УДК 330

И. А. Заярная, А. Р. Петрич
Новороссийский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации», Новороссийск, e-mail: aiamsem@mail.ru

НОВЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ И ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОМПАНИЙ

Ключевые слова: риск, технологии, угрозы.

В данной статье рассматриваются новые технологии в области экономической безопасности и управления рисками различных компаний. Большинство предприятий сообщают, что они столкнулись с проблемами безопасности, пытаясь адаптироваться к ускоренным технологическим изменениям. При огромной глобальной нехватке навыков в области кибербезопасности инструменты, разработанные для нового цифрового мира, необходимы для решения проблемы экономической безопасности. В настоящее время происходит переход на инновационные модели развития риск-менеджмента, которые демонстрируют активное применение цифровых технологий. При этом цифровое преобразование и цифровизация различных процессов стали одними важнейших элементов стратегий, позволяющих обеспечить компаниям успешное управление рисками и обеспечение экономической безопасности. К ярко выраженным барьерам реализации управленческих решений, встречающихся в недалеком прошлом и связанных с внедрением инновационных технологий, можно отнести невысокий уровень готовности к цифровым преобразованиям, недостаточной развитостью нужных компетенций персонала компаний и др. Сейчас растет число предприятий, имеющих необходимое представление о том, как управлять рисками и какие технологии для этого необходимы. Несмотря на наметившуюся тенденцию, авторы придерживаются мнения о важности увеличения количества предприятий, осуществляющих внедрение инновационных технологий в области экономической безопасности и управления рисками и увеличения количества предприятий.

I. A. Zayarnaya, A. R. Petrich
Novorossiysk branch of Federal State Budgetary Institution of Higher Education
«Financial University affiliated to the Government of the Russian Federation»,
Novorossiysk, e-mail: aiamsem@mail.ru

NEW TECHNOLOGIES IN THE FIELD OF RISK MANAGEMENT AND ENSURING THE ECONOMIC SECURITY OF COMPANIES

Keywords: risk, technology, threats.

This article discusses new technologies in the field of economic security and risk management of various companies. Most businesses report that they have faced security challenges as they try to adapt to accelerated technological change. With a huge global shortage of cybersecurity skills, tools designed for the new digital world are needed to address the challenge of economic security. Currently, there is a transition to innovative risk management development models that demonstrate the active use of digital technologies. At the same time, digital transformation and digitalization of various processes have become one of the most important elements of strategies that allow companies to successfully manage risks and ensure economic security. Pronounced barriers to the implementation of management decisions that have been encountered in the recent past and associated with the introduction of innovative technologies include a low level of readiness for digital transformations, insufficient development of the necessary competencies of company personnel, etc. Now the number of enterprises that have the necessary understanding of how to manage risks and what technologies are needed for this. Despite the emerging trend, the authors are of the opinion that it is important to increase the number of enterprises implementing innovative technologies in the field of economic security and risk management and to increase the number of enterprises.

Введение

Цифровые технологии и системы, созданные сегодня, представляют как далеко идущие возможности, так и проблемы как для профессионалов в области безопасности, так и для бизнес-лидеров.

Разрушительные технологии, геополитическая конкуренция и все более жесткие нормативные требования влияют на ландшафты кибер-и физических угроз. Поэтому становится все более важным принять целостный взгляд на то, как переплетенная

глобальная цифровая экосистема завтрашнего дня может повлиять на организацию и ее безопасность. Точечная настройка стратегий управления рисками для навигации по этим меняющимся приливам в глобальном ландшафте цифровых угроз имеет важное значение.

Целью данной статьи является исследование новых технологий в области управления рисками и обеспечения экономической безопасности компаний.

Материалы и методы исследования

В данной работе применяются такие методы исследования как анализ информации, её изучение, классификация и обобщение, метод индукции используется для выделения наиболее важных характеристик объекта.

Результаты исследования и их обсуждение

Повсеместное подключение через 5G и спутниковую связь, а также повышение производительности и масштаба благодаря искусственному интеллекту (ИИ), квантовым вычислениям и облачной инфраструктуре представляют значительные возможности для бизнеса. Однако растущая сложность, темпы и масштабы глобальной взаимосвязанности и архитектуры, на которую она опирается, будут представлять организации с растущими системными цифровыми угрозами, некоторые из которых трудно смягчить.

По словам старшего директора и аналитика Gartner Руджеро Конту, с растущим согласием с тем, что традиционный периметр предприятия и архитектура безопасности мертвы, недавно появился ряд технологий управления безопасностью и рисками, которые стоит рассмотреть на предприятии.

