www.pwc.ru

Игра по новым правилам

Результаты Глобального исследования по вопросам информационной безопасности. Перспективы на 2013 год

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

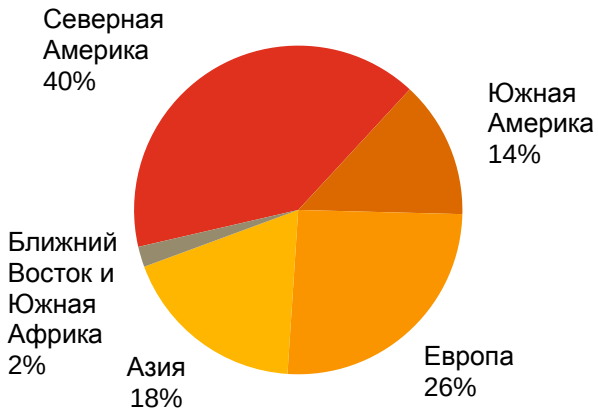
pwc

Раздел 1

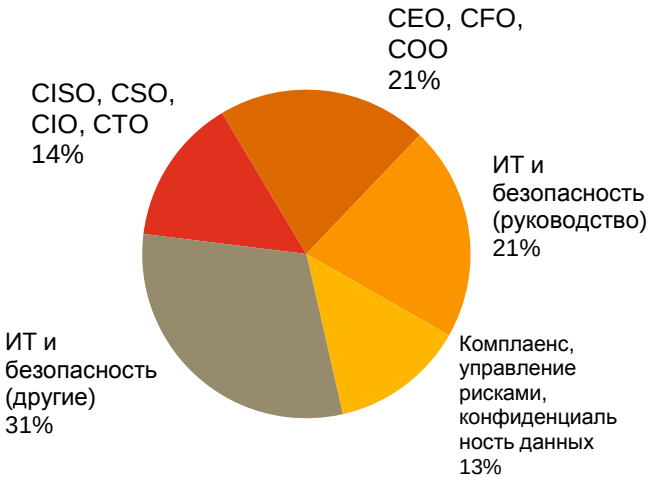
Методика

Глобальный опрос руководителей бизнес-подразделений и ИТ-функций организаций, представляющих различные отрасли

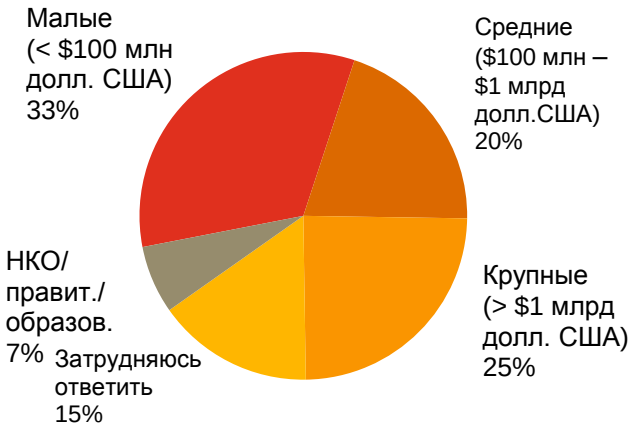
Респонденты по региону деятельности



Респонденты по должности



Респонденты по размеру выручки компании



(Представленные в отчете цифры могут не в полной мере совпадать с исходными данными из-за округления)

