КОД БЕЗОПАСНОСТИ

Информационная безопасность на практике. Итоги 2018 г., перспективы 2019 г.

Аналитическое исследование
Март 2019 г.

Содержание

Резюме

- В 2019 г. ожидается сокращение на **12%** по сравнению с 2018 г. количества компаний-респондентов, где за обеспечение процессов ИБ отвечает профильный отдел/специалист;
- Почти **2/3 участников** рынка имеют разработанную и утвержденную ИБ-стратегию;
- Число компаний, планирующих стратегию информационной безопасности более чем на 3 года, в 2019 г. увеличится **в два раза**;
- При оценке информации об изменениях ландшафта угроз информационной безопасности российские компании в наибольшей степени доверяют сообщениям регуляторов **(80%)** и сообщениям производителей средств защиты информации **(74%)**;
- В 2019 г. **35%** российских организаций планируют увеличить бюджет на информационную безопасность. Наибольшее количество средств на ИБ готовы выделить следующие отрасли: госсектор **(18% от ИТ-бюджета)**, финансовый сектор **(17%)**, промышленность **(15%)** и топливно-энергетический комплекс **(14%)**;
- Защита критической информационной инфраструктуры (КИИ) стала **одним из ключевых факторов**, влияющих на расходы на обеспечение информационной безопасности;
- **97%** компаний испытывают трудности при убеждении руководства в необходимости затрат на ИБ;
- Приоритетными критериями выбора средств защиты данных в 2019 г. становятся производительность, простота развертывания и качество продукта. Клиентоориентированность, лидерство поставщика отодвигаются на второй план;
- В 2019 г. на **13%** увеличилось количество организаций, выбравших долгосрочную стратегию сотрудничества с поставщиками ИБ-решений;
- **Каждая пятая** российская компания в ближайшие три года не планирует внедрять новые ИБ-технологии.

Аннотация

Ситуация в сфере информационной безопасности постоянно меняется: появляются новые угрозы, растет их количество. Информационные ресурсы продолжают оставаться уязвимыми, в силу роста их гибкости и возможностей передачи данных. По мере роста объема информации более значимым становится вопрос обеспечения ее безопасности.

Для оценки уровня востребованности технологий информационной безопасности и подходов к решению ИБ-задач аналитики «Кода безопасности» провели опрос респондентов отечественных компаний. Предметом исследования стали ответы на следующие вопросы:

- Каков горизонт планирования стратегии информационной безопасности в организациях?
- Какой информации об изменениях ИБ-угроз доверяют участники рынка?
- Каковы критерии выбора решений по информационной безопасности?
- Какие технологии в области информационной безопасности планируют внедрить российские компании?

Методика сбора данных

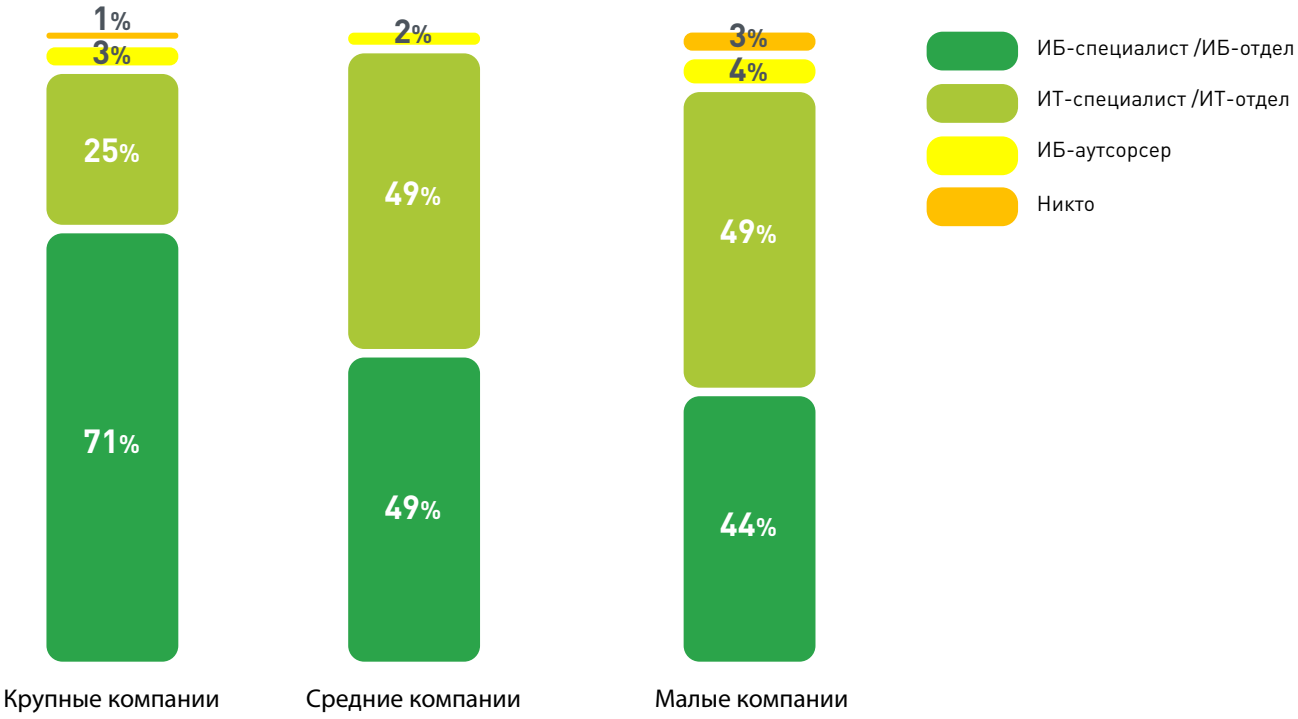
Исследование проводилось по России. Использовался количественный метод в форме онлайн-опроса на сайте компании «Код безопасности» и опросов на офлайн-мероприятиях. В исследование включена информация, собранная на основе ответов 534 специалистов по информационной безопасности, ИТ-специалистов и ТОП-менеджеров, работающих в компаниях 8 отраслей: госсектор, здравоохранение, ИТ, образование, промышленность, транспорт, топливно-энергетический комплекс, финансы.

