DOI:10.33942/sit1364 УДК 004.56:388.45.01(575.2)

АНАЛИЗ РИСКОВ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Затравина С.В.
Кыргызский экономический университет им. М. Рыскулбекова, кандидат экономических наук, доцент, E-mail: zsveta71@mail.ru

Аннотация. *В статье рассматриваются ключевые риски, связанные с кибербезопасностью в условиях автоматизации бизнес-процессов. Исследуются методы идентификации, оценки и управления киберрисками, возникающими при внедрении цифровых технологий, а также влияние этих рисков на устойчивость и эффективность бизнеса.*

Ключевые слова: *кибербезопасность; автоматизация; бизнес-процессы; киберриски; цифровизация; информационная безопасность; управление рисками.*

БИЗНЕС ПРОЦЕССТЕРИН АВТОМАТТАШТЫРУУ ШАРТЫНДА КИБЕРДИК КООПСУЗДУК ТОКУКТУУЛУКТАРЫН ТАЛДОО

Затравина С.В.
М. Рыскулбеков атындагы Кыргыз экономикалык университети, экономика илимдеринин кандидаты, доцент, E-mail: zsveta71@mail.ru

Аннотация. *Макалада бизнес процесстерин автоматташтыруу контекстинде киберкоопсуздук менен байланышкан негизги тобокелдиктер каралат. Санариптик технологияларды ишке ашыруудан келип чыккан кибер тобокелдиктерди аныктоо, баалоо жана башкаруу ыкмалары, ошондой эле бул тобокелдиктердин бизнестин туруктуулугуна жана натыйжалуулугуна тийгизген таасири изилденген.*

Негизги сөздөр: *киберкоопсуздук; автоматташтыруу; бизнес процесстери; кибер тобокелдиктер; санариптештирүү; маалыматтык коопсуздук; тобокелдиктерди башкаруу.*

ANALYSIS OF CYBERSECURITY RISKS IN THE CONTEXT OF BUSINESS PROCESS AUTOMATION

Zatravina S.V.
Kyrgyz Economic University named of M. Ryskulbekov, Candidate of Economic Sciences, Associate Professor, E-mail: zsveta71@mail.ru

Abstract. *The article examines the key risks associated with cybersecurity in the context of business process automation. It examines methods for identifying, assessing and managing cyber risks that arise during the implementation of digital technologies, as well as the impact of these risks on the sustainability and efficiency of business.*

Keywords: *cybersecurity; automation; business processes; cyber risks; digitalization; information security; risk management.*

Введение. Современный бизнес стремительно движется в сторону автоматизации, внедряя передовые цифровые технологии, которые повышают производительность,

улучшают операционную эффективность и способствуют оптимизации бизнес-процессов. Однако автоматизация наряду с очевидными преимуществами несёт с собой и значительные киберриски, которые могут поставить под угрозу как безопасность данных, так и устойчивость самого бизнеса. В условиях цифровой трансформации компании сталкиваются с угрозами, которые требуют эффективного анализа и управления кибербезопасностью.

Актуальность темы и постановка задач. Актуальность темы обусловлена ростом киберугроз в условиях автоматизации бизнес-процессов, что требует внедрения надёжных методов для защиты данных и систем. Киберинциденты могут привести к серьёзным финансовым и репутационным потерям, влияя на устойчивость компаний. В рамках исследования ставятся задачи по анализу киберрисков, оценке их воздействия и разработке рекомендаций по минимизации угроз для повышения безопасности бизнеса.

Результаты исследования и рекомендации. Управление бизнес-процессами – фундаментальная функция, обеспечивающая эффективность, гибкость и устойчивое развитие компании. Оно позволяет структурировать деятельность организации, оптимизировать использование ресурсов и достигать стратегических целей.

В современных условиях цифровизации и автоматизации бизнес-процессов, управление ими приобретает ещё большую значимость, так как оно помогает не только улучшать внутренние операции, но и адаптироваться к изменениям рынка.

