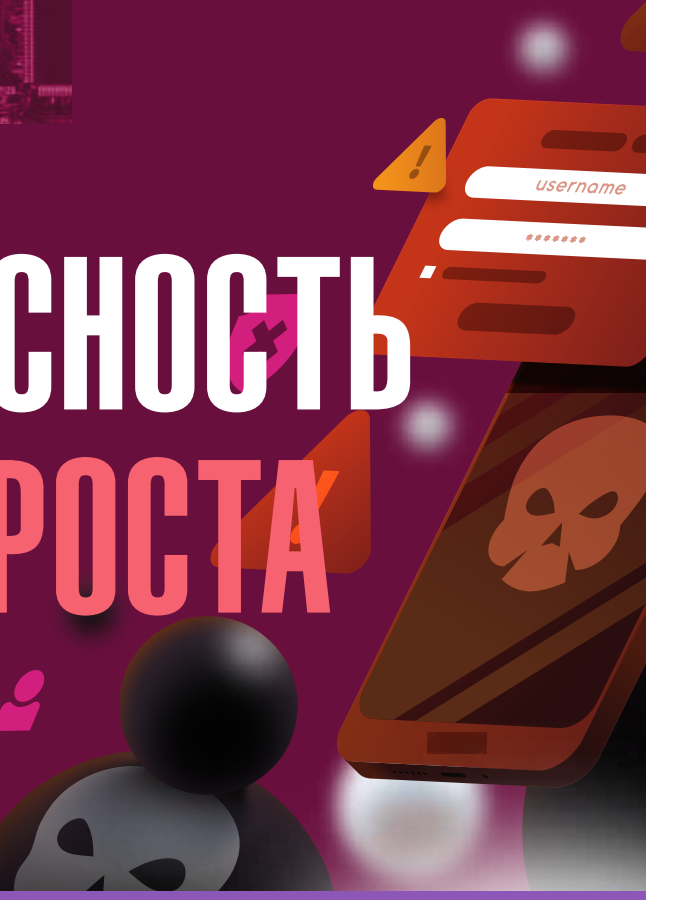
КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР РОСТА БИЗНЕСА



УДК 338

Фото Юлии Василишиной

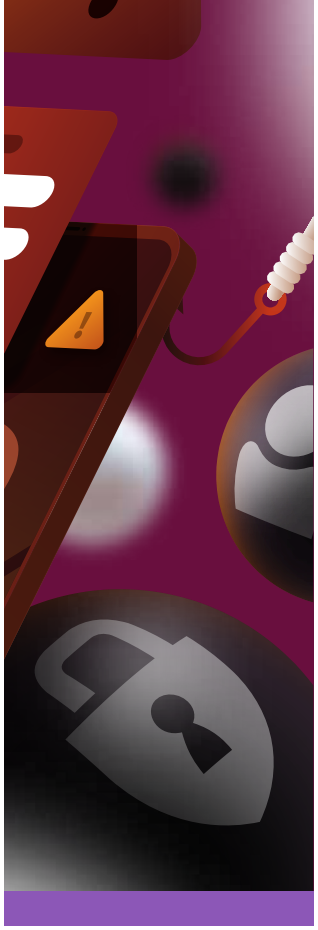
Наталья Лопатова,
завсектором
Института экономики
НАН Беларуси;
nutmegnt@gmail.com

Цифровая трансформация позволяет компаниям расширять свои возможности, обеспечивать значительные экономические и социальные преимущества, создавая при этом проблемы с точки зрения информационной безопасности и конфиденциальности. Последствия несанкционированного вмешательства на техническом и организационном уровне в информационные системы могут привести к ущербу репутации бренда, серьезным финансовым потерям, нормативно-правовым издержкам.

Ожидается, что глобальные затраты, связанные с киберпреступностью, в том числе: повреждением, уничтожением или кражей личных и финансовых данных, снижением производительности оборудования, хищением интеллектуальной собственности, мошенничеством, издержками по восстановлению нормального режима работы организации после атаки, расходами на судебные расследования, восстановление взломанных данных и систем, а также репутации достигнут 10,5 трлн долл. США в год к 2025 г. [1].

Рост большинства отраслей экономики зависит от инновационных технологий, таких как искусственный интеллект (ИИ), продвинутая аналитика, Интернет вещей (IoT), но с их внедрением киберугрозы только усиливаются – компании и клиенты сталкиваются с новыми видами рисков. Чем больше датчиков, интерфейсов и данных, тем значительнее потенциальная поверхность для кибератак; чем сложнее информационная инфраструктура, тем выше вероятность угроз. Недостаточное внимание к средствам защиты информационных сетей, устройств IoT может подвергнуть компанию серьезной опасности заражения вредоносными программами, атакам типа «отказ в обслуживании» (DoS), блокирующим сервисы и оборудование, а также утечке данных и другим угрозам [2].