При обработке полученных результатов компании были сегментированы на 3 категории исходя из численности сотрудников – малые (до 100 чел.), средние (101–500 чел.) и крупные (более 500 чел.).

Кто обеспечивает процессы информационной безопасности

Каждая компания в процессе своего развития и роста обязательно проходит этап, когда необходимо построить целый ряд процессов, связанных с управлением информационной безопасностью.
Для эффективной работы организации по предупреждению инцидентов необходимо иметь отлаженную систему обеспечения информационной безопасности, в которой распределены роли, обязанности и каждый участник процесса знает, за что несет ответственность.
Результаты исследования компании «Код безопасности» показали, что чем крупнее компания, тем выше осознание необходимости выделенного ИБ-отдела. Так, в 71% крупных российских компаний за обеспечение процессов информационной безопасности отвечает специализированный ИБ-отдел или ИБ-специалист. У компаний среднего размера данный показатель составляет 49%, а в малых компаниях – лишь 44%.

Кто отвечает за информационную безопасность, 2019 г.



Большинство организаций возлагают ответственность за обеспечение ИБ на ИТ-подразделения или другие отделы либо предпочитают прибегать к помощи аутсорсинговых ИБ-специалистов.

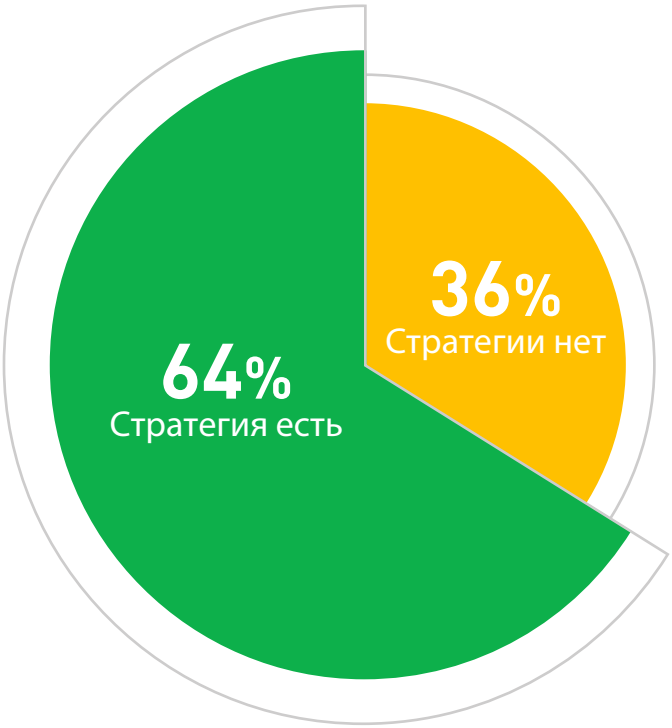
В 2019 г. наметилась тенденция сокращения количества российских компаний, в которых за обеспечение процессов ИБ отвечает профильный отдел/специалист. Сравнительный анализ данных за два года показал, что сокращение составит 12%.

ИБ-стратегия

Стратегия информационной безопасности

Наличие стратегии информационной безопасности, а также ее взаимосвязь с бизнес-стратегией повышают эффективность защиты информации. В настоящее время 64% компаний-респондентов имеют разработанную и утвержденную ИБ-стратегию.

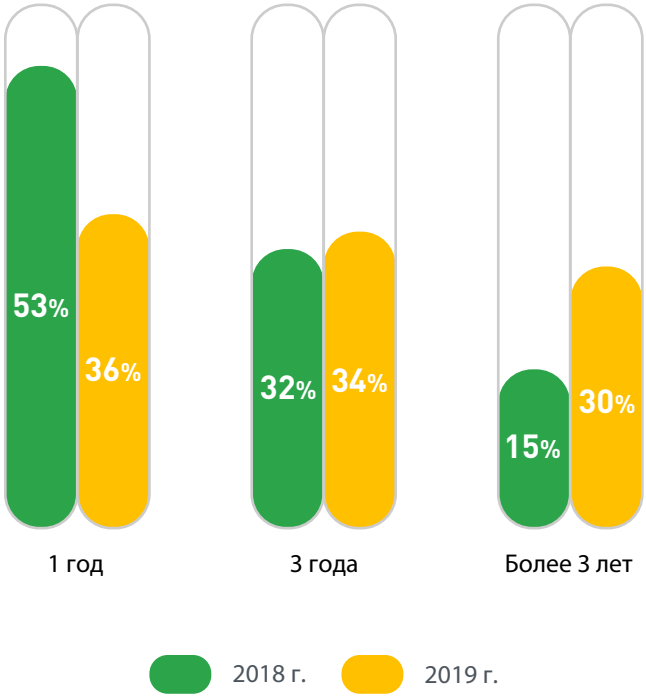
Наличие ИБ-стратегии в российских компаниях, 2019 г.



