

# Под прицелом

Исследование по информационной безопасности  
за 2009 год в России



# Содержание

Предисловие .....	3
Портрет респондента .....	3
Влияние экономического спада на функцию обеспечения информационной безопасности: основные выводы .....	6
Ключевые инициативы по достижению целей обеспечения информационной безопасности в сложных экономических условиях .....	10
Как PricewaterhouseCoopers может вам помочь .....	16



## Предисловие

Представляем вашему вниманию первое исследование для России из серии ежегодного глобального исследования по вопросам обеспечения информационной безопасности, проводимого PricewaterhouseCoopers по всему миру.

Обращаем внимание, что данное исследование проводилось в самый разгар финансового кризиса. Мы искренне благодарим всех, кто нашел время для того, чтобы ответить на наши вопросы. В этом году принять участие в нашем опросе можно было, заполнив анкету в Интернете. Обзор был проведен с мая по июнь 2009 года; в нем приняли участие более 7000 респондентов из 114 стран, в том числе 88 участников из России.

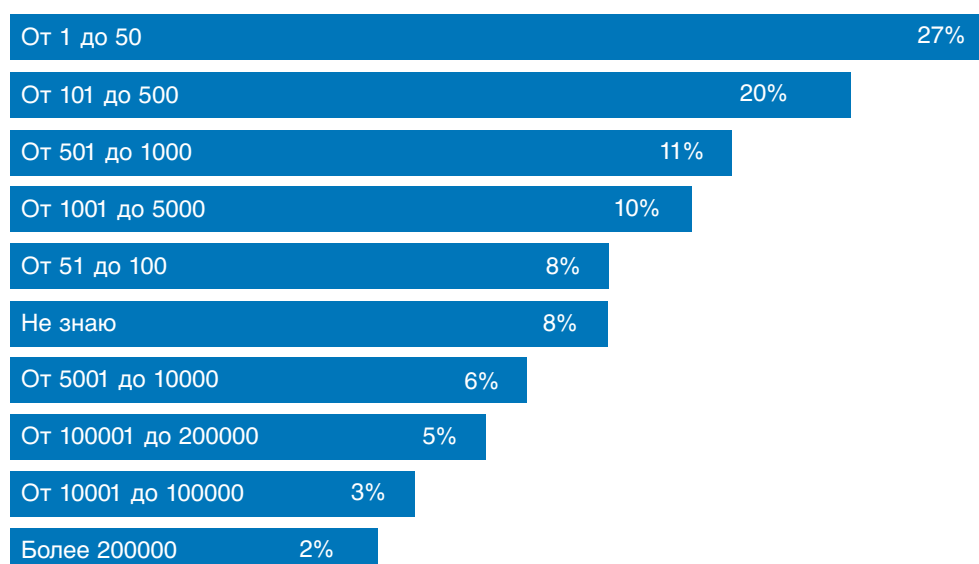
В данной публикации проведен анализ результатов опроса среди российских компаний.

Цель обзора состояла в том, чтобы определить, какое влияние оказывает текущий экономический спад на функции обеспечения информационной безопасности российских компаний, а также выявить ключевые инициативы по достижению целей обеспечения информационной безопасности в сложных экономических условиях. Ответы на вопросы были анонимными, но при желании респондент имел право указать информацию о себе.

## Портрет респондента

Полученная выборка не имеет явного преимущества в сторону больших или маленьких компаний. Таким образом, мы получили равномерное распределение по всему спектру компаний респондентов (рис. 1).

**Рисунок 1. Количество работающих в компании сотрудников**



На долю небольших организаций, в которых работают от 100 до 500 сотрудников, пришлось 20% респондентов, в то время как треть респондентов (34%) работают в компаниях с количеством персонала не более 100 человек. На долю крупных компаний (более 1000 сотрудников) пришлось 34% опрошенных. Около 8% респондентов не смогли дать четкого ответа о количестве сотрудников своих компаний. Таким образом, равномерное распределение ответов позволяет получить реальную картину рынка, свидетельствующую о том, что все организации, независимо от размера, сталкиваются с проблемами в области обеспечения информационной безопасности своих активов.

Отраслевое распределение респондентов дало следующие результаты (см. рис. 2). Лидирующее положение занимают технологические компании (23%), что говорит о более высоком уровне понимания угроз информационной безопасности. В данную категорию также вошли компании, работающие в секторе телекоммуникаций. Второе место (20% от опрошенных) занимают товарные компании, осуществляющие продажу потребительских товаров. Третье место (15%) разделили компании финансового сектора и компании, предлагающие услуги в сфере развлечений и средств массовой информации.