Количество респондентов по отраслевому признаку

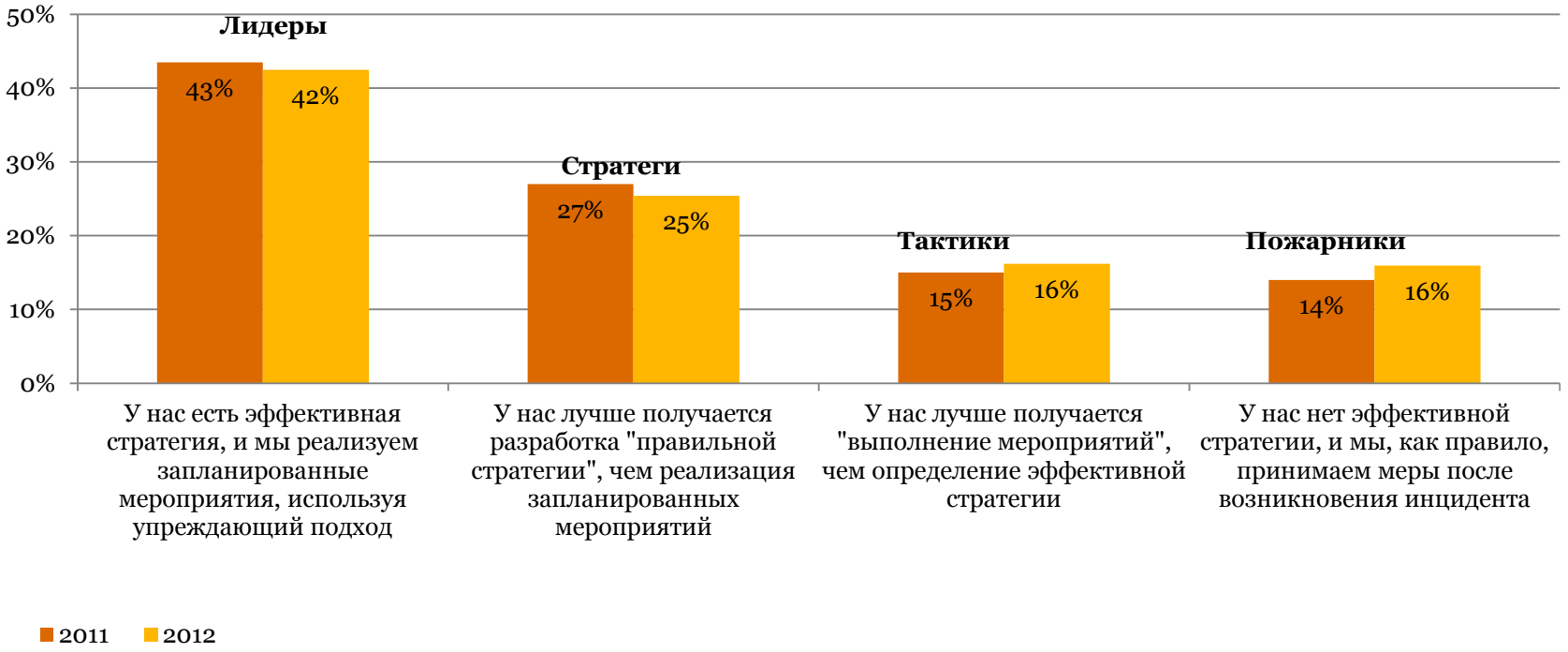
Отрасль	Количество респондентов в этом году
Технологии	1 469
Финансовые услуги	1 338
Розничная торговля и производство потребительских товаров	1 169
Производство товаров промышленного назначения	775
Государственный сектор	730
Телекоммуникации	511
Поставщики медицинских услуг	467
Индустрия развлечений и СМИ	378
Аэрокосмическая и оборонная отрасль	242
Автомобилестроение	218
Электроэнергетика	201
Энергетика (нефтегазовая отрасль)	136
Фармацевтика	112

Раздел 2

Уверенность в игре: компании сами оценивают свои мероприятия по обеспечению информационной безопасности

Респонденты уверены в эффективности проводимых ими мероприятий по обеспечению безопасности

