КОД безопасности

Исследование российского рынка информационной безопасности

Аналитическое исследование
октябрь 2021

КОД безопасности

Пандемия и массовый перевод сотрудников на дистанционную работу существенно расширили ландшафт ИБ-угроз. Частным и государственным структурам приходится открывать ИТ-инфраструктуру для удобства работы удаленных сотрудников. При этом обеспечение безопасности информации, передаваемой по открытым каналам, остается наиболее актуальным вопросом.

«Код Безопасности» провел традиционное исследование востребованности технологий информационной безопасности и подходов к решению ИБ-задач среди отечественных компаний. Предстояло найти ответы на следующие вопросы:

Кто и как занимается обеспечением информационной безопасности в организациях?

Какие бюджеты выделяются на информационную безопасность?

Почему приходится отказываться от ИБ-мероприятий?

Какие ИБ-технологии планируется внедрить в ближайшие 3 года?

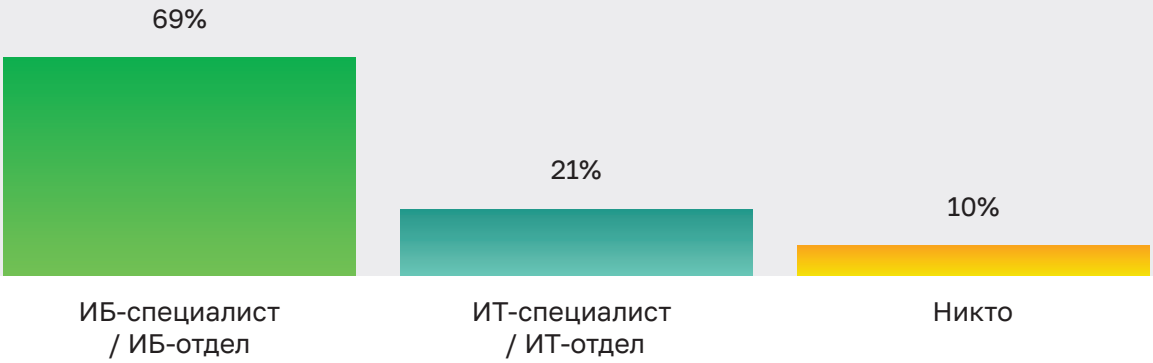
Для объективности исследования были опрошены около 300 специалистов по информационной безопасности, ИТ-специалистов и топ-менеджеров. Полученные данные были разбиты на 5 отраслей: госсектор, информация и связь, образование, обрабатывающая промышленность, финансы. Дополнительно данные сегментированы на 3 категории по количеству работающих сотрудников: малые предприятия с численностью персонала до 100 человек, средние – от 101 до 500 человек, крупные – более 500 человек.

Кто занимается информационной безопасностью

Громкие инциденты с кражей ценной информации и блокировкой работы зарубежных организаций заставляют отечественные компании задуматься о необходимости внедрения стратегии информационной безопасности.

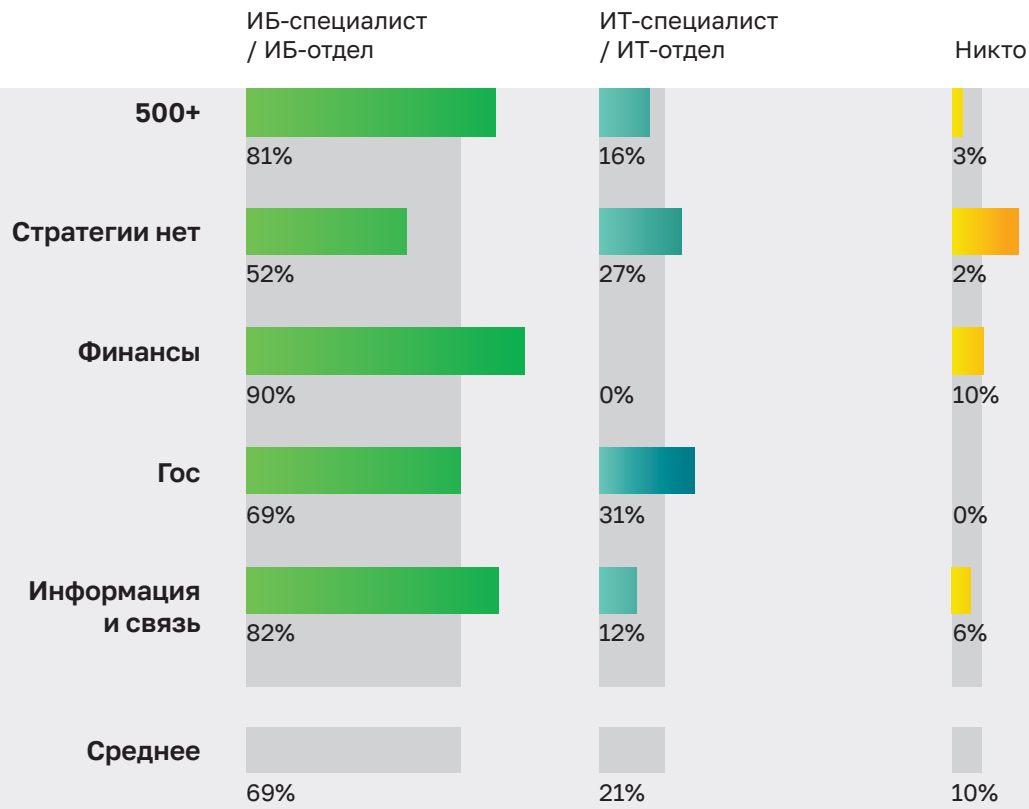
69% респондентов сообщили, что у них есть отдельный специалист или даже отдел, которые отвечают за защиту данных.

У 21% информационной безопасностью в нагрузку занимаются ИТ-специалисты или ИТ-отдел. 10% опрошенных признались в отсутствии специалистов или отделов, занимающихся информационной безопасностью.



Если говорить в разрезе отраслей, то чаще всего отдельные специалисты и отделы по информационной безопасности есть в компаниях из отраслей финансов, информации и связи. А больше всего ответов о том, что никто не занимается инфобезом – у отрасли образования.

Государственные структуры распределяют ответственность за информационную безопасность между специализированными и общими ИТ-отделами. У них нет ситуации, чтобы никто не отвечал за ИБ.