Управление бизнес-процессами включает в себя организацию, контроль и анализ операций, которые необходимы для достижения стратегических целей бизнеса. Сюда входят как внутренние процессы, так и взаимодействие с внешними партнёрами и клиентами [8]. Вышеперечисленные процессы и дальнейшее управление ими требуют от собственников компаний повышенного внимания к сфере безопасности, так как малейшая утечка данных и ее обнародование могут привести не только к возникновению финансовых трудностей, но и существенно отразиться на деловой репутации. Одним из главных вызовов области кибербезопасности является то, что технологии и угрозы постоянно меняются, и защитные меры должны быть адаптированы под эти изменения [6]. Поэтому управление бизнес-процессами тесно связано с управлением рисками, позволяющим систематизировать и контролировать действия в компании, обеспечивая предсказуемость и надёжность операций.

Сильная стратегия кибербезопасности может обеспечить хорошую защиту от вредоносных атак, направленных на доступ, изменение, удаление или уничтожение систем и конфиденциальных данных организации или пользователя [1].

Чтобы кибербезопасность стала управляемым бизнес-процессом, важно автоматизировать управление рисками, включая процессы идентификации, оценки, мониторинга и реагирования на угрозы. Это позволяет внедрить стандартизированные процедуры для оперативного выявления киберугроз, анализа их возможного воздействия и принятия своевременных мер по минимизации ущерба. Автоматизация управления рисками в области кибербезопасности создаёт целостную систему, в которой процессы защиты становятся частью общей бизнес-стратегии компании, что повышает прозрачность, снижает вероятность человеческих ошибок и усиливает способность компании к быстрой адаптации в условиях изменяющегося киберпространства.

При автоматизации бизнес-процессов можно выделить основные риски кибербезопасности (рис.1.).

Рис.1. Основные риски кибербезопасности при автоматизации бизнес-процессов [сост. автором]

Многие компании не проводят достаточно глубокий анализ уязвимостей своей информационной системы и не понимают, какие риски существуют, и какие меры безопасности нужно принимать для их устранения. Для решения этой проблемы компании должны проводить регулярный аудит и тестирование своей информационной системы на наличие уязвимостей. Это поможет выявить потенциальные уязвимости и принять меры по их устранению [2].

На сегодняшний день идентификация киберрисков является первым и важнейшим шагом в процессе управления кибербезопасностью, направленным на выявление слабых мест и потенциальных угроз в системе. Этот процесс позволяет определить, какие элементы цифровой инфраструктуры могут быть подвержены атакам, а также понять, какие типы угроз наиболее вероятны в условиях автоматизации.

Идентификация киберрисков требует системного подхода и применения специализированных методов, позволяющих обнаружить как явные, так и скрытые уязвимости, которые могут использовать злоумышленники. Поэтому *основными методами идентификации киберрисков* можно обозначить:

- анализ уязвимостей, который позволяет выявить слабые места в системах и ПО, через которые злоумышленники могут получить доступ к данным;

- пенетрационное тестирование, которое дает возможность смоделировать атаки для выявления и оценки слабых мест системы;
- мониторинг сетевой активности, позволяющий постоянно отслеживать сетевые соединения для обнаружения подозрительных действий;
- аудит безопасности, заключающийся в регулярной проверке политик и процедур безопасности на соответствие нормативам и стандартам;
- анализ инцидентов, посредством которого можно исследовать прошлые киберинциденты для выявления возможных паттернов и предсказания будущих рисков.

После того как основные угрозы были идентифицированы, необходимо оценить их значимость и возможное воздействие на компанию. Оценка киберрисков позволяет измерить, насколько серьёзны выявленные угрозы, и определить приоритеты в управлении ими. Существует два основных подхода к оцениванию информационных рисков – количественная и качественная [4]. Поэтому к ключевым *методам оценки киберрисков* относятся:

- качественная оценка рисков - оценка вероятности и последствий рисков на основе экспертных мнений и описательных данных;
- количественная оценка рисков - использование количественных показателей, таких как вероятность событий и потенциальные финансовые потери;
- анализ сценариев - моделирование различных сценариев развития киберинцидентов для оценки их воздействия;
- анализ на основе исторических данных - использование данных прошлых инцидентов для прогнозирования вероятности и ущерба от будущих событий;
- SWOT-анализ - оценка сильных и слабых сторон киберсистемы, возможностей и угроз.