Горизонт планирования ИБ-стратегии

Как уже отмечалось выше, ИБ-стратегия неразрывно связана с развитием ИТ и бизнесом в целом. Поэтому грамотно спланированная стратегия и ее оптимальные сроки окажут влияние на правильность распределения финансовых и человеческих ресурсов, а также планомерность внедрения организационных и технических мер обеспечения информационной безопасности в компании.

Изменение горизонта планирования ИБ-стратегии

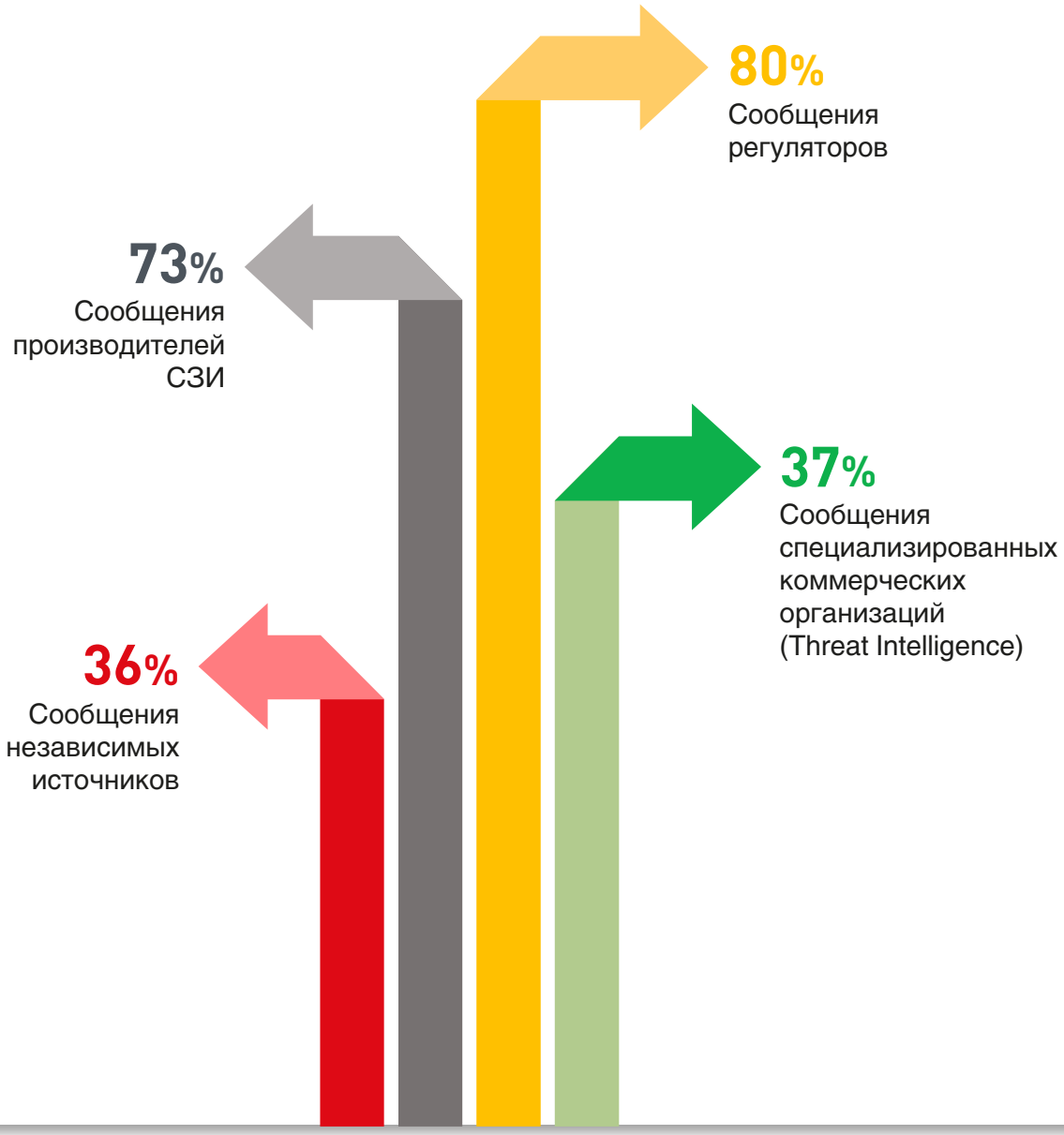


В 2019 г. будет наблюдаться тенденция перехода к более долгосрочной (по сравнению с предыдущим годом) стратегии информационной безопасности. 17% российских компаний выбрали более длительный период действия ИБ-стратегии. На 2% больше компаний в 2019 г. будут планировать ИБ-стратегии на 3 года; в два раза увеличится число компаний, выбравших планирование стратегии информационной безопасности на период более 3 лет.

