РОСКОНГРЕСС
Пространство доверия

ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Логика принятия решений и роль руководителей служб ИБ **в формировании бюджета**

ИИМР
Институт Изучения Мировых Рынков

ДЕКАБРЬ
2025

Глобальный рынок решений и услуг в сфере кибербезопасности устойчиво растет. По оценкам тройки крупнейших консалтинговых компаний, его объем к 2030 году может достигнуть 350-500 млрд долларов при среднегодовых темпах роста 9-14%. На этом фоне российский рынок кибербезопасности занимает особое положение и растет вдвое быстрее.

За первое полугодие 2025 года, по данным Татьяны Матвеевой, начальника Управления Президента РФ по развитию информационно-коммуникационных технологий и инфраструктуры связи, озвученным в ходе XIX международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» было зафиксировано более 63 тыс. кибератак, при этом две трети из них нацелены на критическую информационную инфраструктуру. По данным Банка России, в 2024 году зафиксировано более 750 кибератак на финансовые компании, причем в первом полугодии 2025 года их число выросло еще на 13%. В таких условиях важно понимать, как **главы служб информационной безопасности (ИБ) оценивают свою роль в обеспечении защищенности компаний** и чем их видение **отличается от взгляда топ-менеджеров** — исполнительных и финансовых директоров.

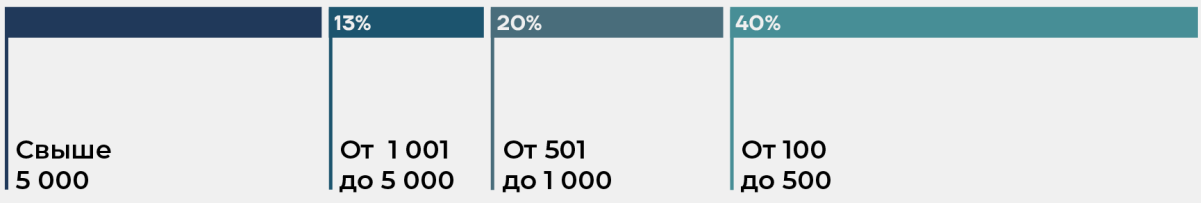
СОСТАВ РЕСПОНДЕНТОВ

10%
Заместители руководителей служб ИБ

56%
Руководители служб ИБ и занимающие аналогичную должность

33%
Руководители служб ИТ с ответственностью за ИБ

РАСПРЕДЕЛЕНИЕ ПО РАЗМЕРУ КОМПАНИЙ



В основе настоящего исследования лежат результаты веб-опроса руководителей служб информационной безопасности российских компаний, проведенного во второй половине 2025 года.

Главной особенностью исследования, в котором приняли участие представители 107 компаний, является **сопоставление результатов опроса руководителей служб ИБ (CISO) с информацией, полученной из серии глубинных интервью с топ-менеджерами**, которая была проведена в первой половине 2025 года. Первая часть исследования была представлена в июне 2025 года на ПМЭФ и опубликована на сайте **Института изучения мировых рынков**.

КЛЮЧЕВЫЕ НАБЛЮДЕНИЯ

- Директора по информационной безопасности **чаще топ-менеджеров видят связь между инвестициями в защиту и стоимостью бизнеса** — 60% против 38%. Разрыв в 22 п.п. говорит, что **ИБ-руководитель не умеет объяснить ценность защиты топ-менеджменту**.

- Компании, активно использующие **пентесты и Red Team упражнения, оценивают стоимость взлома в 1,5 раза выше среднего**. Исследование «Недопустимое событие 2025. Цифровой краш-тест российского бизнеса» на базе данных «Кибериспытание экспресс» показало, что бюджета в 1 млн рублей достаточно для реализации недопустимого события у 3 из 5 компаний. **Специалисты переоценивают техническую сложность защиты**, не учитывая реальную экономику киберпреступности. Зрелость подходов кибербезопасности дает противоположный результат — **компании с утвержденными списками критичных активов дают на 26% более низкие оценки** стоимости успешного нападения. Более глубокое понимание рисков приводит к более трезвым оценкам.

- Службы безопасности **обосновывают бюджеты результатами аудитов и требованиями регуляторов**. А вот результаты пентестов остаются в тени. Хотя **ИБ-директора оценивают объективность пентестов на четыре балла из пяти, а регуляторные требования — меньше трех баллов**.

