
ФОКУС НА БЕЗОПАСНОСТЬ

Исследование влияния экономического кризиса
на рынок ИБ в России

Оглавление

Аннотация	3
Ключевые выводы	4
Методология исследования и профиль участников	5
Взаимоотношение с вендорами	6
Финансирование ИБ	9
Кадровый вопрос	11
Заключение	13

Аннотация

Аналитический центр Zecurion провёл исследование более чем 200 российских организаций различных отраслей, чтобы понять, насколько экономическая ситуация повлияла на планы компаний по реализации проектов в области защиты информации, как изменилась их стратегия закупок, какими они видят изменения модели поведения разработчиков и поставщиков решений по безопасности на рынке.

Акцент в исследовании сделан на динамике изменений, которые произошли в отрасли информационной безопасности (ИБ) за последний год, когда тема санкций, антисанкций и импортозамещения вошла в ежедневную повестку. Изменения эти видны и невооружённым глазом. К примеру, единичные призывы к импортозамещению в области ИТ и ИБ за прошедший год вылились в конкретные законодательные инициативы. Так, в конце июня 2015 года Президент РФ подписал Федеральный закон №188, предусматривающий отказ от иностранного софта в госсекторе, если имеются аналогичные российские продукты.

Текущая ситуация с защищённостью компаний от внешних и внутренних угроз, уровень их зрелости в отношении ИБ остались за рамками данного отчёта. Последнее исследование по данным вопросам среди российских, казахстанских и украинских компаний аналитический центр Zecurion опубликовал в декабре 2013 года. Ознакомиться с его результатами можно по ссылке: http://www.zecurion.ru/upload/iblock/9e4/Zecurion_Roadshow_2013.pdf

Ключевые выводы

■ РЫНОК ИБ НЕ ТОЛЬКО «ВЫЖИЛ», НО И РАЗВИВАЕТСЯ

Влияние экономического кризиса на отрасль к середине 2015 года достаточно ограничено — уменьшение расходов на ИБ в компаниях не было слишком значительным, а в рублях рынок даже растёт.

■ СТРАДАЮТ ИНОСТРАННЫЕ ВЕНДОРЫ И НЕЭФФЕКТИВНЫЕ КОМПАНИИ

Некоторое сокращение бюджетов на безопасность слабо отразится по итогам 2015 года на крупных отечественных вендорах — спад продаж придётся преимущественно на зарубежные компании. Оптимизация расходов компенсируется активным развитием программ импортозамещения, прежде всего, в госсекторе и на предприятиях, связанных с госзаказом. Кроме того, пострадают разработчики корпоративных продуктов, продающие свои решения через партнёрскую сеть.

■ ПОТРЕБИТЕЛИ ВЫИГРЫВАЮТ

Кризис практически не отразился на потребителях. Формальное повышение цен компенсируется более гибкими скидками, которые поставщики решений готовы предоставить корпоративным заказчикам. Этому же способствует ужесточение конкуренции.

■ БОЛЬШЕ ВЗВЕШЕННЫХ РЕШЕНИЙ

Компании стали тщательнее выбирать продукты в области ИБ, всё чаще перед внедрением крупных систем заказчики предпочитают заказывать пилотный проект. Существенно сократилась практика закупки нескольких аналогичных решений.

■ СОБСТВЕННЫЕ СОТРУДНИКИ — ИСТОЧНИК ПРОБЛЕМ И КЛЮЧ К ИХ РЕШЕНИЮ

Негативный экономический фон и ухудшение ситуации на рынке труда обостряют проблемы внутренней безопасности. Респонденты отмечают рост внутренних угроз, всё больше сотрудников намеренно или случайно компрометируют корпоративные данные. Здесь же кроются и основные возможности по минимизации информационных рисков. Организационные мероприятия и внедрение DLP-систем станут эффективным средством профилактики утечек.

■ ИМПОРТОЗАМЕЩЕНИЕ — ПАЛКА О ДВУХ КОНЦАХ

С точки зрения выручки, ощутимых результатов от программы импортозамещения пока нет, но это не показатель, т. к. времени пока прошло слишком мало. Программа импортозамещения, безусловно, окажет влияние на рынок в 2015-16 гг., но в долгосрочной перспективе победа над иностранным софтом может оказаться пирровой при отсутствии конкуренции и мотивации развивать собственные продукты.