Источники информации о рисках и ИБ-угрозах

Какой информации об изменениях ландшафта угроз ИБ доверяют российские компании? Как показали результаты исследования, по сравнению с предыдущим годом уровень доверия к сообщениям регуляторов не изменился – показатель составил 80%. В 2019 г. незначительно (на 2%) повысилось доверие к сообщениям производителей средств защиты информации (71% в 2018 г.; 73% в 2019 г.). Немного сократилось (на 2%) доверие к информации Threat Intelligence, чуть больше (на 6%) – к сообщениям независимых источников.

Доверие российских компаний к источникам информации, 2019 г.

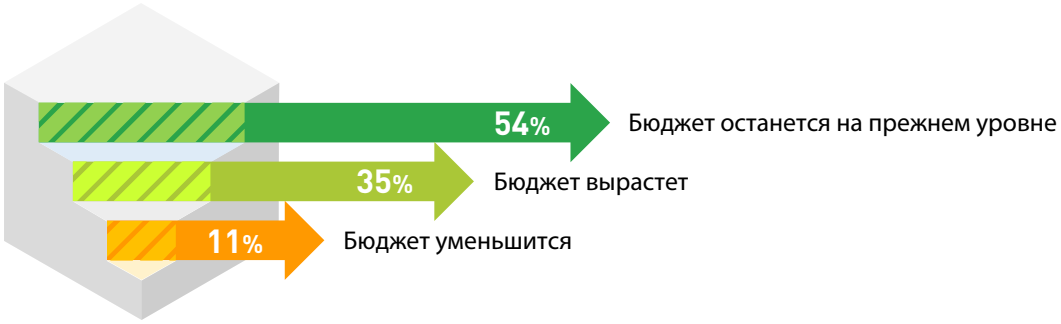


Бюджет

Как изменится бюджет на информационную безопасность в 2019 г.

Изменения общей экономической ситуации в стране не отразились негативно на ИБ-бюджетах российских организаций. 35% участников опроса планируют в 2019 г. увеличить бюджет на информационную безопасность. Больше половины (54%) оставят ИБ-бюджет на прежнем уровне. И лишь 11% компаний в 2019 г. будут сокращать объем бюджета.

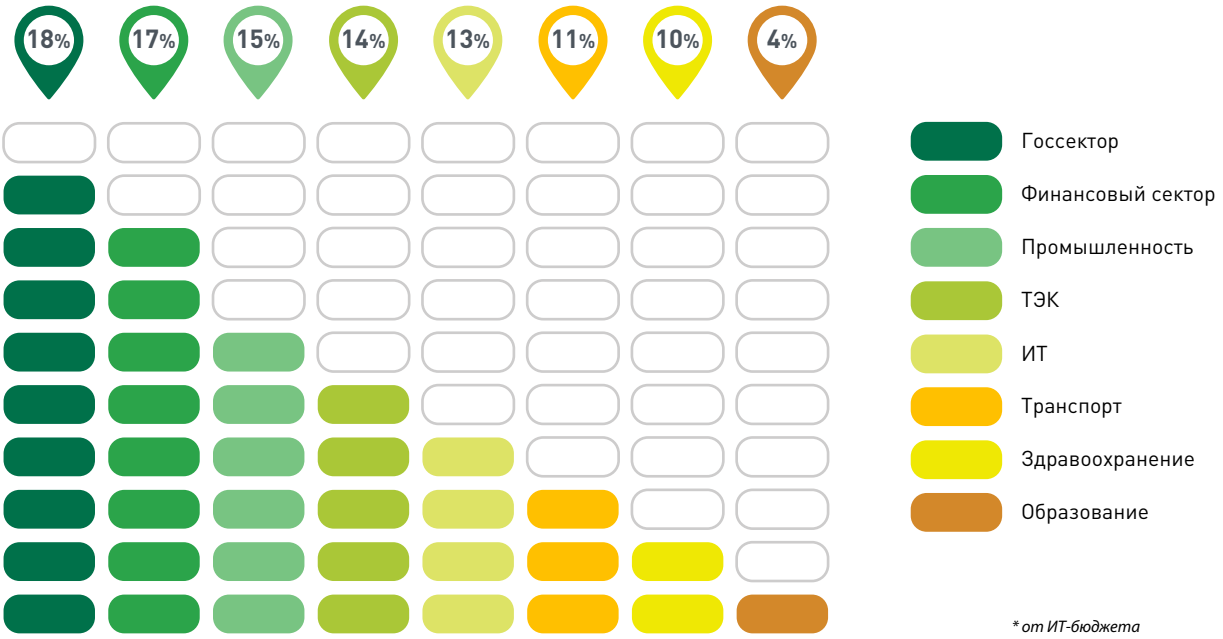
Изменение ИБ-бюджета в 2019 г.



Доля расходов на безопасность

Задача формирования бюджета на информационную безопасность во многом зависит от расстановки ИБ-приоритетов и их соотнесения с размером информационной инфраструктуры, от оценки рисков, от особенностей бизнес-процессов организации. Результаты исследования показали, что доля бюджета, выделяемого на информационную безопасность, не так высока. 18% от ИТ-бюджета готов выделить на обеспечение информационной безопасности госсектор. 17% и 15% – финансовый сектор и промышленность соответственно. Наименьшие доли ИБ-бюджетов характеризуют образование, это лишь 4% в 2019 г.