- **Самые довольные своей работой — те директора по безопасности, которых никогда не привлекают к стратегическим решениям**. 75% из них удовлетворены своей позицией. Они не ожидают участия в управлении компанией и не пытаются его добиться.

- **Каждый второй директор по безопасности готов смириться с зависимостью от одного поставщика ради удобства**. Они видят операционные выгоды. **88% топ-менеджеров считают такую зависимость критической проблемой**. Для них это стратегический риск потери контроля.

- Больше всего готовы отдать функции безопасности на аутсорсинг те компании, у которых нет списка критичных активов (63%). **Отсутствие понимания собственных рисков толкает к аутсорсингу**.

- **67% респондентов называют социальную инженерию серьезной или критической угрозой.** Но регулярное обучение сотрудников проводят только 27% компаний. ИБ-руководители признают проблему, но не вкладываются в ее решение.

- **Отсутствие методик оценки эффективности защиты — последняя по приоритету проблема в глазах ИБ-руководителей**. Это мешает директорам по безопасности выстроить диалог с топ-менеджментом на языке экономических результатов.

- Директора по безопасности считают главными препятствиями технические проблемы: стоимость решений, дефицит кадров, качество продуктов. А топ-менеджеры видят барьеры в другом: слабая интеграция в бизнес, непонимание целей. **Разные ценности формируют разные приоритеты**.

- **Директора по информационной безопасности** хорошо понимают угрозы, но **не говорят на языке бизнеса**. Они завышают оценки стоимости взлома, недооценивают стратегические риски вроде зависимости от вендоров и остаются в стороне от принятия ключевых решений в компаниях.

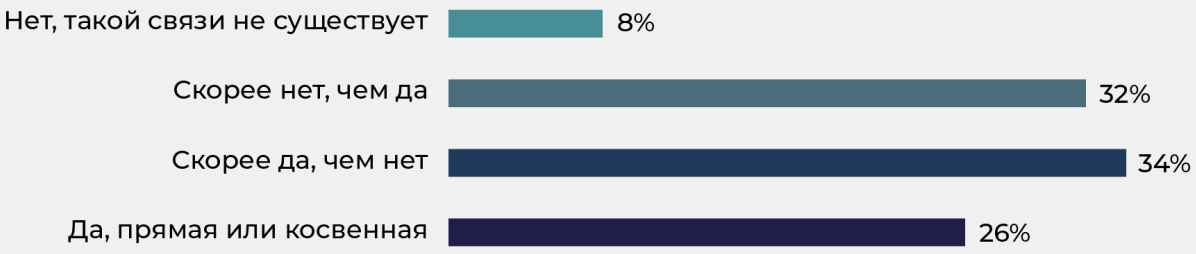
ЭКОНОМИЧЕСКАЯ ЦЕННОСТЬ ИБ

Исследование выявило разницу в понимании экономической ценности кибербезопасности. Директора по ИБ значительно чаще видят связь между инвестициями в информационную безопасность и стоимостью бизнеса компании по сравнению с топ-менеджерами.

Данные опроса показали, что 60% ИБ-руководителей отмечают прямую или косвенную связь инвестиций в кибербезопасность со стоимостью компании. Интервью с топ-менеджерами показало иную картину: только 38% руководителей компаний видят связь между инвестициями в кибербезопасность и стоимостью бизнеса.

Разрыв в 22 процентных пункта указывает на проблему коммуникации между службами ИБ и руководством компаний. Она обусловлена, с одной стороны, неспособностью ИБ-руководителей эффективно доносить это понимание вверх по организационной иерархии, а с другой — непониманием топ-менеджерами результатов работы службы информационной безопасности. Директора по ИБ осознают влияние защищенности на бизнес-результаты, но не могут убедить в этом руководство.

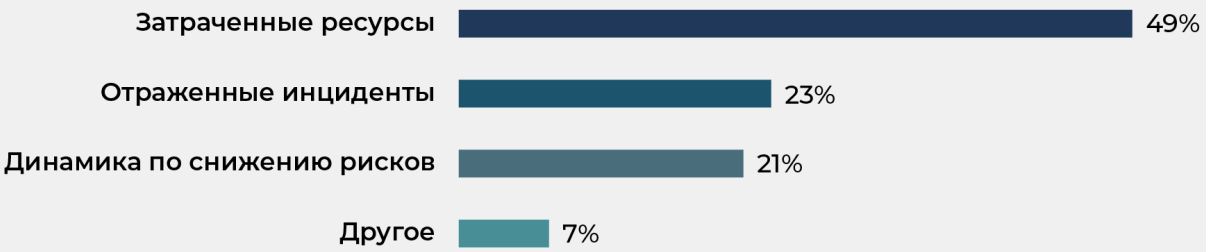
ВИДЯТ ЛИ СВЯЗЬ МЕЖДУ ИНВЕСТИЦИЯМИ В КИБЕРБЕЗОПАСНОСТЬ И СТОИМОСТЬЮ БИЗНЕСА РУКОВОДИТЕЛИ СЛУЖБ ИБ?