И замыкают список участников опроса по отраслевому принципу производственные компании (13%)

## Рисунок 2. Сфера деятельности компании

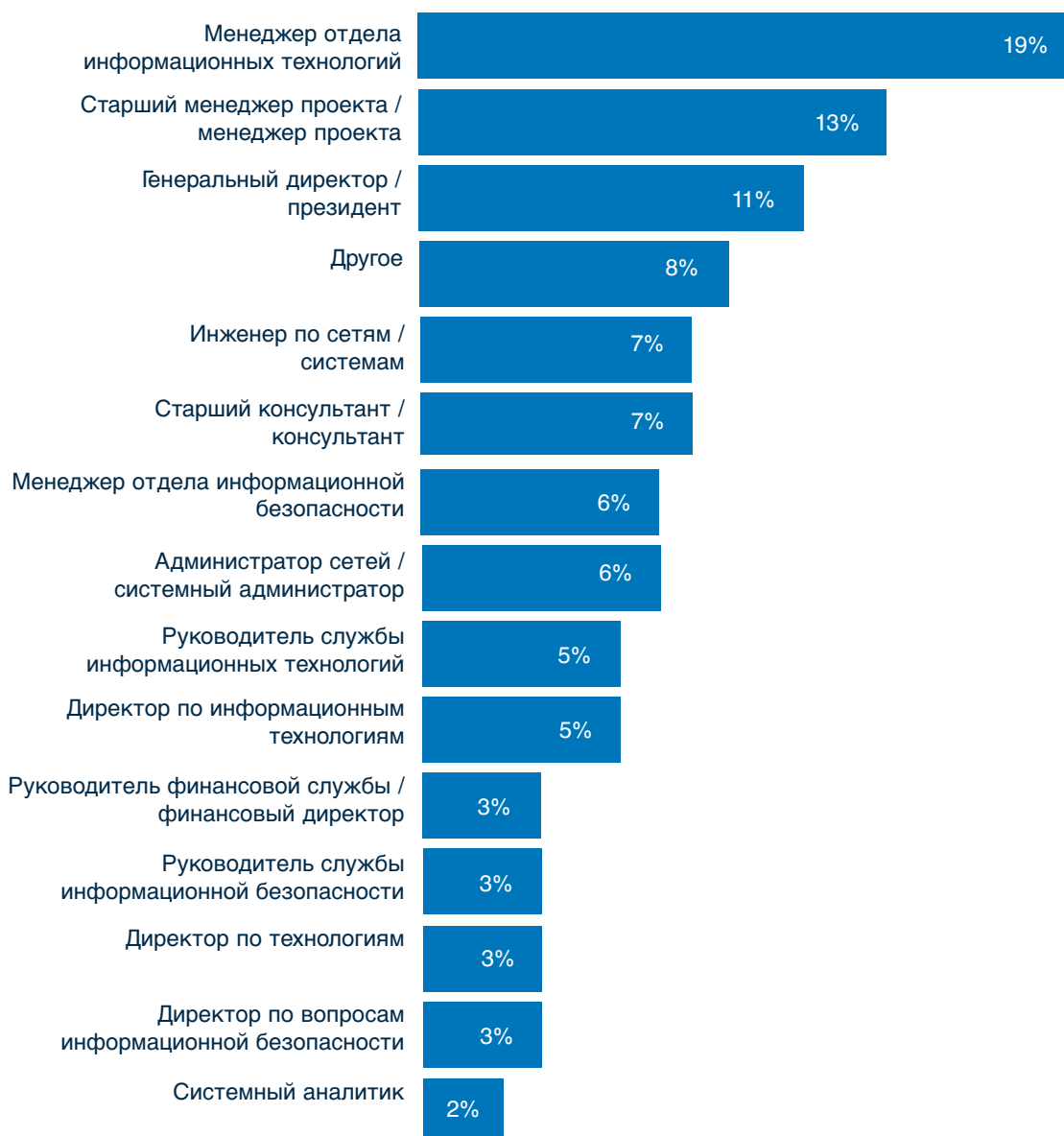
Технологии	23%
Розничная торговля и производство потребительских товаров	20%
Индустрия развлечений и СМИ	15%
Финансовые услуги	15%
Промышленное производство	13%
Отрасль здравоохранения	5%
Сельское хозяйство	3%
Другое	3%
Топливо-энергетическая и горнодобывающая промышленность	2%
Аэрокосмическая и оборонная промышленность	1%

Вызвал удивление тот факт, что компании финансового сектора заняли лишь третью позицию в обзоре, что не является характерным для компаний данного сегмента, обычно занимающих первые позиции в опросах подобного рода. Вероятнее всего, это связано с неустойчивым положением в финансовом секторе; возможно, часть усилий специалистов по информационной безопасности финансовых компаний сосредоточена на оказании помощи в минимизации финансовых рисков (кредитного, ликвидности и нестабильности кредитного спреда).

Важно отметить, что две трети опрошенных специалистов могут влиять на процесс принятия решений в области управления и обеспечения информационной безопасности. Таким образом, можно утверждать, что полученные в результате исследования данные отражают основные направления деятельности российских компаний по обеспечению информационной безопасности в условиях экономического спада (рецессии).