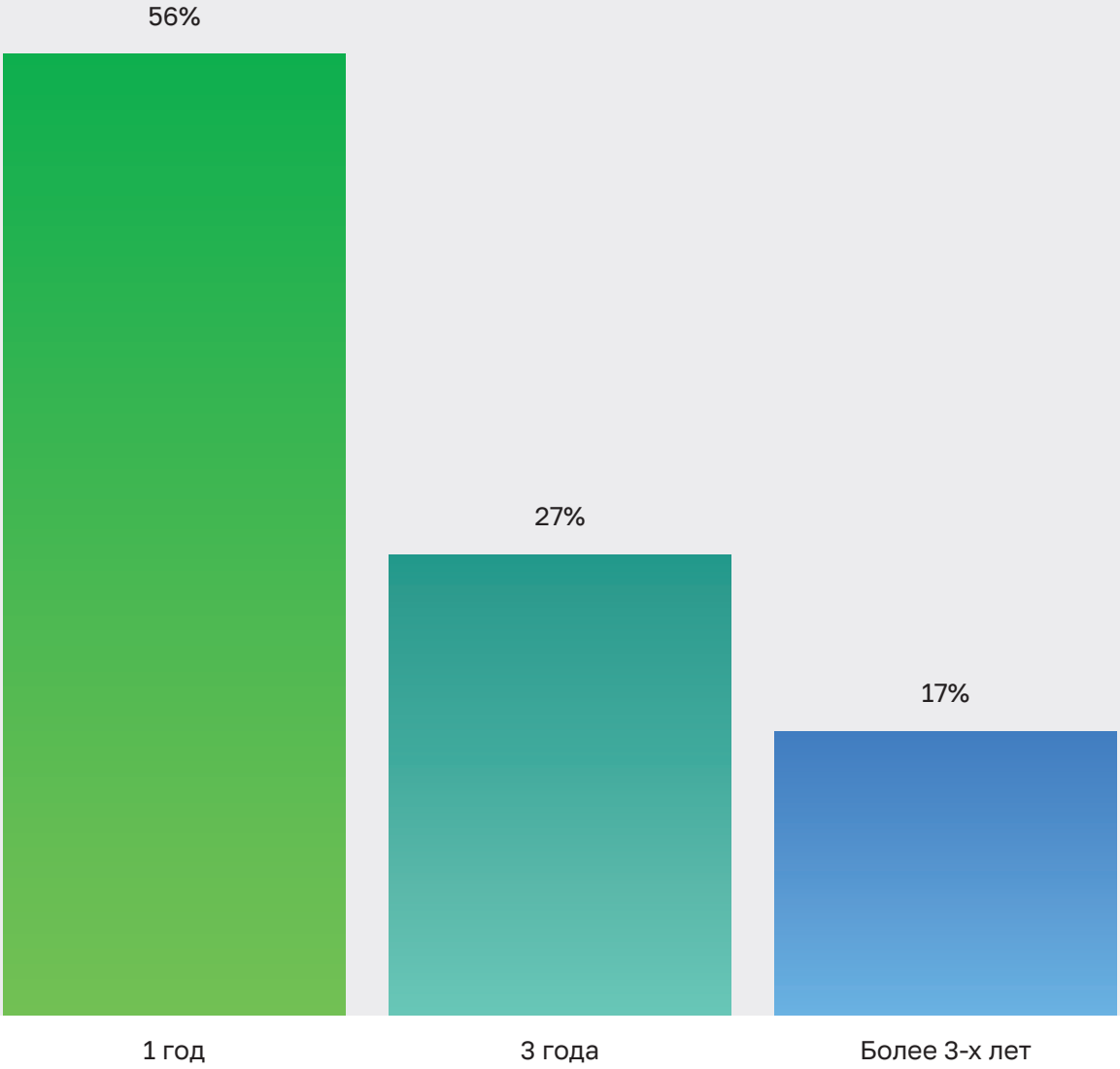


КОД безопасности

Горизонт планирования ИБ-стратегии

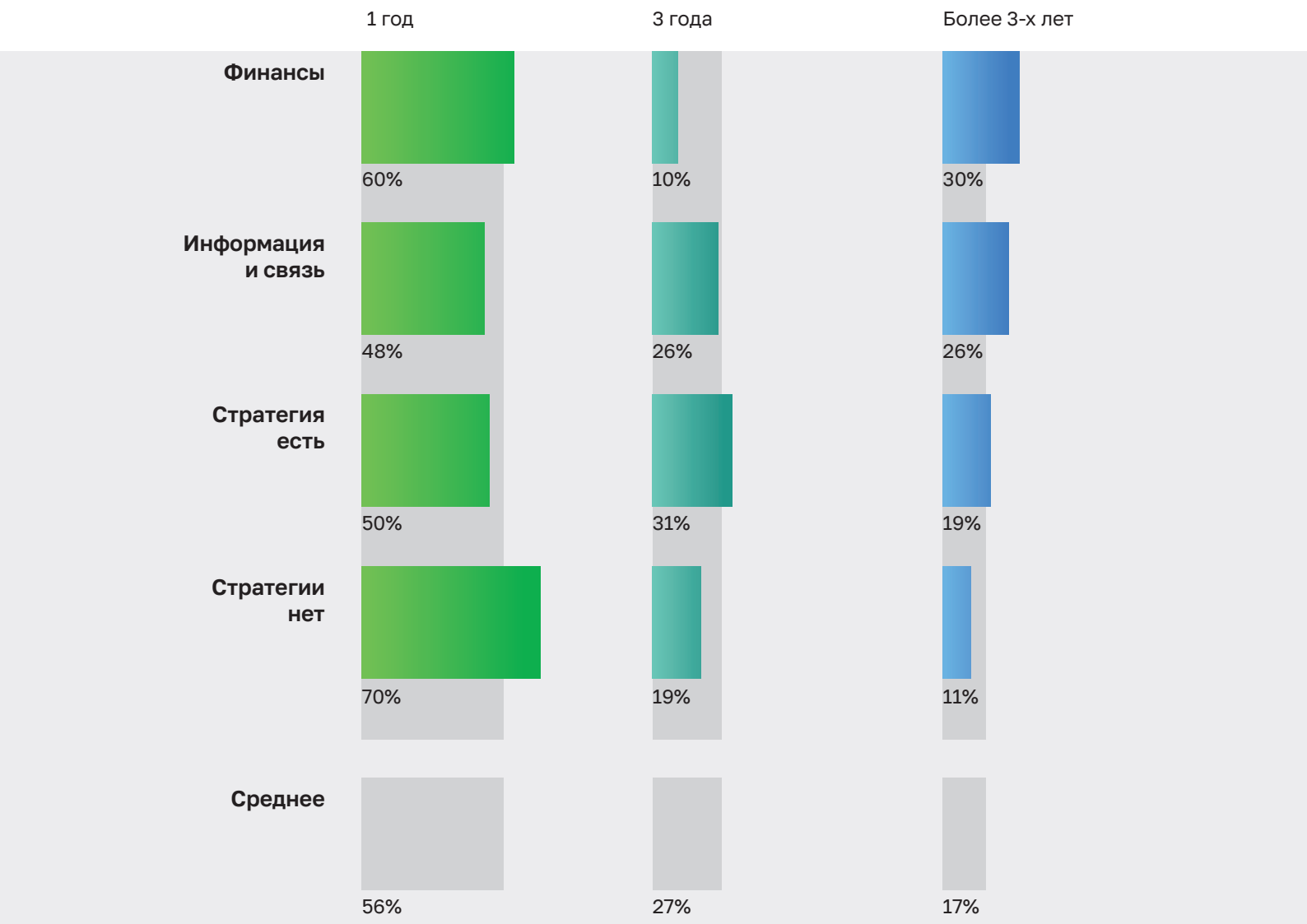
События 2020 года показали, что сложно планировать долгосрочные расходы на ИТ-проекты. Изменение внешней ситуации и конъюнктуры рынка заставило компании перейти к краткосрочному планированию.

56% респондентов отметили, что горизонт планирования ИБ-стратегии составляет год. В 2019 году таковых было 36%, а в 2018-м – 53%. Планированием на 3 года занимаются 27% опрошенных.



В 2019 году таковых было 34%, а в 2018-м – 32%. Долгосрочным планированием занимаются только 17% участников опроса. В 2019 году ИБ-стратегию на срок более 3 лет планировали 30%, а в 2018-м – 15%.

Интересно, что предприятия финансового сектора чаще всего планируют ИБ-стратегию на год или более чем на 3 года. В отрасли информации и связи чаще остальных занимаются долгосрочным планированием.



