ABISS
НП «АБИСС»

Практика применения Комплекса документов Банка России по обеспечению информационной безопасности

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ 2012

ОГЛАВЛЕНИЕ

Введение....2
Методология исследования и портрет респондентов....3
Общие выводы....5
Бюджет и присоединение к Стандарту....6
Кадровый вопрос....10
Выполненные работы и планы по внедрению Стандарта....16
Заключение....23

ВВЕДЕНИЕ

Первая версия Стандарта Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее - Стандарт) введена более 8 лет назад. На момент своего создания в 2004 году, во время острой нехватки гармонизированной международной методологической базы по защите информации, Стандарт стал передовым источником ценных знаний о подходах к организации и управлению системой обеспечения информационной безопасности. В 2010 г. вышла четвертая версия Стандарта, включавшая нормативные требования в области защиты персональных данных, кроме того были опубликованы дополнительные документы, содержащие методические рекомендации по внедрению и оценке на соответствие Стандарту, составившие в совокупности Комплекс документов Банка России по обеспечению информационной безопасности (Комплекс БР ИББС).

В целях популяризации Стандарта, обмена опытом, а также обеспечения контроля качества на рынке профессиональных услуг в области внедрения, оценки соответствия и обучения Стандарту еще в 2006 году было создано Сообщество пользователей Стандарта Банка России ABISS (Association for Banking Information Security Standards). В конце 2011 г. Сообщество ABISS было преобразовано в Некоммерческое партнерство «Сообщество пользователей стандартов по информационной безопасности АБИСС» (НП «АБИСС»), объединившее юридических лиц — аудиторов и консультантов, а также учебные центры. НП «АБИСС» сотрудничает с Банком России, регуляторами в области защиты персональных данных, с кредитными организациями и другими участниками национальной платежной системы.

Далее представлены результаты исследования, проведенного НП «АБИСС» при участии компании СТЭП ЛОДЖИК в первом квартале 2012 года.

НП «АБИСС» также выражает благодарность Ассоциации российских банков и компании «Авангард Центр», которые приняли активное участие в рассылке и сборе результатов по вопросам исследования.

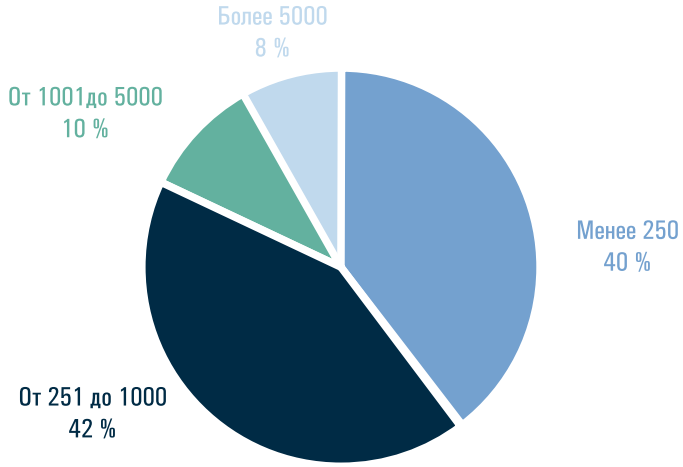
МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ И ПОРТРЕТ РЕСПОНДЕНТОВ

Сбор исходных данных проводился среди кредитных организаций. Опрос носил адресный характер, а в качестве целевой аудитории опроса были выбраны сотрудники кредитных организаций, ответственные за обеспечение информационной безопасности. Использовались закрытые и многовариантные вопросы. В случае если участник опроса отвечал не на все вопросы, такие данные не сохранялись.

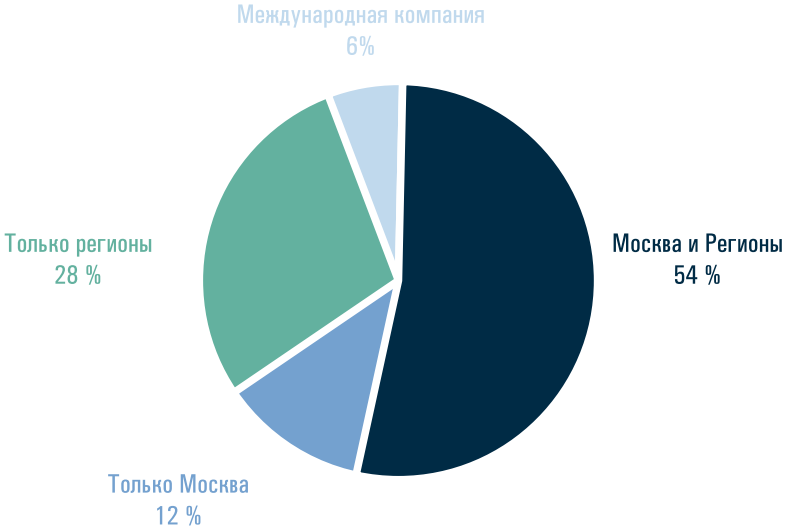
В результате исследования получены данные из 50 кредитных организаций различного масштаба и территориальной распределенности.

