Количество кибератак на российский бизнес продолжает расти динамичными темпами – в первом полугодии их число увеличилось вдвое в сравнении с 2025 годом. Причем, масштабы бизнеса не имеют значения – риск стать жертвой преступников актуален для всех компаний. Поэтому предпринимателям необходимо не только развивать меры кибербезопасности, но и позаботиться о киберустойчивости своего бизнеса.

О том, как обеспечить киберустойчивость бизнеса и о роли страхования киберрисков рассказали эксперты Страхового Дома ВСК в рамках выступления на сессии «Столкновение с киберрисками. Опыт организации восстановления» форума FintechFest-26.

По оценкам экспертов, в 2025 году было зафиксировано более 105 тыс. кибератак, причем более 20% преступлений пришлось на госучреждения, еще 13% на промышленные компании, 6% — на медицинские учреждения. Киберрискам подвержены предприятия практически всех отраслей экономики. Цель большинства киберпреступлений — частичная или полная остановка работы компании и кража персональных данных. Опытом восстановления работоспособности компании после кибератаки поделился Александр Путилин, член Совета директоров, руководитель блока развития бизнеса Страхового Дома ВСК. В результате инцидента, который длился меньше суток, была повреждена ИТ инфраструктура компании. Восстановление внутренних и внешних сервисов продающего контура заняло у компании примерно 3 недели.

Восстановление инфраструктуры компании можно разделить на несколько основных этапов. Прежде всего, были восстановлены базовые сетевые и вычислительные мощности, системы хранения и доступов. На втором этапе были развернуты сервисы, необходимые для работы приложений, а затем восстановлены пользовательские приложения, организован доступ для сотрудников. Последним шагом стало восстановление ЛК для клиентов, API-интеграций с партнерами, сайта для агентов ВСК.

«По итогам происшествия мы сформировали для себя четыре основные составляющие киберустойчивости компании:

1) Информационная безопасность. Задачи и инвестиции в развитие сервисов

безопасности должны идти с нулевым приоритетом.

2) Безопасное резервное копирование. Защищённость резервных копий, скорость и полнота восстановления систем после атаки – основной фактор минимизации последствий атаки.

3) Готовность ИТ и бизнес-команд к переходу на аварийный режим работы. Понимание характера угрозы и умение реализовывать план восстановления характеризуют уровень готовности команды. Необходимы регулярные тренировки.

4) Киберстрахование. От момента начала восстановления до выхода на нормальный режим работы требуются ресурсы для поддержания непрерывности деятельности организации. Страхование киберрисков это надежный инструмент поддержки решения ключевых задач восстановления.

В совокупности эти четыре фактора позволяют бизнесу системно подходить к вопросам минимизации возможных последствий киберугроз. Киберустойчивость компании также зависит от возможностей оперативного привлечения внешней экспертизы по вопросам информационной безопасности. Руководству компании важно заблаговременно озаботиться созданием пула надежных и профессиональных партнеров. Причем коммуникация с ними должна быть налажена на уровне топ-менеджмента», — отметил Александр Путилин, член Совета директоров, руководитель блока развития бизнеса Страхового Дома ВСК.

Страхование киберрисков позволяет сформировать финансовый резерв на случай ЧП, отметил Антон Казиев, вице-президент, руководитель дирекции страхования киберрисков, ответственности директоров и финансовых институтов Страхового Дома ВСК. Например, покрывает расходы на привлечение внешних экспертов для проведения форензика, пересборки и конфигурации систем, восстановление инфраструктуры из бэкапов, а также оплату переработок собственного персонала. Кроме того, результатом кибератаки всегда становится простой бизнеса, соответственно – убытки, как из-за оттока клиентов и приостановки продаж, так и за счет сохранения операционных расходов. Полис киберстрахования позволяет, в том числе, получить компенсацию упущенной выгоды из-за киберинцидентов. Кроме того, для бизнеса возрастают и юридические риски – появляется вероятность исков от третьих лиц, пострадавших в результате происшествия. Страховка обеспечивает и покрытие расходов на

урегулирование, судебные издержки.

«Киберстрахование – это не просто дополнительная строка расходов, а инструмент, который позволяет компании не тратить свой оборотный капитал на ликвидацию атаки, а спокойно восстанавливаться за счет страховых средств. Сколько бы мы не инвестировали в кибербезопасность, это всего лишь снизит вероятность инцидента, но не гарантирует безопасность бизнеса. Преступники постоянно развивают инструменты и методики хакерских атак. Отсутствие страховой защиты в перспективе может обойтись компании в разы дороже расходов на оформление полиса», — отметил Антон Казиев, вице-президент, руководитель дирекции страхования киберрисков, ответственности директоров и финансовых институтов Страхового Дома ВСК.

Википедия страхования, 03.09.2026 г.