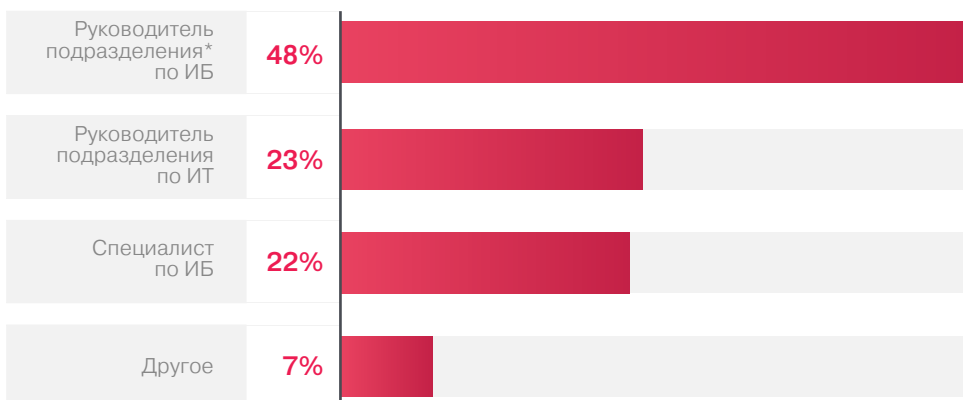
Методология исследования

Исследование проводилось с 17 июня по 17 июля 2015 года путём анкетирования (в ходе личных встреч, телефонных интервью и путём заполнения электронных анкет) представителей различных областей бизнеса и госсектора, не связанных с производством и дистрибуцией продуктов в области информационной безопасности. Полностью на вопросы анкеты ответили 243 респондента.

Рисунок 1

Профиль участников

* — (департамент, отдел, группа в зависимости от размера организации)



Основная масса респондентов напрямую связана с обеспечением ИБ в своих организациях — это руководители и сотрудники подразделений по ИБ, а также руководители ИТ-подразделений. В компаниях малого и среднего бизнеса до сих пор вопросы защиты информации решаются в рамках автоматизации деятельности и не выделяются в отдельное направление, поэтому руководители ИТ одновременно отвечают и за ИБ. Среди непрофильных специалистов на вопросы анкеты отвечали топ-менеджеры и менеджеры по закупкам, так или иначе курирующие направление защиты информации.

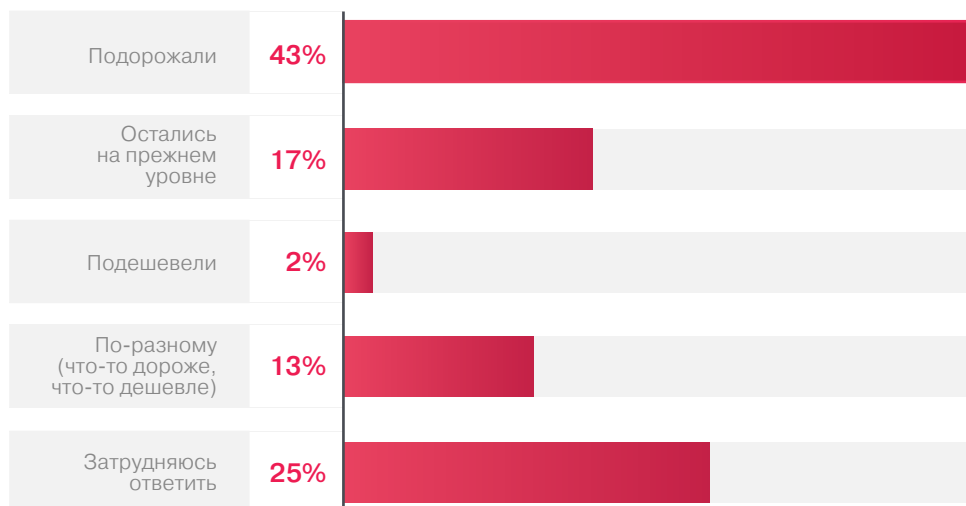
Взаимоотношение с вендорами

Два наиболее актуальных вопроса, от которых напрямую зависит реализация большинства запланированных проектов по ИБ в компаниях, это стоимость необходимых продуктов и услуг и сохранение бюджета на безопасность. Начнём с первого (см. рис. 2).

Субъективная оценка заказчиков говорит о том, что в целом уровень цен на решения в области ИБ увеличился по сравнению с первой половиной 2014 года. Заказчики приводят разные ориентиры повышения цен, и это объясняется различиями в структуре закупаемых продуктов, используемых схемах и предпочтениях по поставщикам. Усредняя, можно говорить о 10-20% роста цен по отрасли на программное обеспечение (на аппаратное обеспечение — заметно выше), хотя встречаются и исключения, а некоторые респонденты указывают на то что цены даже снизились.

