УДК 338.4
DOI 10.36511/2588-0071-2020-1-37-43

Захаров Владимир Яковлевич
доктор экономических наук, профессор, профессор кафедры экономики предприятий и организаций
Национальный исследовательский Нижегородский государственный университет имени Н.И. Лобачевского (603950, Нижний Новгород, пр. Гагарина, 23)

Vladimir Ya. Zakharov
doctor of sciences (economy), professor, professor of the department of economics of enterprises and organizations
National Research Lobachevsky State University of Nizhny Novgorod (23 Gagarina av., Nizhny Novgorod, Russian Federation, 603950)

E-mail: zaxarov48@yandex.ru

Фролов Владислав Генрихович
кандидат экономических наук, доцент, доцент кафедры экономики предприятий и организаций
Национальный исследовательский Нижегородский государственный университет имени Н.И. Лобачевского (603950, Нижний Новгород, пр. Гагарина, 23)

Vladislav G. Frolov
candidate of sciences (economy), associated professor, associate professor of the department of economics of enterprises and organizations
National Research Lobachevsky State University of Nizhny Novgorod (23 Gagarina av., Nizhny Novgorod, Russian Federation, 603950)

E-mail: frolov.unn@gmail.com

Управление рисками цифровой трансформации сложных экономических систем

Digital transformation risk management complex economic systems

В статье представлен обзор результатов последних исследований, выполненных в разных странах, посвященных управлению киберрисками в сложных экономических системах. Показано, что руководители крупных предприятий стремятся сбалансировать распределение средств между различными направлениями кибербезопасности для снижения общего риска цифровой трансформации. Выявлены слабые места в управлении киберрисками, наиболее значимыми среди которых, по мнению руководителей, являются управление данными и приорити-

зация киберрисков. Особое внимание предлагается обратить на защиту данных, ибо незащищенность данных может привести к потере ключевых компетенций компании, ее доходов и доверия к ней потребителей.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-010-00781.

Ключевые слова: сложные экономические системы, цифровая трансформация, управление киберрисками, кибербезопасность.

The article provides an overview of the results of recent studies carried out in different countries on the management of cyber risks in complex economic systems. It is shown that the leaders of large enterprises strive to balance the distribution of funds between different areas of cyber security to reduce the overall risk of digital transformation. Weaknesses were identified in cyber risk management, the most significant of which, according to managers, are data management and cyber risk prioritization. It is proposed to pay special attention to data protection, because data insecurity can lead to the loss of key competencies of companies, its revenues and consumer confidence in it.

The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of the scientific project no. 18-010-00781.

Keywords: complex economic systems, digital transformation, cyber risk management, cybersecurity.

Введение. Сегодняшние корпоративные лидеры сосредоточены на цифровой трансформации как важной стратегии для достижения большей корпоративной эффективности и лучшей защиты бизнеса. Для руководителей цифровая трансформация — один из самых сложных аспектов управления киберрисками, в особенности когда речь идет о цифровой трансформации сложных экономических систем.

В своей работе мы рассматриваем понятие «сложные экономические системы» как синоним понятий «сложные социально-экономические системы» и «сложные социально-технические системы», не проводя между ними различий. Общим способом описания системы признается определение набора заинтересованных сторон, которым приходится взаимодействовать, чтобы система в целом выполняла заданную функцию (достигала поставленных целей). В нашем исследовании мы исходим из общности совокупности заинтересованных групп, следовательно, полагаем, что всякое системное изменение является одновременно техническим, экономическим и социальным [1].

Экономическими системами мы называем все организации и их объединения, занимающиеся производством, продажей и потреблением товаров и услуг. В процессе роста экономические системы усложняются, приобретают новые элементы, связи и свойства. Их поведение, будучи изначально целенаправленным, становится все более вероятностным, менее предсказуемым. Наиболее ярким проявлением непредсказуемости развития сложных экономических систем являются организационные и общие экономические кризисы.

Считается, что к 2021 году ущерб от киберпреступности составит 6 триллионов долларов в год, в ближайшей перспективе — почти 10% мировой экономики [2].

Цель статьи — представить обзор результатов последних исследований, выполненных в разных странах, который позволил бы сделать более четкими и обоснованными ответы на вопросы относительно стратегий снижения киберрисков развития сложных экономических систем в период их цифровой трансформации.

