УПРАВЛЕНИЕ РИСКАМИ ПРИ ВНЕДРЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРЕДПРИЯТИИ

И.И. Шалдыбин, Ю.В. Веселова

Самарский государственный университет путей сообщения, Самара, Россия

Обоснование. Розничная торговля в новом тысячелетии — сложный и динамичный сектор бизнеса. И это в равной степени касается как высокоразвитых, так и развивающихся стран. Появление новейших торговых сетей и, как следствие, увеличение конкуренции в сфере розничной торговли ставят новейшие задачи перед предприятиями. В современном ритейле происходят стремительные перемены. Такие основные тренды, как изменение потребностей потребителей и их все больший интерес не только в товарах, но и в положительном опыте покупки, консолидация ритейлеров, появление стратегий многоканальной торговли, изменение природы конкуренции как внутри, так и между форматами торговли, глобализация и т.д.

Цель — определение факторов, которые могут повлиять на проект, обоснование подходов к содержанию профилактических мер по обработке рисков, касающихся научных ведомств, заказчика и исполнителей и формулировка предложений.

Методы. В работе применялись методы группировки и синтеза, что позволяет сформировать массив информации для дальнейшего анализа.

Результаты. Технологические прорывы влияют на способы ведения ритейл-бизнеса в новом веке.

За последние годы сегмент розничной торговли стал набирать обороты по количеству внедряемых информационных технологий, особенно это касается части мобилизации бизнес-процессов. В этой связи продукты и услуги в области информационной безопасности стали для розничной торговли как никогда актуальны [4].

Поддержка безопасности предстает главным правилом в сфере управления предприятием. Множащееся число угроз представляет опасность не только для ТМЦ, но и для здоровья и жизни персонала, а также и для становления бизнеса.

В ритейле в 2020 г. большинство кибератак (52 %) было направлено на веб-приложения, предпочтительно онлайн-маркеты [3]. В ходе таких атак злоумышленники угоняли учетные данные клиентов, данные их платежных карт, ломали функционирование сервисов. Притом, почти каждая четвертая атака (25 %) крылась во внедрении вредоносного программного обеспечения (см. рисунок) [1].

Учитывая, что крупные предприятия розничной торговли могут обрабатывать тысячи транзакций ежедневно через свои POS-терминалы, и существует преуспевающий рынок для похищенных данных кредитных карт, из этого следует, что POS-терминалы являются желаемой целью для киберпреступников.

Растет признание того, что информационная безопасность влияет на более широкий спектр бизнес-рисков, и программы безопасности больше не являются исключительной компетенцией департаментов информационных технологий [2]. Желание обладать более комплексным подходом к безопасности перешло

Рис. Распространенные методы атак на предприятия розничной торговли

к лидерам бизнеса. Уделяется больше внимания сотрудникам, внедряются проверки на полиграфах, ведь значительная часть атак до сих пор осуществляется внутренними злоумышленниками. Не следует упускать из виду риски, которые несут третьи стороны. В современной взаимозависимой бизнес-экосистеме состояние безопасности третьих сторон может оказать огромное влияние на безопасность предприятий розничной торговли и создавать новые риски. В исследовании PwC сообщается о 27 % увеличении числа инцидентов, связанных со сторонними поставщиками услуг, подрядчиками и деловыми партнерами, часто имеющими доступ к сети и данным компании.

Выводы. В статье приведены направления для учета рисков и возможностей, которые необходимо учитывать при составлении планов управления рисками заинтересованными сторонами в процессе проекта создания и внедрения информационных ресурсов. Дополнить существующую нормативную базу по управлению рисками нормативными документами из порядка организации проектного менеджмента, в частности в сфере управления рисками, которые должны предусматривать и меры по аудитам управления рисками и аудит информационных технологий и кибербезопасности.

Ключевые слова: управление рисками; информационные ресурсы; классификация рисков; анализ рисков.

Список литературы

1. deloitte.com [Электронный ресурс]. Cyber risk in retail: Protecting the retail business to secure tomorrow's growth [дата обращения 27.02.2022]. Доступ по ссылке: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/us-risk-retail-cyber-risk-report-04070.335.pdf
2. grantthornton.ie [Электронный ресурс]. Cyber security concerns in the retail sector [дата обращения 27.02.2022]. Доступ по ссылке: https://www.grantthornton.ie/globalassets/0.33.-member-firms/ireland/insights/factsheets/grant-thornton---cyber-security-concerns---retail.pdf
3. cisco.com [Электронный ресурс]. Информационная безопасность и розничная торговля [дата обращения: 27.02.2022]. Режим доступа: https://www.cisco.com/c/ru_ru/about/press/press-releases/200.335/08–20.33d.html
4. Веселова Ю.В., Чекулдова С.В. Управление рисками в деятельности логистических организаций // Наука и образование транспорту. 2019. № 1. С. 206–208.

Сведения об авторах:

Илья Игоревич Шалдыбин — студент, группы ММ-1з, заочный; Самарский государственный университет путей сообщения, Самара, Россия. E-mail: ilja.ust@yandex.ru

Юлия Валерьевна Веселова — доцент кафедры «Менеджмент и логистика на транспорте»; Самарский государственный университет путей сообщения, Самара, Россия. E-mail: veselova-uv@yandex.ru