализация IT-процессов предприятия без связи с внешним миром почти нереальна. Повсеместное использование ресурсов глобальной сети; децентрализация, приводящая к необходимости связи между собой различных филиалов; работа с глобальными цифровыми платформами и облачными ресурсами — все это требует надежной и безопасной среды передачи данных по раз-

личным каналам связи: эфирным (Wi-Fi), кабельным, оптоволоконным. Современная сетевая инфраструктура предприятия подразумевает наличие большого количества промежуточных узлов (шлюзов), через которые проходит трафик. Любой из таких АПК может стать точкой захвата/ анализа/хищения/подмены информации [7]. Кроме того, в рамках локального обмена данными внутри предприятия существует вероятность несанкционированных подключений к корпоративной сети. Подобные уязвимости можно нивелировать средствами криптозащиты передаваемого трафика. Для связи между разнесенными территориально филиалами предприятий обычно используется сеть Интернет. Использование виртуальных частных сетей позволяет, с одной стороны, избежать расходов по созданию индивидуальных каналов связи; с другой — обеспечить надежное шифрование/дешифровку передаваемой по общедоступной сети информации. Кроме того, по мнению авторов, для защиты трафика во внутренней (локальной) сети целесообразно использование сетевых протоколов на базе IPSec, которые позволяют устанавливать соединение между любыми двумя устройствами исключительно по защищенному каналу передачи данных. В этом случае любые несанкционированные подключения к сетевой инфраструктуре предприятия будут бессмысленны, так как нелегитимно используемое устройство не сможет взаимодействовать ни с одним из АПК, работающих внутри организации. При этом как для конечных пользователей, так и для разработчиков, процесс сетевого взаимодействия будет проходить штатно, т.е. меры по защите трафика будут осуществляться автоматически.

Использование облачных ресурсов (с моделями IaaS, PaaS, SaaS, DBaaS и других), равно как и АПК (зачастую работающих с применением описанных моделей), порождает дополнительные уязвимости, связанные с хранением и обработкой данных в рамках центров обработки данных (ЦОД) организаций, являющихся сторонними по отношению к адресатам услуг. Любой современный центр обработки данных, рассчитанный на работу с большим количеством внешних клиентов, представляет собой распределенную кластерную инфраструктуру, в которой имеются уязвимости, как присущие локальным системам (рассмотренные выше), так и дополненные спецификой, свойственной кластерным решениям [6, 7]. Гибридные и распределенные гипервизоры (такие, как Hyper-V, vSphere, Proxmox и др.), с помощью которых реализуется работа большого количества изолированных сервисов, представляют собой программные решения, в которых регулярно обнаруживаются новые уязвимости [8]. При этом организации, арендующие вычислительные ресурсы в рамках той или иной облачной модели обслуживания, не могут влиять на инфраструктуру провайдера и даже получать информацию о средствах/уровне защиты конфиденциальных ресурсов. Вследствие этого меры, которые могут быть приняты для снижения вероятности несанкционированного доступа/хищения информации, следует реализовывать исходя из предположения, что ЦОД облачного провайдера является ненадежным и имеется риск компрометации хранящихся и обрабатываемых там данных. Рациональным будет лишь использование вычислительных мощностей, но не хранение данных, которые значимы для организации. При необходимости использования систем хранения данных облачных провайдеров следует применять криптографическую защиту — например, шифрующие файловые системы в рамках модели IaaS.

Технические риски, связанные с цифровой трансформацией предприятия, не ограничиваются рассмотренными в статье. Можно констатировать, что в современных условиях недостаточно обеспечивать защиту информации предприятия лишь в пределах его внутреннего контура. Каждый из рассмотренных аспектов безопасности значим для работы организации. Цифровая трансформация, осуществляемая без учета всего спектра потенциальных сложностей, которые будут возникать в процессе перехода, может быть провальной и нести лишь убытки. Проблемы, которые всегда будут возникать при внедрении новых технологий, порождают и новые технические риски, которые зачастую связаны с социальными рисками, например, использование технологий роботизации бизнес-процессов приводит к массовым увольнениям сотрудников, что повышает уровень напряженности [9]. Недостаточное владе-