КОД безопасности

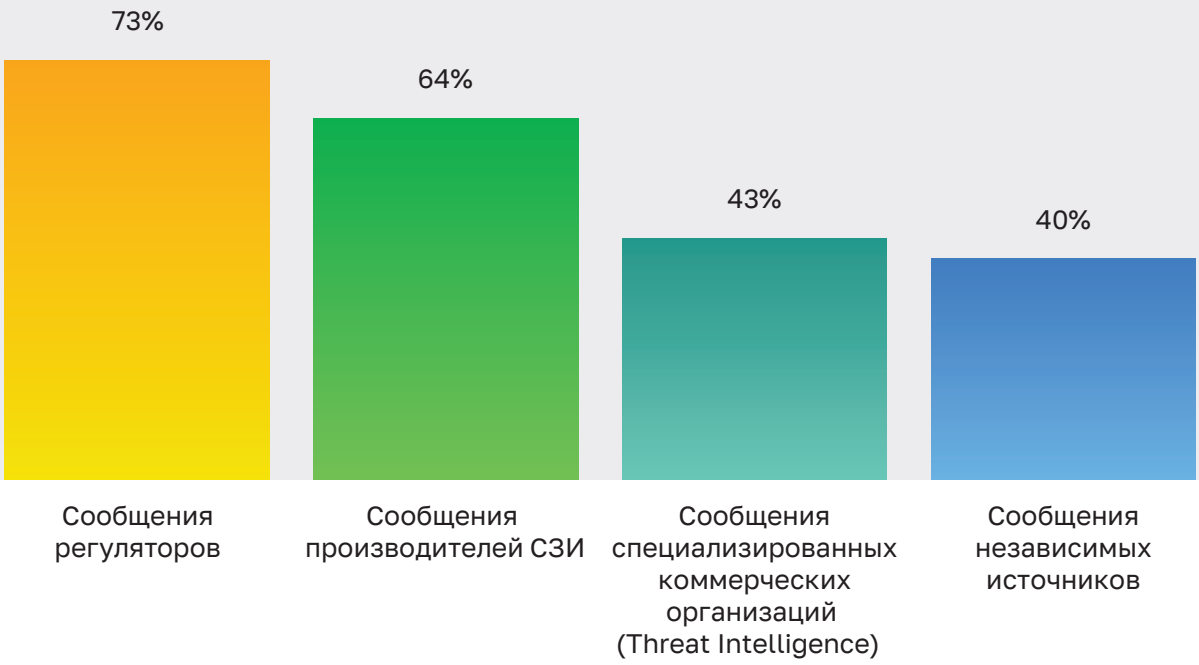
Источники информации о рисках и угрозах

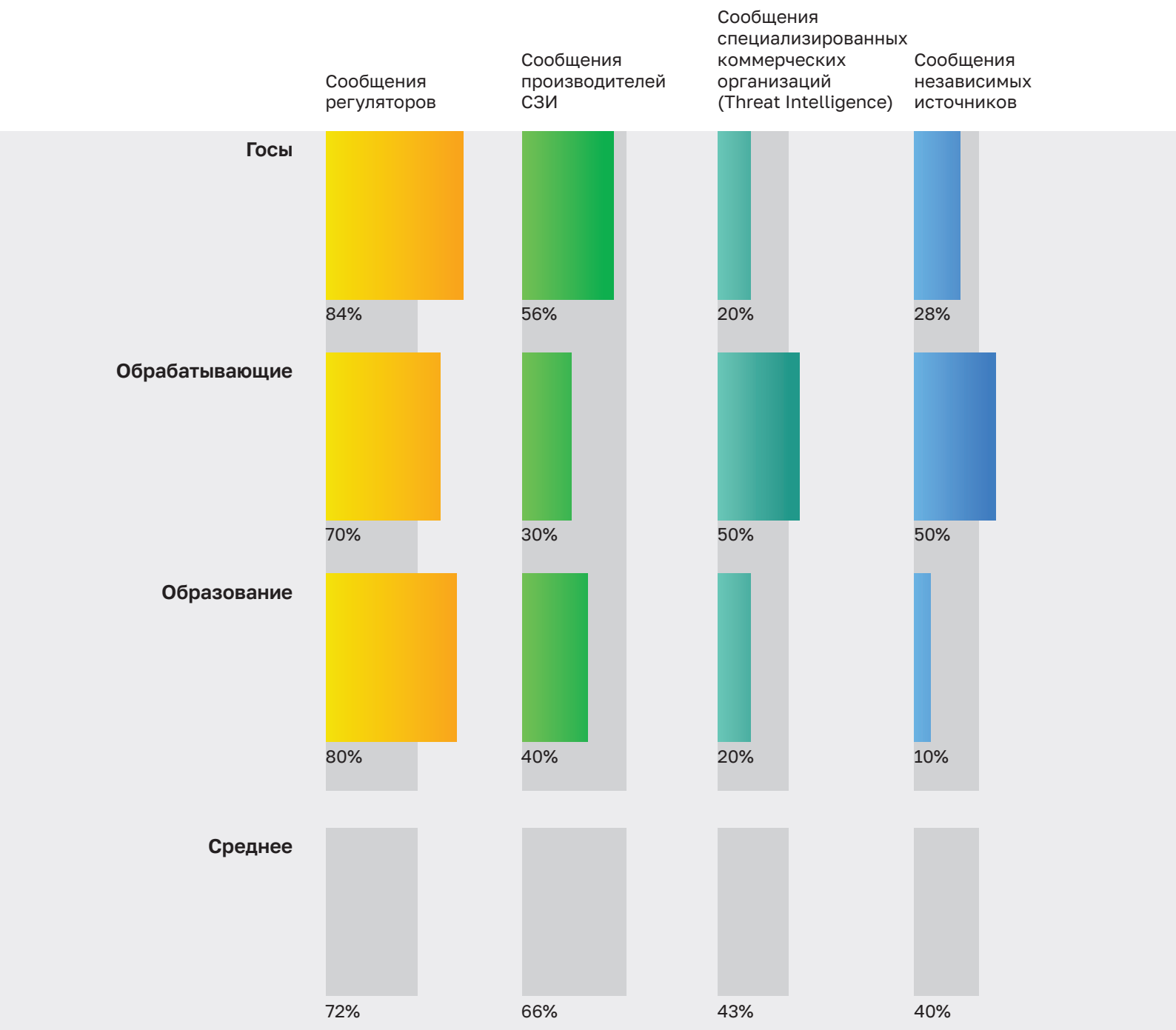
Для формирования ИБ-стратегии компаниям приходится анализировать множество источников информации о рисках и ИБ-угрозах. Однако некоторые источники заслуживают большего доверия, чем другие.

73% респондентов отметили, что доверяют сообщениям официальных регуляторов. В 2018-м и 2019 годах регуляторам доверяли 80% опрошенных. На втором месте по степени доверия оказались производители средств защиты информации, которым доверяют 64%. В 2019 году разработчикам СЗИ доверяли 73%, а в 2018-м – 71%. Замыкают тройку лидеров по доверию специализированные коммерческие организации – им доверяют 43% респондентов. В 2019 году Threat Intelligence доверяли 37%, а в 2018-м – 39%.

В качестве еще одного источника информации об ИТ-угрозах используются независимые источники. В 2021 году им доверяли около 40% опрошенных, в 2019-м – 36%, в 2018-м – 30%. Низкий уровень доверия связан с необходимостью иметь высокую компетенцию у специалиста, работающего с данными от источников информации. Однако на российском рынке до сих пор отмечается нехватка ИБ-специалистов с необходимыми полными знаниями и умениями.

Госсектор наименее доверяет сообщениям специализированных коммерческих организаций, тогда как финансовая отрасль, наоборот, больше смотрит в сторону Threat Intelligence. Интересно, что обрабатывающая промышленность меньше всего реагирует на сообщения производителей средств защиты информации, а образование – на сообщения независимых источников.




Сообщения регуляторов
Сообщения производителей СЗИ
Сообщения специализированных коммерческих организаций (Threat Intelligence)
Сообщения независимых источников
Госы
84%
56%
20%
28%
Обрабатывающие
70%
30%
50%
50%
Образование
80%
40%
20%
10%
Среднее
72%
66%
43%
40%

КОД безопасности

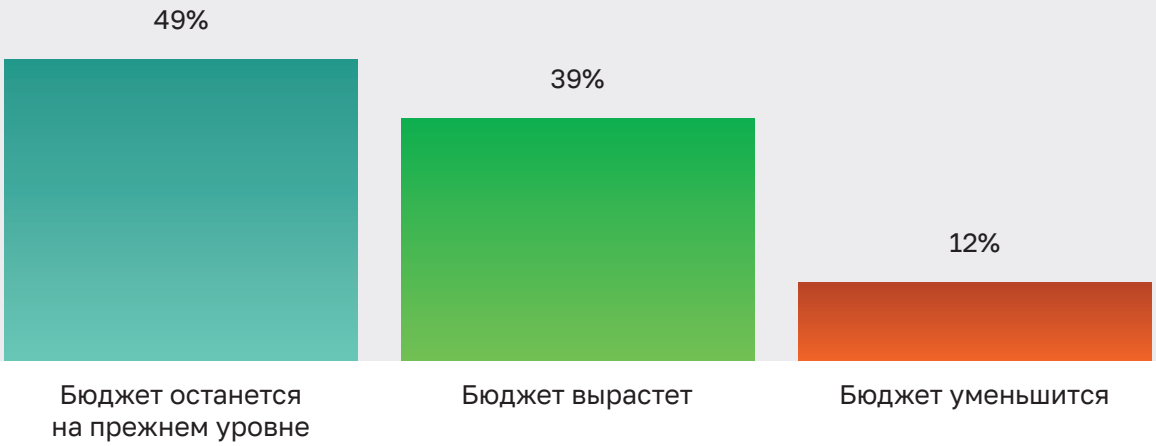
Изменение бюджета на ИБ в 2022 году

Последовавший после пандемии и серии локдаунов экономический кризис до сих пор негативно сказывается на формировании бюджетов на информационную безопасность. 12% респондентов заявили об уменьшении бюджета, в 2019 году таковых было только 11%.

Практически каждый второй респондент заявил о сохранении уровня бюджета на ИБ. В 2019 году таковых было 54%.

Увеличение затрат на ИБ планируют 39% респондентов, а в 2019 году их доля составляла 35%.

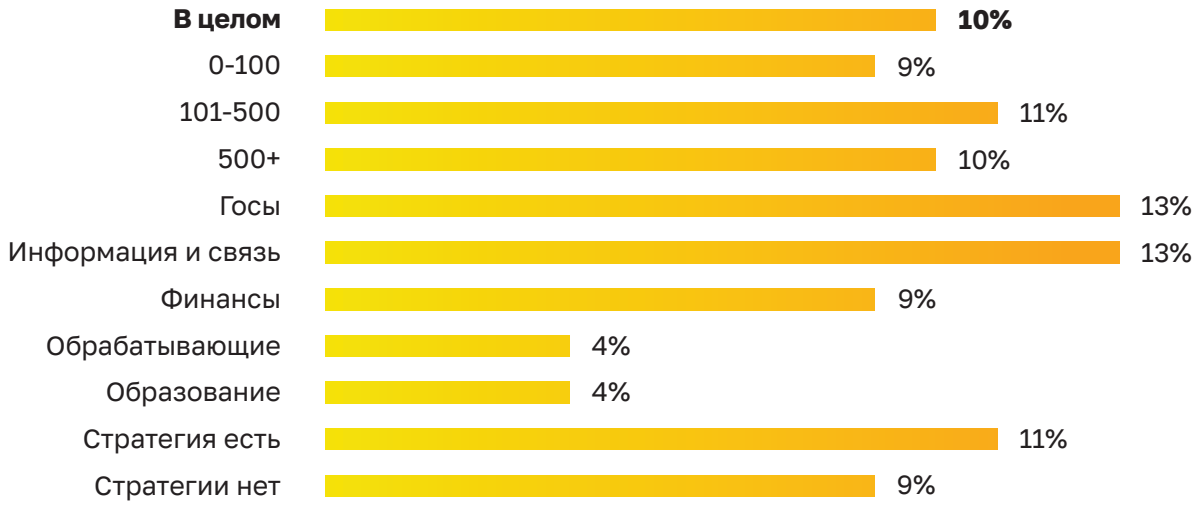
Увеличить ИБ-бюджет планируют в отраслях финансов, информации и связи. А вот уменьшение бюджета чаще всего ждет представителей обрабатывающей промышленности и госсектора.