Полученные статистические данные округлены до целых чисел. В некоторых случаях сумма долей ответов превосходит 100% из-за использования многовариантных вопросов.

Число рабочих мест



Территориальное распределение



По количеству сотрудников большую часть респондентов составили микро-банки (40 %) и малые банки (42 %), до 250 и от 251 до 1000 сотрудников соответственно. Средние банки, с количеством сотрудников от 1000 до 5000, составили 10%. Крупные банки, с количеством сотрудников более 5000 сотрудников, составили 8 % опрошенных.

По территориальной распределённости большую часть - 54 % составили банки, имеющие представительства в Москве и других регионах страны. Региональные банки, не имеющие представительств в Москве, составили 28 % опрошенных. На исключительно московские банки пришлось 12 % респондентов, на международные – 6 %.

Сравнение данных об участниках опроса позволяет сформировать определить типового респондента как кредитную организацию, с количеством сотрудников до 1000 человек и с распределенной информационной инфраструктурой, объединяющей несколько филиалов в пределах России.

ОБЩИЕ ВЫВОДЫ

1. Текущая ситуация по присоединению к Стандарту.

- Количество кредитных организаций, принявших стандарт, неуклонно растет и на период исследования составляло 80 %.
- Более 60 % кредитных организаций в 2011 году выполняли работы по внедрению Стандарта.
- Более 40 % кредитных организаций имеют в штате сотрудников, прошедших авторизованные курсы в области применения Стандарта Банка России.
- Проблемы нехватки кадров в области обеспечения информационной безопасности кредитных организаций, зафиксированные во время предыдущего исследования, проведенного в 2008 году, уже не носят критичный характер.

2. Планы кредитных организаций по дальнейшему приобщению к Стандарту:

- 68 % организаций банковской системы запланировали работы по оценке соответствия в 2012 году, а 26 % опрошенных будут привлекать для этих работ внешних аудиторов. Около 70% кредитных организаций планируют на 2012 год работы по внедрению Стандарта, и почти 50 % из общего числа респондентов планируют привлекать для этих работ внешних консультантов.
- 18% опрошенных запланировали на 2012 год обучение в области применения Стандарта Банка России, 38 % пока не планируют обучение.

3. Проблемы:

- В 50 % кредитных организаций финансирование задач информационной безопасности остается на уровне менее 3 % от ИТ-бюджета, что является недостаточным по сравнению с общемировыми тенденциями. Следствием этого являются сложности как при подборе квалифицированного персонала, так и в случае привлечения внешних аудиторов и консультантов.
- Более 50 % респондентов отметили сложность технических и организационных аспектов применения Стандарта.

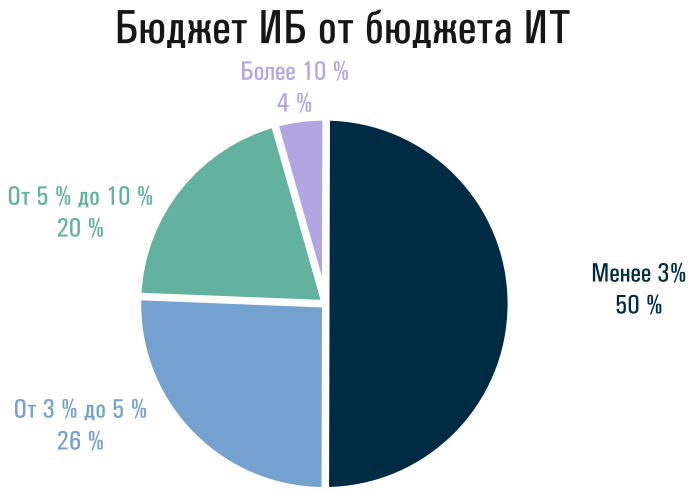
4. Развитие стандарта

- Почти 90 % респондентов приветствуют объединение в Стандарте требований информационной безопасности организаций банковской системы.
- 52 % считают необходимым шагом для дальнейшего распространения Стандарта получение им статуса обязательного.

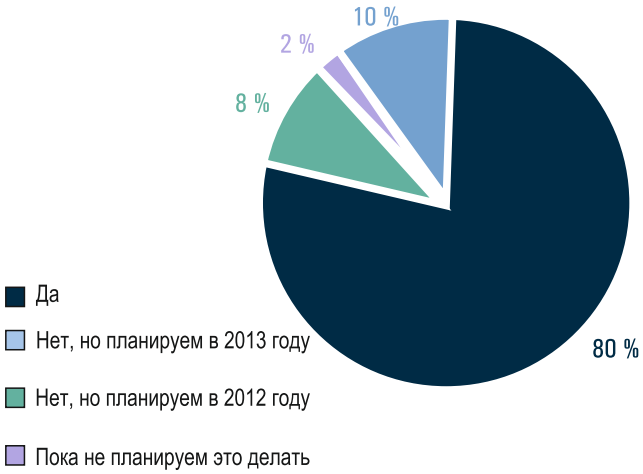
БЮДЖЕТ И ПРИСОЕДИНЕНИЕ К СТАНДАРТУ

Как уже не раз отмечалось пользователями Стандарта, основной проблемой его применения является размер финансовых вложений, которые не всегда выделяются в должном объеме. Дополнительные затраты связаны как с высокой стоимостью привлечения внешних организаций, так и оплатой труда собственных квалифицированных специалистов по защите информации. Полученные в ходе исследования данные о затратах кредитных организаций на информационную безопасность относительно общих затрат на информационные технологии подтвердили обоснованность беспокойства пользователей Стандарта.