ние основным спектром современных технологий порождает низкий уровень технической грамотности кадрового состава и затруднения при переходе к использованию более современных решений [10]. Любое изменение (особенно связанное с внедрением технологий, кардинально меняющих многие аспекты работы предприятия) должно быть тщательно проанализировано, смоделировано и только после этого поэтапный, плавный переход может иметь шансы на успех.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 21.07.2020 г. № 474 „О национальных целях развития РФ на период до 2030 года“ [Электронный ресурс]: <https://bazanpa.ru/prezident-rf-ukaz-n474-ot21072020-h4825501/> (01.08.2023).
2. *Лопатова Н. Г.* Риски цифрового преобразования предприятия // Экономическая наука сегодня. Сб. науч. статей. Вып. 13. Минск: БНТУ, 2021. С. 112—118.
3. Стратегия цифровой трансформации: написать, чтобы выполнить / Под ред. *Е. Г. Потаповой, П. М. Потеева, М. С. Шклярук*. М.: РАНХиГС, 2021. 184 с.
4. *Абдрахманова Г. И., Васильковский С. А., Вишневский К. О., Гершман М. А., Гохберг Л. М.* Цифровая трансформация: ожидания и реальность // Сб. докл. XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества. М.: Изд. дом Высшей школы экономики, 2022. 221 с.
5. *Добринская Д. Е.* Киберпространство: территория современной жизни. // Вестн. Московского ун-та. Сер. 18. Социология и политология. 2018. Т. 24, № 1. С. 52—70.
6. *Богатырев В. А.* Оценка надежности и оптимальное резервирование кластерных компьютерных систем // Приборы и системы. Управление, контроль, диагностика. 2006. № 10. С. 18—21.
7. *Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.* Model and interaction efficiency of computer nodes based on transfer reservation at multipath routing // Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2019). 2019. P. 8840647.
8. *Демидов А. В., Емельянов А. А.* Анализ уязвимостей и разработка требований к безопасности в современной IT-инфраструктуре // Цифровые опасности информационного общества. СПб: СПбГЭУ, 2023. С. 42—48.
9. *Емельянов А. А., Коршунов И. Л., Микадзе С. Ю.* К вопросу о цифровом суверенитете России // Изв. СПбГЭУ. 2022. № 6. С. 84—90.
10. *Колбанёв М. О., Коршунов И. Л., Микадзе С. Ю., Тумарев В. М.* К вопросу о терминологии в области цифровой экономики // Экосистема цифровой экономики. СПб: СПбГЭУ, 2021. С. 4—12.

Сведения об авторах

Александр Александрович Емельянов — канд. техн. наук; Санкт-Петербургский государственный экономический университет, кафедра информационных систем и технологий; доцент; E-mail: s1_alex2000@mail.ru

Игорь Львович Коршунов — канд. техн. наук, доцент; Санкт-Петербургский государственный экономический университет, кафедра информационных систем и технологий; заведующий кафедрой; E-mail: dept.ait@unecon.ru

Поступила в редакцию 11.09.2023; одобрена после рецензирования 01.10.2023; принята к публикации 17.12.2023.

REFERENCES

1. https://bazanpa.ru/prezident-rf-ukaz-n474-ot21072020-h4825501. (in Russ.)
2. Lopatova N.G. *Economic Science Today. Collection of Scientific Articles. Issue 13*, Minsk, Belarus, 2021, pp. 112–118. (in Russ.)
3. Potapova E.G., Poteev P.M., Shklyaruk M.S., eds., *Strategiya tsifrovoy transformatsii: napisat', chtoby vypolnit'* (Digital Transformation Strategy: Write to Execute), Moscow, 2021, 184 p. (in Russ.)
4. Abdrakhmanova G.I., Vasilkovsky S.A., Vishnevsky K.O., Gershman M.A., Gokhberg L.M. *Tsifrovaya transformatsiya: ozhidaniya i real'nost'* (Digital Transformation: Expectations and Reality), Reports of the XXIII Yasinsk (April) Intern. Scientific Conf. on Problems of Economic and Social Development, Moscow, 2022, 221 p. (in Russ.)
5. Dobrinskaya D.E. *Moscow State University Bulletin. Series 18. Sociology and Political Science*, 2018, no. 1(24), pp. 52–70. (in Russ.)

6. Bogatyrev V.A. *Instruments and Systems: Monitoring, Control, and Diagnostics*, 2006, no. 10, pp. 18–21. (in Russ.)
7. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2019)*, 2019, pp. 8840647.
8. Demidov A.V., Emelyanov A.A. *Tsifrovyye opasnosti informatsionnogo obshchestva* (Digital Dangers of the Information Society), St. Petersburg, 2023, pp. 42–48. (in Russ.)
9. Emelyanov A.A., Korshunov I.L., Mikadze S.Y. *Izvestiâ Sankt-Peterburgskogo gosudarstvennogo èkonomičeskogo universiteta*, 2022, no. 6, pp. 84–90. (in Russ.)
10. Kolbanev M.O., Korshunov I.L., Mikadze S.Yu., Tumarev V.M. *Ekosistema tsifrovoy ekonomiki* (Ecosystem of the Digital Economy), St. Petersburg, 2021, pp. 4–12. (in Russ.)

Data on authors

Alexander A. Emelyanov — PhD; St. Petersburg State University of Economics, Department of Information Systems and Technologies; Associate Professor; E-mail: s1_alex2000@mail.ru

Igor L. Korshunov — PhD, Associate Professor; St. Petersburg State University of Economics, Department of Information Systems and Technologies; Head of the Department; E-mail: dept.ait@unecon.ru

Received 11.09.2023; approved after reviewing 01.10.2023; accepted for publication 17.12.2023.