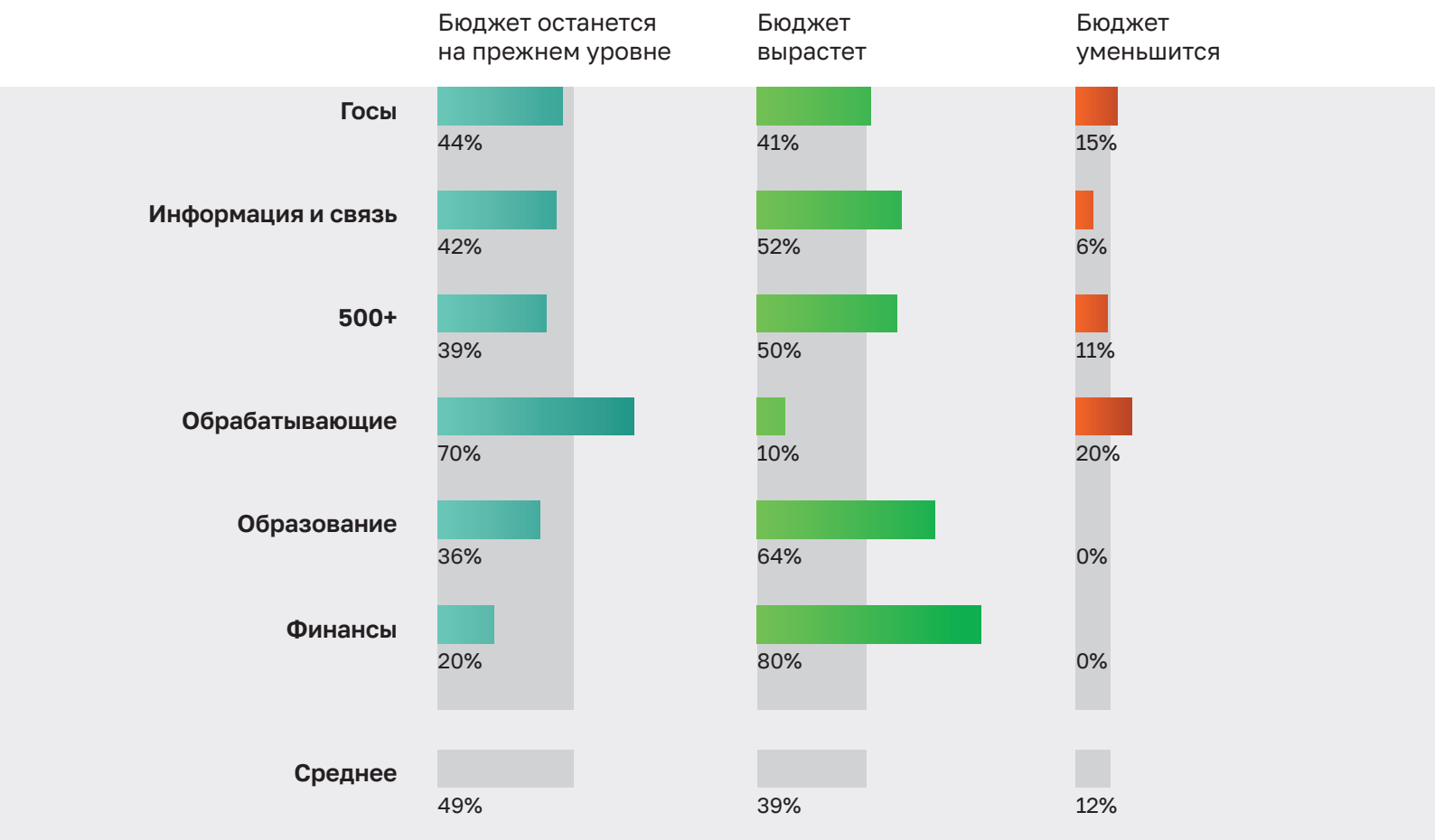


ИБ как доля бюджета ИТ

Большинство респондентов планируют заложить 10% доли ИТ-бюджета на информационную безопасность. По 4% от общего ИТ-бюджета потратят на ИБ предприятия обрабатывающей промышленности и образования.

Наибольшую долю в 13% показали предприятия государственного сектора и отрасли информации и связи.


В целом **10%**
0-100 9%
101-500 11%
500+ 10%
Госы 13%
Информация и связь 13%
Финансы 9%
Обрабатывающие 4%
Образование 4%
Стратегия есть 11%
Стратегии нет 9%


Бюджет останется на прежнем уровне
Бюджет вырастет
Бюджет уменьшится
Госы 44% 41% 15%
Информация и связь 42% 52% 6%
500+ 39% 50% 11%
Обрабатывающие 70% 10% 20%
Образование 36% 64% 0%
Финансы 20% 80% 0%
Среднее 49% 39% 12%

КОД безопасности

Ключевые факторы формирования ИБ-бюджета

Наиболее значимыми факторами, которые влияли на формирование бюджета на информационную безопасность, стали защита персональных данных (54%), критической информационной структуры (45%) и государственных информационных систем (40%).
В исследовании 2019-го и 2018 годов ключевые факторы были аналогичными.

В числе ключевых факторов также отмечались проблемы конфиденциальности данных (38%), предписание к устранению нарушений требований регуляторов (35%), требования сотрудников, отвечающих за безопасность (32%).

Наименее приоритетными факторами стали положение Банка России ГОСТ 57580.1-2017 (5%) и переход на облачные технологии для оптимизации затрат (6%).

Интересно, что уже произошедший инцидент безопасности способствовал выделению денег на информационную безопасность у 20% респондентов.
А внешние потери или мошенничество – у 17%. Преднамеренные действия инсайдера заставили 18% опрошенных увеличить бюджет на ИБ, а случайный инсайд повлиял на бюджет у 32% респондентов.

Факторы ограничения выделения денег на ИБ-бюджет

Сформировать или увеличить бюджет на информационную безопасность чаще всего мешает ограниченность общего ИТ-бюджета. Этот фактор в 2021 году отметили 39% респондентов, в 2019-м – 4%, в 2018-м – 2%. Значительный рост объясняется тяжелым экономическим положением ряда компаний после пандемии COVID-19, а также вынужденным локдауном.

Недостаточный уровень информированности высшего руководства в вопросах информационной безопасности в этом году отметили 22% респондентов. Доля аналогичного ответа в 2019-м и 2018 годах составила 34% и 35% соответственно.

Ограничивают выделение бюджета на ИБ слишком технические показатели, которые затрудняют понимание руководством значимости вопроса, – это отметили 11% респондентов. В 2019 году аналогично считали 30%, а в 2018-м – 32%.

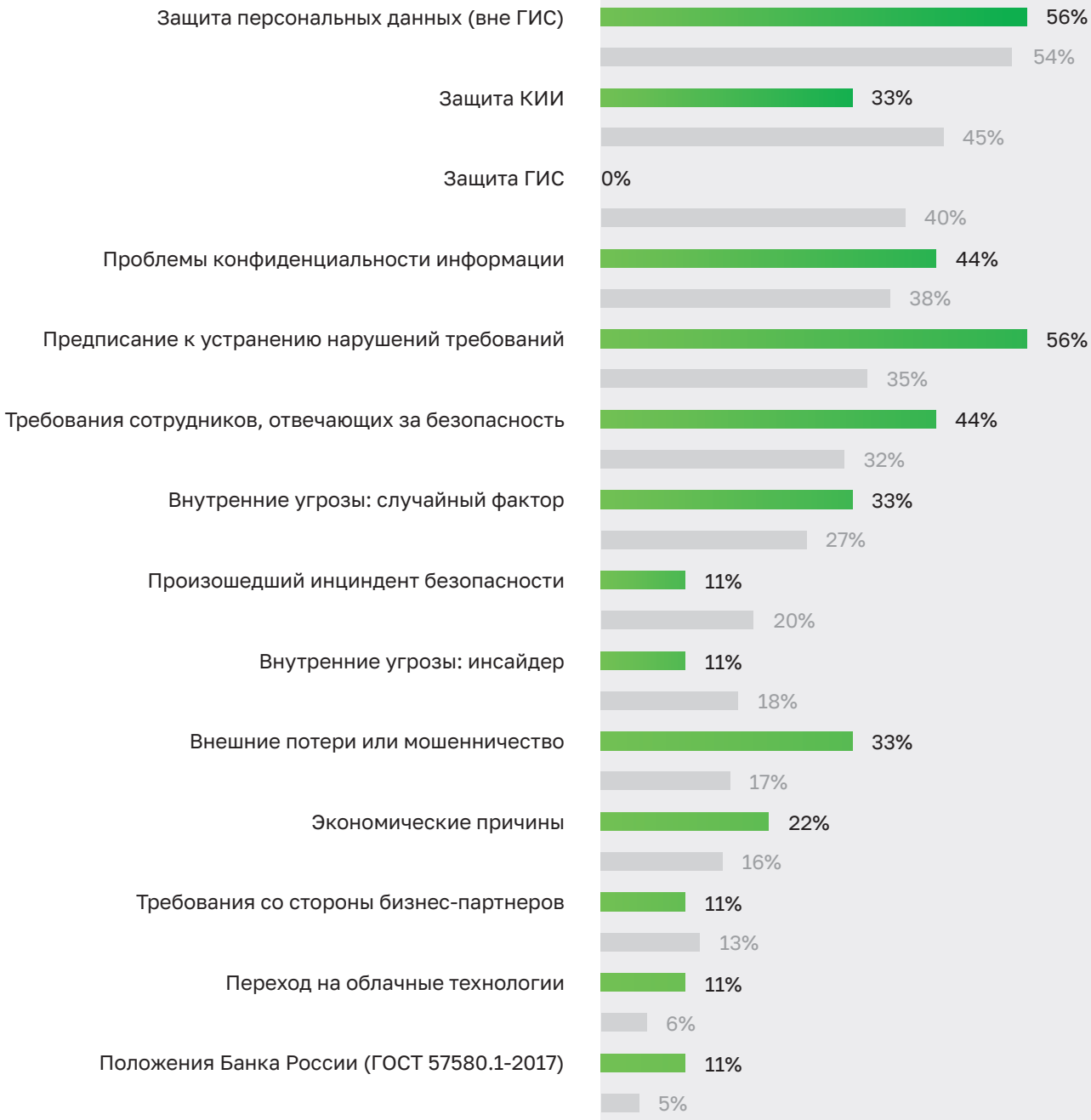
Интересно, что руководители 19% респондентов считают, что потери в результате ИБ-инцидентов будут меньшими, чем затраты на развитие системы информационной безопасности. В 2019 году доля подобных ответов составил 29%, в 2018 году – 28%.

Финансовая отрасль, а также отрасль информации и связи чаще всего указывали, что возможные потери от ИБ-инцидентов будут меньше затрат на формирование и поддержание решений по информационной безопасности.