Опрос показал, что половина опрошенных кредитных организаций инвестируют в информационную безопасность менее 3 % ИТ бюджета, 26 % опрошенных указали затраты 3 % до 5 %, только пятая часть – от 5 % до 10 %, и и лишь около 10 % банков тратят на защиту информации 4 % ИТ-бюджета. Сравнение полученных данных с результатами проведенного в 2011 году опроса Gartner IT Key Metrics Data свидетельствует что у более чем 70 % отечественных кредитных организаций инвестиции в информационную безопасность ниже средних по отрасли в мире (5,6 %).



Присоеденилась ли ваша организация к Стандарту?

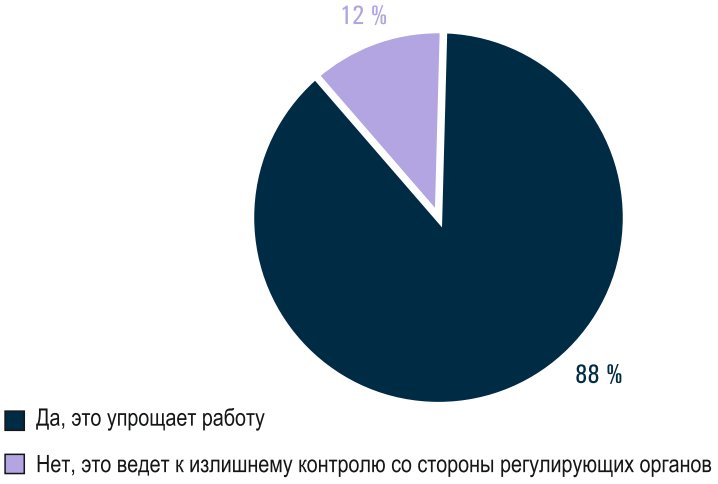


Причины присоединения к Стандарту

В тоже время свидетельством роста внимания к вопросам обеспечения информационной безопасности может служить присоединение большинства опрошенных организаций к Стандарту. Оптимизм внушает тот факт, что 90 % опрошенных уже присоединились или планируют присоединиться к Стандарту в ближайшие два года.

Как и следовало ожидать, 80 % респондентов основной причиной присоединения назвали согласование требований Стандарта по защите персональных данных со стороны Роскомнадзора, ФСБ России и ФСТЭК России. При этом абсолютное большинство – 58% отметили и положительное влияние Стандарта на общий уровень обеспечения информационной безопасности, а 30% основывались на планах по развитию Стандарта и включению в него требований защиты платежных систем. Важным показателем является указание большинства опрошенных на положительное влияние Стандарта на общий уровень обеспечения информационной безопасности.

Объединение в Стандарте требований информационной безопасности



Поддерживают респонденты и дальнейшее объединение в Стандарте требований к кредитным организациям по защите информации, об этом высказались 88 % опрошенных. Полученные результаты можно назвать полной поддержкой со стороны респондентов дальнейших шагов Банка России по включению в Стандарт требований по различным направлениям банковской деятельности, среди которых можно назвать обсуждаемые в последнее время планы по усилению взаимодействия с регулирующими органами, а также объединению в стандарте отечественных и международных требований к защите данных платежных карт.

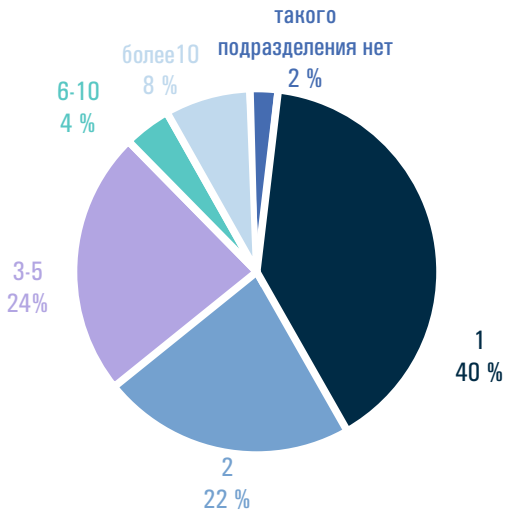
Пути дальнейшего распространения Стандарта

Интересные результаты дал вопрос о дальнейших шагах по распространению Стандарта. Так, 52 % опрошенных считают наиболее действенным шагом обязательность выполнения требований Стандарта. Как вариант, включение требований Стандарта в распорядительные документы Банка России, обязательные для исполнения всеми кредитными организациями.