Быстрые темпы цифровой трансформации, переход к облаку и распределение рабочей силы означают, что стандартные средства контроля безопасности «не так эффективны, как в прошлом», – сказал Конту во время виртуальной конференции исследовательской фирмы Security & Risk Management Summit-Americas [7].

Большинство предприятий сообщают, что они столкнулись с проблемами безопасности, пытаясь адаптироваться к ускоренным технологическим изменениям последних двух лет. Недавний отчет Forrester, заказанный кибер-поставщиком Tenable, показал, что 74% компаний связывают недавние кибератаки с уязвимостями в технологиях, созданных во время пандемии.

Новые технологии в области безопасности и управлении рисками сосредоточены на шести областях:

- Конфиденциальные вычисления. Для обработки данных эти данные должны быть расшифрованы, что может привести к несанкционированному доступу или вмешательству. Таким образом, существует риск воздействия на данные, которые находятся в использовании. Конфиденциальные вычисления снижают риск разоблачения, когда данные расшифровываются во время использования. Он делает это с помощью доверенной среды выполнения, которая изолирует и защищает данные во время обработки.

Исследовательская фирма Everest Group недавно опубликовала отчет, в котором прогнозируется, что траектория рынка конфиденциальных вычислений может вырасти до 54 миллиардов долларов к 2026 году. Этот экспоненциальный рост подпитывается корпоративными облачными инициативами и инициативами в области безопасности, расширяя правила, особенно в чувствительных к конфиденциальности отраслях, таких как здравоохранение и финансовые услуги.

Все сегменты конфиденциальных вычислений готовы к росту, включая программное обеспечение, оборудование и услуги. Ожидается, что регулируемые отрасли будут доминировать в принятии конфиденциальных вычислений, причем более 75% спроса приходится на регулируемые отрасли, такие как банковское дело, финансы и здравоохранение [2].

1) Децентрализованная идентификация.

2) Аутентификация без пароля. Печально известно, что пароли имеют серьезные ограничения – от широкого использования слабых паролей до фишинговых и социальных инженерных атак, направленных на кражу паролей, до потенциальных компрометаций хранимых паролей. Скомпрометированные пароли ответственны за 81% взломов, связанных с нарушениями, сообщает Verizon.

Как отмечают многие исследователи, аутентификация без пароля заменяет использование паролей с применением альтернативных методов аутентификации, таких как смарт-карты, биометрия [4].

3) Служба безопасного доступа edge (SASE).

Хотя все еще относительно новый, secure access service edge (SASE) получил значительную тягу на рынке, потому что это «очень мощный» подход к повышению безопасности, сказал Конту. Этот термин был впервые введен аналитиками Gartner в 2019 году. SASE предлагает более динамичную и децентрализованную архитектуру безопасности, чем существующие архитектуры сетевой безопасности, и учитывает растущее число пользователей, устройств, приложений и данных, расположенных за пределами периметра предприятия.

SASE предлагает гибкий подход «в любом месте и в любое время» к обеспечению безопасного удаленного доступа, предоставляя множество возможностей, включая secure web gateway для защиты устройств от веб-угроз; cloud access Security broker (CASB), который служит посредником между пользователями и облачными провайдерами для обеспечения соблюдения правил безопасности, а также политики безопасности; и доступ к сети с нулевым доверием, который учитывает контекст, такой как личность, местоположение и состояние устройства, прежде чем предоставлять удаленный доступ к приложениям.

Нулевое доверие как основа для обеспечения безопасности современных предприятий существует уже много лет, но привлекает новое внимание с увеличением числа кибератак. Согласно недавнему опросу ThycoticCentrify, 77% организаций уже используют подход с нулевым доверием в своей стратегии кибербезопасности. Для 42% респондентов «снижение киберугроз» было главным мотиватором для принятия, за которым следовали улучшение соответствия (30%), снижение злоупотребления привилегированным доступом (14%), а также проверка и регистрация запросов трафика / доступа (также 14%).

Организации нуждаются в более автоматизированных подходах к определению конечных точек, которым нужны самовосстанавливающиеся приложения, клиенты или агенты безопасности, прошивки и операционные системы. Каждая организация может использовать большую видимость и контроль над системами ИТ [10].

Включение принципов с нулевым доверием в современную безопасность данных гарантирует отсутствие единой точки отказа при взломе систем. Принципы с нулевым доверием могут гарантировать, что даже если злоумышленники знают местоположение / IP базы данных, имя пользователя и пароль, они не смогут использовать эту информацию для доступа к привилегированной информации, предоставленной определенным ролям приложений, управлению идентификацией и доступом и периметрам облачной сети [9].

4) Управление правами облачной инфраструктуры.

