Результаты исследования рисков, связанных с непрерывностью бизнеса

Опрос проводился с 1 по 27 декабря 2019 года

Участвовали 152 респондента из России

Распределение по отраслям

Как долго предприятия Вашей отрасли смогут продолжать функционировать в случае недоступности ИТ-систем?

40% предприятий могут продолжать работать не более часа

24% могут продолжать работать не более минуты

	Меньше минуты	Меньше часа	Несколько дней и больше	Рабочий день
Малый бизнес	17%	9%	28%	45%
Средний бизнес	**30%**	**20%**	29%	21%
Крупный бизнес	**28%**	**22%**	19%	31%

50% средних и крупных предприятий не могут продолжать функционировать, если ИТ-система компании недоступна более часа

Основные риски прерывания бизнеса в России

** - Респондентам было предложено оценить степень влияния рисков на непрерывность бизнеса по шкале 0-10*

6.3

Кибер-атаки, утечка или потеря данных

6.3

Риски, связанные с изменениями в государственном регулировании (например, изменения в законодательстве)

5.7

Риски, вызванные различного рода форс-мажорами

Ожидания относительно роста рисков

49%

рост рисков ИТ-безопасности, а также рисков, связанных с изменениями в законодательстве

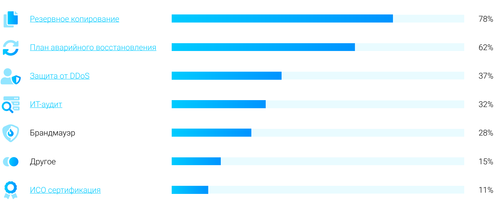
37%

увеличение геополитических рисков (например, внешнеполитических санкций)

24%

рост рисков, связанных с недобросовестной конкуренцией

Резервное копирование и план аварийного восстановления считаются самыми эффективными решениями для предотвращения риска недоступности ИТ-систем



Узнайте больше о современных решениях плана аварийного восстановления и резервного копирования!

Скачайте Руководство по созданию плана аварийного восстановления!