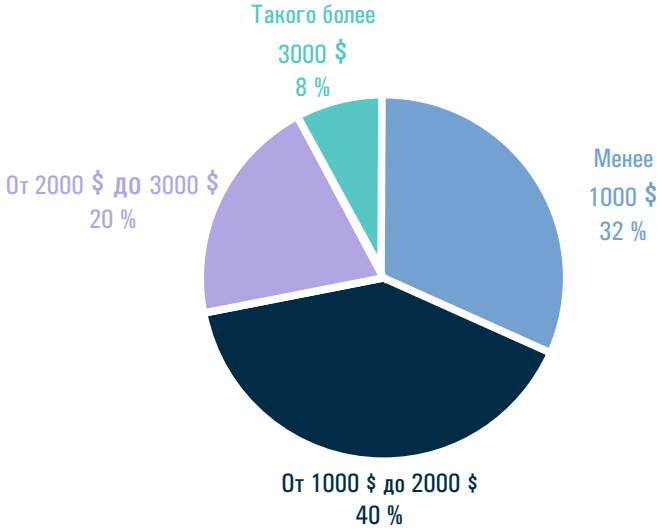
КАДРОВЫЙ ВОПРОС

Данные о присоединении большинства опрошенных кредитных организаций к Стандарту подтверждают выполнение одного из важнейших требований Стандарта о наличие выделенного подразделения по информационной безопасности. Полученные результаты позволяют сделать вывод, что практически во всех кредитных организациях это требование успешно выполнено. Распределение числа сотрудников таких подразделений представлено на графике. Стоит отметить, что по сравнению с результатами предыдущих исследований Сообщества АБИСС, количество кредитных организаций без выделенного подразделения ИБ упало с 30 % до 2 %. Эти данные особенно показательны с учетом того, что большая часть опрошенных – малые и средние банки.

Число сотрудников в подразделении ИБ

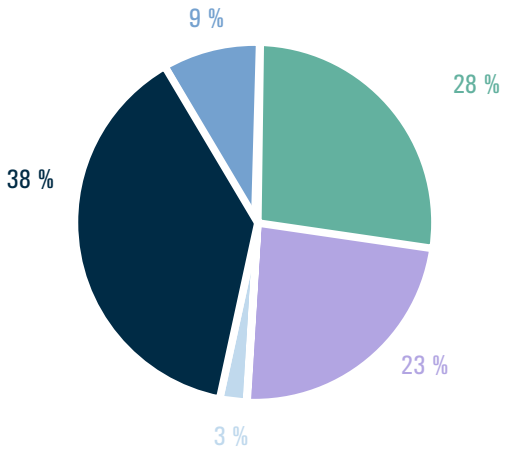


Средняя заработная плата сотрудников ИБ



Хотя по сравнению с предыдущими исследованиями сделан ощутимый шаг на пути решения организационных вопросов менеджмента информационной безопасности, основной вопрос мотивации сотрудников, обеспечивающих информационную безопасность, пока не решен. Треть (32 %) опрошенных указали, что средняя зарплата специалистов, обеспечивающих информационную безопасность в их организации, составляет менее 1000 $. Еще более трети (40 %) указали доход от 1000 $ до 2000 $, пятая часть (20 %) опрошенных назвали доходы таких специалистов от 2000 $ до 3000 $, а достаточно высокую зарплату – более 3000 $ указали только 8 % респондентов. Сравнение полученных данных с результатами наблюдений сайта hh.ru приводит к выводу, что средняя заработная плата системного администратора – 1500 $ – как минимум в 30% случаев превышает зарплату администратора информационной безопасности кредитной организации - менее 1000 $. С учетом особого значения защиты информации в кредитно-финансовой деятельности, полученные результаты могут свидетельствовать о повышенных рисках, связанных с недостаточной мотивацией сотрудников ИБ.

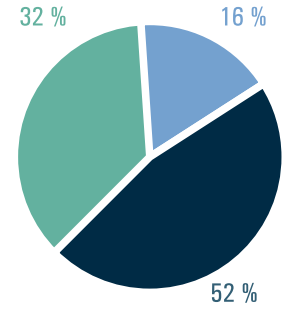
Проблемы при поиске специалистов ИБ



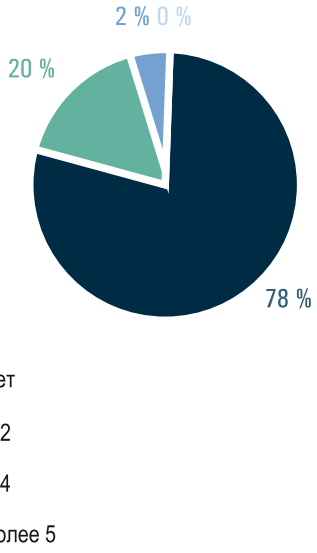
- Недостаточная квалификация в области обеспечения информационной безопасности
- Недостаточные знания в области банковских технологических процессов
- Недостаточные знания в области защиты персональных данных
- Недостаточный уровень зароботной платы
- Другое

Недостаточную заработную плату респонденты отметили и при ответе на вопрос о проблемах поиска специалистов по информационной безопасности, так считают 38 % опрошенных. Другими важными причинами можно считать недостаточные знания в области обеспечения информационной безопасности и банковских технологий, на которые указали соответственно 28 и 23 % респондентов.