Рисунок 2

Как, по вашей оценке, изменились ценовые ориентиры поставщиков ИБ-решений с весны 2014 года



Сразу несколько респондентов в своих комментариях к ответам сообщили любопытный факт. Несмотря на то, что официально стоимость решений в области ИБ повысилась, компании предоставляют заказчикам большие скидки, и в результате конечная стоимость в рублях остаётся примерно той же, что и год назад. Также продавцы ИБ-продуктов практикуют гибкую ценовую политику, когда цена подстраивается под конкретного заказчика, исходя из его бюджета и потребностей. Подобные хитрости позволяют удерживать приемлемую планку прибыльности и сохранить рыночную долю.

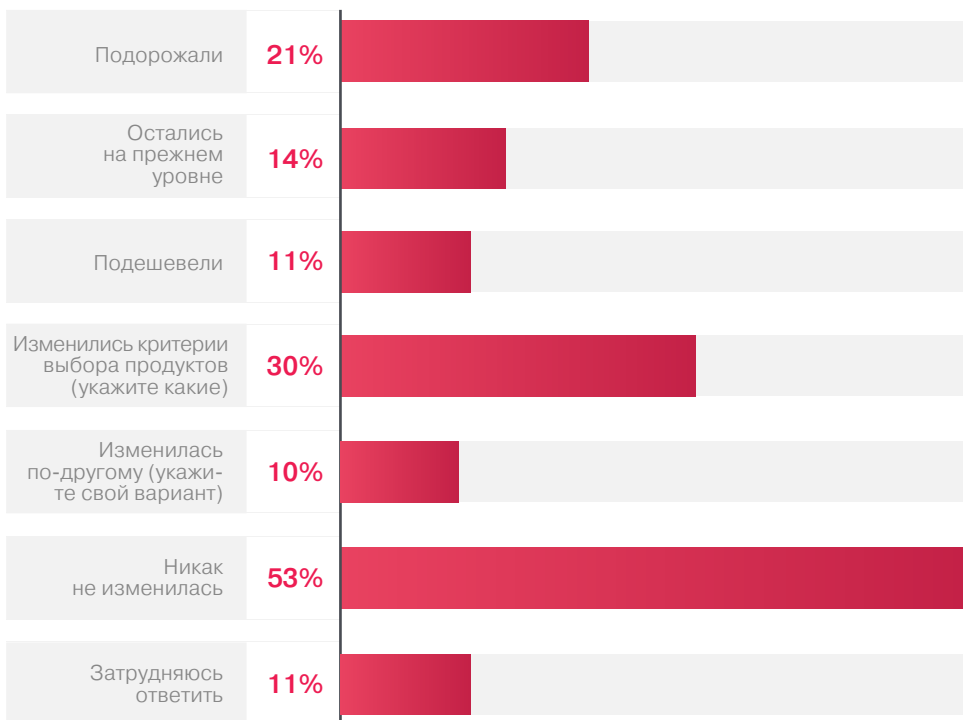
Из-за увеличения стоимости продуктов по ИБ компании изменили и собственный подход к выбору конкретных решений. В каждой пятой компании увеличились сроки реализации проектов по ИБ. Теперь компании дольше выбирают продукты (см. рис. 3). При этом 14% заказчиков начали тестировать решения до покупки (чего раньше не практиковали), а 11% теперь заказывают пилотный проект. Пилотный проект — это хороший способ для заказчика убедиться в правильности сделанного выбора либо вживую сравнить несколько продуктов.

Пилотный проект — это хороший способ для заказчика убедиться в правильности сделанного выбора либо вживую сравнить несколько продуктов. Пилотные проекты чаще всего бесплатны для заказчика и обременительны лишь выделением на них дополнительных ресурсов. При этом польза от пилотов очевидна. Специалисты по ИБ знакомятся с возможностями внедряемых продуктов, осваивают и настраивают под собственную инфраструктуру, отказываются от эксплуатации с минимальными негативными последствиями, даже если продукт не отвечает потребностям заказчика. Наконец, оценивают соответствие продуктов, техническому заданию и собственным ожиданиям, понимают, насколько удобно пользоваться системой. Кстати, в области DLP-решений первые инсайдеры выявляются именно при пилотном внедрении на ограниченном количестве рабочих станций.