Подавляющее большинство ответов (19%) было получено от менеджеров (начальников отделов) департаментов информационных технологий компаний, участвующих в опросе.

**Рисунок 3. Распределение респондентов по должности**



# Влияние экономического спада на функцию обеспечения информационной безопасности: ОСНОВНЫЕ ВЫВОДЫ

Для определения того, в какой степени текущий экономический спад влияет на функцию обеспечения информационной безопасности в российских компаниях, мы сформулировали ряд утверждений и попросили участников опроса указать свое отношение к этим утверждениям.

## **Вывод 1**

Большинство респондентов считают, что в условиях нынешнего экономического спада стало больше угроз для ИТ-активов компаний.

## **Вывод 2**

Также большинство участников подтвердили, что сокращение финансирования усложняет поддержку обеспечения информационной безопасности.

## **Вывод 3**

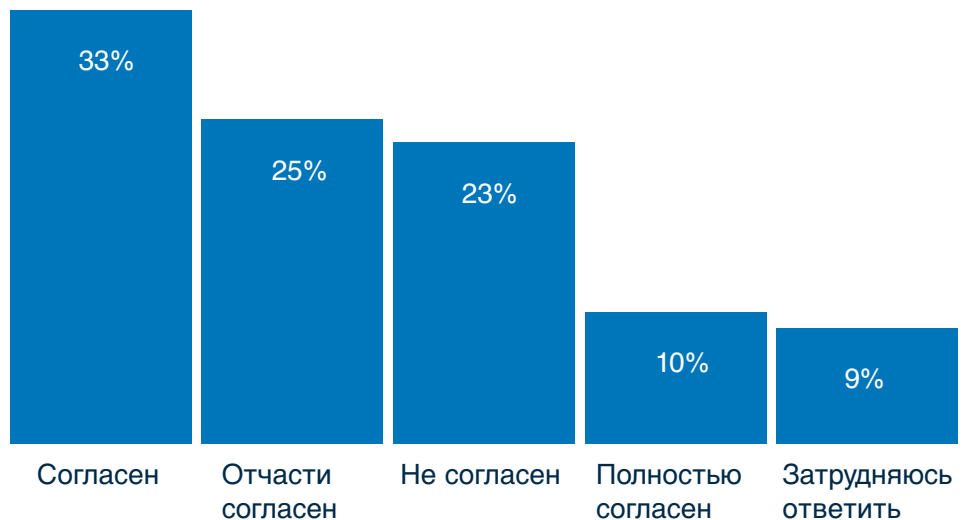
Однако почти половина респондентов полагают, что финансовый кризис не оказал значительного влияния на обеспечение функции информационной безопасности в их компаниях.

## Вывод 1

Большинство респондентов считают, что в условиях нынешнего экономического спада стало больше угроз для ИТ-активов компаний.

Для респондентов было сформулировано утверждение: «Угрозы информационной безопасности для ИТ-активов компании возросли».

**Рисунок 4. Ответы респондентов на утверждение «Угрозы информационной безопасности для ИТ-активов компании возросли»**



Ответы респондентов распределились следующим образом (см. рис. 4):

43% участников опроса согласились с данным утверждением, причем 10% из них выразили полное согласие с этим утверждением. 25% участников отчасти согласились с этим утверждением. 23% считают, что количество угроз информационной безопасности не увеличилось и не зависит от экономического спада. 9% опрошенных затруднились оценить количество угроз информационной безопасности для ИТ-активов своих компаний.

Таким образом, можно сделать вывод о том, что в условиях экономического кризиса количество угроз информационной безопасности, по мнению участников обзора, увеличилось. В сложившейся ситуации нужно прежде всего позаботиться о том, чтобы компания могла обеспечить защиту от существующих и возникающих угроз и противодействовать им. Одним из возможных путей может стать оповещение на регулярной основе всех сотрудников компании о возможных и вновь появившихся угрозах.

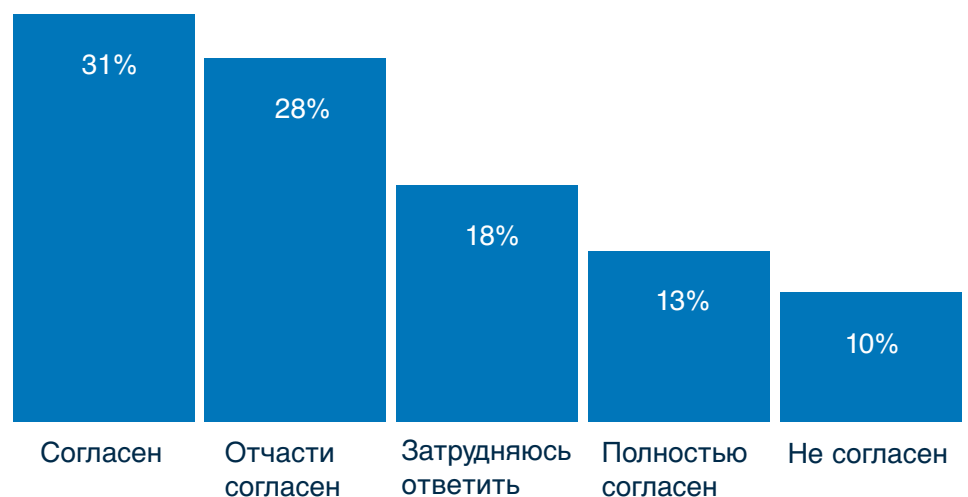
## Вывод 2

### Большинство участников подтвердили, что сокращение финансирования усложняет поддержку обеспечения информационной безопасности.