Потребность в специалистах ИБ



Вакансии специалистов ИБ

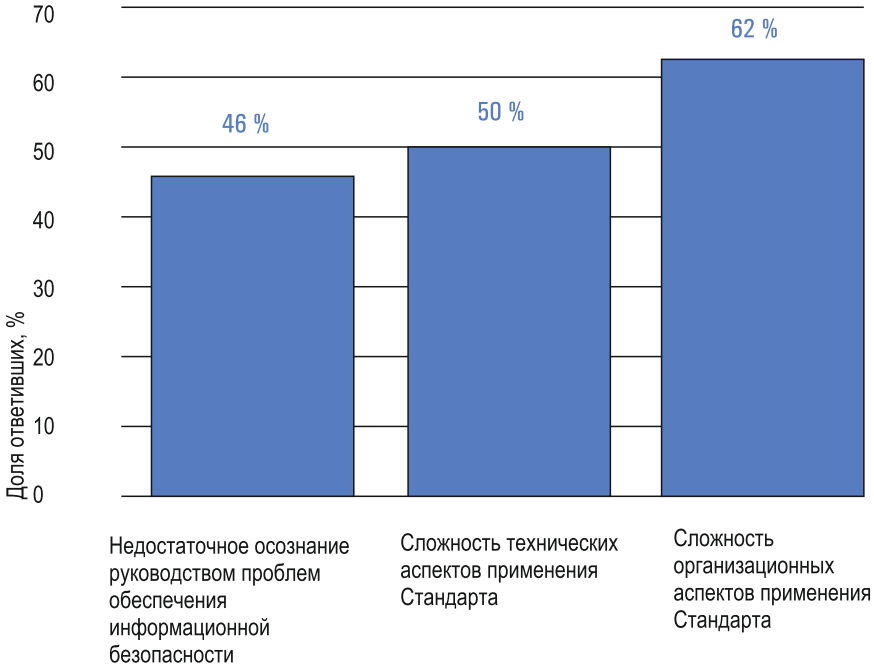


В то же время нужно признать, что выявленные до кризиса 2009 года во время предыдущих исследований АБИСС проблемы нехватки кадров в настоящее время уже не так масштабны. В настоящий момент только 16 % опрошенных банков испытывают острую потребность в специалистах информационной безопасности, и только в 22 % организаций открыты вакансии для таких специалистов.

Обучение по стандарту

При обзоре кадрового обеспечения задач внедрения Стандарта необходимо упомянуть и об отмеченной в ходе предыдущих исследований АБИСС и подтвержденной в настоящем исследовании проблеме повышения квалификации специалистов информационной безопасности. Эффективной мерой по повышению квалификации работников, занятых в обеспечении информационной безопасности кредитных организаций, можно считать сертифицированные АБИСС курсы обучения по различным аспектам применения Стандарта. Как указано на графике, уже 45 % опрошенных организаций воспользовались этой возможностью и имеют в штате как минимум одного сотрудника, прошедшего такие курсы. Полученные результаты позволяют рассчитывать, что дальнейшее совершенствование программы курсов и рост их популярности со временем смогут положительно повлиять на отмеченную респондентами проблему недостатка знаний в области информационной безопасности кредитных организаций.

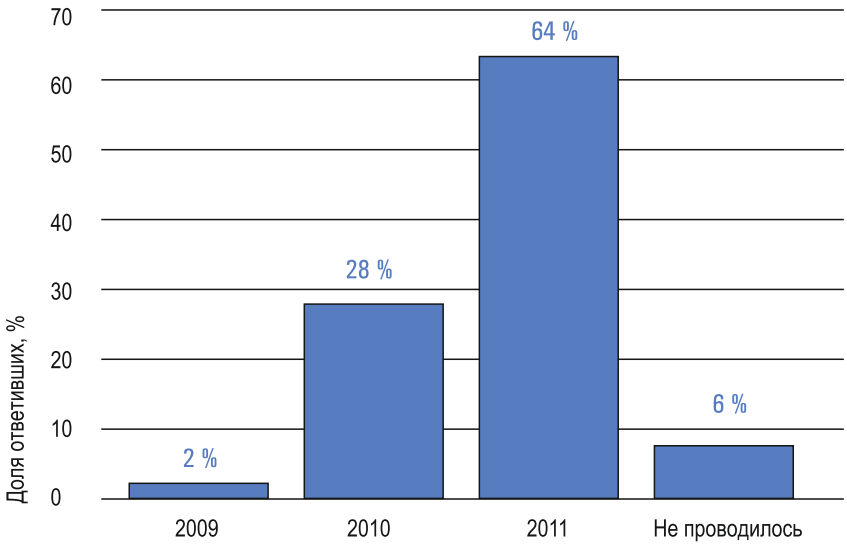
Сложности применения Стандарта



На необходимость дальнейшего обучения и обмена опытом указывает и процент обративших внимание на организационные и технические сложности при внедрении Стандарта. Как показал опрос, на недостаточное осознание руководством проблем обеспечения информационной безопасности указали 45 %, при этом на сложность Стандарта ссылаются более 50 % опрошенных.