По словам Forrester и Tenable, Расширение цепочки поставок программного обеспечения и миграция в облако – это два других основных источника кибер-уязвимости, с которыми сталкиваются предприятия. Опрос Forrester и Tenable показывает, что 80% лидеров безопасности и бизнеса считают, что их организации более подвержены риску в результате удаленной работы. По словам респондентов, более половины удаленных работников получают доступ к данным клиентов с помощью личного устройства, но 71% лидеров безопасности не имеют высокой или полной видимости в домашних сетях удаленных сотрудников. К сожалению, этот пробел хорошо понимают плохие актеры, что отражается в том факте, что 67% кибератак, влияющих на бизнес, нацелены на удаленных сотрудников [3].

По словам Forrester и Tenable, расширение цепочки поставок программного обеспечения и миграция в облако – это два других основных источника кибер-уязвимости, с которыми сталкиваются предприятия. Шестьдесят пять процентов лидеров безопасности и бизнеса связывают недавние кибератаки с компрометацией стороннего программного обеспечения, в то время как 80% лидеров безопасности и бизнеса считают, что перемещение критически важных для бизнеса функций в облако повысило их риск. Более того, 62% организаций сообщают о том, что подверглись атакам, влияющим на бизнес, с использованием облачных активов.

Недавнее исследование Dimension Research для Tripwire аналогичным образом определило облачную безопасность как главную проблему среди предприятий. Почти все опрошенные специалисты по безопасности сказали Dimensional, что использование нескольких облачных провайдеров создает проблемы безопасности и что усилия провайдеров по обеспечению безопасности «едва ли» адекватны. Среди других проблем они указали на отсутствие согласо-

ванных рамок безопасности и целесообразность сообщать о проблемах безопасности.

Чтобы решить проблемы, две трети или более лидеров безопасности сказали Forrester и Tenable, что они планируют увеличить свои инвестиции в кибербезопасность в течение следующих 12-24 месяцев. Более того, 64% лидеров, которым не хватает сотрудников службы безопасности, планируют увеличить численность персонала в течение следующих 12 месяцев.

Управление идентификационными данными и их правами, такими как привилегии доступа, как известно, сложно. Это в мультиоблачных и гибридных средах добавляет дополнительный уровень сложности. Известно, что злоумышленники используют эти слабые места для проникновения и компрометации облачных сервисов.

В ответ на проблемы облачной безопасности и растущую популярность облака – по оценкам Gartner, 70% рабочих нагрузок будут работать в публичном облаке в течение трех лет, по сравнению с 40% сегодня – спрос на облачную безопасность вырос. Исследовательская фирма MarketsandMarkets прогнозирует, что расходы на облачную безопасность достигнут 68,5 миллиардов долларов к 2025году по сравнению с 34,5 миллиардами долларов в прошлом году [8].

5) Услуги по защите цифровых рисков. С цифровой трансформацией растет число цифровых активов, и предприятия нуждаются в защите и видимости этих цифровых активов, которые не могут быть обеспечены традиционными средствами контроля безопасности. услуги по защите цифровых рисков могут обеспечить защиту бренда, защиту от утечки данных и услуги по защите от захвата учетных записей и мошеннических кампаний. Сервисы предлагают доступ к открытой сети, социальным сетям и темной сети, чтобы выявить такие угрозы, как мошеннические/нарушающие права вебдомены и мобильные приложения.

6) Управление поверхностью внешних угроз. Управление внешней поверхностью угроз фокусируется на выявлении всех интернет-активов, оценке уязвимостей, а затем управлении любыми обнаруженными уязвимостями. Например, это может включать неправильно сконфигурированные общедоступные облачные сервисы, серверы с непреднамеренно открытыми портами или третьи стороны с плохой безопасностью, которая представляет потенциальный риск [2].

В настоящее время принято считать, что это больше не вопрос «если», а «когда» организация пострадает от кибератаки. Это означает, что предприятия должны будут обеспечить защиту операций даже при нарушении. Организации с целостной стратегией устойчивости и планом непрерывности бизнеса смогут поддерживать или быстро возобновлять бизнес-функции в случае крупного разрушительного события, независимо от того, связано ли это нарушение непосредственно с кибератакой или физическим нарушением, связанным с ней. Регулярное тестирование таких планов и обеспечение их развития наряду с технологиями, потребностями бизнеса и рисками имеют решающее значение для обеспечения готовности вашей организации в случае кризиса [5].