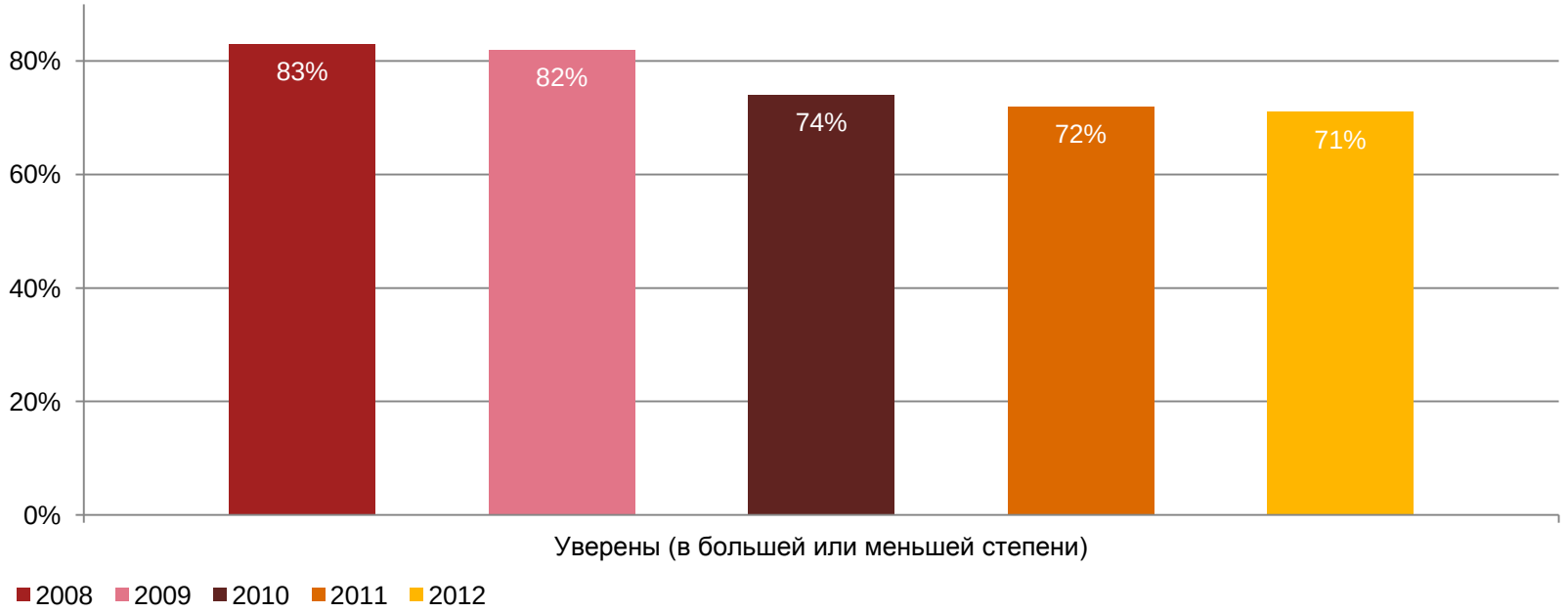
Сорок два процента респондентов утверждают, что в их компаниях принята соответствующая стратегия, для реализации которой они используют упреждающий подход. На основании полученных ответов можно выделить две характерные черты компании-лидера.



Вопрос 28: «Какое из перечисленных ниже утверждений наилучшим образом характеризует подход Вашей организации к обеспечению информационной безопасности?» (Представленные в отчете цифры могут не совсем совпадать с исходными данными из-за округления.)

По мнению большинства респондентов, в их организациях осуществляются эффективные мероприятия по обеспечению информационной безопасности, однако этот показатель снижается

Уверенность – хорошее чувство. Более 70% респондентов абсолютно уверены (32%) или уверены, но в меньшей в меньшей степени (39%) в том, что в их организациях осуществляются эффективные мероприятия по обеспечению информационной безопасности. Однако они, возможно, не знают, что после 2008 года показатель уверенности начал снижаться.



Вопрос 41: «Насколько Вы уверены в том, что в Вашей организации осуществляются эффективные мероприятия по обеспечению информационной безопасности?»

Раздел 3

Познакомьтесь с лидерами: сравнение результатов оценки компаниями положения дел в своих организациях с нашими критериями, по которым мы относим компании к группе лидеров

