

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ

Компания Cisco провела опрос специалистов в сфере информационной безопасности, представляющих более 200 российских организаций. Его результаты приведены в данной инфографике.

57% российских компаний уже привлекли к себе пристальное внимание в результате взлома систем безопасности

Каждая **третья** российская компания уже требует от своих поставщиков строго придерживаться рекомендаций по кибербезопасности

Почти **половина** российских компаний пострадала от простоев длительностью более 5 часов, вызванных нарушениями защиты



Алексей Лукацкий, бизнес-консультант Cisco по информационной безопасности, считает, что в России многие компании вместо того, чтобы использовать комплексный подход к кибербезопасности, уделяют основное внимание «традиционной защите периметра»: «Облако, оконечные точки, мобильные устройства, приложения, филиалы, центры обработки данных — все это расширяет границы «традиционной сети». У киберпреступников появляется огромное множество потенциальных точек входа, и защитить их все — задача непростая. Чтобы бороться с новыми угрозами, компаниям следует присмотреться к таким новым средствам кибербезопасности, как сетевой мониторинг или защита DNS. Пока же многие считают, что им достаточно межсетевое экрана и антивируса».

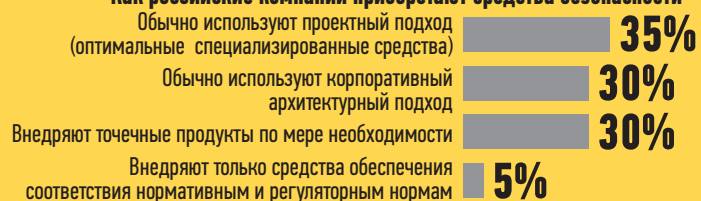
Лишь **42%** организаций в России вкладывают средства в новейшие технологии информационной безопасности, тогда как в других странах доля таких компаний достигает **59%**

37% аварийных сигналов безопасности, полученных российскими компаниями, остаются без внимания

Доля российских компаний, пострадавших в 2016 г. в результате взлома систем безопасности



Как российские компании приобретают средства безопасности



Доля российских компаний, использующих различные средства безопасности



Что же делать?

- Упростить инфраструктуру обеспечения информационной безопасности, пересмотреть принципы закупки и внедрения средств безопасности.
- Повысить эффективность уже имеющихся инструментов.
- Отдать на субподряд функции обеспечения информационной безопасности.
- Изменить модель расходов: например, перенести часть функций в облако.