Утверждение было сформулировано следующим образом: «Считаете ли Вы, что сокращение затрат на обеспечение информационной безопасности затруднит достижение адекватного уровня безопасности ИТ-активов компании?»

Ответы, полученные от участников опроса, не вызвали удивления (см. рис. 5). Большинство респондентов (72%) считают, что сокращение инвестиций может повлиять на обеспечение необходимого уровня информационной безопасности. Из них 31% опрошенных согласился с данным утверждением, 13% выразили полное согласие, а 28% респондентов частично согласны с данным утверждением. И только 10% участников опроса выразили мнение, что сокращение затрат на обеспечение безопасности не окажет существенного влияния на поддержание необходимого уровня информационной безопасности ИТ-активов. При этом 18% опрошенных затруднились оценить влияние сокращения затрат на обеспечение необходимого уровня информационной безопасности.

**Рисунок 5. Ответы респондентов на утверждение "Сокращение затрат на обеспечение информационной безопасности затруднит достижение адекватного уровня безопасности ИТ-активов компании"**



Такое положение приводит к тому, что в настоящее время предпочтение должно отдаваться наименее затратным, но эффективным технологическим решениям, при этом не стоит забывать и об организационных мерах и решениях по обеспечению информационной безопасности ИТ-активов компании.

## Вывод 3

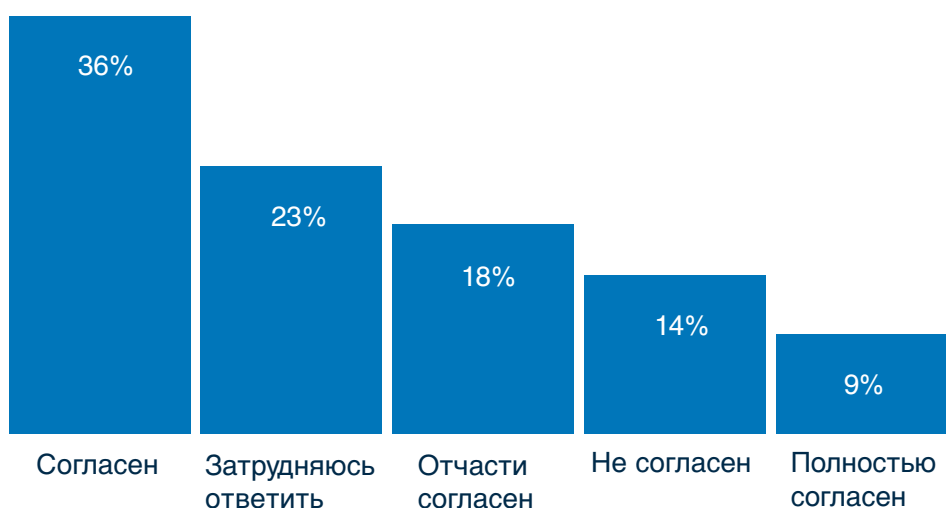
Почти половина респондентов полагают, что финансовый кризис не оказал значительного влияния на обеспечение функции информационной безопасности для их компаний.

Участникам опроса было предложено следующее утверждение: «Экономический спад не оказал значительного влияния на функцию информационной безопасности Вашей компании».

Большинство участников опроса согласны с тем, что из-за последствий финансового кризиса возросли угрозы для ИТ-активов компании, связанные со снижением лояльности сотрудников, партнеров и поставщиков (см. рис. 6). Вынужденное сокращение штата компаний (увольнение сотрудников) также негативно сказывается на уровне информационной безопасности компаний-респондентов (см. Вывод 1). Кроме того, респонденты отметили, что сокращение финансирования усложняет поддержку информационной безопасности на необходимом уровне (см. Вывод 2).

Тем не менее 64% опрошенных сообщили, что последствия экономического кризиса практически не затронули функцию информационной безопасности. Из них 36% респондентов согласны с данным утверждением, 9% выразили полное согласие, а 18% участников опроса согласны с данным утверждением частично. И только 14% опрошенных сообщили, что ощутили влияние экономического кризиса на обеспечении функции информационной безопасности.