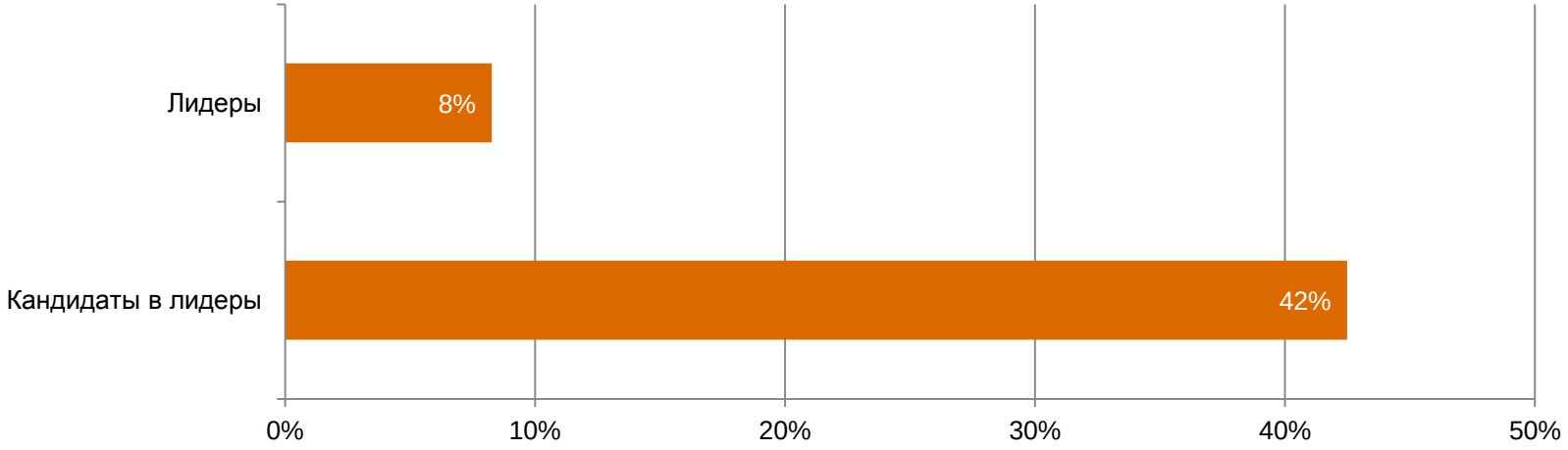
Контрольный список для определения лидеров в области информационной безопасности

Результаты самооценки не всегда соответствуют истине. Для определения настоящих лидеров в области информационной безопасности мы проанализировали результаты самооценки респондентов по четырем основным критериям, по которым определяется лидерство в этой сфере. Чтобы войти в число ведущих компаний, организация должна:

- иметь общую стратегию в области информационной безопасности;
- иметь в штате директора по информационной безопасности или равноценное должностное лицо, находящееся в подчинении у членов высшего руководства – например, у президента/генерального директора, финансового директора, директора по производству или советника по правовым вопросам;
- выполнить оценку и анализ эффективности своей системы информационной безопасности за прошедший год;
- иметь четкое представление о том, какого рода инциденты в области информационной безопасности имели место в прошедшем году.

Проверка на соответствие требованиям, предъявляемым к настоящим лидерам

Результаты проведенного нами анализа показывают, что лишь 8% респондентов могут быть отнесены к категории настоящих лидеров в области информационной безопасности. Сравнительный анализ этой группы с более многочисленной группой респондентов, которые сами назвали себя лидерами, позволяет предположить, что у многих организаций есть возможности повысить эффективность процессов и мероприятий в области информационной безопасности.



Лидеры определяются на основании ответов на вопрос 13А: «Какой организационной единице/ должностному лицу подотчетен директор по информационной безопасности, руководитель службы безопасности или иное лицо, занимающее аналогичную руководящую должность в сфере информационной безопасности?»; вопрос 14: «Какие средства обеспечения информационной безопасности, связанные с процессами, используются в Вашей организации?»; вопрос 18: «Какого рода инциденты в сфере безопасности (нарушение установленных правил или вынужденный простой) имели место?» и вопрос 31: «Проводилась ли в Вашей компании оценка и анализ эффективности правил и процедур по обеспечению информационной безопасности за прошедший год?».

Как эта группа лидеров обеспечивает конкурентное преимущество в игре

Ведущие компании значительно опережают остальных респондентов по таким параметрам, как наличие более развитой программы по обеспечению информационной безопасности, реализация стратегий с учетом новейших технологий и использование современного технологического инструментария для защиты данных.