КОД безопасности

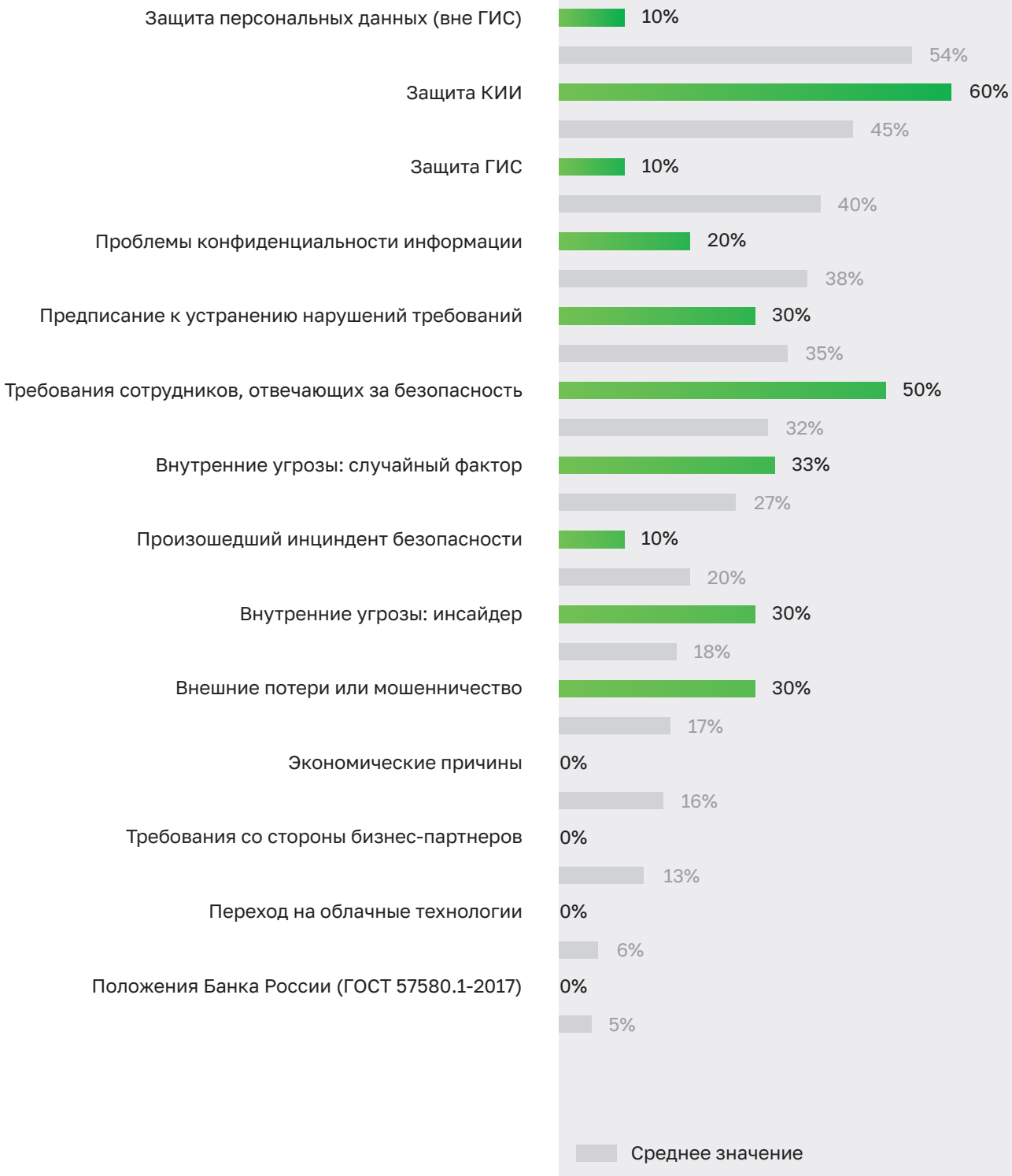
Госы

Финансы


Защита персональных данных (вне ГИС)
56%
54%
Защита КИИ
33%
45%
Защита ГИС
0%
40%
Проблемы конфиденциальности информации
44%
38%
Предписание к устранению нарушений требований
56%
35%
Требования сотрудников, отвечающих за безопасность
44%
32%
Внутренние угрозы: случайный фактор
33%
27%
Произошедший инцидент безопасности
11%
20%
Внутренние угрозы: инсайдер
11%
18%
Внешние потери или мошенничество
33%
17%
Экономические причины
22%
16%
Требования со стороны бизнес-партнеров
11%
13%
Переход на облачные технологии
11%
6%
Положения Банка России (ГОСТ 57580.1-2017)
11%
5%
Среднее значение

КОД безопасности

Обрабатывающая



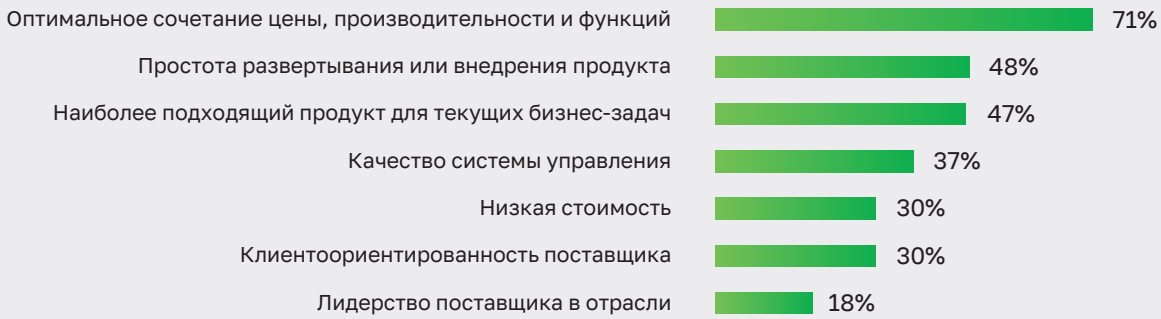

Госы
Финансы
Недостаточный уровень информированности высшего руководства в вопросах информационной безопасности
27%
22%
22%
22%
Показатели безопасности являются слишком техническими, это затрудняет понимание значимости вопроса
8%
11%
11%
11%
Возможные потери в результате ИБ-рисков руководство считает меньшими по сравнению с затратами на развитие системы ИБ
15%
22%
19%
19%
Ограниченный бюджет
50%
33%
39%
39%
Нет препятствий
0%
11%
9%
9%
Среднее значение

КОД безопасности

Критерии выбора поставщика

Рынок средств защиты информации в России можно считать развитым и конкурентным. У заказчиков достаточный выбор производителей СЗИ, который позволяет удовлетворить потребности в обеспечении информационной безопасности.

Для отечественного рынка основным критерием выбора поставщика несколько лет подряд остается оптимальное сочетание цены, производительности и функций (71%). В тройке наиболее упоминаемых критериев оказались простота развертывания или внедрения продукта (48%) и наиболее подходящий продукт для текущих задач (47%).



Низкая цена была критерием выбора поставщика у 30% респондентов. В 2019 году на цену ориентировались также 30%, а в 2018-м — 25%.

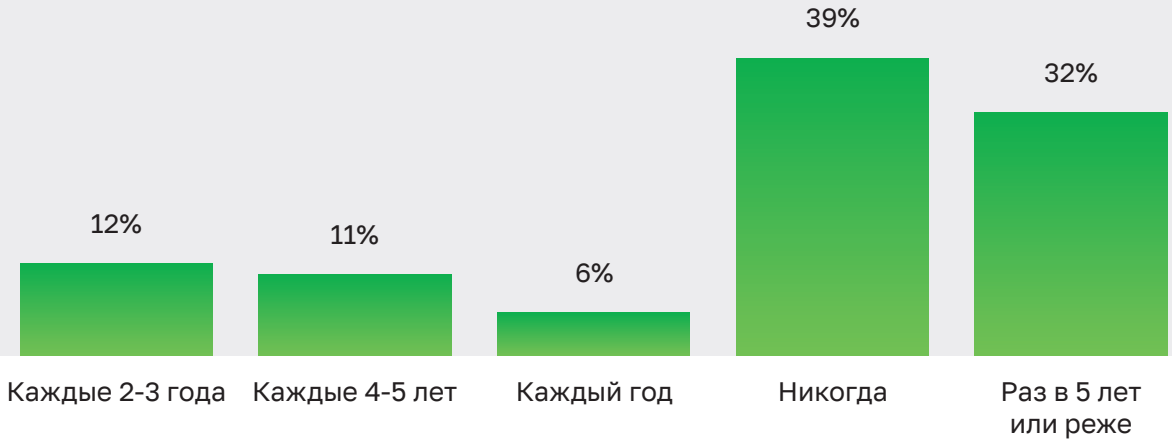
Интересно, что наименее приоритетным фактором выбора поставщика оказалось лидерство в отрасли. Его отметили только 18% респондентов.