Небезопасно и использование облачных сервисов, предоставляющих услуги по хранению инфор-



мации, которые, как правило, расположены в других странах, а доступ к таким хранилищам зависит от скорости соединения и возможных сбоев. Опрос, проведенный консалтинговой компанией McKinsey, показал, что большинство хозяйствующих субъектов по всему миру неохотно отдают IT-услуги на аутсорсинг за пределы своих государств, а предпочитают пользоваться услугами локальных поставщиков облачных вычислений и систем хранения [3].

Аутсорсинг информационной безопасности (ИБ) представляет собой совершенно новый вид вызовов для предприятий. Речь идет о выборе подходящей третьей стороны, которая имеет достаточный уровень киберзащиты и специализированные платформы безопасности для эффективной борьбы с враждебным ландшафтом угроз [4]. Тенденция такова, что все большая доля инфраструктуры организаций будет переходить под контроль внешних поставщиков облачных или интернет-услуг, в том числе управляемых услуг по обеспечению безопасности (MSSP), сосредоточенных исключительно на этой сфере [5, 6]. По данным исследовательской компании Gartner, к 2024 г. свыше 90% компаний будут использовать услуги управляемого обнаружения и реагирования на угрозы (MDR) [7].

Вместе с тем бизнес испытывает трудности с наймом и сохранением специалистов по кибербезопасности. Их число, согласно исследованию Международного консорциума по сертификации в области безопасности информационных систем (ISC), сейчас составляет 3,1 млн человек [8]. Согласно рейтингу американского журнала U.S. News and World Report, среди наиболее востребованных технологических профессий – аналитики в области ИБ, которые занимают 5-ю позицию по популярности в их списке [9]. Несмотря на то, что уровень образования для работодателей по-прежнему остается важным показателем, предпочтение отдается опыту. Спрос на специалистов ИБ постоянно растет, а число профессионалов, владеющих компетенциями в узкоспециализированных нишах, относительно небольшое [10]. Также эксперты указывают на острую нехватку соответствующих навыков и знаний в сфере безопасности, необходимых для решения сложных задач. Оценка уязвимости систем организации к различным кибератакам, реагирование на инциденты и мониторинг угроз – три области IT, нуждающиеся в персонале, имеющем максимально широкий набор знаний. Проблема усугубляется стремительно возникающими и развивающимися новыми вызовами, что требует постоянного повышения квалификации сотрудников, и она не решается простым увеличением их количества в соответствующих структурах [11, 12].

Исходя из этого, вполне обоснованно, что предприятия считают обеспечение безопасности приоритетом, а недостаточный уровень защиты от киберугроз заставляет их откладывать важные цифровые инициативы и ограничивает инвестирование в цифровые инновации [13].

Если ранее топ-менеджеры в основном рассматривали кибербезопасность как меру снижения рисков, то сегодня видят в ней фактор конкурентного превосходства. Компании все чаще просят своих потенциальных партнеров B2B предоставлять гарантии обеспечения киберзащиты и доступ к корпоративным отчетам о существующих мерах безопасности на постоянной основе, а правительственные структуры добавляют подобные требования в свои контракты на закупки. Растет число предприятий, занимающихся страхованием информационных рисков, которые изучают способы оценки киберрисков и их привязки к надбавкам. Рейтинговые агентства по облигациям также планируют учитывать уровень кибербезопасности компаний при оценке их деятельности [14].

Аннотация. *Обоснована необходимость стратегического управления киберрисками, возникающими в информационном пространстве на фоне расширения ландшафта цифровых угроз, использования комплексного подхода при принятии инвестиционных решений в области кибербезопасности. Определены ключевые аспекты формирования эффективных программ информационной безопасности.*

Ключевые слова: *цифровизация, инновации, кибербезопасность, киберриски, стратегия кибербезопасности, инвестиции.*

Для цитирования: *Лопатова Н. Кибербезопасность как фактор роста бизнеса // Наука и инновации. 2021. №3. С 38–41. https://doi.org/10.29235/1818-9857-2021-3-38-41*

Многие фирмы считают наличие сертификатов, обеспечивающих внешнюю проверку (валидацию) программ и методов конфиденциальности, например ISO 27701 (в части управления конфиденциальностью), EU/Swiss-U.S. Privacy Shield (правовой механизм для передачи данных в США), APEC Cross-Border Privacy Rules (соответствие рамкам конфиденциальности АТЭС и обеспечение международной передачи данных), важным фактором при выборе поставщика и принятии решений о покупке продукта в своей цепочке поставок. Более того, они расценивают получение компанией одного или нескольких из существующих сертификатов как выгодную инвестицию в свой бизнес [15].