Рисунок 3

Как изменилась ваша стратегия закупок ПО и «железа» в области ИБ

* — Сумма долей свыше 100%, т. к. количество вариантов ответа не ограничено



Если говорить об изменении критериев выбора продуктов, здесь наметились два основных вектора. Во-первых, заказчики стали больше внимания уделять локализации. Несмотря на отсутствие прямого запрета на поставку иностранных решений, отечественные разработки оказываются в более выгодной ситуации. Во-вторых, заказчики обращают большее внимание на стоимость решения. Причём не прайсовую, а ТСО. Отмечая важность такого подхода, приходится также констатировать, что большинство заказчиков ещё не созрело до выбора продуктов на основе другой метрики — ROI, учитывающей ещё и эффективность закупаемого софта или оборудования.

Заказчики с сожалением отмечают, что между прайсовой ценой и ТСО итоговой стоимостью проекта и поддержки разница становится всё больше.

Виной тому во многих случаях является удлинение цепочки разработчик — потребитель, где каждое звено стремится урвать свою долю пирога. В некоторых случаях и сами разработчики стремятся сделать цену субъективно более привлекательной, выставляя минимальную цену на лицензии, но увеличивая плату за техническую поддержку или ограничивая срок действия лицензии. Например, в сегменте DLP стоимость технической поддержки может варьироваться от 20%-30% (большинство вендоров) до 50% стоимости лицензий в год. При этом и стоимость технической поддержки тоже могут разбивать, например, отдельно выделяя обновление продуктов и собственно поддержку. В таких условиях, учитывая дополнительные услуги по установке, настройке решений и прочее, ТСО может существенно отличаться от прайсовой стоимости продуктов даже при покупке напрямую.

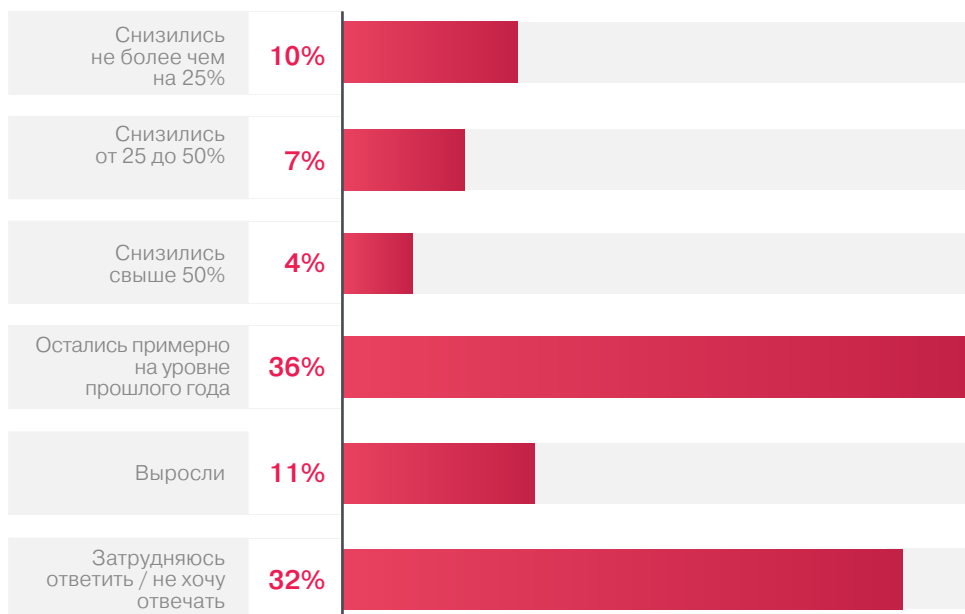
Вообще, доля прямых продаж в кризис заметно увеличилась. Цель — сократить издержки. Прямые продажи в большинстве случаев выгодны и разработчикам, и потребителям, поэтому даже те вендоры, которые исторически опирались на каналные продажи, стремятся больше продавать напрямую. Кроме того, квалификация партнёров или отсутствие интереса не всегда позволяют внедрять действительно сложные решения корпоративного уровня.

Финансирование ИБ

Необходимо отметить, что более правильными терминами в контексте исследования являются «финансирование» или «расходы» на ИБ. Говорить о бюджете не всегда корректно, т. к. выделенный бюджет на ИБ есть у относительно небольшого процента организаций (порядка 20%). Тем не менее, далее по тексту часто будет встречаться термин «бюджет», под которым подразумеваются именно расходы компаний, которые могут выделяться из собственного бюджета на ИБ, из общего бюджета на ИТ или по заявкам на конкретные проекты.