**Рисунок 6. Ответы респондентов на утверждение «Экономический спад не оказал значительного влияния на функцию информационной безопасности Вашей компании»**



# Ключевые инициативы по достижению целей обеспечения информационной безопасности в сложных экономических условиях

Вторая часть опроса была посвящена идентификации ключевых инициатив по достижению целей обеспечения информационной безопасности в сложных экономических условиях. Респондентам были предложены 17 инициатив по информационной безопасности, из которых нужно было выбрать наиболее актуальные для компаний-респондентов в настоящее время. По результатам анализа мы отобрали пять ключевых инициатив, которые набрали наибольшее количество голосов участников опроса.

## **Инициатива 1**

Обеспечение защиты данных – основной приоритет

## **Инициатива 2**

Применение средств автоматизации для обеспечения информационной безопасности

## **Инициатива 3**

Увеличение доверия к аутсорсингу функции обеспечения информационной безопасности

## **Инициатива 4**

Анализ рисков – основа для инвестиций в информационную безопасность

## **Инициатива 5**

Соответствие требованиям регуляторов

# Инициатива 1

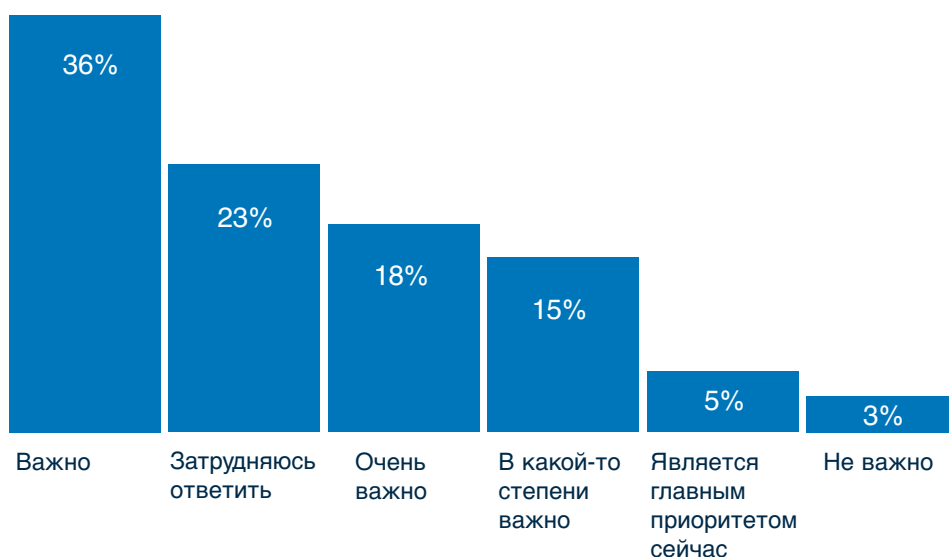
## Обеспечение защиты данных – основной приоритет

Абсолютное большинство респондентов отдали свое предпочтение данной инициативе (см. рис. 7). Обеспечение защиты данных (информации) становится основным приоритетом информационной безопасности.

В нынешней ситуации, когда большинство компаний переживают последствия экономического кризиса, такое единодушие вполне объяснимо. В связи со сложными экономическими условиями, когда компании вынуждены сокращать персонал и снижать уровень вознаграждения для сотрудников, когда различные организации прекратили свое существование, а компаниям, сумевшим выстоять, зачастую приходится заново привлекать бизнес-партнеров и поставщиков, защита информационных активов становится не только очевидной, но и необходимой для любой компании. Хищение информационных активов и передача чувствительной информации конкурентам может быть осуществлена сотрудниками компании, например с целью обогащения.

Положительную оценку важности и необходимости реализации данной инициативы дали 74% респондентов. Из них 5% отдали наивысший приоритет осуществлению данной инициативы. 18% опрошенных считают, что обеспечение защиты информационных активов является крайне необходимым мероприятием для их компаний. 36% участников опроса заявили, что данная инициатива является важной для их компаний. 15% не полностью уверены, что должны сосредоточить свои усилия на мероприятиях, обеспечивающих защиту информационных активов. И только 3% опрошенных сообщили, что инициатива по сохранению информации не является для их компаний важной. При этом 23% респондентов затруднились оценить, насколько данная инициатива важна для их компаний.