Доля ИБ-бюджета* (среднеотраслевое значение)



** от ИТ-бюджета*

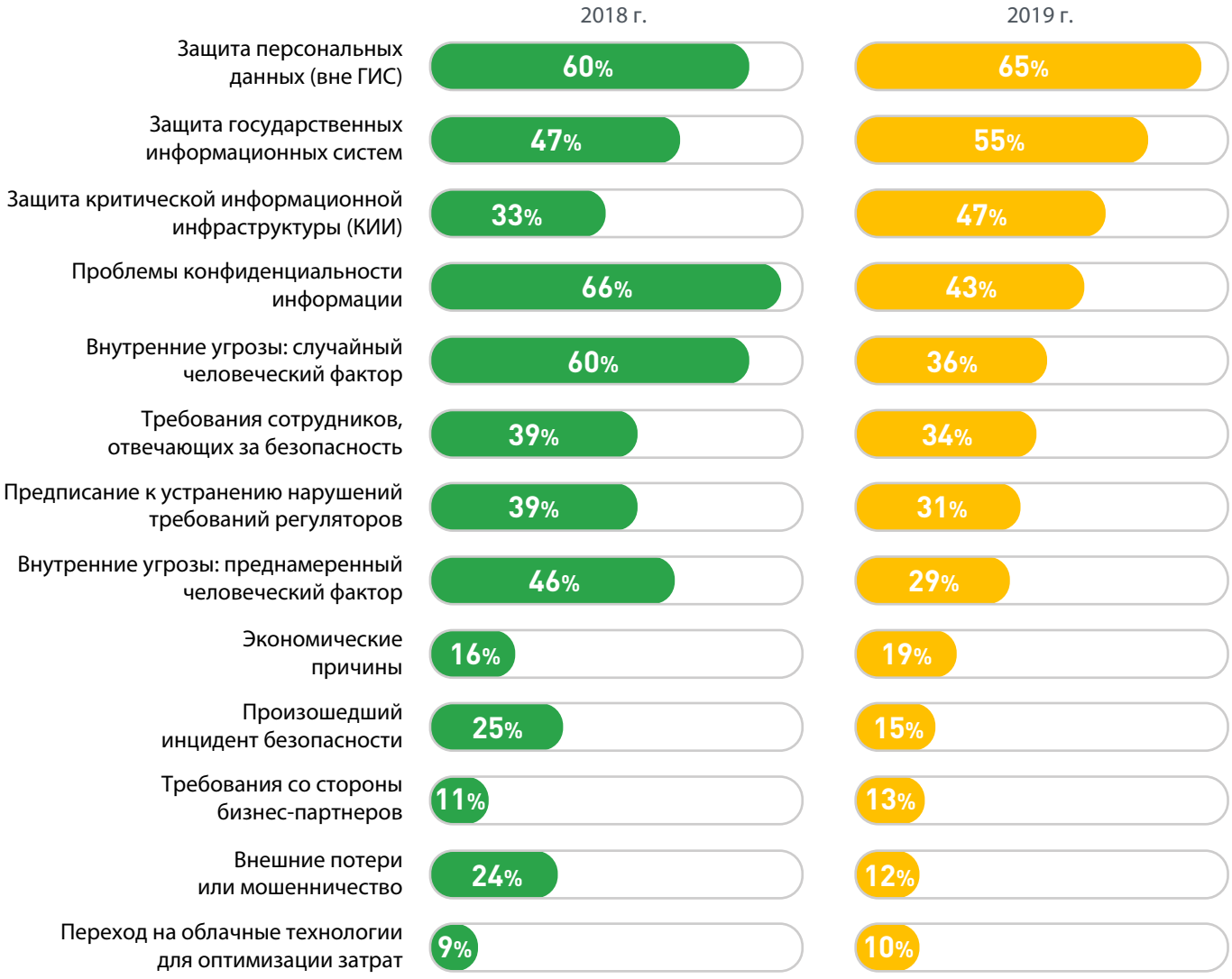
Бюджет

Ключевые факторы, определяющие расходы на безопасность

Одним из значимых факторов, определяющих расходы организаций на обеспечение информационной безопасности, участники опроса назвали защиту критической информационной инфраструктуры (КИИ). Значение этого показателя по сравнению с предыдущим годом выросло с 33% до 47%. Несмотря на то что 187-ФЗ вступил в силу с 1 января 2018 г., тема защиты КИИ по-прежнему доминирует в списке актуальных. К настоящему моменту, по данным ФСТЭК России, около 1100 субъектов КИИ прошли категорирование. Примерно 20% присвоена категория (значимая). Эффективно подошли к выполнению 187-ФЗ такие отрасли, как здравоохранение, ТЭК и оборонно-промышленный комплекс. Пока выжидательную позицию заняли операторы связи и банковский сектор.

Также в числе ключевых факторов, которые будут стимулировать расходы на безопасность, в 2019 г. – защита персональных данных вне ГИС (рост 5%) и защита ГИС (рост 8%).

Что способствует выделению денег на ИБ



Бюджет

Ключевые факторы, сдерживающие расходы на безопасность

Что препятствует выделению руководством средств на обеспечение информационной безопасности? Аналитики компании «Код безопасности» провели сравнительную оценку значимости сдерживающих факторов за два года. Результаты представлены на графике ниже.