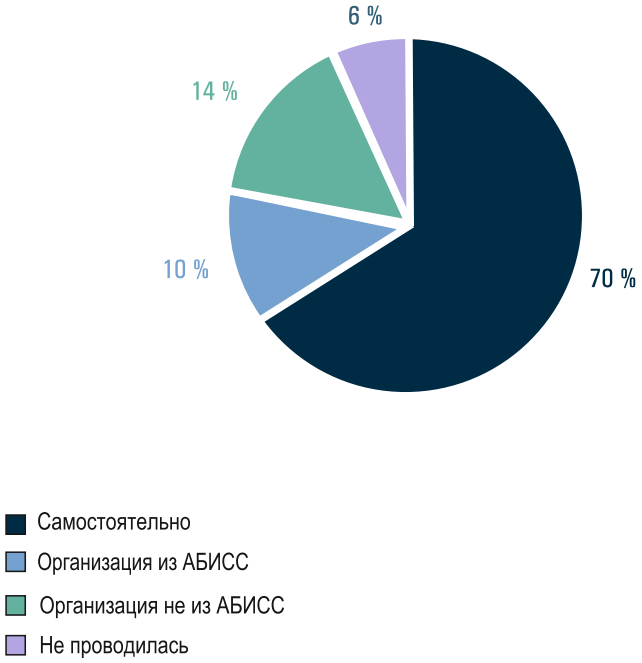
ВЫПОЛНЕННЫЕ РАБОТЫ И ПЛАНЫ ПО ВНЕДРЕНИЮ СТАНДАРТА

Когда проведена последняя оценка соответствия Стандарту



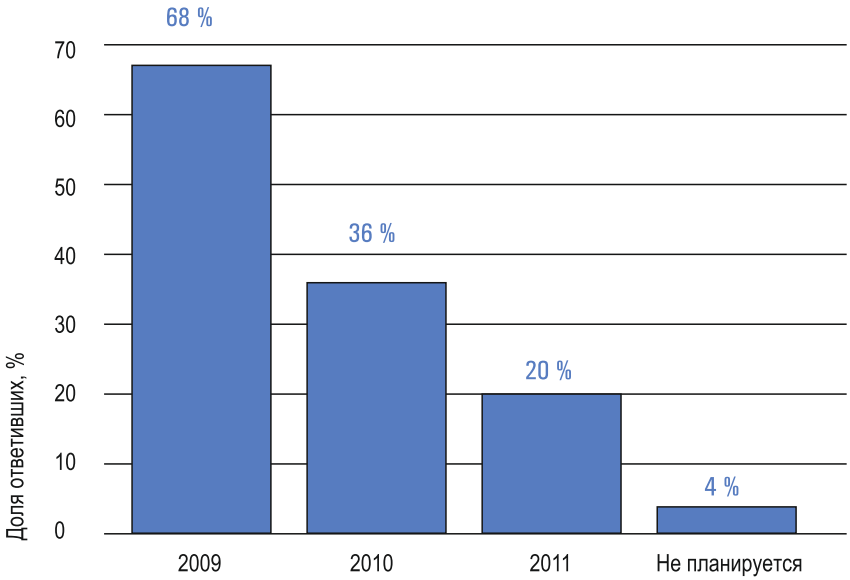
Определенный уровень внедрения Стандарта также подтверждается статистикой проведенных работ по оценке соответствия. Абсолютное большинство участников опроса (64 %) провели оценку соответствия в 2011 году, 28 % организаций выполнили такие работы в 2010 году, 2 % в 2009 году, и только 6 % опрошенных ее пока не проводили.

Кто выполнял оценку соответствия Стандарту?



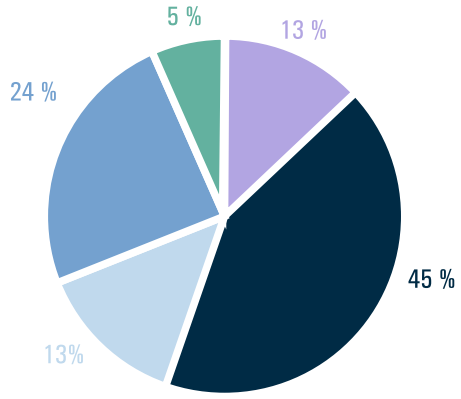
В условиях ограниченного финансирования данную работу абсолютное большинство кредитных организаций осуществляли самостоятельно, хотя независимая оценка, проводимая внешней организацией, особенно членом АБИСС, представляется более объективной. Для обращения к членам АБИСС на сайте abiss.ru созданы удобные механизмы регистрации и поиска, позволяющие получить подробную информацию об организациях, аккредитованных на проведение работ по внедрению Стандарта.