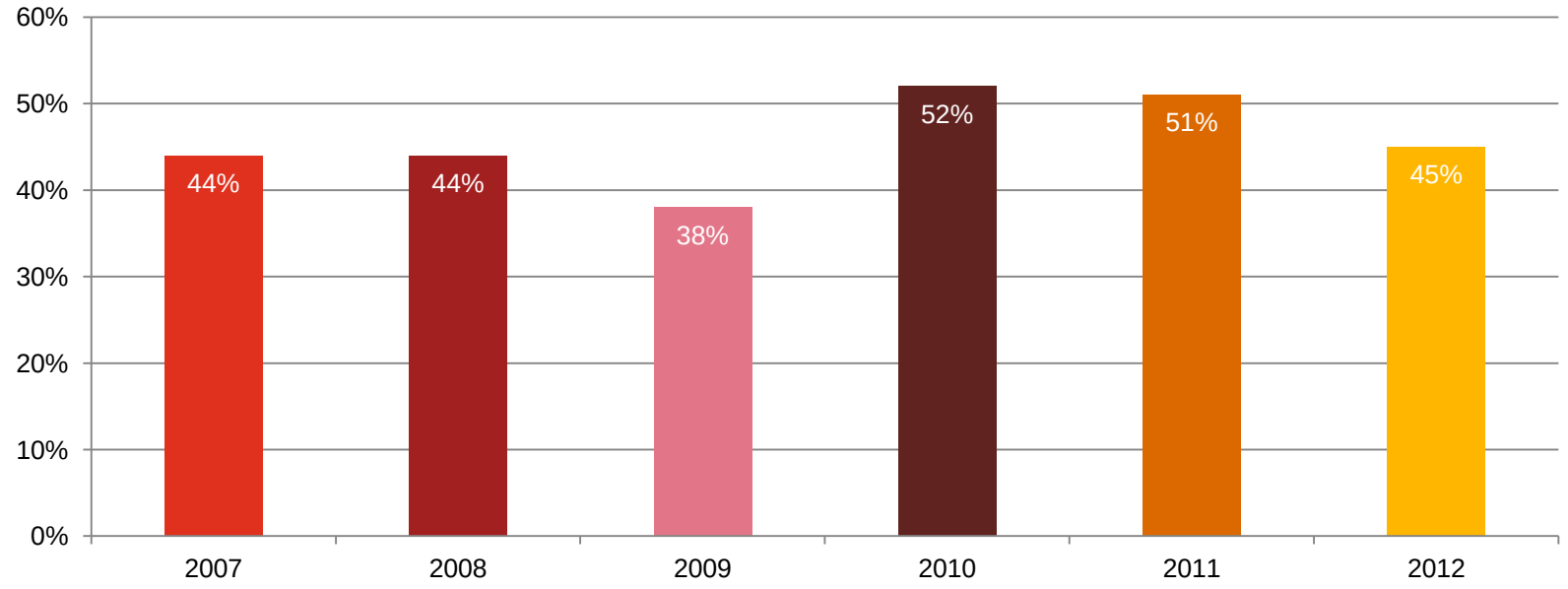
	Лидеры	Все участники опроса
Ожидают увеличения расходов на информационную безопасность в следующем году	74%	45%
В штате есть директор по информационной безопасности или равнозначная должность	90%	42%
Привлекают специалистов по информационной безопасности в рамках крупных проектов на начальном этапе проекта	45%	25%
Расходы на информационную безопасность полностью соответствуют бизнес-целям	50%	30%
Уверены, что в компании сформирована корпоративная культура, основанная на принципах поведения, которые обеспечивают эффективность системы информационной безопасности	94%	68%
Имеется комплексная система, регулирующая вопросы соблюдения внешних и внутренних нормативных документов, обеспечения конфиденциальности/ использования данных, безопасности, хищения идентификационных данных	92%	60%
Имеется стратегия обеспечения безопасности при использовании мобильных устройств	57%	44%
Используют инструменты, позволяющие обнаружить вредоносный программный код	86%	71%
Используют инструменты, позволяющие предотвратить вторжения	78%	59%
В течение прошедшего года выполнили оценку и анализ состояния информационной безопасности	100%	49%