Топ-менеджеры воспринимают кибербезопасность преимущественно как статью затрат, а не как фактор создания ценности.

Этот тезис подтверждает распределение ответов на вопрос, какие метрики руководство компаний запрашивает у подразделений ИБ. **Структура запросов преимущественно ориентирована на учет ресурсов, а не на измерение эффективности защиты.** Почти половина компаний (49%) сталкивается с требованиями отчитываться о затраченных ресурсах. Количество отраженных инцидентов запрашивают 23% руководителей, динамику снижения рисков — 21%. Остальные 7% используют другие показатели, среди которых руководители ИБ выделяют соответствие регуляторным требованиям и выполнение планов защиты.

КАКИЕ ФИНАНСОВЫЕ И БИЗНЕС-МЕТРИКИ ЗАПРАШИВАЕТ У ВАС ТОП-МЕНЕДЖМЕНТ?



Доминирование запросов о затратах указывает на восприятие информационной безопасности преимущественно как статьи расходов, требующей контроля и оптимизации, а не как фактора создания ценности для бизнеса.

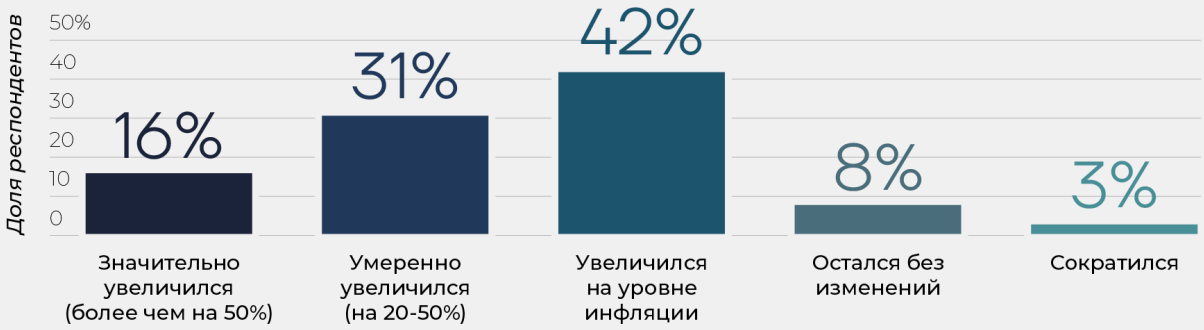
Руководство интересуется прежде всего тем, сколько компания тратит на защиту, а не тем, насколько эффективно эти средства используются для минимизации рисков или повышения устойчивости к киберугрозам.

Относительно низкая доля запросов о динамике снижения рисков (21%) свидетельствует о недостаточном внимании к результативным показателям работы служб ИБ. Руководители не формулируют четких ожиданий относительно того, какого уровня защищенности должна достичь компания и как измерять прогресс в этом направлении.

Отсутствие фокуса на результатах создает ситуацию, при которой службы безопасности отчитываются о процессах и затратах, но не демонстрируют связь своей деятельности с бизнес-целями организации.

Подавляющее большинство респондентов указывают на увеличение инвестиций в защиту, при этом рост быстрее темпов инфляции происходит практически в половине компаний. Сокращение финансирования или сохранение его без изменений представляет собой редкое исключение, затрагивающее около 11% организаций.