План проведения оценки соответствия Стандарту



Практически все респонденты уже запланировали работы по оценке соответствия на ближайшие годы. При этом, вероятно, в соответствии с принятой в организации стратегией долгосрочного планирования, 68 % будут проводить оценку соответствия в 2012 году, 36 % уже запланировали работы на 2013 год, 20 % строят долгосрочные планы по оценке на 2014 год, и только 4 % организаций пока не планируют проводить такие работы.

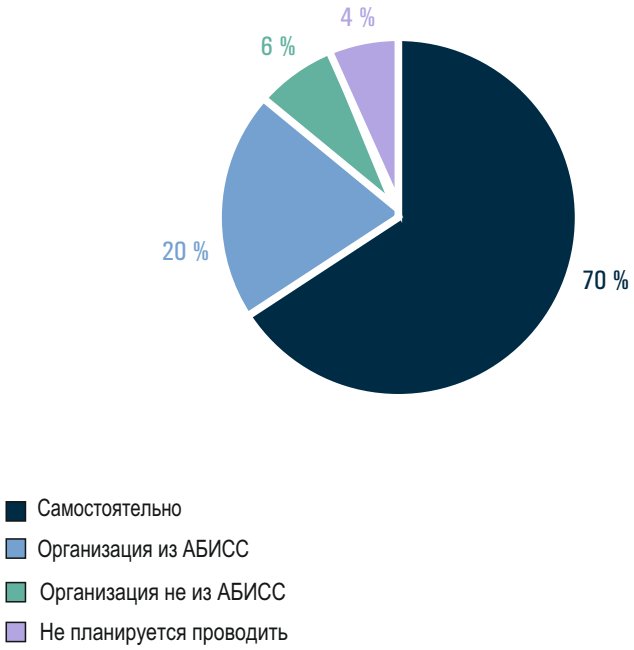
В чем преимущество внешней оценки?



- Возможность получить опыт и знания для проведения в будущем самостоятельной оценки
- Возможность получить качественный и непредвзятый результат
- Возможность использовать людские ресурсы сторонней организации в связи с недостатком собственных
- Не вижу преимуществ
- Преимущество в другом

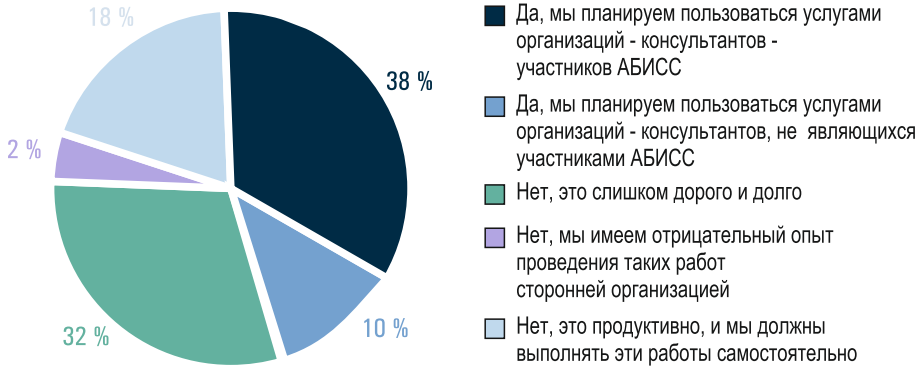
Необычным выглядит мнение респондентов о преимуществах внешней оценки. Хотя большинство и признаёт рекомендации Банка России по привлечению внешних аудиторов, почти четверть (24 %) кредитных организаций не видят связанных с этим преимуществ. Отсутствие доверия к внешним аудиторским организациям можно объяснить как относительно молодым рынком таких услуг, так и отсутствием требования обязательности внешней оценки, как, например, при аудите финансовой отчетности банков.

Кто будет выполнять оценку?



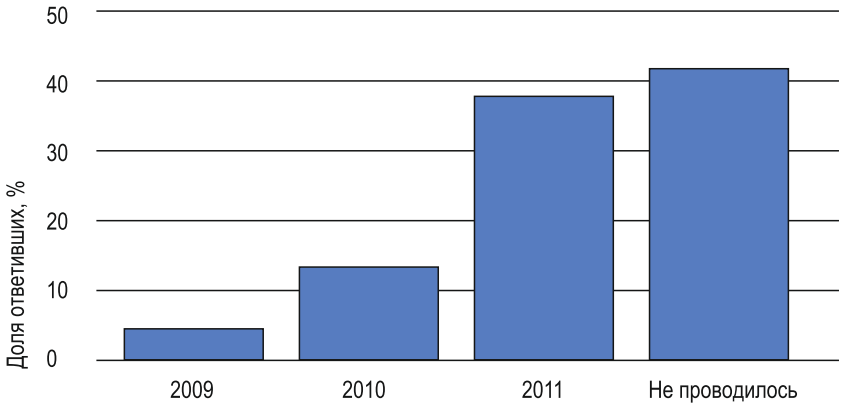
Для внешней оценки опрошенные кредитные организации, из тех, кто планирует привлекать внешние организации, ориентируются на членов НП «АБИСС» 20%, подтверждая важность предъявляемых требований к качеству услуг.