Что препятствует выделению бюджета на ИБ

Лишь 3% участников исследования не испытывают проблем с выделением руководителями средств на информационную безопасность. Данный показатель остается неизменным на протяжении двух лет. Немного выросла доля организаций, ИТ-бюджет которых ограничен (2% в 2018 г., 4% в 2019 г.). В таких компаниях бюджет на информационную безопасность формируется по остаточному принципу. 97% участников российского рынка испытывают трудности с убеждением руководства в актуальности затрат на обеспечение информационной безопасности.

Требования к средствам защиты информации (СЗИ) и к их поставщикам

Критерии выбора

Процесс выбора средств защиты информации является непростой задачей и требует специальных знаний и компетенций, понимания целей и методологий внедрения, грамотной проработки требований к программным/аппаратным продуктам и их производителям.

Для российского рынка основными критериями выбора стали оптимальное сочетание цены, производительности и функций. На протяжении двух лет данный показатель выбрало наибольшее количество участников опроса (73% в 2018 г.; 75% в 2019 г.). 48% считают, что продукт должен в наибольшей степени подходить для текущих бизнес-задач. 46% респондентов выделяют важность критерия «качество системы управления».

Критерии выбора СЗИ и поставщика

Всё в большей степени заказчикам требуется от продукта реальная безопасность, которая обеспечивается просто, легко и надежно. При этом ценовой фактор перестает быть определяющим.

Приоритетными критериями выбора средств защиты данных стали производительность, простота развертывания и качество продукта. Клиентоориентированность, лидерство поставщика отодвигаются на второй план.

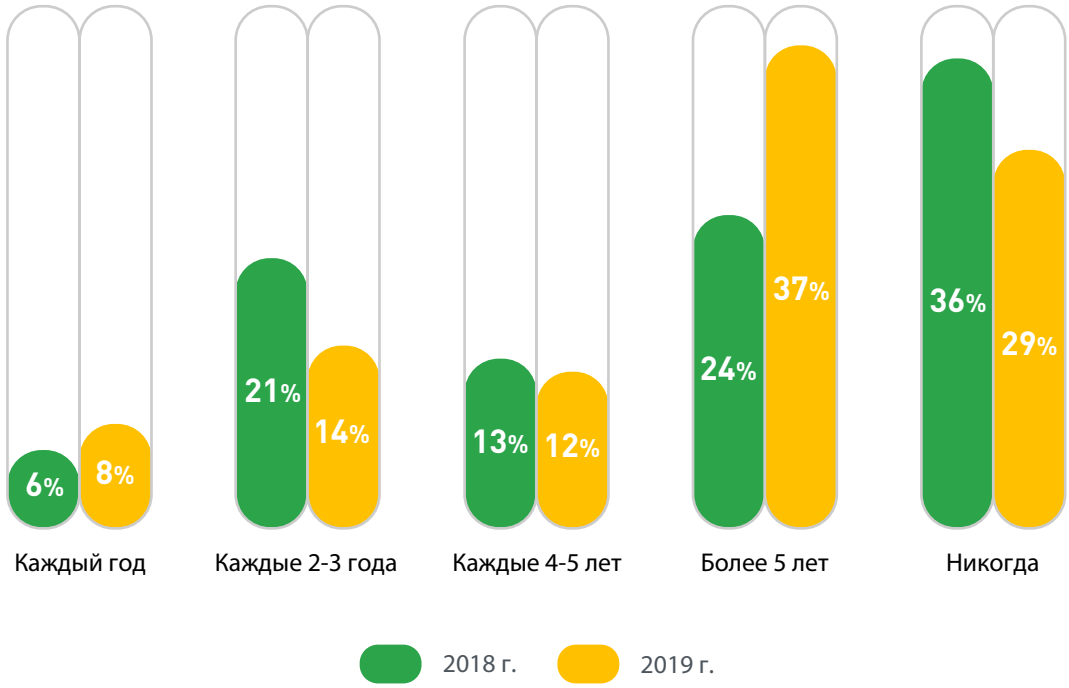
Требования к средствам защиты информации (СЗИ) и к их поставщикам

Смена поставщика решений по информационной безопасности

Чтобы вложения в решения, обеспечивающие кибербезопасность, были своевременными и оправданными, руководителям предприятий приходится менять свою стратегию защиты. Часто это происходит со сменой продукта и/или его поставщика.

Как часто российские компании меняют поставщика решений по информационной безопасности? В 2019 г. на 2% возрастет количество компаний, которые ежегодно меняют ИБ-поставщика. Наблюдается тенденция перехода от среднесрочного сотрудничества с вендорами (2–4 года) к более длительному (свыше 5 лет). В 2019 г. на 13% увеличилось количество организаций, выбравших данную стратегию. Кроме того, стало меньше на 7% организаций, которые никогда не меняют поставщика СЗИ. Это означает, что к руководителям предприятий приходит понимание, что любой бизнес требует пересмотра стратегии использования средств информационной безопасности.