**Рисунок 7. Степень важности обеспечения защиты данных**



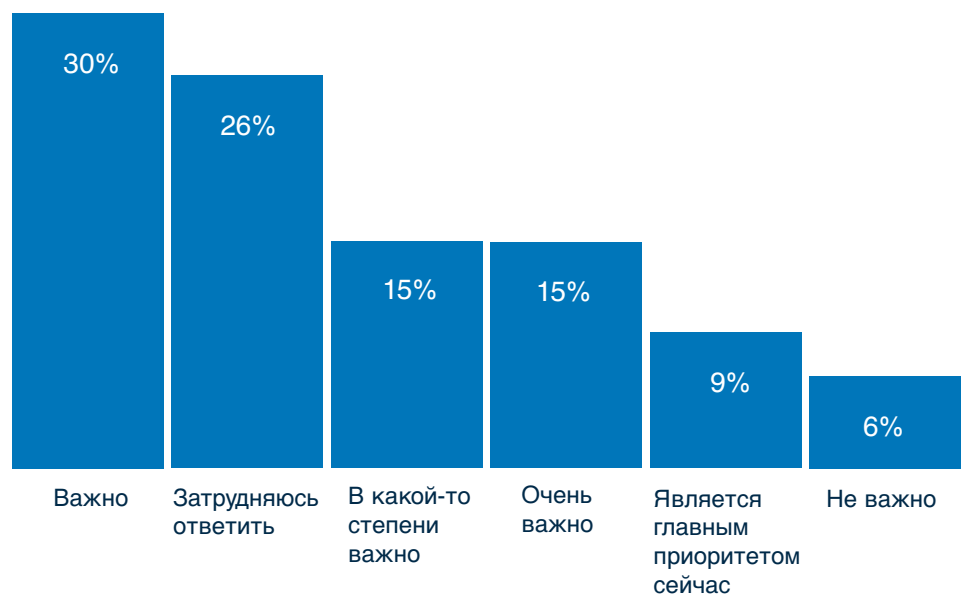
## Инициатива 2

### Применение средств автоматизации для обеспечения информационной безопасности

Инициатива по применению и внедрению средств автоматизации информационной безопасности, согласно результатам опроса участников, оказалась очень популярной и заняла второе место среди предложенных инициатив. Участники опроса сообщили, что за счет внедрения систем автоматизации для обеспечения функции информационной безопасности они планируют достичь сокращения затрат и повышения производительности при обеспечении функции информационной безопасности (см. рис. 8). К системам такого рода можно отнести решения по предотвращению утечек информации, антивирусные решения, системы фильтрации трафика. Данные средства автоматизации обеспечения информационной безопасности получили наибольшее количество голосов участников опроса. Мнения наших респондентов о необходимости использования средств автоматизации распределились следующим образом.

30% респондентов считают приобретение и внедрение средств автоматизации информационной безопасности важной инициативой для своей организации. 15% опрошенных сообщили, что данная инициатива крайне важна для обеспечения защиты компании, а 9% отдали наивысший приоритет данной инициативе и планируют уже в ближайшее время реализовать проекты по автоматизации функции информационной безопасности. 15% участников опроса не в полной мере согласны с такой инициативой и считают, что приобретение и внедрение средств автоматизации в сложных экономических условиях не может быть приоритетной задачей. 6% респондентов сообщили, что являются противниками этой инициативы в данный период и не собираются осуществлять приобретение и внедрение систем подобного рода в ближайшее время. При этом 26% респондентов затруднились оценить, насколько данная инициатива важна для их компании.

**Рисунок 8. Степень важности применения средств автоматизации для обеспечения информационной безопасности**

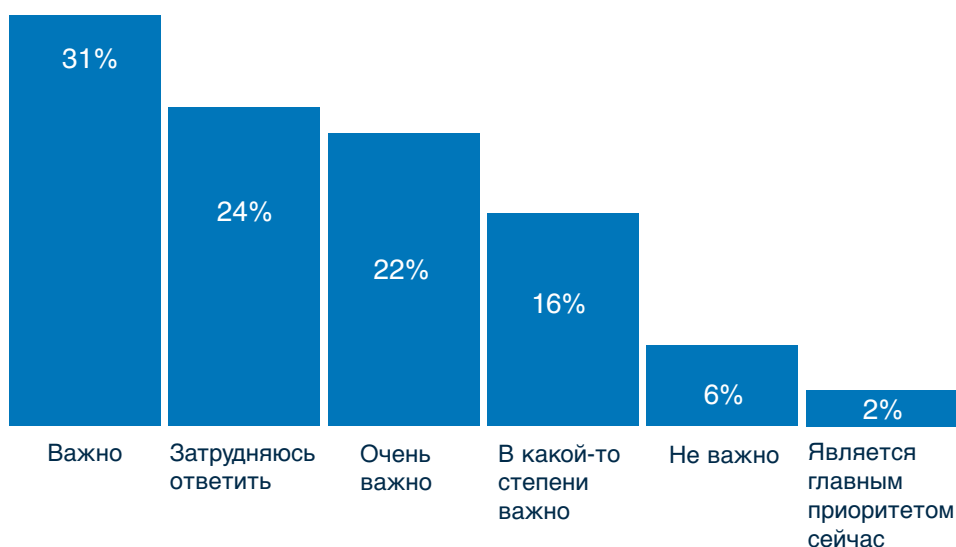


## Инициатива 3 Передача функции по обеспечению информационной безопасности на аутсорсинг

Инициатива по передаче части функций (а в некоторых случаях и полностью) по обеспечению информационной безопасности на аутсорсинг заняла третье место в нашем опросе (см. рис. 9). Общая тенденция прослеживается очень четко. 70% респондентов сообщили, что они в той или иной мере заинтересованы в передаче ряда полномочий по обеспечению информационной безопасности третьим компаниям (аутсорсинг), специализирующимся на выполнении такого рода работ. В настоящее время на рынке наблюдается усиление конкуренции в данной нише среди компаний – провайдеров услуг обеспечения информационной безопасности и жесткая борьба за удержание существующих и привлечение новых клиентов.