Раздел 4

Рискованная игра: постепенное сокращение технических возможностей

На фоне восстановления после глобального экономического кризиса бюджетные расходы на информационную безопасность растут более медленными темпами

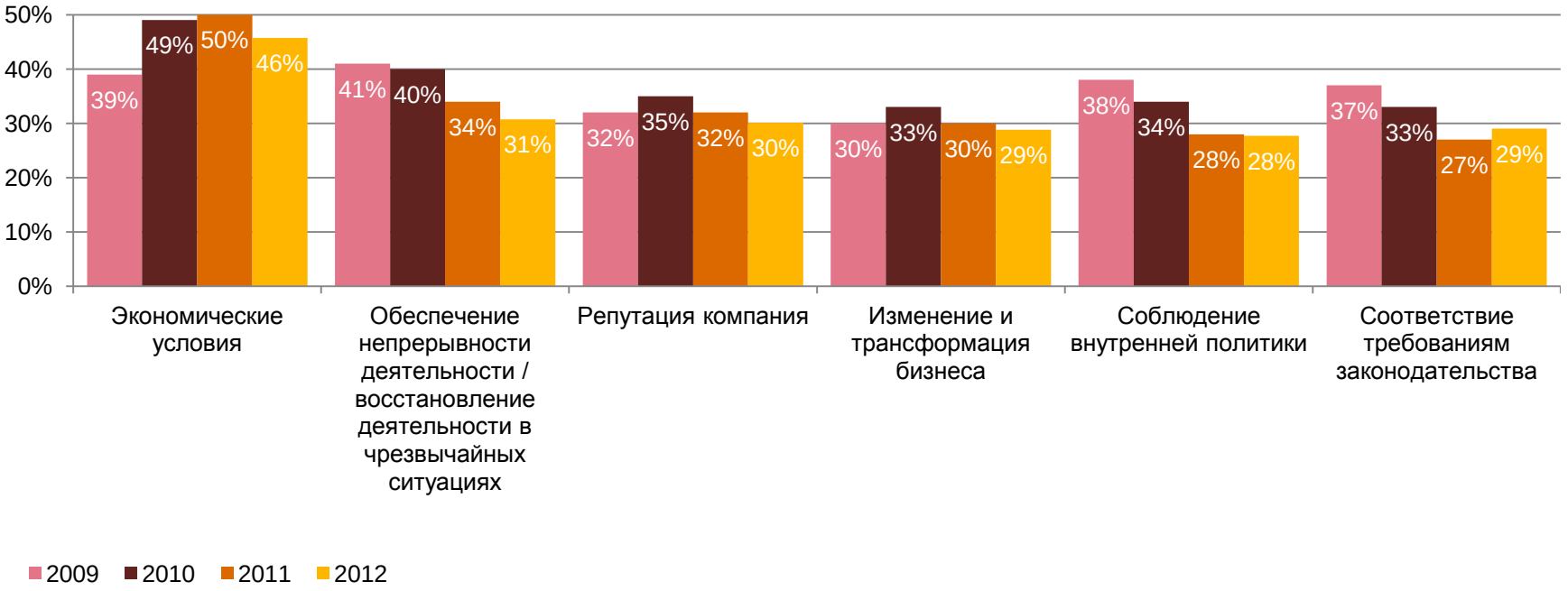
В настоящее время выделяется больше средств, чем во время экономического спада, однако наблюдается выравнивание линии повышательного тренда, т. е. рост бюджетных расходов на обеспечение безопасности, наблюдавшийся в докризисные годы, сменился их стабилизацией. Менее половины респондентов ожидают увеличения бюджетов в ближайший год, а 18% ответили, что они не знают, куда будут направлены средства.



Вопрос 8: «Если сравнивать с прошлым годом, как изменятся расходы на обеспечение информационной безопасности в ближайшие 12 месяцев?» (Респонденты, ответившие «Увеличатся до 10%», «Увеличатся на 11-30% или «Увеличатся более чем на 30%».)