Как часто компании меняют поставщика СЗИ

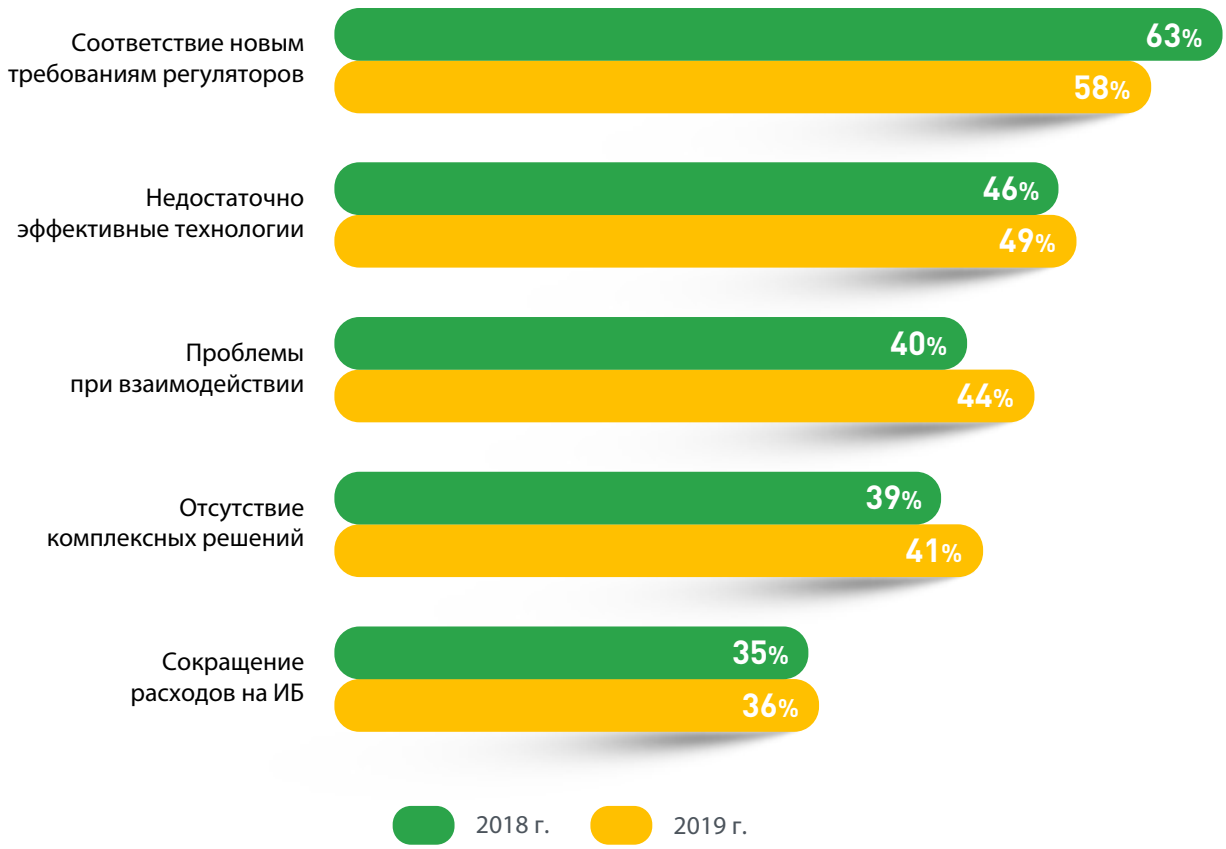


Требования к средствам защиты информации (СЗИ) и к их поставщикам

Почему меняют поставщика СЗИ

Второй год подряд основной причиной смены поставщика средств защиты информации является критерий соответствия новым требованиям регуляторов. В 2018 г. размер этого показателя составил 63%, в 2019 г. – 58%. Но развитие рынка информационной безопасности не определяется только законодательными инициативами и действиями регуляторов. Здесь во многом драйвером развития являются потребности заказчиков (49%), технологические возможности (41%), бюджет потребителя (36%).