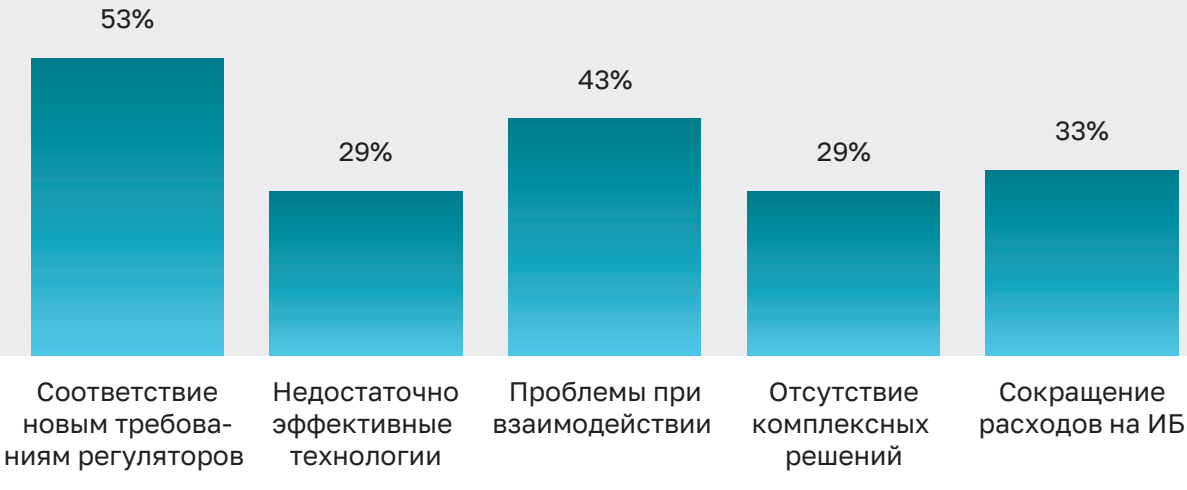
Смена поставщика ИБ-решений

На российском рынке поставщика ИБ-решений предпочитают выбирать на длительный срок. Никогда не меняли поставщика 39% респондентов, а раз в 5 лет и реже – 32%.

Наиболее частой причиной смены поставщика является несоответствие новым требованиям регуляторов. Ее указали 54% респондентов, в 2019 году – 58%, в 2018-м – 63%. Также часто поставщика меняют из-за проблем при взаимодействии – 43%.

В этом году 33% опрошенных указали причиной смены поставщика сокращение расходов на ИБ. В 2019 году такую причину выбрали 36% опрошенных, в 2018-м – 35%.





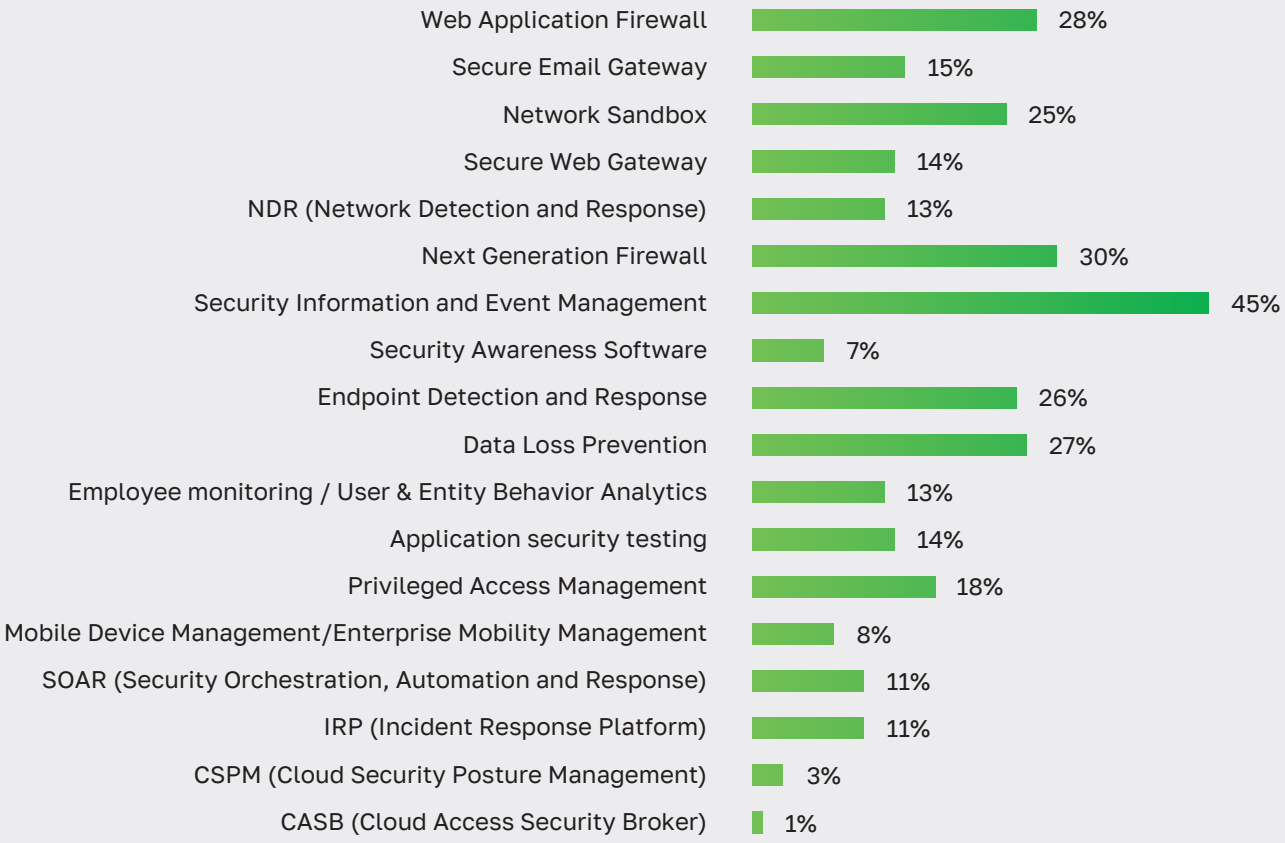
КОД безопасности

Внедрение технологий ИБ в ближайшие 3 года

В топ-6 технологий информационной безопасности, которые интересно внедрить российским организациям в ближайшие 3 года, вошли Security Information and Event Management (45%), Next Generation Firewall (30%), Web Application Firewall (28%), Data Lost Prevention (27%), Endpoint Detection and Response (26%) и Network Sandbox (25%). Интересно, что топ практически полностью совпадает с исследованием 2019 года.

Security Information and Event Management – централизованный механизм сбора и обработки событий безопасности для корпоративной сети. В него сливается информация от всех средств защиты и остальной ИТ-инфраструктуры, что позволяет вовремя заметить ИБ-инциденты.

Next Generation Firewall – межсетевой экран следующего поколения, занимающийся глубоким анализом трафика. Он умеет определять конкретные приложения и пользователей для классификации трафика. Внутри находится множество механизмов проверки трафика для защиты периметра от угроз снаружи.

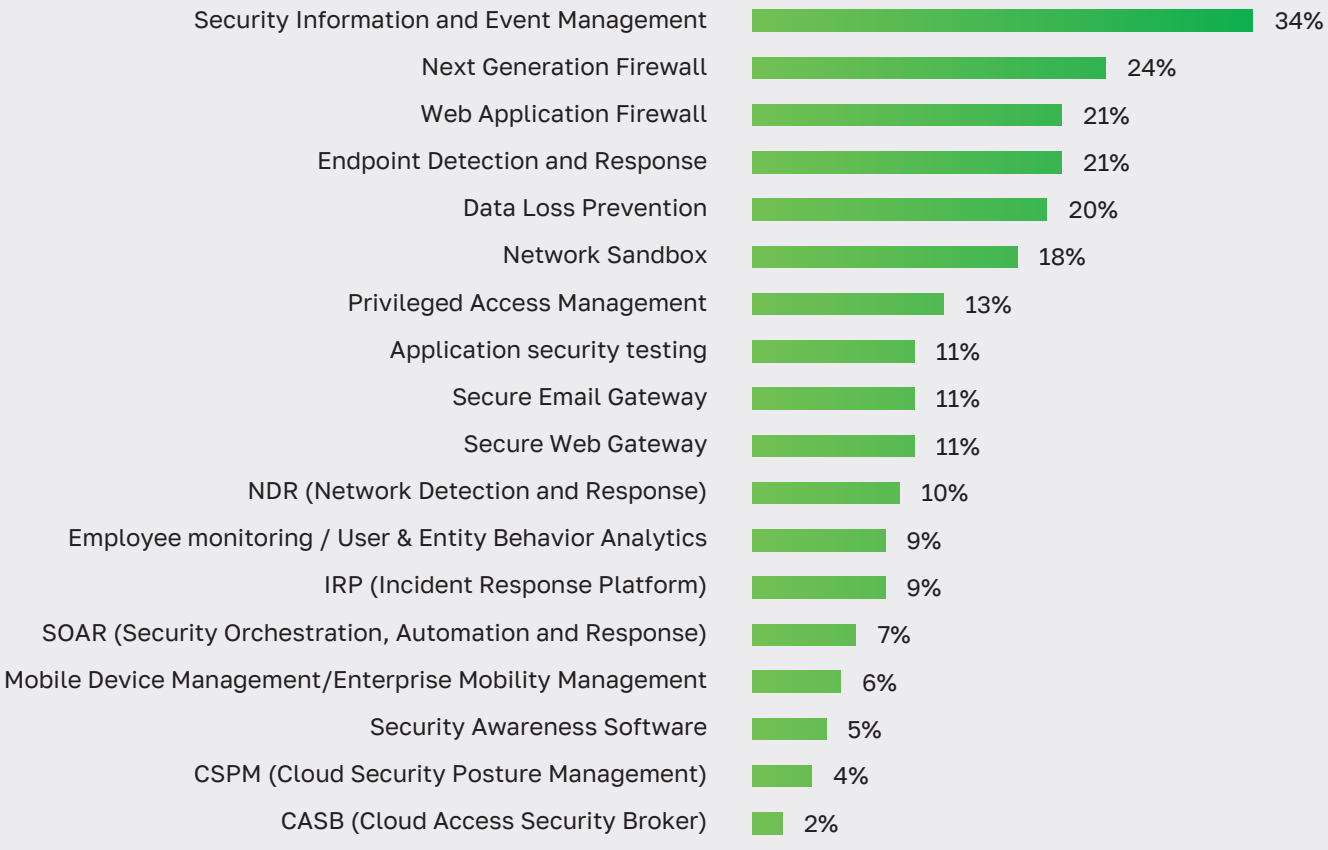


Web Application Firewall – специализированный файервол для веб-приложений. Веб-приложения из-за гибкости сложно написать безопасными. Это повышает риск того, что собранные с пользователей данные могут оказаться в руках злоумышленников. WAF устанавливается перед веб-приложением и анализирует трафик, выявляя попытки киберпреступников манипулировать с трафиком.