Бюджеты на обеспечение безопасности составляются исходя из экономических условий, а не требований безопасности

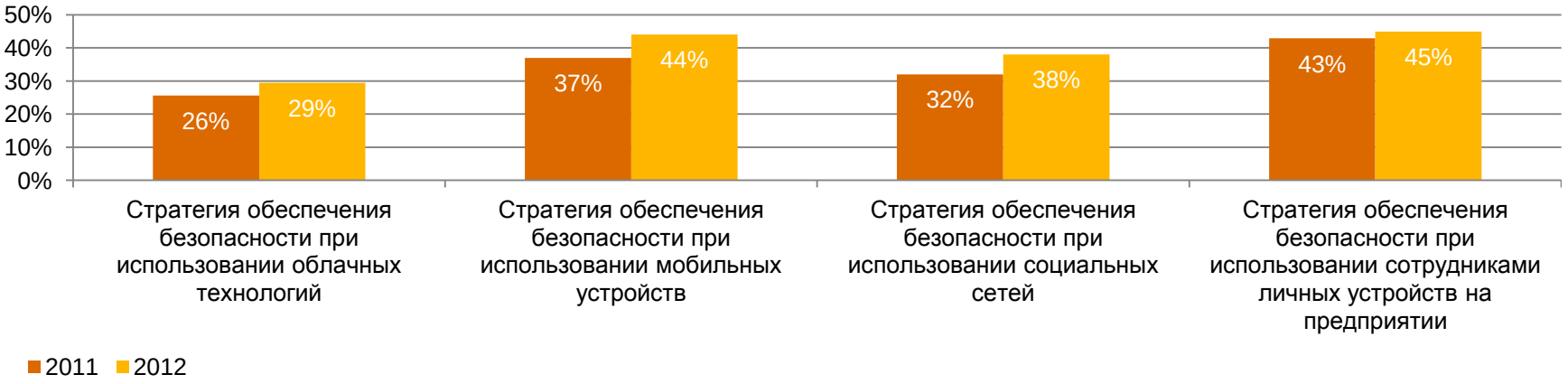
Почти половина (46%) респондентов отметили, что экономические условия являются главным фактором, определяющим объем расходов на информационную безопасность. Самым важным мероприятием в ответ на требования безопасности является план действий по обеспечению непрерывности бизнеса/ восстановления деятельности в чрезвычайных ситуациях.



Вопрос 37: «Какие бизнес-проблемы или факторы определяют величину расходов на информационную безопасность в Вашей компании?» (Показаны не все факторы.)

Использование новых технологий идет более быстрыми темпами, чем реализация соответствующих мер по обеспечению безопасности

Компании прилагают массу усилий, чтобы оперативно реагировать на использование облачных вычислений, социальных сетей, мобильных и личных устройств. Тем не менее часто в общих планах по обеспечению информационной безопасности отсутствуют мероприятия, необходимые в связи с внедрением новых технологий. Например, по результатам последнего опроса выяснилось, что 88% потребителей используют персональные мобильные устройства как для личных целей, так и для выполнения рабочих заданий [2].



Вопрос 14: «Какие используются средства обеспечения информационной безопасности, связанные с процессами?» (Показаны не все факторы. Сумма ответов не равна 100%.)

[2] Защита персональных данных потребителей. Какими данными потребители готовы обмениваться? PwC, июль 2012 г.

Раздел 5

Что это значит для вашего бизнеса

Что можно сделать, чтобы повысить эффективность деятельности в области информационной безопасности

Компании, которые хотят повысить эффективность деятельности по обеспечению безопасности, должны:

- реализовать стратегию комплексной оценки рисков и учитывать выявленные риски при определении объема инвестиций, выделяемых на обеспечение безопасности;
- иметь четкое представление о содержании корпоративной информации, и о том, кто в ней заинтересован и какие действия могут предпринять злоумышленники, чтобы получить эту информацию;
- использовать новый подход к решению задач, основанный на том, что обеспечение информационной безопасности включает в себя не только использование средств защиты данных, но и возможность создания дополнительных преимуществ для компании.

Спасибо!

Евгений Климов
Старший менеджер
Тел.: +7 (495) 967-6086
evgeny.klimov@ru.pwc.com