Рисунок 4

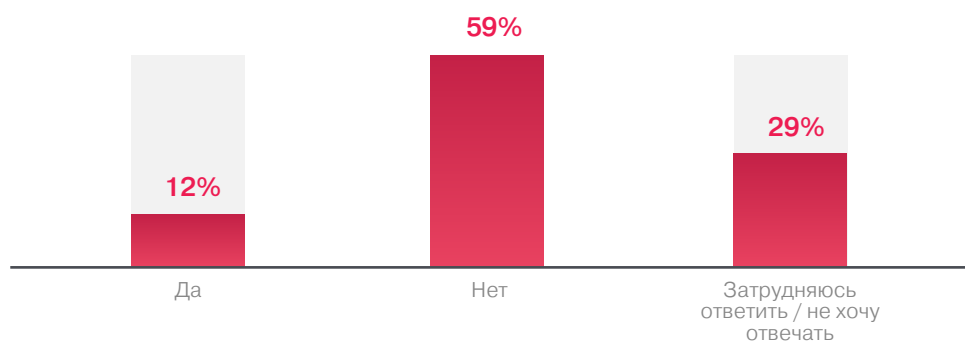
Как изменились планируемые расходы на ИБ на 2015 год по сравнению с 2014 годом



В целом снижение расходов не критично (см. рис. 4), и фактического «замораживания» бюджетов, как было на рубеже 2008–2009 гг., не наблюдается. В то же время российские компании всё больше используют дифференцированный подход к защите данных — наиболее критичные данные защищаются тщательнее, и на эти проекты выделяется больше средств. В большинстве компаний внутренняя информация крайне разнородна, и защищать все типы данных одинаково — нецелесообразно и неэффективно.

Рисунок 5

Планируется ли сокращение расходов на проекты по ИБ в 2016 году относительно 2015 года

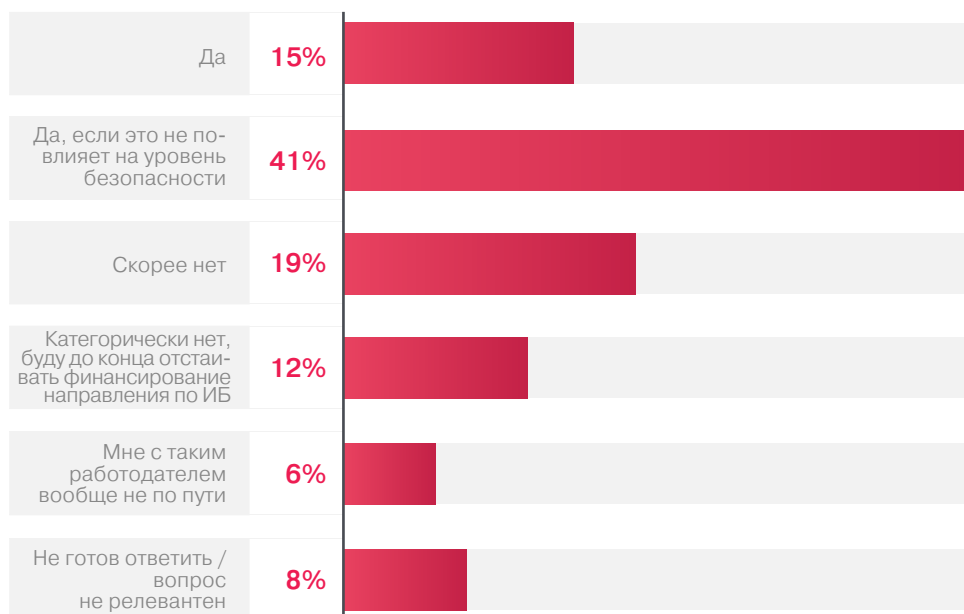


Что касается перспектив дальнейшего сокращения расходов на ИБ, ситуация выглядит достаточно оптимистичной (см. рис. 5). Лишь 12% респондентов говорят о том, что финансирование может быть урезано. Это лишь предварительные оценки, но по ним можно сделать вывод, что пик условного кризиса на рынке ИБ уже пройден. Безусловно, ситуация может измениться под влиянием внешних (нерыночных) факторов, которые заставят компании активнее урезать траты или наоборот, увеличить расходы на безопасность, однако по состоянию на лето 2015 года наиболее вероятным сценарием развития рынка ИБ следует считать постепенное его восстановление. Более того, выручка (в рублях) многих российских вендоров уже в текущем году даже увеличится за счёт иностранных поставщиков.