Многие организации уже располагают большими и обширными базами данных, находящимися в стадии разработки, и многие ИТ-отделы активно интегрируют их с существующими приложениями, чтобы извлечь больше пользы из инвестиций в ИТ. Многие базы данных содержат точки данных о рисках, которые также могут быть извлечены, «добыты» или поглощены более мощными вычислительными платформами, чтобы со временем обеспечить еще большую организационную ценность. Инструменты, которые в настоящее время используют ИТ-директора организаций для содействия таким усилиям, включают электронные хранилища данных, «big data», приложения бизнес-аналитики и информационно-аналитические технологии.

Эти инструменты могут быть дополнены мощными технологиями извлечения, преобразования и загрузки данных, которые обеспечивают большую свободу в извлечении значения из труднодоступных и анализируемых файлов данных. Хотя риск-менеджеры изначально не могут быть предполагаемыми бенефициарами таких инвестиций в интеграцию данных, многие организации, тем не менее, используют эти инструменты для этой цели.

Также аналитика больших данных может помочь во многих областях, касающихся анализа рыночных рисков:

- Управление мошенничеством: быстрая идентификация мошенничества, сводит ущерб к минимуму.

- Управление кредитами: лучшие возможности прогнозирования, новые источники данных позволяют прогнозировать поведение пользователей.

- Отмывание денег: выявление проблем быстрее, реакция в режиме реального времени.

- Рыночные и коммерческие кредиты: позволяют лучше моделировать и прогнозировать рынки и компании.

- Операционный риск: предлагает больше контроля и знаний над взаимодействием с клиентами, повышает безопасность.

- Интегрированное управление рисками: предлагает глобальное видение в различных секторах и областях, где появляется финансовый риск.

В настоящее время активно используется Интернет вещей, который подразумевает под собой внедрение слоя технологий поверх бизнеса. Операции не нужно изобретать заново. Это предоставляет организациям, которые полагаются на управление рисками, незаменимый инструмент. Оснащая компанию большим количеством датчиков и устройств, подключенных к Интернету, организации могут собирать значительно больше данных в реальном времени для повышения ценности бизнеса. Также оказывает большое влияние на управление рисками.

Например, использование Интернета вещей для помощи в маркировке активов метками радиочастотной идентификации. Это помогает контролировать все, начиная от интервалов обслуживания оборудования, такого как краны, и заканчивая обеспечением правильного уровня топлива в генераторах.

Используя преимущества новых технологий, таких как Интернет вещей, и внедряя интегрированные системы, организация может собирать и анализировать огромные объемы данных из неограниченного числа источников в нескольких местах [6].

Заключение

В заключении можно отметить, что новые средства защиты с поддержкой искусственного интеллекта и машинного обучения, а также мощные системы анализа угроз и обмена информацией могут помочь сетевым защитникам автоматизировать политики безопасности, обнаруживать угрозы и более широко поддерживать смягчение последствий. Технология станет решающим катализатором в реагировании на новые технологические угрозы. Тем не менее, это должно быть дополнено приверженностью бизнес-лидеров к принятию целостного подхода к управлению рисками, принятию стратегических решений при разработке дорожных карт трансформации, управлению ИТ и поставщиками через управление и контроль, а также инвестированию в навыки и более широкую организационную культуру безопасности.

Библиографический список

1. Бабикова А.В., Никишина А.Ю. Проблемы и перспективы инвестиционного климата в Российской Федерации // Современные научные исследования и инновации. 2015. № 12. С. 591-594.

2. Чараева М.В. Реальные инвестиции: учебное пособие для студентов вузов. Москва: ИНФРА-М, 2018. 265 с.

3. Лукасевич И.Я. Инвестиции: учебник для студентов вузов. Москва: ИНФРА-М, 2018. 413 с.

4. Как привлечь инвестиции в бизнес? [Электронный ресурс]. URL: https://www.ey.com/en_ru/news/2021/10/russia-maintains-its-position-as-a-strategic-market-for-foreign-inverstors (дата обращения: 09.02.2022).

5. Васильева Н.В. Инвестиционный менеджмент: учебное пособие. Йошкар-Ола: ПГТУ, 2018. 96 с.

6. Терехова Е.В. Правовое регулирование иностранных инвестиций: теоретические и практические проблемы: монография. Москва: Русайнс, 2021. 112 с.

7. Большой экономический словарь [Электронный ресурс]. URL: https://rus-big-economic-dict.slovaronline.com/ (дата обращения: 12.03.2022).

8. Инвестиции и инвестиционная деятельность организаций: учебное пособие / Т.К. Руткаускас и др.; под общ. ред. д-ра экон. наук, проф. Т.К. Руткаускас. Екатеринбург: Изд-во Урал. ун-та, 2019. 316 с.

9. Шапкин А.С., Шапкин В.А. Управление портфелем инвестиций ценных бумаг. 6-е изд. Москва: Дашков и К°, 2021. 510 с.