Как оценить обоснованность бюджета на информационную безопасность

Редакция

Фото: pexels.com

Бюджеты компаний на информационную безопасность растут с каждым годом в попытке предотвратить убытки, которые несут в себе киберугрозы. Часто совету директоров или руководству компании предлагается оценить и утвердить расходы, в обоснованности которых весьма непросто разобраться без «переводчика». Realist собрал рекомендации специалистов, которые помогут управленцу оценить эффективность предлагаемых затрат на информационную безопасность.

Почему растут затраты на безопасность

По оценке «Лаборатории Касперского», стоимость одного происшествия в сфере информационной безопасности для крупного бизнеса в России в 2017 году составляла в среднем $861 000, а в 2018 – уже $992 000. За прошлый год более 80% крупнейших компаний сталкивались с атаками киберпреступников. Почти в половине случаев нападения были успешными, свидетельствуют данные опроса Positive Technologies, самой быстрорастущей компанией международного рынка информационной безопасности.

Необходимость дополнительных вложений в

средства защиты информации продиктована также меняющимися требованиями со стороны государства. Кроме закона «О персональных данных» с начала 2018 года практически любая крупная компания попадает под действие нового закона «О безопасности критической информационной инфраструктуры РФ». За его несоблюдение предусмотрены серьезные санкции, вплоть до уголовной ответственности.

> *В результате, бизнес вынужден увеличивать расходы на информационную безопасность. В 2018 году именно так поступили 25% российских компаний, опрошенных Positive Technologies. При этом в каждом пятом случае бюджет вырос на 50%.*

На этом фоне все острее встает вопрос эффективности расходования средств. «Бюджеты российских компаний на информационную безопасность сложно назвать оптимальными. Традиционные средства защиты не справляются даже с малой долей угроз», - рассказал Realist Николай Агринский, основатель компании Phishman, специализирующейся на разработке программных комплексов в области информационной безопасности (ассоциированный партнер British Standards Institute).

Сколько нужно тратить

Оптимальный объем инвестиций в кибербезопасность может колебаться от 5 до 20% всего бюджета на IT, предупреждают опрошенные Realist эксперты. Алексей Комаров, региональный представитель одной из крупнейших в РФ компаний в сфере защиты информации «Уральский центр систем безопасности» (14 место в рейтинге CNews Security) и автор популярного профильного блога оценивает объем вложений в 10-15%. Независимый эксперт Андрей Прозоров считает наиболее подходящей долю в 10% от IT-бюджета компании. Однако, оценивая размер запрашиваемых средств, также следует учесть, как долго в компании занимаются информационной безопасностью. Если различные IT-решения внедряются последовательно несколько лет, названная специалистами доля расходов (до 20%), скорее всего, будет оптимальной. В том же случае, если компания только начинает этот процесс или приступает к выполнению требований регуляторов, доля на информационную безопасность в общем бюджете на информационные технологии может доходить и до 50%.

Цели и средства

Одним из признаков оптимального бюджетирования эксперты называют связанность конкретных статей расходов с теми или иными задачами бизнеса. Внедрение защитных мер должно помочь снизить

финансовые потери и простои, привести к росту производительности труда, например, при автоматизации ручного контроля или рутинных процедур. Инвестиции на запуск и обслуживание таких новаций следует закладывать в бюджет в первую очередь, советуют эксперты в области IT.

Сбалансированность расходов

Еще один важный шаг при оценке бюджета на информационную безопасность – анализ его структуры. Необходимо убедиться, что разработчики документа предусмотрели основные возможные угрозы: кражу ценной информации сотрудниками и конкурентами, вирусные атаки, отказы оборудования, ошибки персонала, штрафы регуляторов. Негативные сценарии должны быть четко описаны, а финансовые ресурсы запланированы для исправления ситуации, если угрозы все-таки реализуются.

Кроме того, бюджет должен предусматривать статьи расходов на организационные меры защиты: обучение пользователей информационных систем, внутренние проверки, тестирование на проникновение. Как считает Николай Агринский, доля подобных затрат должна составлять 20-30% от общих расходов на информационную безопасность.

> *По мнению опрошенных Realist экспертов, наиболее оптимальной можно считать бюджет,*

> *который основан на оценке всех рисков компании и интегрирован в систему риск-менеджмента. По оценке Андрея Прозорова, обычно риски, связанные с информационной безопасностью, составляют в среднем около 5% от всех рисков компании.*

Соответствие стандартам

В пользу составителей бюджета на информационную безопасность будет говорить соответствие документа определенным международным или российским стандартам. Среди мировых стандартов наиболее применимым считается, например, ISO 27000 и немецкий IT-Grundschutz. Многие российские компании из банковского сектора ориентируются на Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС).

Однако ни один из этих стандартов не содержит мероприятий по проверке процессов на соответствие законодательству. Следовательно, при рассмотрении бюджета необходимо убедиться в том, что документ предусматривает отдельные расходы на выполнение требований законов «О персональных данных», «О защите критической информационной инфраструктуры», «О государственной тайне» и т.п.

Кадры и стратегия

Чтобы снизить риски получения необоснованного бюджета на информационную безопасность, важно повышать квалификацию профильных руководителей, их вовлеченность в работу компании. Эксперты рекомендуют включать руководителя службы информационной безопасности в состав руководства, предоставлять ему возможность участвовать в планировании важных проектов.

В век всеобщей цифровизации обойти тему информационной безопасности, в том числе при принятии управленческих решений, весьма рискованно. Если не хватает компетенций в этой области, специалисты советуют привлекать внешний аудит, повышать собственную информированность, но ни в коем случае не полагаться на случай. Для многих бизнесов в современной экономике кибербезопасность относится уже не столько к операционным рискам, сколько к стратегическим.