Сравнивая ситуацию с 2008–2009 гг., можно отметить, что тогда спад был более выраженным, а продажи продуктов в области ИБ просели значительно сильнее, однако кризис был пройден достаточно быстро. Уже в 2010 активный рост рынка возобновился.

Рисунок 6

Готовы ли вы сократить расходы на ИБ в случае распоряжения сверху?



Вопросы, связанные с развитием проектов часто связаны не только с прагматическими задачами, стоящими перед компаниями, но и эмоционально с людьми, которые эти проекты реализуют. Нередко решение о том, какое направление пойдёт в компании «под нож» принимается с учётом позиции руководителя направления, сможет ли он отстоять своё детище, обосновать его важность для бизнеса или нет.

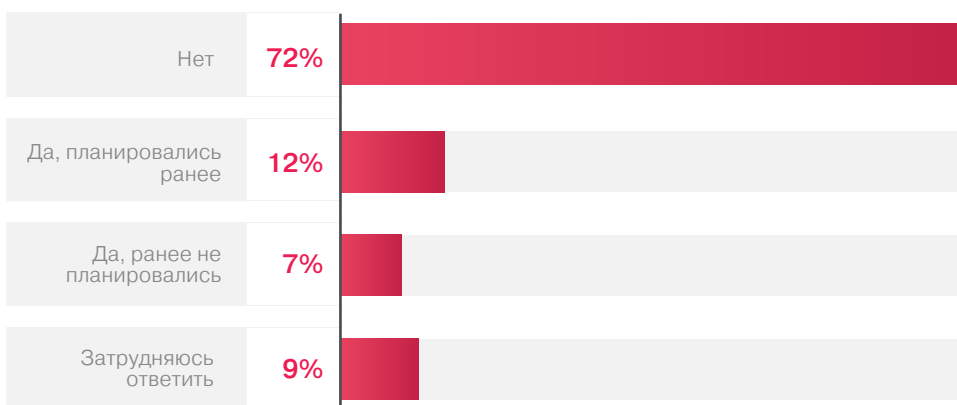
Вопрос о готовности сократить расходы на ИБ изначально носил несколько провокационный характер. И в данном случае мы видим некоторое расхождение с реальной ситуацией. Ответы, скорее, отражают мнение специалистов о статусе службы ИБ в организации. В целом, большинство респондентов не склонны сокращать расходы на ИБ в ущерб уровню безопасности. Степень категоричности приведена на рис. 6. Были ли сотрудники столь же принципиальны, отстаивая свою позицию внутри компании — покажет объём рынка по итогам 2015 года.

Кадровый вопрос

Сокращение сотрудников, занимающихся обеспечением ИБ — одна из мер сокращения расходов по данному направлению, однако практикуется она сравнительно редко. Причин тому сразу несколько. Во-первых, штаты подразделений по ИБ в российских компаниях сложно назвать раздутыми. Наоборот, часто приходится слышать о том, что в компаниях ощущается нехватка квалифицированных кадров. Ещё тяжелее приходится тем организациям, где выделенных ИБ-подразделений нет. При сокращении кадров возрастёт нагрузка на оставшихся коллег, и выполнять непрофильные функции придётся неподготовленным сотрудникам, что негативно скажется на качестве работ.

Рисунок 7

Были ли в вашей компании сокращения сотрудников, занимающихся информационной безопасностью?