Исследования компаний Cisco и Vodafone показывают ряд очевидных преимуществ, которые может дать организации способность цифровых систем выдерживать атаки и восстанавливаться, в том числе укрепление бренда и репутации на рынке, повышение лояльности клиентов при формировании «цифрового доверия» потребителей и возможность привлечения новых партнеров и клиентов. Многие субъекты создают надежную систему кибербезопасности для поддержки и ускорения инноваций (например, внедряя цифровые элементы защиты в дизайн продуктов или услуг) [13, 16].

По мере роста конкуренции происходит быстрое освоение инновационных цифровых бизнес-моделей, постоянное стремление предоставить клиентам более индивидуальный и улучшенный цифровой опыт, который, по мнению последних, так же важен, как продукты или услуги [17]. В то же время многие потребители не согласны с утверждением, что компании, располагающие большим объемом информации, могут предлагать более качественные и персонализированные товары и услуги. Сегодня они больше всего беспокоятся о том, как собираются, хранятся, используются их личные данные, и рассматривают конфиденциальность как важный компонент бренда, часто отказываясь от товаров и услуг при низком уровне доверия к системе безопасности [18, 19].

Для большинства организаций обеспечение конфиденциальности – критически важное требование. С каждым годом они все больше осознают различные преимущества от инвестиций в защиту персональных данных, включая усиление конкурентного преимущества, использование инноваций, повышение удовлетворенности клиентов и привлекательности компании для инвесторов. Согласно исследованию компании Cisco [15], многие фирмы видят положительный эффект от своих инвестиций в конфиденциальность. В среднем на каждый вложенный доллар они могут получить 2,7 долл. прибыли.

Цифровые инициативы меняют облик бизнеса независимо от его размера и отрасли, порождают как уникальные риски, так и эволюционные изменения традиционных вызовов. По мере все большего взаимодействия с потребителями в цифровом пространстве и увеличения организациями инвестиций в цифровые технологии риски на стратегическом, операционном и IT-уровне будут только усиливаться, и их невозможно избежать. Цифровой бизнес требует интегрированного управления угрозами, что позволит уменьшить влияние неопределенности на эффективность компании. Согласно данным Gartner, в 2021 г. более 50% крупных предприятий будут использовать комплексные решения для управления рисками [20].

Киберриск можно рассматривать как любой критический нефинансовый риск, который в настоящее время занимает первое место в повестке дня корпоративных вызовов. Отношение к кибербезопасности как функции IT-отделов меняется. Все чаще вопросы инвестиций в цифровые технологии безопасности рассматриваются на уровне высшего руководства [8, 12, 21]. Согласно опросу, проведенному консалтинговой компанией Deloitte [22], во многих организациях эти проблемы стоят на повестке дня советов директоров не реже одного раза в квартал. При этом Gartner прогнозирует рост числа рабочих мест, связанных с управлением цифровыми рисками, на более чем 40% в 2021 г. [23]. К этому времени 100% крупных мировых корпораций будут иметь в штате директора (глава, высшее руководство) по информационной безопасности [4].

Каждая компания осуществляет цифровое преобразование, исходя из собственных целей и задач, определяет принципы, приоритеты и подходы к управлению киберрисками в контексте стратегического видения, сопоставляя их влияние с возможностями для роста. Зачастую многие инициативы требуют анализа в этом вопросе не только на уровне технологий, но и бизнес-процессов. Поэтому предприятия чаще всего отдают предпочтение комплексному подходу к управлению киберрисками, включающему оценку, измерение, меры по смягчению и планирование мероприятий по предотвращению потенциальных угроз, а также создание организационной структуры и формирование таких подходов, которые обеспечивают прозрачность и позволяют управлять рисками в реальном времени с контролем ключевых параметров [21, 24]. В 2021 г. 75% крупных европейских компаний планируют интегрировать мониторинг киберрисков в свое бизнес-планирование и отражать показатели в ежеквартальной отчетности [6].