Data Lost Prevention – система защиты от утечек информации. Она анализирует контент файлов. Если он напоминает контент файла, ранее промаркированный как конфиденциальный, то DLP-система сообщит профильному сотруднику безопасности о попытке копировать конфиденциальную информацию или проактивно запретит передачу файла наружу.

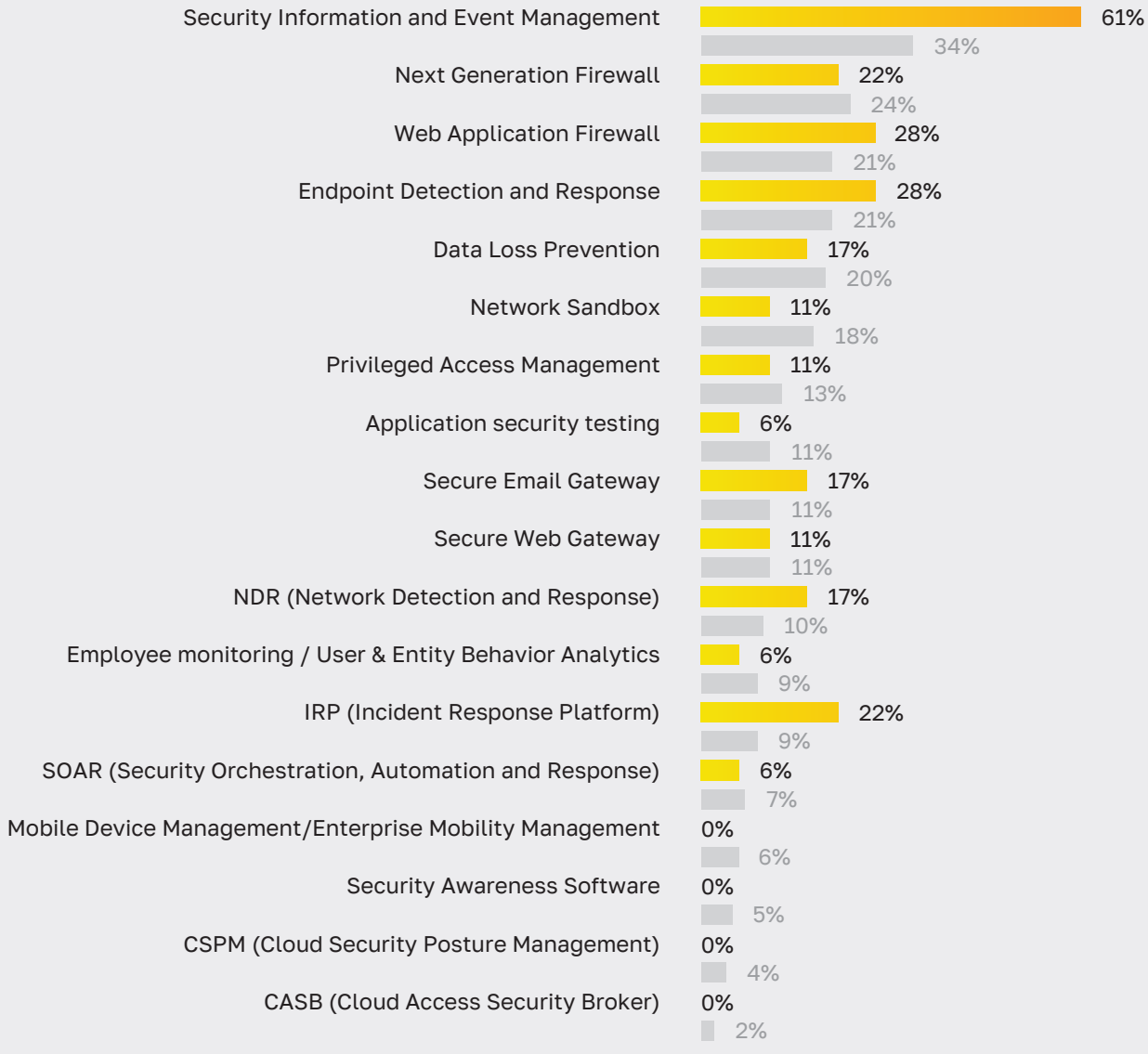
Endpoint Detection and Response – технология отслеживания аномальной активности на конечных точках. Например, система знает, что файлы с определенным хэшем являются вредоносными. Она сканирует сеть на их наличие. Если подобные файлы найдены, то их можно отправить в карантин, удалить или посмотреть, к каким ресурсам вредоносный код обращался. EDR помогает своевременно реагировать на ИБ-инциденты.

Network Sandbox – сетевая песочница, которая находится между файерволом и конечным пользователем. Когда пользователь из интернета загружает файл, то он сначала запускается в NS. Сетевая песочница анализирует его поведение. Если обнаруживаются характерные признаки вируса, то файл не передается пользователю. Идея в том, что сетевая песочница ловит вирусы, которые не описываются известными сигнатурами.



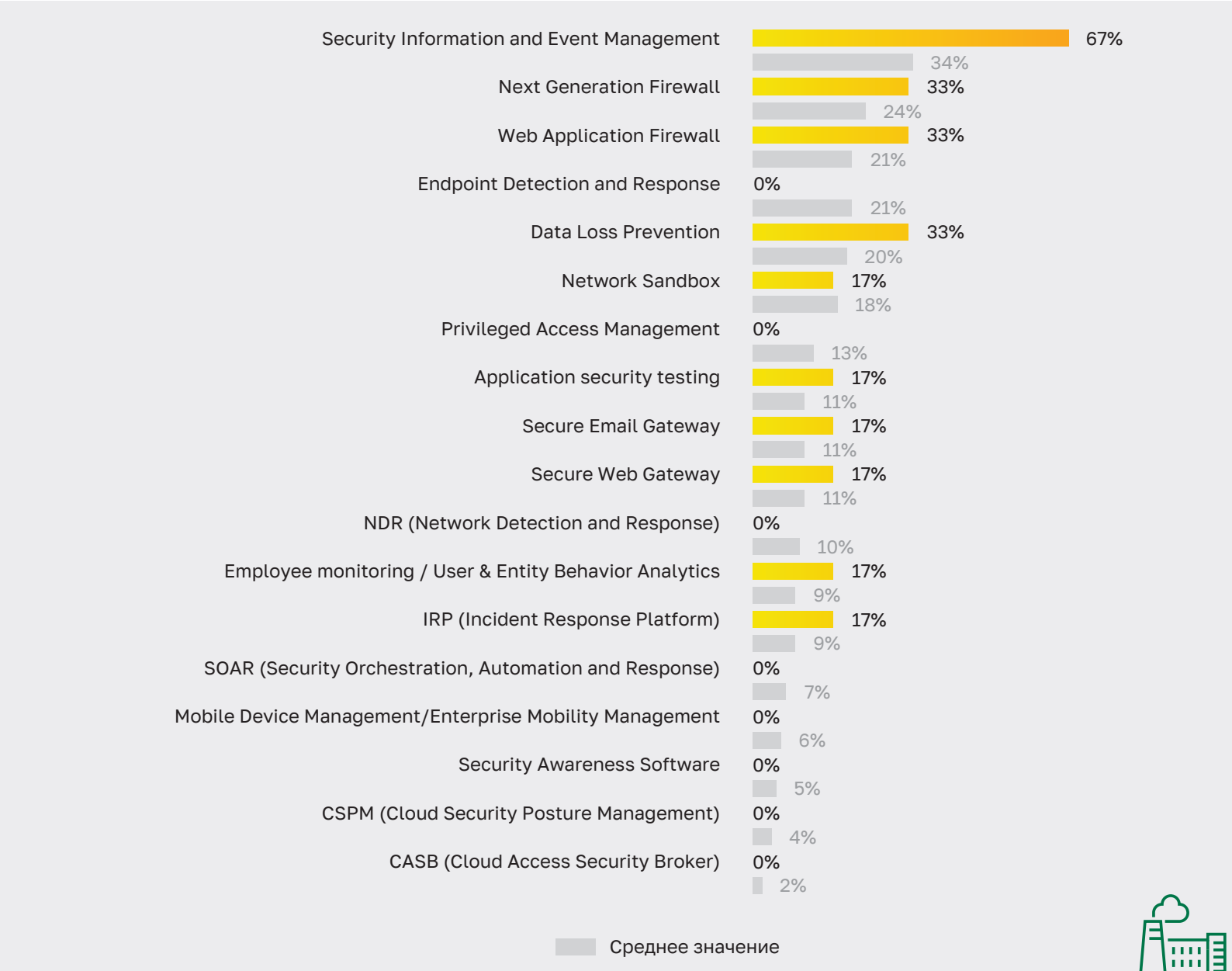
Госсектор в ближайшие 3 года будет делать упор на SIEM, WAF и Incident Response Platform. В отрасли информации и связи приоритет сетевой песочнице и WAF. В финансовой отрасли строят планы внедрения SIEM, WAF и NGF.