Наивысший приоритет данной инициативе отдали лишь 2% участников опроса. Очень важной данную инициативу сочли 22% респондентов, важной – 31%. Указанные респонденты планируют передать часть функций на аутсорсинг, тем самым полагая, что такой подход позволит им обеспечить более эффективную и недорогую защиту информационных активов, чем развитие данных функций и направлений в собственной компании. 16% респондентов настороженно относятся к данной инициативе, но тем не менее полагают, что передача части полномочий по обеспечению функции информационной безопасности все же возможна. 6% опрошенных выразили категорическое несогласие с данной инициативой. Здесь явно прослеживается консервативный подход к обеспечению функции информационной безопасности. И, наконец, 24% респондентов затруднились ответить, насколько данная инициатива важна для их компаний.

**Рисунок 9. Степень важности передачи функции по обеспечению информационной безопасности на аутсорсинг**



Результаты опроса свидетельствуют об основной тенденции, которая четко прослеживается в ответах респондентов, а именно: большинство участников опроса в той или иной мере готовы передать часть своей функции по обеспечению информационной безопасности на аутсорсинг.

## Инициатива 4

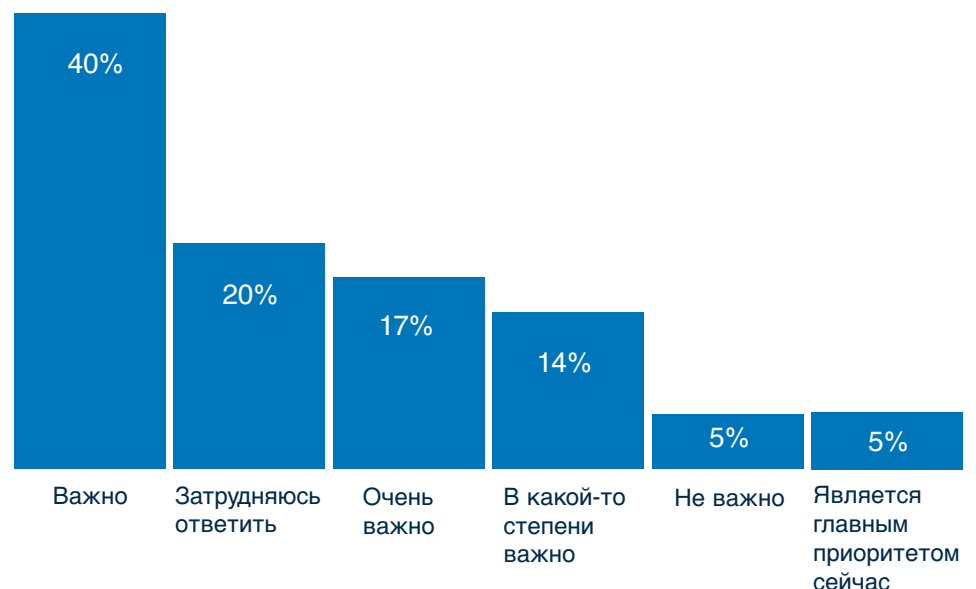
### Анализ рисков – основа для инвестиций в информационную безопасность

Согласно результатам опроса, 61% респондентов полагают, что именно анализ информационных рисков должен лечь в основу при формировании пакета инвестиций в обеспечение информационной безопасности компании (см. рис. 10).

Создание методики оценки рисков, проведение регулярной оценки рисков и анализа результатов такой оценки, по мнению 40% опрошенных, должны лечь в основу при формировании бюджета на обеспечение информационной безопасности. 17% опрошенных считают данную инициативу крайне важной для своей компании, и 5% участников отдали наивысший приоритет этой инициативе, планируя осуществить её реализацию в ближайшее время несмотря на трудности с финансированием.

14% респондентов полагают, что при формировании инвестиций в обеспечение информационной безопасности результаты анализа рисков могут быть учтены, но не являются основой для формирования бюджета на обеспечение информационной безопасности компании. Всего 5% респондентов утверждают, что формирование статей финансирования на обеспечение информационной безопасности не должны базироваться на методике и результатах анализа рисков. При этом 20% респондентов затруднились ответить, насколько данная инициатива важна для их компаний. Тем не менее основная тенденция явно прослеживается: результаты оценки информационных рисков будут являться основой при формировании финансирования для целей обеспечения информационной безопасности компаний.