Управление киберрисками. Результаты международного опроса 500 директоров и руководителей крупных компаний (сложных экономических систем), отвечающих за кибербезопасность, проведенного компанией *Deloitte* в 2019 году, показывают, что проблемы управления рисками связаны не только с ограниченностью бюджетов и ресурсов, но и с приоритизацией усилий по киберзащите в процессе интеграции кибербезопасности в критически важные цифровые бизнес-стратегии и операции.

Обнаружено, что руководители больше времени уделяют трем областям кибербезопасности: мониторингу (выявлению) киберугроз, реагированию на них, восстановлению (устойчивости) и управлению кибербезопасностью. Остальным аспектам кибербезопасности уделяется несколько меньшее и примерно одинаковое время [3].

Аналогичным образом относительно равномерно распределяются бюджеты между различными направлениями работы по обеспечению кибербезопасности. Сбалансированное распределение средств — широко распространенная стратегия снижения общего риска цифровой трансформации компании.

Опрос показал, что есть заметные пробелы в способности организаций соответствовать требованиям кибербезопасности. Ответы респондентов на вопрос, что является самым сложным аспектом управления безопасностью в вашей организации, распределились следующим образом [3]:

— сложность управления данными — 16%;

— лучшая приоритизация киберрисков по всему предприятию — 15%;

— быстрые изменения в информационных технологиях — 15%;

— недостаток квалифицированных киберпрофессионалов — 14%;

— отсутствие согласованности в руководстве относительно приоритетов — 14%;

— недостаток адекватного финансирования — 13%;

— неадекватное управление организацией — 12%.

Как видим, недостаточна способность организаций определять приоритеты рисков из-за отсутствия концептуальных рамок или модели управления рисками; нередко различные внутренние команды используют разные концептуальные рамки. Эти команды должны работать, опираясь на одну модель, чтобы не тратить лишнее время и ресурсы. Нужно более отчетливо видеть влияние технических уязвимостей на бизнес и его стоимость. И хотя многие организации хотели бы, чтобы их киберпрограммы как минимум шли в ногу с цифровой трансформацией, а лучше — чтобы они были драйвером цифровых преобразований, эти программы неадекватно финансируются и позиционируются в управлении организацией.

Ответственность за кибербезопасность компании должен нести лидер, имеющий полномочия для проведения необходимых изменений. В половине опрошенных организаций (49%) вопросы кибербезопасности ежеквартально рассматриваются на совете директоров, и только в 4% компаний — ежемесячно. От степени внимания совета директоров к кибербезопасности зависит уровень киберрисков. Советы директоров должны иметь адекватный доступ к экспертным знаниям в области кибербезопасности и регулярно оценивать состояние кибербезопасности в компании, чтобы успокоить клиентов, акционеров, регуляторов и принимать своевременные инвестиционные решения для защиты компании.

Принимая решения о затратах на кибербезопасность, половина опрошенных руководителей (50%) используют количественные инструменты оценки рисков, другая половина полагается на собственный опыт оценки киберзрелости компании.

Организации, которые не проводят анализ кибербезопасности на каждом этапе своего развития, рискуют потерять большую часть своей стоимости. Каждый выводимый на рынок продукт должен иметь такую характеристику: проверено, безопасно и надежно. Внутренние и внешние пользователи не должны тратить время на борьбу с киберсюрпризами. Могут возникнуть разрывы между приоритетами цифровой трансформации и возможностями обеспечения кибербезопасности организации. Преодоление таких разрывов в ключевых точках жизненного цикла стимулирует цифровую трансформацию.

Защита (целостность) данных вызывает наибольшую озабоченность у руководителей: среди трех наиболее опасных киберугроз безопасность данных выбрали 35% опрошенных, тогда как на действия сотрудников указали 32%, на технические уязвимости — 31%. Эти результаты совпадают с данными исследований, проведенных Национальной академией наук и инжиниринга Германии и Нижегородским государственным университетом имени Н.И. Лобачевского [4; 5]. Эксперты в Германии, Китае, Южной Корее, Японии и Великобритании поставили безопасность данных на первое место среди киберугроз, в России — на второе место, в США — на третье место. Эксперты опасаются, что невысокая безопасность данных приведет к потере ключевых компетенций, которые станут общим достоянием. В России, как и в других странах, более других обеспокоены безопасностью данных малые и средние предприятия.