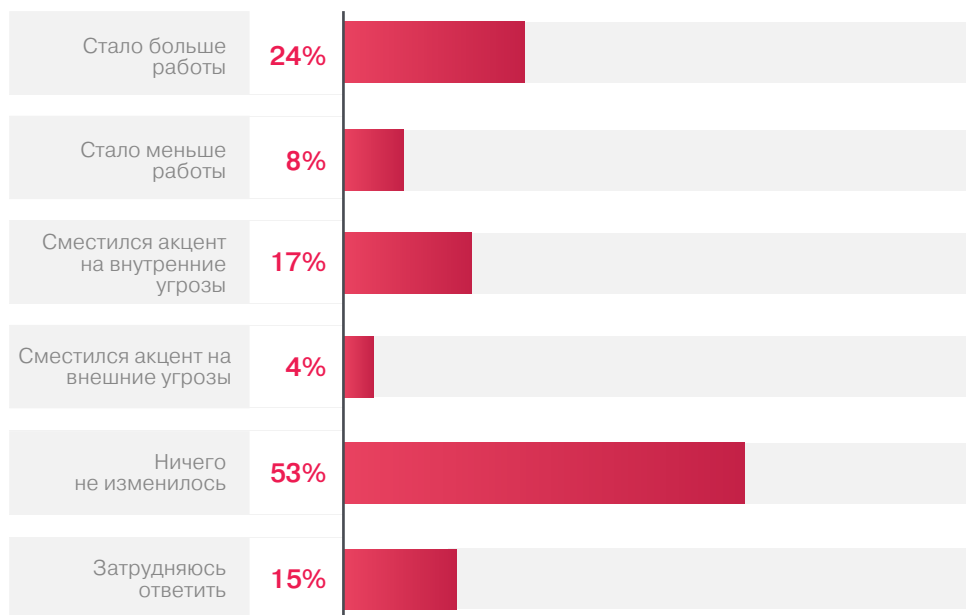
Во-вторых, найти качественного специалиста по ИБ с должным опытом и необходимым для соответствия должности образованием бывает проблематично. В-третьих, безопасники часто имеют высокий уровень допуска к конфиденциальной информации, и расставание с такими сотрудниками по инициативе работодателя нежелательно.

Проблема кадров по-прежнему является актуальной в области ИБ в России. Несмотря на то, что вузы готовят большое количество профильных специалистов, качество подготовки оставляет желать лучшего. Учебные программы сильно оторваны от реалий практической работы. Молодые специалисты к ней не готовы, часто после окончания учебного заведения даже не представляют, чем бы хотели заниматься, в чём заключается работа безопасников в разных отраслях. У них относительно неплохая теоретическая база, но малоприменимая на практике. Этого недостаточно для успешной работы. А работы, как отмечают респонденты исследования, в последний год стало больше (см. рис. 8).

Рисунок 8

Как изменился характер
вашей работы за последний
год?

* — сумма ответов свыше
100%, т. к. можно было вы-
брать до 2 вариантов ответа



Четверть респондентов отмечает, что за последний год у них прибавилось работы. Участники исследования объясняют это несколькими основными причинами:

- увеличилось количество угроз либо они стали более изощрёнными;
- в целях экономии средств часть работы, которая могла быть автоматизирована или отдана на аутсорсинг, приходится делать самостоятельно;
- приходится дольше и сложнее выбирать продукты и услуги;
- уменьшилось количество сотрудников в службе ИБ, и нагрузка на каждого оставшегося возросла.

Кроме того, 17% респондентов отмечает увеличение угроз со стороны собственных сотрудников. Причиной тому — ухудшение ситуации на рынке труда. Беспокоясь за собственное будущее в компании, сотрудники начинают копировать информацию, даже если сокращение им не угрожает. Более того, в ходе расследования часто выясняется, что люди не представляют, как эту информацию можно использовать, какую выгоду может принести или как помочь трудоустроиться. Подчиняясь чувству тревоги, сотрудники копируют доступную им информацию. Проблема заключается в том, что даже без злого умысла информация может оказаться скомпрометированной, попасть в руки конкурентов.

Заключение

Развитие проектов по информационной безопасности требует существенных человеческих и финансовых ресурсов. А отдача не всегда очевидна топ-менеджерам, стремящихся к оптимизации затрат и улучшению бизнес-показателей своих компаний. Поэтому соблазн пустить под нож статьи бюджета, связанные с защитой информации, понятен. В то же время принятый во всём мире риск-ориентированный подход к обеспечению ИБ позволяет рассматривать расходы на безопасность как инвестиции с достаточно быстрым сроком окупаемости.

Разница в подходах, которые применяют российские компании, хорошо заметна на фоне кризиса. В то время как одни пытаются сэкономить на собственной безопасности, другие вкладывают в новые технологии с тем, чтобы повысить свою конкурентоспособность.

Рост интереса компаний к решениям по защите информации от утечек, к сожалению, во многом является следствием увеличившегося количества инцидентов, связанных с кражей или попыткой кражи конфиденциальной информации. При снижении реальных доходов работников вследствие экономической ситуации и сокращения расходов на персонал, уменьшения премиального фонда, лояльность сотрудников неизбежно падает, а риски утечки информации увеличиваются. Эти же риски увеличивают сокращения и в целом беспокойная ситуация на рынке труда.