Обеспечение безопасности в цифровом пространстве – финансовый приоритет для большинства субъектов хозяйствования. При этом вопрос определения объема инвестиций в решения по управлению рисками пропорционально мерам по поддержке цифровых инициатив становится самым важным, так как модернизация систем безопасности после их внедрения, как правило, гораздо более дорогостоящее и менее эффективное мероприятие [8, 25].

Компании все чаще рассматривают кибербезопасность не как статью расходов, а как инвестиционную стратегию. Приоритеты в распределении финансовых средств они устанавливают на основе анализа всего портфеля осуществляемых инициатив, приоритизации цифровых активов, от которых зависит непрерывность и стабильность бизнес-процессов, оценки рисков по степени критичности и возможностей в области киберзащиты в сравнении с отраслевыми показателями. По мнению экспертов консалтингового агентства McKinsey, около 50% систем компаний не являются критичными с точки зрения кибербезопасности. Повышая цифровую устойчивость, они могут экономить до 20% затрат, направленных на защиту наиболее значимых, чувствительных цифровых активов [24].

При принятии обоснованных инвестиционных решений и возможности измерения эффективности снижения рисков или сравнения с другими корпоративными инвестициями важна их экономическая оценка, что дает возможность реализации более широкого спектра мероприятий по обеспечению кибербезопасности фирмы, включая обучение, поставщиков и цепочки поставок, киберстрахование [21]. Последнее представляет собой передачу компаниями некоторых рисков, которые могут нанести значительный финансовый и операционный ущерб, специализированным страховым агентствам. Киберстрахование становится важным элементом управления рисками, при этом его продукты не могут заменить надежную корпоративную программу информационной безопасности, а лишь дополняют ее, обеспечивая страховое покрытие, например, в таких областях, как ответственность за утечку данных, затраты на расследование нарушений, уведомление пострадавших сторон, штрафы и другие расходы [26]. Сегодня это неотъемлемая часть ведения бизнеса.

Каждая организация предпринимает определенные действия по защите целостности инфраструктуры и программного обеспечения своих цифровых цепочек поставок, меры по управлению данными рисками, взаимодействию на общих стандартах во всей Сети, внедрению принципов безопасного поведения в киберпространстве. Многие инциденты – результат человеческой ошибки, особенно в таких сферах, как фишинг, взлом деловой электронной почты – самых распространенных форм кибератак. При этом слишком мало компаний предпринимают действия по созданию сильной культуры кибербезопасности. Ознакомление сотрудников с потенциальными угрозами, их осведомленность на всех уровнях о видах кибератак и лучшими методами их отражения, повышение квалификации и тестирование кибернавыков – наиболее эффективные формы смягчения последствий, которые могут значительно снизить вероятность возникновения киберсобытия или минимизировать его последствия [21, 24].

Таким образом, цифровая трансформация открывает множество новых возможностей для бизнеса, создавая при этом значительные проблемы в сфере цифровой безопасности. Все чаще предупреждение и ослабление киберрисков рассматривается как часть бизнес-процесса, становится фактором поддержки и ускорения инноваций, бизнес-приоритетом для высшего руководства. Сегодня кибербезопасность как модель управления рисками, обеспечения доверия и взаимовыгодного сотрудничества может стать для компаний фактором роста и развития. М

Summary. The article considers cybersecurity as an opportunity for further business growth and a source of competitive advantage. The main cyber risks that can lead to serious and destructive consequences for companies are identified. The article substantiates the need for strategic management of risks arising in the information space against the background of expanding the cyber threat landscape, as well as an integrated approach to making investment decisions in the field of cybersecurity. The key aspects of forming effective information security programs are identified.

Keywords: digitalization, innovation, cybersecurity, cyber risks, cybersecurity strategy, investment.

https://doi.org/10.29235/1818-9857-2021-3-38-41

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cybercrime Damages $6 Trillion By 2021. Cybersecurity Ventures, 2020 // https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/.
2. Internet of Things Cybersecurity Readiness Report. Trustwave, 2018 // https://trustwave.azureedge.net/media/15351/iot-cybersecurity-readiness-report-prt.pdf?rnd=131992184400000000/.
3. Industry 4.0 How to navigate digitization of the manufacturing sector. McKinsey Digital, 2015 // https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Industry%2040%20How%20to%20navigate%20digitization%20of%20the%20manufacturing%20sector/Industry-40-How-to-navigate-digitization-of-the-manufacturing-sector.ashx.
4. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Cybersecurity Ventures, 2020 // https://cybersecurityventures.com/jobs/.

Полный список использованных источников размещен

SEE http://innosfera.by/2021/03/Cybersecurity

Статья поступила в редакцию 03.02.2021