Не хватает времени или ресурсов, необходимых организации для защиты всех данных, созданных или привлеченных. Поэтому организации должны сосредоточиться на защите данных, которые являются наиболее ценными для их бизнеса. Если киберпреступники получат в свои руки данные, они смогут влиять на поведение общественности, и негативные последствия этого могут быть значительными. Интернет вещей значительно расширяет сферу потенциальных слабых сторон компаний.

Одной точки взлома может быть достаточно, чтобы подвергнуть опасности всю сеть интернета вещей. Данные интернета вещей гораздо более подробны и чувствительны, потому что они собираются в режиме реального времени непосредственно у их источников. В. Овчинский и Е. Ларина отмечают, что атака на любой фрагмент умного города может вызвать веерные

отказы и парализовать жизнь в умном городе, функционирование которого основано на интернете вещей. Они полагают, что с увеличением размера и сложности территориальных экономических систем расходы на обеспечение их безопасности могут расти более высокими темпами, чем повышение эффективности сложных систем в результате их цифровизации [6].

На вопрос об утечке данных 9 из 10 организаций (90%) ответили, что в течение последних 12 месяцев произошло раскрытие конфиденциальных производственных данных, в том числе 41% отметили, что это было 5 и более раз [3]. Почти все руководители высшего уровня (92%) считали необходимым улучшить работу по предотвращению раскрытия конфиденциальных данных о производстве. Управление рисками раскрытия данных — это ответственность групп из разных подразделений предприятия, в том числе занимающихся маркетингом, человеческими ресурсами, операциями, информационными технологиями, правовыми вопросами. Тем не менее многие организации назначают сотрудника, который отвечает за управление рисками данных и ведет эту работу совместно с руководителями предприятия.

Многие бизнес-лидеры осознают, что, несмотря на строгий контроль безопасности, киберинциденты будут происходить. Как сильно эти инциденты повлияют на организационную репутацию, результаты работы компании и ее положение на рынке — это зависит в том числе от того, насколько хорошо организация подготовлена к анализу и предотвращению инцидента, сдерживанию его развертывания, решительному реагированию и управлению его последствиями.

Почти все (95%) руководители высшего звена признали, что их компании подверглись широкому диапазону кибератак, и более половины (57%) сообщили, что последнее кибернарушение произошло в последние два года. Эти атаки оказали серьезное влияние на доходы компаний, их репутацию и стабильность руководства. Существует согласие среди руководителей относительно того, что нарушения в работе из-за киберинцидентов сильнее всего повлияли на потерю доходов и потерю доверия потребителей. Об этом свидетельствуют ответы на вопрос, какое воздействие оказывают кибернарушения на организации [3]:

— потеря дохода из-за нарушения работы — 21%;
— потеря доверия потребителей — 21%;
— изменения в руководстве — 17%;
— репутационные потери — 16%;
— штрафы регуляторов — 14%;
— падение цены акций — 12%.

Обеспечение подготовленности к киберугрозам требует непрерывных изменений в компаниях, что является самым трудным в управлении любой сложной экономической системой («высший пилотаж»). Реализация новых способов ведения бизнеса, модернизация технологий, изменения в персонале, нормативные корректировки и изменения во внешних участниках могут создавать новые, непредвиденные уязвимости. Эти изменения в сочетании с постоянным развитием тактики киберугроз постоянно изменяют профиль киберрисков организации и уменьшают ее общую киберготовность.

Из-за того что ландшафт угроз быстро меняется и реакции не могут быть полностью реализованы, моделирование кибернетических войн становится ведущей стратегией в стремлении обеспечить кибербезопасность. Игры, имитирующие кибернетические войны, представляют собой интерактивную технику, которая погружает компании, реагирующие на киберинциденты, в смоделированные киберсценарии, чтобы помочь организациям оценить свою готовность к реагированию на киберинциденты. Эти упражнения проверяют организационные рефлексы реагирования, выявляют пробелы в возможностях и обучают разработке передовых методов обеспечения киберготовности. Однако только около трети руководителей высшего уровня указали, что их организации проводят киберучения для подготовки к реальным кибернарушениям [3].

