

Информационная составляющая бизнес-рисков

написано Александр Астахов | 10 июня, 2023

Организации подвержены различным типам рисков, которые неизбежно сопровождают любую деятельность. Мы называем такие риски бизнес-рисками. Бизнес-риски отличаются большим разнообразием. Они могут быть классифицированы различными способами. Один из возможных подходов заключается в том, чтобы рассматривать источник риска. Примерами таких рисков являются инвестиционный, юридический, политический или рыночный риски. При другом подходе рассматривается природа актива, подвергающегося риску, примерами являются люди, имущество или информация. Еще один подход рассматривает последствия риска с точки зрения его долгосрочного, среднесрочного либо краткосрочного влияния на деятельность организации; примерами являются стратегический, тактический и операционный риски.

Категории бизнес-рисков:

- *финансовые;*
- *политические;*
- *экономические;*
- *физические;*
- *юридические;*
- *стратегические;*
- *операционные;*
- *информационные;*
- *инвестиционные.*

Риски информационной безопасности (информационные риски) – риски, которым подвергаются информационные активы организации.

Информационные риски должны рассматриваться в качестве одной из основных категорий бизнес-риска. В зависимости от используемой классификации они могут быть отнесены к другим категориям, таким как стратегические и операционные риски. Система управления рисками информационной безопасности имеет дело со всеми информационными рисками, независимо от способа классификации.

Информационная составляющая есть во многих категориях рисков. Надо уметь выделять эту составляющую в любых бизнес-рисках. В следующей таблице приведены примеры угроз информационной безопасности, обуславливающих различные категории рисков, а также возможные последствия этих угроз.

Таблица. Примеры угроз информационной безопасности, обуславливающих различные категории рисков

Категория риска	Информационные угрозы	Последствия
Юридические (санкции со стороны регулирующих и правоохранительных органов)	Неисполнение требований законодательства и нормативной базы в области защиты информации Отсутствие необходимых лицензий Ошибки в договорах или налоговой отчетности	Штрафы, испорченная репутация, запрещение деятельности, выход из бизнеса
Рыночные (изменение ситуации на рынке, дефолты, девальвации и т.п.)	Несвоевременное получение информации Ошибки в прогнозах Фальсификация финансовой отчетности	Финансовые потери, потеря бизнеса

Инвестиционные (неправильные решения по вложению средств)	Недостаточная либо ложная информация, используемая для принятия инвестиционных решенийНесвоевременное получение информации	Финансовые потери
Финансовые (ошибки учета, планирования, неправильное управление финансовыми активами, кража наличности, финансовое мошенничество и т.п.)	Финансовые махинации инсайдеров с использованием компьютерных системКибератаки на банковские счетаКибермошенничество с пластиковыми картамиФальсификация финансовой отчетности	Финансовые потери, ущерб репутации
Репутационные(негативные воздействия на имидж и репутацию компании)	Утечка конфиденциальной информацииНевыполнение обязательств по причине недоступности информационных сервисов	Сокращение клиентской базы
Природные катаклизмы (Пожары, наводнения, землетрясения и т.п.)	Утрата информационных носителей и находящейся на них критичной для бизнеса информацииНедоступность информационных сервисов	Финансовые потери, дезорганизация деятельности, потеря бизнеса
Техногенные(сбои оборудования или ПО)	Потеря критичной для бизнеса информацииПотеря результатов работы	Финансовые потери, дезорганизация деятельности, невозможность исполнения обязательств

Физические (кража, ограбление, саботаж и т.п.)	Потеря критичной для бизнеса информации Утечка конфиденциальной информации Недоступность информационных сервисов	Ущерб репутации, финансовые потери, дезорганизация деятельности
--	--	---

Подробный перечень угроз безопасности, рассматриваемых при оценке информационных рисков, приведен в Приложении № 5.