В складывающихся условиях сотрудники считают, что наработки и файлы с текущей работы могут помочь в трудоустройстве. В некоторых отраслях это действительно актуально. Если менеджер по продажам переходит в другую компанию, но не меняет специализацию, наработанные контакты и базы клиентов могут оказать серьёзную помощь при налаживании продаж. В то же время основная масса сотрудников копирует конфиденциальные сведения, но не планирует или даже не сможет ими воспользоваться. Работники сливают информацию «на всякий случай», при этом резко возрастают риски компрометации данных, в т. ч. и случайно.

В то же время некоторые респонденты отмечают, что часть сотрудников стала более ответственно относиться к вопросам защиты информации, поскольку нарушение существующих регламентов в области ИБ чревато санкциями со стороны руководства вплоть до увольнения.

Помимо традиционной риторики в пользу отечественных продуктов, Правительство России предпринимает конкретные шаги по изоляции иностранных решений в области ИБ. Так, в конце июня 2015 года был подписан №188-ФЗ, согласно которому для отечественного ПО устанавливается режим благоприятствования при осуществлении госзакупок, а конкурентоспособность иностранных продуктов ограничивается.

В 2015 году компания «Код безопасности» проводила исследование, посвящённое импортозамещению в области ИБ, результаты которого показывают, что большинство компаний активно переходят на отечественный софт. В целом, тенденция к замещению иностранных продуктов прослеживается хорошо, однако по результатам текущего исследования Zecurion, корректнее говорить о поэтапной замене.

Лавинообразного отказа от иностранных решений не следует ожидать. Во многих крупных организациях уже внедрены и успешно используются зарубежные средства защиты информации. А в такой консервативной отрасли как ИБ внезапная смена курса развития, кардинальное обновление ПО могут повредить, поэтому большинство компаний резких движений не будет совершать. Тем не менее, не приходится сомневаться, что тенденция к замещению импортных решений в области ИБ в ближайшие годы сохранится.

Усложнение продаж иностранных продуктов создаёт искусственные условия не для развития отрасли, но для увеличения продаж отечественного софта. Хорошо это или плохо? Однозначного ответа, пожалуй, нет. С одной стороны, у российских разработчиков появляется заинтересованность в развитии продуктовой линейки. Больше выручка — больше возможностей. Можно увеличить штат программистов, нанять более квалифицированных специалистов. С другой стороны, в тепличных условиях без реальной конкурентной среды качество продуктов будет неизбежно снижаться. В результате через несколько лет ситуация в отрасли лишь усугубится. Делать продукты лучше мотивации не будет — ведь они и так неплохо продаются.

Ещё один аспект защиты информации — кадровый вопрос. С одной стороны, ситуация вроде бы становится лучше, вузы выпускают сотни специалистов по ИБ ежегодно, но подготовлены к решению реальных задач они крайне слабо. Общение с молодыми специалистами показывает, что они плохо представляют, с чем придётся столкнуться на практике, какие задачи решать. Не понимают специфики настоящей работы, однако имеют высокие зарплатные ожидания. Между тем, в отношении кадров спрос смещается в сторону отраслевой экспертизы, наиболее востребованными становятся сотрудники с опытом работы в конкретных отраслях.

Отдельное направление — защита цифрового суверенитета и противоборство в киберпространстве. Это новое для специалистов по безопасности направление ставит новые задачи и бросает новые вызовы. Известно о существовании специализированных подразделений по кибербезопасности в других странах, и всё чаще слышатся взаимные обвинения в целенаправленных хакерских атаках на госучреждения и даже коммерческие компании. В 2010 году США заявляли о праве применять реальное оружие в ответ на атаки в цифровом пространстве, а в 2015 готовы вводить экономические санкции против отдельных компаний и даже физических лиц, уличённых в атаках на американские компании. Таким образом, спрос на кадры в области защиты информационных ресурсов от кибератак формируется в том числе и со стороны государств, и мало подвержен негативному влиянию даже в период экономического спада.

Все перечисленные факторы являются достаточно сильными драйверами, и совместное их влияние позволит удержаться рынку программных средств по информационной безопасности на текущих уровнях по итогам 2015 года, и вновь показать двузначный рост уже в 2016-17 гг.

Контактная информация

Ксения Головки

Заместитель руководителя пресс-службы
Тел.: +7 967 091-65-50
pr@zecurion.com

Аналитический центр Zecurion

analytics@zecurion.com

129164, Российская Федерация, Москва,
Ракетный бульвар, 16
Телефон/факс: +7 495 221-21-60