На основе результатов оценки разрабатываются стратегии и меры для управления киберрисками. Управление рисками – это процессы, связанные с идентификацией, анализом рисков и принятием решений, которые включают максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий [3]. Основные методы управления киберрисками представлены на рис.2.

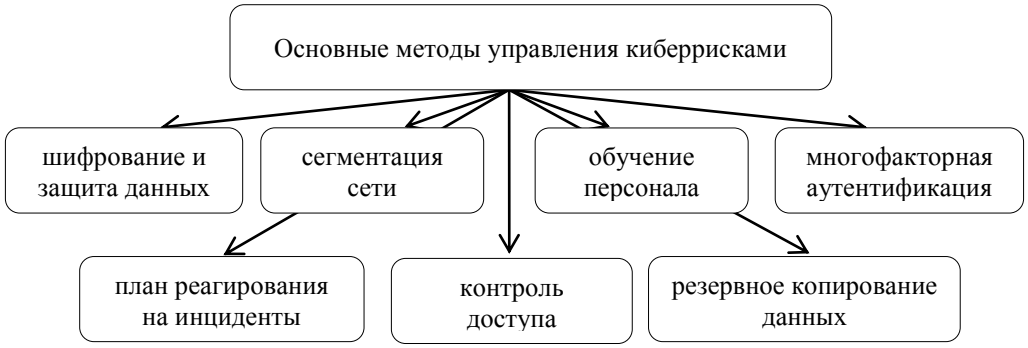

Рис.2. Методы управления киберрисками при автоматизации бизнес-процессов [сост. автором]

Раскрывая сущность вышеуказанных методов, можно увидеть, что шифрование и защита данных обеспечат их конфиденциальность и целостность для предотвращения от несанкционированного доступа, сегментация сети ограничит перемещение угроз в случае

взлома, а многофакторная аутентификация усилит процессы доступа к системам для предотвращения несанкционированного доступа.

Обучение персонала основам кибербезопасности позволит распознавать фишинг и другие атаки, а план реагирования на инциденты даст возможность оперативно реагировать на киберинциденты, что в лучшем случае минимизирует возможный ущерб. Резервное копирование и регулярное создание резервных копий позволят восстановить данные в случае потерь или атак, а контроль доступа обеспечит внедрение строгих правил доступа к системам и данным на основе ролей и полномочий.

Заключение. На основании вышеизложенного можно прийти к выводу, что в условиях цифровизации управление киберрисками становится существенным моментом для обеспечения устойчивости и эффективности бизнеса. Интеграция кибербезопасности в бизнес-процессы позволяет компании минимизировать угрозы, защищая данные и операционную непрерывность, что способствует укреплению позиций компании в условиях возрастающих киберугроз.

Список литературы:

1. Афанасьева С.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации // Вестник Самарского университета. Экономика и управление. 2023. №2.

2. Гололобов Ф. А. Проблемы управления рисками в сфере информационной безопасности // Вестник науки. 2023. №5 (62).

3. Дроздова Д. В. Управление рисками в рамках обеспечения кибербезопасности предприятий ТЭК // Теория и практика современной науки. 2024. №7 (109).

4. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51–57.

5. Ивасюк О.Н. Современные проблемы противодействия киберпреступности // Вестник экономической безопасности. 2022. № 6. С. 117–120.

6. Назарова А.Д. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации // Столыпинский вестник. 2023. №5.

7. Саратов, Д. Н. Автоматизация управления информационными рисками в информационно-вычислительных сетях МВД России // Региональная информатика и информационная безопасность: Сборник трудов, СПб, 23–25 октября 2019 года. Том Выпуск 7. 2019. – С. 186-190.

8. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества России. 2018. Т. 210. С. 23–34.

9. Безопасность управления бизнес - процессами. [Электронный ресурс]. — URL: https://apptask.ru/blog/bezopasnost-upravleniia-biznes-processami

10. Кибербезопасность для бизнеса: минимизация рисков и оптимизация затрат. [Электронный ресурс]. — URL: https://www.mobilis.ru/news/kiberbezopasnost-dlya-biznesa-minimizatsiya-riskov-i-optimizatsiya-zatrat/