Причины смены поставщика решений по ИБ



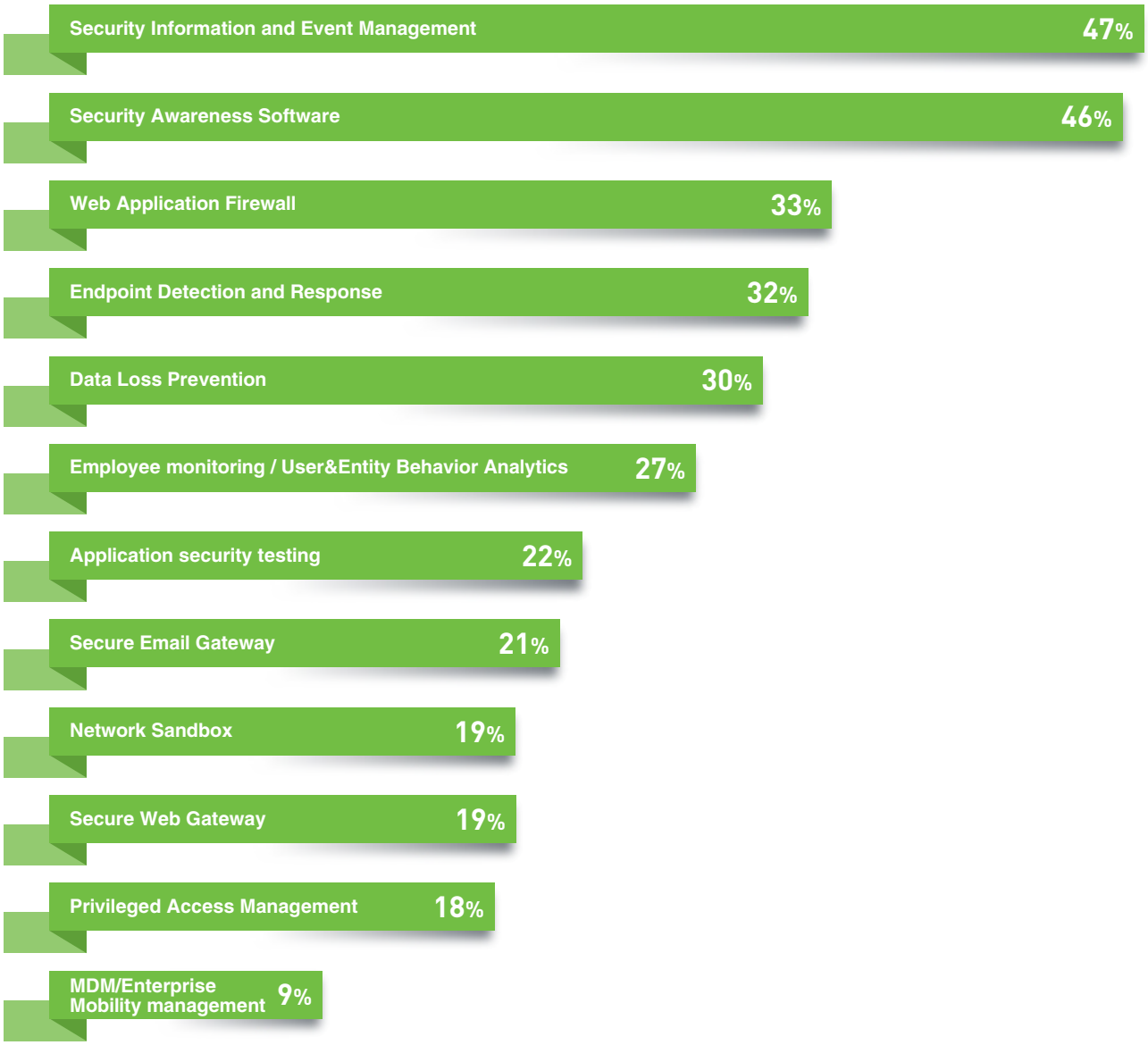
Требования к средствам защиты информации (СЗИ) и к их поставщикам

Внедрение технологий информационной безопасности

Российский рынок информационной безопасности динамично развивается. Какие технологии в данной области планируют внедрять российские компании в ближайшие три года? В ТОП-3 направлений, интересующих заказчиков, вошли Security Information and Event Management (47% ответов); Security Awareness Software (46% ответов) и Web Application Firewall (33% ответов).

22% российских компаний не собираются внедрять новые ИБ-технологии в ближайшие три года.

Внедрение технологий ИБ в ближайшие 3 года



Заключение

Чем больше становится объем корпоративной информации, тем актуальнее вопрос обеспечения ее безопасности.

Для эффективного управления ИБ в компании должен существовать пусть и небольшой, но специализированный отдел, который будет сфокусирован на вопросах обеспечения информационной безопасности. В то же время в 2019 г. на 14% возросло число организаций, где защиту информации обеспечивает ИТ-отдел. Также увеличилось число компаний, которые передали данный вопрос на аутсорсинг.

По сравнению с предыдущим годом, в 2019 г. повысилась долгосрочность планирования стратегии информационной безопасности. Число компаний, перешедших от краткосрочной стратегии к долгосрочной, выросло в два раза.

Изменения общей экономической ситуации в стране не отразились негативно на ИБ-бюджетах российских организаций. 35% участников опроса планируют повысить бюджет на информационную безопасность в 2019 г. Больше половины (54%) оставят бюджет на информационную безопасность на прежнем уровне. И лишь 11% компаний в 2019 г. будут сокращать бюджет на обеспечение безопасности.

Одним из значимых факторов, определяющих расходы организаций на обеспечение информационной безопасности, участники опроса назвали защиту критической информационной инфраструктуры (КИИ). Значение этого показателя по сравнению с предыдущим годом выросло с 33% до 47%.

97% участников российского рынка испытывают трудности с тем, чтобы убедить руководство в актуальности затрат на обеспечение информационной безопасности. Основной причиной сложностей является недостаточный уровень информированности высшего руководства в вопросах информационной безопасности, это отметили 34% российских компаний.

Выбор ИБ-решений для предприятия – одна из важнейших задач его высшего руководства. От этого зависит успешность функционирования информационной системы предприятия, которая на протяжении ряда последующих лет будет являться платформой развития конкурентных преимуществ предприятия и обеспечения его эффективности.

Для российского рынка основными критериями выбора средств защиты информации стали оптимальное сочетание цены, производительности и функций (так считают 75 участников опроса). 48% считают, что продукт должен быть наиболее подходящим для текущих бизнес-задач. 46% компаний отметили важность критерия «качество системы управления».

КОД БЕЗОПАСНОСТИ

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

analytics@securitycode.ru

www.securitycode.ru