**Рисунок 10. Степень важности анализа рисков**



## Инициатива 5

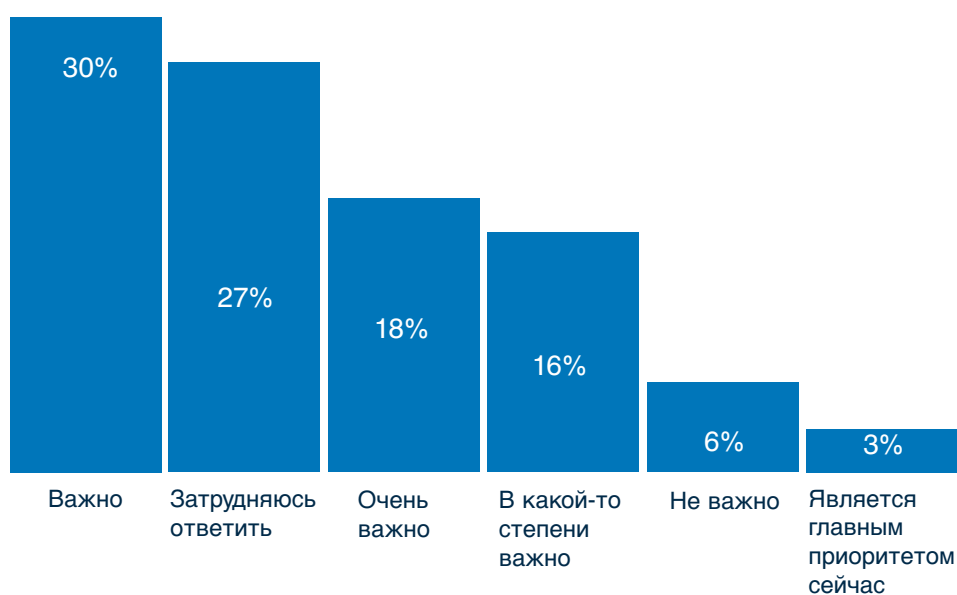
### Соответствие требованиям регуляторов

И завершает пятерку лидеров инициатива о необходимости соответствия требованиям регуляторов в части обеспечения безопасности. Наши респонденты уделили должное внимание данной инициативе (см. рис. 11). Вероятнее всего, здесь участники опроса имели в виду требования по обеспечению защиты персональных данных. Как известно, с 1 января 2010 года в соответствии с Законом № 152-ФЗ от 27 июля 2006 года все операторы персональных данных будут обязаны обеспечивать адекватный уровень сохранности персональных данных с целью «обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну».

Более половины респондентов (51%) считают, что реализация данной инициативы необходима, даже несмотря на трудные экономические условия и последствия мирового финансового кризиса.

Голоса распределились следующим образом: 30% респондентов уверены в необходимости соответствовать требованиям регуляторов. 18% участников опроса считают, что данная инициатива крайне важна для их организаций. 3% ответили, что данная инициатива имеет в настоящее время самый высокий приоритет для их компаний. Однако 49% респондентов выразило мнение, что данная инициатива может быть отнесена на второй план с учетом проблем, связанных с финансированием и неоднозначностью требований законодательства. Тем не менее 16% опрошенных считают, что в какой-то мере соблюдение требований регуляторов важно и для их компаний. И только 6% от общего числа опрошенных сообщили, что данная инициатива абсолютно не важна для них, а 27% участников не смогли дать оценку необходимости совершения действий, направленных на выполнение требований регуляторов.

**Рисунок 11. Степень важности соответствия требованиям регуляторов**



## Как PricewaterhouseCoopers может вам помочь

Группа консультационных услуг в области информационных технологий PricewaterhouseCoopers имеет богатый опыт оптимизации деятельности в области ИТ в различных отраслях и включает как российских, так и зарубежных специалистов, демонстрирующих уникальное сочетание глубокого понимания специфики рынков России и стран СНГ и знания лучшей мировой практики. Мы оказываем следующие услуги в области ИТ:

- Анализ и разработка корпоративной стратегии в области ИТ
- Проведение анализа ИТ-систем и содействие в их трансформации в изменившихся экономических условиях, а также в рамках проектов слияния и поглощения
- Консультации по вопросам информационной безопасности и непрерывности бизнеса
- «Безопасное» сокращение затрат на ИТ
- Оценка и консультирование по вопросам соответствия ИТ правовому и нормативному регулированию

## Контактная информация



Майк Смит  
Директор  
Тел.: +7 (495) 967-6162  
[mike.smith@ru.pwc.com](mailto:mike.smith@ru.pwc.com)



Григорий Кацман  
Руководитель направления по оказанию услуг  
в области информационной безопасности  
Тел.: +7 (495) 232-5580  
[grigory.katsman@ru.pwc.com](mailto:grigory.katsman@ru.pwc.com)



Александр Зинин  
Младший менеджер  
Тел.: +7 (495) 232-5580  
[aleksander.zinin@ru.pwc.com](mailto:aleksander.zinin@ru.pwc.com)

