УДК 658.18

УПРАВЛЕНИЕ ЗАТРАТАМИ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ: БАЛАНС МЕЖДУ РИСКАМИ И БЮДЖЕТОМ

© Мухин В.В.

Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнёва, г. Красноярск, Российская Федерация

e-mail: vyacheslav.mukhin78@bk.ru

Научный руководитель: Данильченко Ю.В., канд. экон. наук, доцент
Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнёва, г. Красноярск, Российская Федерация

Ключевые слова: управление предприятием, информационная безопасность, риски и затраты.

В условиях роста киберугроз и ужесточения регуляторных требований (ФЗ-152, ФЗ-149, ФСТЭК, ФСБ, ЦБ РФ, РКН и др.) российские компании сталкиваются с необходимостью эффективного распределения бюджета на информационную безопасность (ИБ). С одной стороны, недостаточные инвестиции в защиту данных могут привести к катастрофическим последствиям: утечкам конфиденциальной информации, финансовым потерям, репутационному ущербу и даже административной ответственности. С другой – необоснованно высокие расходы на ИБ снижают рентабельность бизнеса, что особенно критично в условиях экономической нестабильности.

По данным РАЭК, только в 2025 году совокупный ущерб российского бизнеса от кибератак оценивался в 3,5 триллиона рублей. При этом многие компании сталкиваются с дефицитом квалифицированных кадров в сфере ИБ, что дополнительно увеличивает затраты на защиту данных.

В этих условиях управление затратами на ИБ требует всестороннего подхода, учитывающего специфику российского рынка, включая санкционные ограничения, импортозамещение и локальные угрозы. В российских реалиях расходы на информационную безопасность определяются тремя основными группами факторов.

Во-первых, это регуляторные требования. Законодательство РФ (152-ФЗ «О персональных данных», требования ФСТЭК, отраслевые стандарты ЦБ для финансовых организаций) устанавливает строгие правила защиты информации. Несоблюдение этих норм грозит серьезными штрафами – до 1 миллиона рублей за утечку персональных данных по КоАП, а для критической инфраструктуры возможны и более суровые санкции, вплоть до приостановки деятельности и лишения лицензии [1].

Во-вторых, санкционное давление и курс на импортозамещение. Многие зарубежные решения в области кибербезопасности стали недоступны, или их использование сопряжено с дополнительными рисками. Переход на российские аналоги (такие как Kaspersky, Astra Linux или VipNet) часто требует значительных инвестиций – как в сами продукты, так и в переобучение персонала, интеграцию новых решений в существующую ИТ-инфраструктуру.

В-третьих, это специфические киберугрозы, характерные для российского рынка. Речь идет о целенаправленных атаках на предприятия (особенно в госсекторе и финансовой сфере), активности таких хакерских группировок как APT29 или TA505, росте числа ransomware-атак. Отдельную проблему представляют инсайдерские угрозы – утечки данных по вине сотрудников или бывших работников.

Говоря про нахождение должного баланса между эффективностью ИБ-политики и экономической эффективностью, современные подходы к управлению информационной безопасностью предлагают несколько действенных стратегий:

– risk-based подход, предполагающий приоритизацию инвестиций в ИБ на основе оценки реальных рисков. Международные стандарты (такие как ISO 27005 или FAIR-модель) позволяют количественно оценить потенциальный ущерб от различных киберугроз и сосредоточить ресурсы на защите наиболее критичных активов;

– подход на основе Softwareasa-Service (SaaS). Тогда можно в короткие сроки получить полноценный сервис и существенно сэкономить при единовременной закупке (иногда до 70%). СЗИ обслуживаются владельцем сервиса, а также наблюдается снижение CAPEX и увеличение OPEX, если финансовая модель предприятия приветствует снижение собственных активов (снижение налогооблагаемой базы) [2];

– подход на основе перевода инфраструктуры в защищенные облачные ЦОД (применим для небольшой организации). Затраты на СЗИ входят в общий договор, возможно снижение бюджета ИБ почти до 0. Среди минусов риск нарушения конфиденциальности или потери данных; сложно найти ЦОД, который будет по умолчанию обеспечивать все потребности по защите, особенно в части выполнения требований регуляторов.

Необходимо учитывать и человеческий фактор. По данным Positive Technologies, до 60 % успешных кибератак происходят из-за ошибок персонала. Автоматизация рутинных процессов (например, с использованием playbooks для реагирования на типовые инциденты) позволяет высвободить ресурсы ИБ-специалистов для решения более сложных задач.

Другой тренд – брать в аренду специалистов у внешних компаний под решение определенных задач. Например, при необходимости участия ИБ в крупном проекте и отсутствии своих свободных экспертов есть возможность "взять напрокат" специалиста у интегратора и вернуть его после завершения проекта.

Опыт ведущих российских компаний показывает, что оптимизация затрат на ИБ возможна даже в текущих сложных условиях.

Сбербанк, например, успешно реализует программу перехода на отечественные решения информационной безопасности, РЖД удалось сократить расходы на ИБ примерно на 20 % за счет внедрения системы риск-ориентированного управления, позволившей более точно распределять бюджет между различными направлениями защиты. В случае с государственными предприятиями стоит выделить также переход на отечественные операционные системы, преимущественно специального назначения.

Затраты на информационную безопасность могут включать расходы на приобретение и обновление программного обеспечения, обеспечение безопасных сетевых соединений, криптографические средства обеспечения безопасности, обучение персонала и аудит безопасности информационных систем. Оценка выгод информационной безопасности может включать защиту от потери конкурентных преимуществ, увеличение уровня доверия и уважения со стороны клиентов, улучшение

репутации компании, снижение рисков в случае нарушения безопасности и снижение потерь при инцидентах информационной безопасности [3].

Библиографический список

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». – URL: http://www.consultant.ru.

2. Иванов, А.С. Четыре проверенных способа оптимизировать расходы на ИБ / А.С. Иванов // IT Security. – 2023. – URL: https://www.itsec.ru/articles/chetyre-proverennyh-sposoba-optimizirovat-raskhody-na-ib.

3. Барейко, С.Н. Экономическая и информационная безопасность России в условиях цифровой экономики / С.Н. Барейко, К.А. Кожухина // Наука Красноярья. – 2019. – Т. 8, № 5. – С. 7–18.