Госы



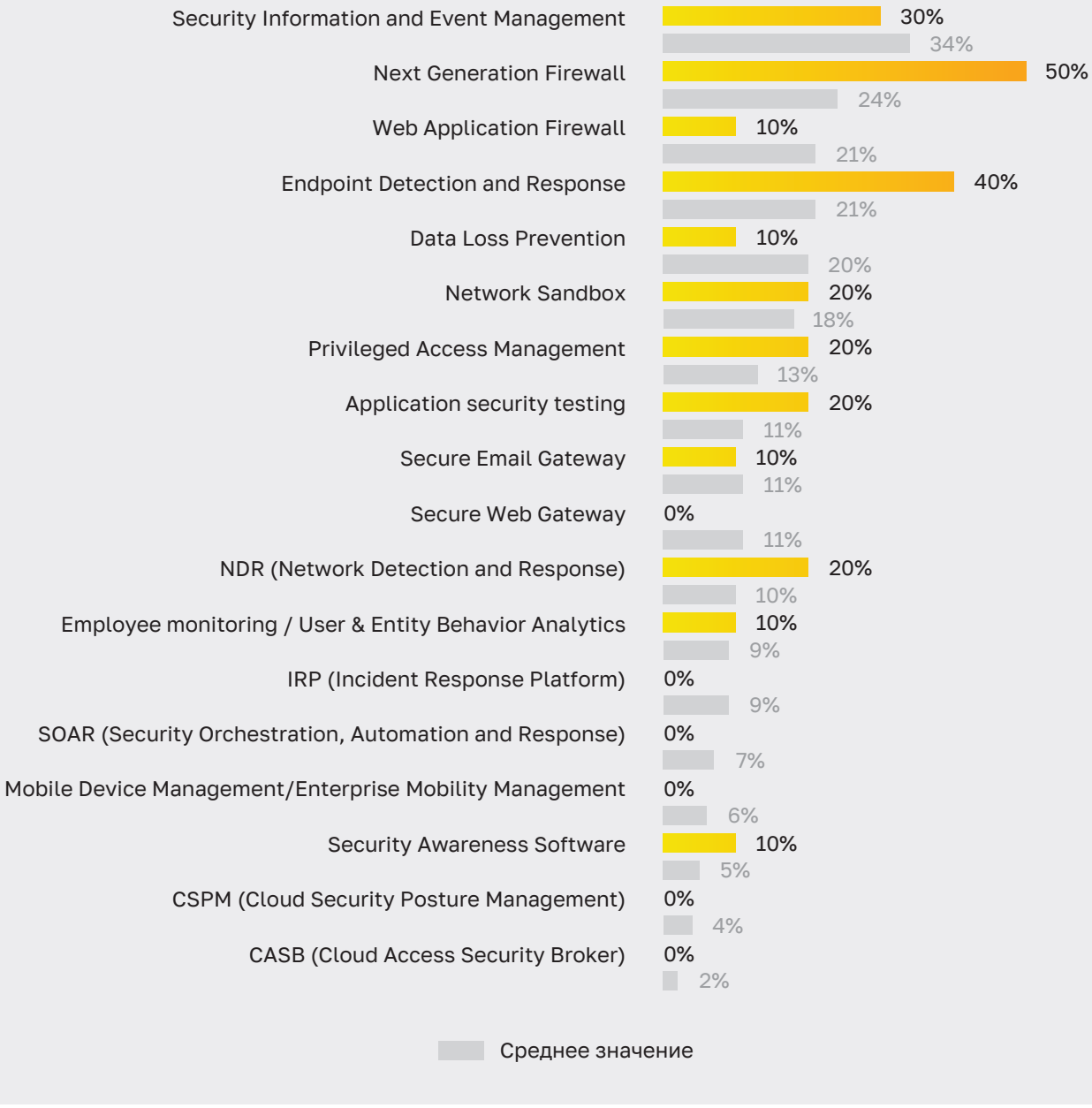
Представители финансового сектора чаще всего планируют внедрять SIEM, на втором месте идут межсетевые экраны, обычный и уровня приложений – Next Generation Firewall, Web application firewall, а также системы защиты от утечек (DLP).

Финансы



Для предприятий обрабатывающей промышленности наиболее перспективной технологией является Next Generation Firewall, на втором месте – обнаружение и реагирование на инциденты (EDR), на третьем – SIEM.

Обрабатывающая



Резюме

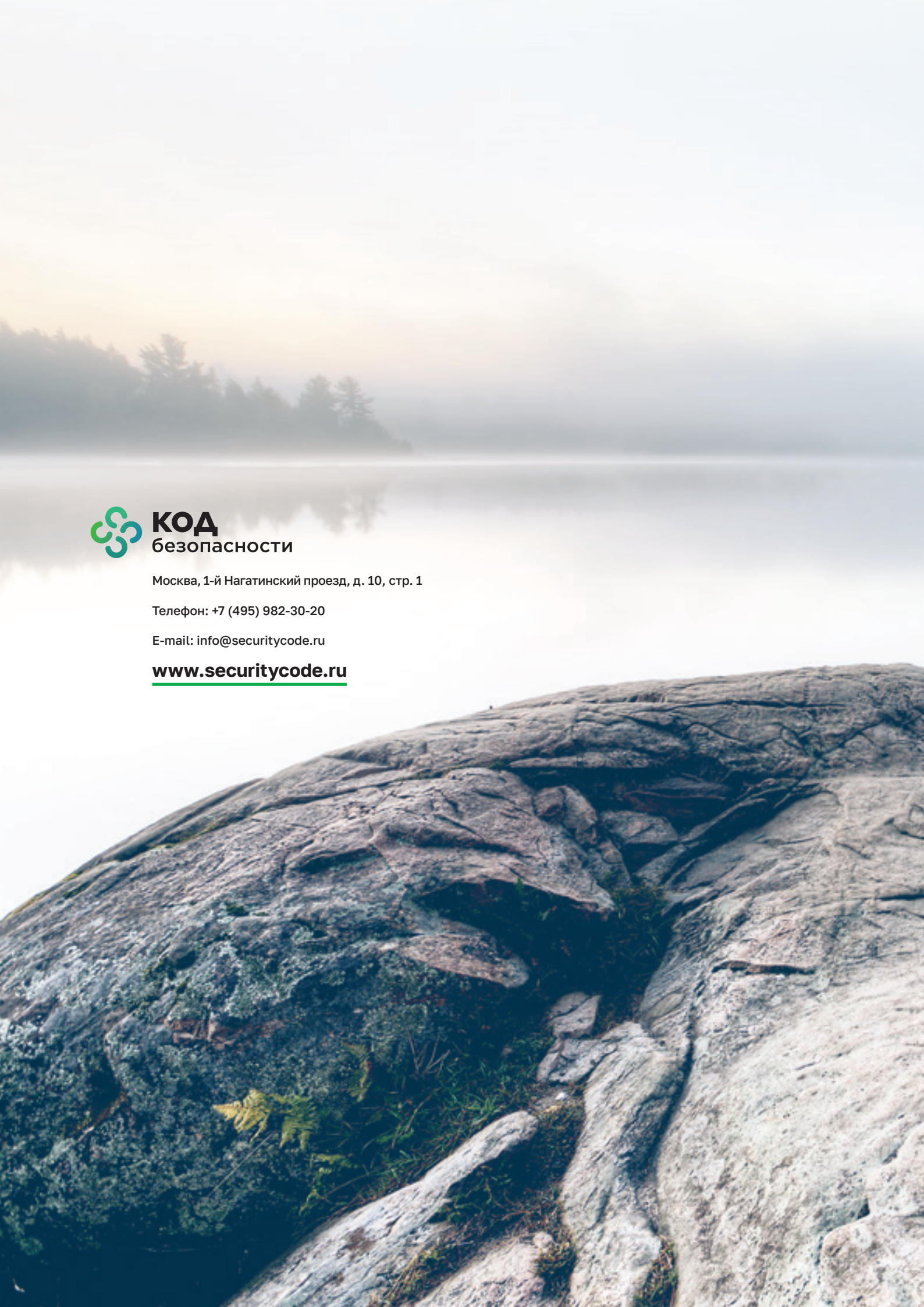
Большинство российских предприятий понимают необходимость обеспечения информационной безопасности. Только каждое десятое предприятие до сих пор не определило специалистов или отдел, которые отвечают за ИБ. Остальные предпочитают заниматься кибербезопасностью еще до первых инцидентов.

Несмотря на тяжелую экономическую ситуацию после пандемии коронавирусной инфекции, растет количество предприятий, которые будут увеличивать бюджет на ИБ. По сравнению с 2019 годом их доля выросла на 4 процентных пункта. Предприятия правильно оценивают риски возможных потерь от ИБ-инцидентов и стараются застраховаться от них. В среднем до 10% от всего бюджета на ИТ выделяется на информационную безопасность.

При этом все чаще препятствием на выделение денег для внедрения ИБ-решений становится ограниченный бюджет. Этот пункт опроса показал десятикратный рост по сравнению с 2019-м и двадцатикратный рост по сравнению с 2018 годом.

Чаще всего причиной роста ИБ-бюджета становятся требования регуляторов. Это показывает, что именно государство в первую очередь заинтересовано в защите конфиденциальной информации.

Наиболее перспективными для внедрения ИБ направлениями стали технологии обеспечения сетевой безопасности, а также обнаружение и реагирование на ИБ-инциденты.



КОД
безопасности

Москва, 1-й Нагатинский проезд, д. 10, стр. 1

Телефон: +7 (495) 982-30-20

E-mail: info@securitycode.ru

www.securitycode.ru