Привлечение консультантов

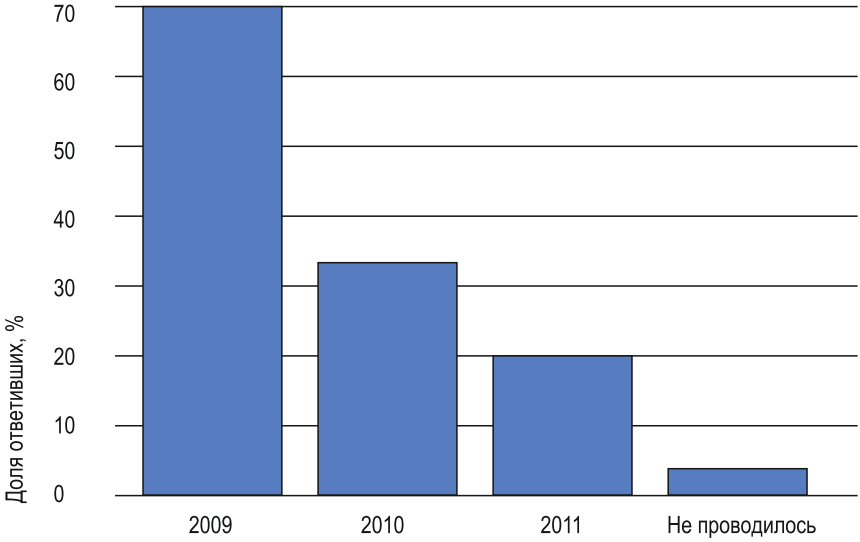


В отношении выбора сторонних консультантов для внедрения Стандарта также видно предпочтение в пользу организаций – членов НП «АБИСС».

Когда проводился последний анализ рисков?



План анализа рисков



Одной из основных задач создания и функционирования системы менеджмента информационной безопасности является анализ рисков информационной безопасности. В связи с этим был задан вопрос об актуальности данных работ. Большая часть опрошенных (58 %) уже проводили такие работы в период с 2009 года по настоящее время, в то время как 42 % организаций пока не выполняли анализ рисков информационной безопасности. При этом 70 % кредитных организаций планируют проводить анализ рисков в 2012 году, более 30 % запланировали такие работы на 2013 год, 10 % на 2014 год, и 4 % еще не планируют проводить эту работу.

ЗАКЛЮЧЕНИЕ

По результатам исследования можно сделать следующие общие выводы:

Комплекс документов Банка России по обеспечению информационной безопасности получил широкое признание со стороны подавляющего большинства кредитных организаций, что подтверждено существенным ростом числа проектов по его внедрению и оценки соответствия.

Комплекс БР ИББС постоянно развивается, включая в себя последние нормативные требования в области информационной безопасности, а также передовые практики управления информационными рисками.

Многие из опрошенных отмечают целесообразность придания основному документу Комплекса – Стандарту СТО БР ИББС 1.0 статуса обязательного с целью большей мотивации руководства кредитных организаций по присоединению к Стандарту и выделению необходимых ресурсов.

Постепенно решается задача обеспечения служб ИБ кредитных организаций квалифицированными кадрами, что подтверждается значительным ростом числа обученных специалистов на сертифицированных НП «АБИСС» курсах, однако в небольших банках пока еще не решена в полной мере проблема мотивации таких профессионалов.

По мере развития рынка профессиональных услуг в области ИБ все более актуальной становится проблема контроля их качества, и здесь отмечается роль НП «АБИСС» в части содействия кредитным организациям по выбору квалифицированных аудиторов, консультантов и учебных центров.

В целом, налицо положительная динамика внедрения Стандарта в кредитных организациях, однако для сохранения ее темпов и получения качественных результатов с целью повышения общего уровня информационной безопасности банковской отрасли требуются дальнейшие скоординированные усилия регулирующих и контрольных органов, НП «АБИСС» и самих кредитных организаций по совершенствованию Комплекса БР ИББС, его продвижению, а также постоянному обмену опытом и повышению квалификации профессионалов в области ИБ.

О некоммерческом партнерстве «Сообщество пользователей стандартов по информационной безопасности»

Некоммерческое партнерство «Сообщество пользователей стандартов по информационной безопасности АБИСС» является некоммерческой организацией, основанной на принципах добровольного объединения ее членов – субъектов предпринимательской и профессиональной деятельности, оказывающих профессиональные услуги в области обеспечения информационной безопасности для кредитных и других организаций – участников национальной платежной системы Российской Федерации.

ДЛЯ ЗАМЕТОК

Российская Федерация,
109052, г. Москва, Рязанский проспект, дом 2, строение 49
Тел.: +7 (495) 745-77-88
E-mail: abiss@abiss.ru
www.abiss.ru