За последние годы несколько крупных предприятий были полностью «заблокированы» киберпреступниками, производство на них было остановлено. Некоторые предприятия развивают стратегии, процедуры и другие обходные пути, позволяющие их командам продолжать выполнять критически важные задачи даже после потери доступа к своим технологиям. Одновременно мы наблюдаем рывок в реагировании на киберинциденты путем синхронизации действий всех составляющих сложной экономической системы с целью сокращения времени простоя: киберспециалистов, специалистов по непрерывности бизнеса, аварийному восстановлению и антикризисному управлению.

Заключение. Киберугрозы постоянно развиваются, и по мере того как компании готовят и внедряют новые меры безопасности, киберпреступники находят новые способы прорвать эту защиту и монетизировать кибератаки; разнообразные террористические группы все чаще переходят в киберпространство. Иногда люди без видимых мотивов стремятся продемонстрировать свои технические навыки, присоединяясь к атакующим.

Новые организации будут создавать и развивать новую киберкультуру и новую систему кибербезопасности, с самого начала основывая свой подход на цельной концепции управления киберрисками.

Руководители существующих организаций пересматривают способы достижения бизнес-результатов, проводят стратегии реинжиниринга, связанные с нейтрализацией киберрисков без операционных прыжков. С каждым новым вызовом приходят новые возможности. Какие бы прорывные цифровые технологии ни внедряли организации в процессе своей трансформации, все их действия связывает воедино задача снижения киберрисков, развития культуры кибербезопасности.

Примечания

1. Захаров В.Я., Трофимов О.В., Фролов В.Г., Каминченко Д.И., Павлова А.А. Концептуальные основы оценки факторов и системных эффектов сбалансированного развития сложных экономических систем в соответствии с концепцией «Индустрия 4.0» // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. 2018. № 3 (51). С. 7—23.

2. US Department of Homeland Security, Secretary Kirstjen M. Nielsen Remarks at the RSA Conference, April 17, 2018. URL: https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference (дата обращения: 04.03.2020).

3. Deloitte. The future of cyber survey 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf (дата обращения: 04.03.2020).

4. Kagermann H., Anderl R., Gausemeier J., Schuh G., Wahlster W. (Eds.), 2016. Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners (acatech STUDY), Munich: Herbert Utz Verlag. URL: https://en.acatech.de/wp-content/uploads/sites/6/2018/03/acatech_eng_STUDIE_Industrie40_global_Web.pdf (дата обращения: 04.03.2020).

5. Opportunities and Risks from Cooperation among Companies within the Production Sphere and the Sphere of Services in Russia in the Context of Industry 4.0 // AMAZONIA INVESTIGA. 2019. V. 20. No. 8. PP. 596—608.

6. Овчинский В., Ларина Е. Умные города и умная полиция: для кого? URL: http://zavtra.ru/blogs/umnie_goroda_i_umnaya_politciya_dlya_kogo (дата обращения: 04.03.2020).

References

1. Zakharov V.Ya., Trofimov O.V., Frolov V.G., Kaminchenko D.I., Pavlova A.A. Conceptual framework for estimating factors and system effects of balanced development of complex economic systems in accordance with the concept “Industry 4.0”. *Vestnik of Lobachevsky State University of Nizhni Novgorod. Series: Social Sciences*, 2018, no. 3 (51), pp. 7—23. (In Russ.)

2. US Department of Homeland Security, Secretary Kirstjen M. Nielsen Remarks at the RSA Conference, April 17, 2018. URL: https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference (accessed 04.03.2020).

3. Deloitte. The future of cyber survey 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf (accessed 04.03.2020).

4. Kagermann H., Anderl R., Gausemeie, J., Schuh G., Wahlster W. (Eds.), 2016. Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners (acatech STUDY), Munich: Herbert Utz Verlag. URL: https://en.acatech.de/wp-content/uploads/sites/6/2018/03/acatech_eng_STUDIE_Industrie40_global_Web.pdf (accessed 04.03.2020).

5. Opportunities and Risks from Cooperation among Companies within the Production Sphere and the Sphere of Services in Russia in the Context of Industry 4.0. *AMAZONIA INVESTIGA*, 2019, v. 20, no. 8, pp. 596—608.

6. Ovchinsky V., Larina E. Smart cities and smart police: for whom? URL: http://zavtra.ru/blogs/umnie_goroda_i_umnaya_politciya_dlya_kogo (accessed 04.03.2020). (In Russ.)