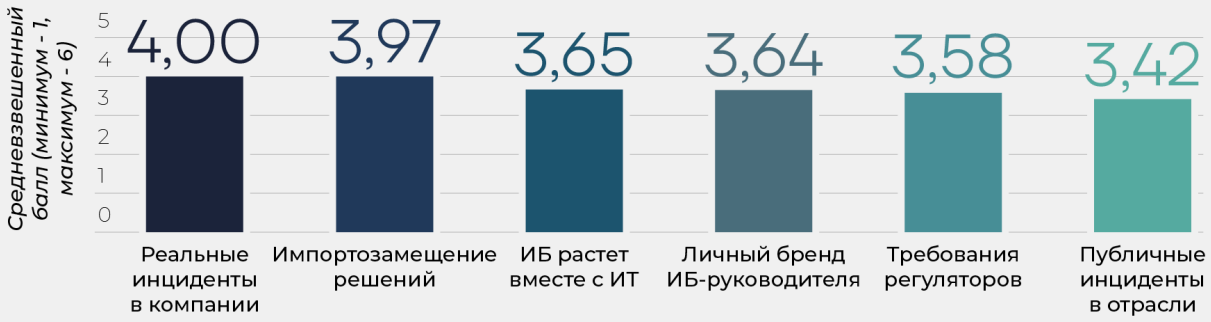
КАК ИЗМЕНИЛСЯ БЮДЖЕТ НА ИБ В ВАШЕЙ КОМПАНИИ С 2022 ГОДА?



Специфика общения между ИБ отделами и руководителями компаний указывает на расхождение между тем как сами CISO понимают проблему и приоритетами в диалоге с топ-менеджерами при формировании бюджетов. Руководители служб ИБ при общении с топ-менеджментом ссылаются на факторы, которые сами они не считают важными, и держат при себе собственное мнение о фактических драйверах роста бюджетов.

Опрошенные выделяют две наиболее значимые причины роста бюджетов: реальные инциденты безопасности внутри компаний и необходимость замещения западных решений отечественными аналогами. Усиление регуляторного давления оказывает меньшее влияние на решения об увеличении финансирования, занимая пятую позицию среди факторов из шести возможных.

ПРИОРИТЕТЫ ДРАЙВЕРОВ ИЗМЕНЕНИЙ В БЮДЖЕТЕ ИБ (ПО УБЫВАНИЮ ВАЖНОСТИ)



Однако при обосновании инвестиций в ИБ значимость практических результатов отходит на задний план и на первых местах по важности респонденты расположили формальные методы аргументации: результаты внешнего и внутреннего аудита и изменения требований регуляторов. Итоги пентестов, то есть проверок на проникновение, при которых имитируются действия злоумышленников для выявления уязвимостей, которые назвали самым важным из практических методов, оказались на 4 месте из 10.

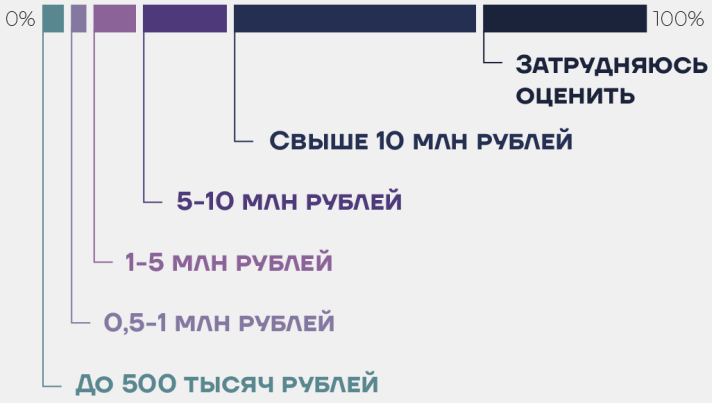
ПРИОРИТЕТЫ ОБОСНОВАНИЯ ИНВЕСТИЦИЙ В ИБ ПЕРЕД РУКОВОДСТВОМ (ПО УБЫВАНИЮ ВАЖНОСТИ)

ПРОБЛЕМЫ С ОЦЕНКАМИ СТОИМОСТИ ВЗЛОМА

Исследование выявило, что большинство респондентов (72%) способны дать оценку стоимости взлома своей инфраструктуры, что опровергает предположение о неспособности CISO мыслить экономическими категориями. Таким образом, проблема отсутствия экономического мышления не является массовой. Однако сопоставление результатов опроса с реальными итогами проверок защищенности компаний указывают на то, что оценка стоимости взлома может быть завышена.

В КАКУЮ СУММУ ВЫ ОЦЕНВАЕТЕ «СТОИМОСТЬ ВЗЛОМА» ЗАЩИТЫ ВАШЕЙ КОМПАНИИ?

Стоимость взлома складывается из квалификации хакеров, используемого инструментария (эксплоиты, 1-day, 0-day и др.), инфраструктуры (VPN, VPS, proxy и др.), отрасли, уровня зрелости информационной безопасности, предпринятого реагирования, цепочки кибератаки и времени атакующего

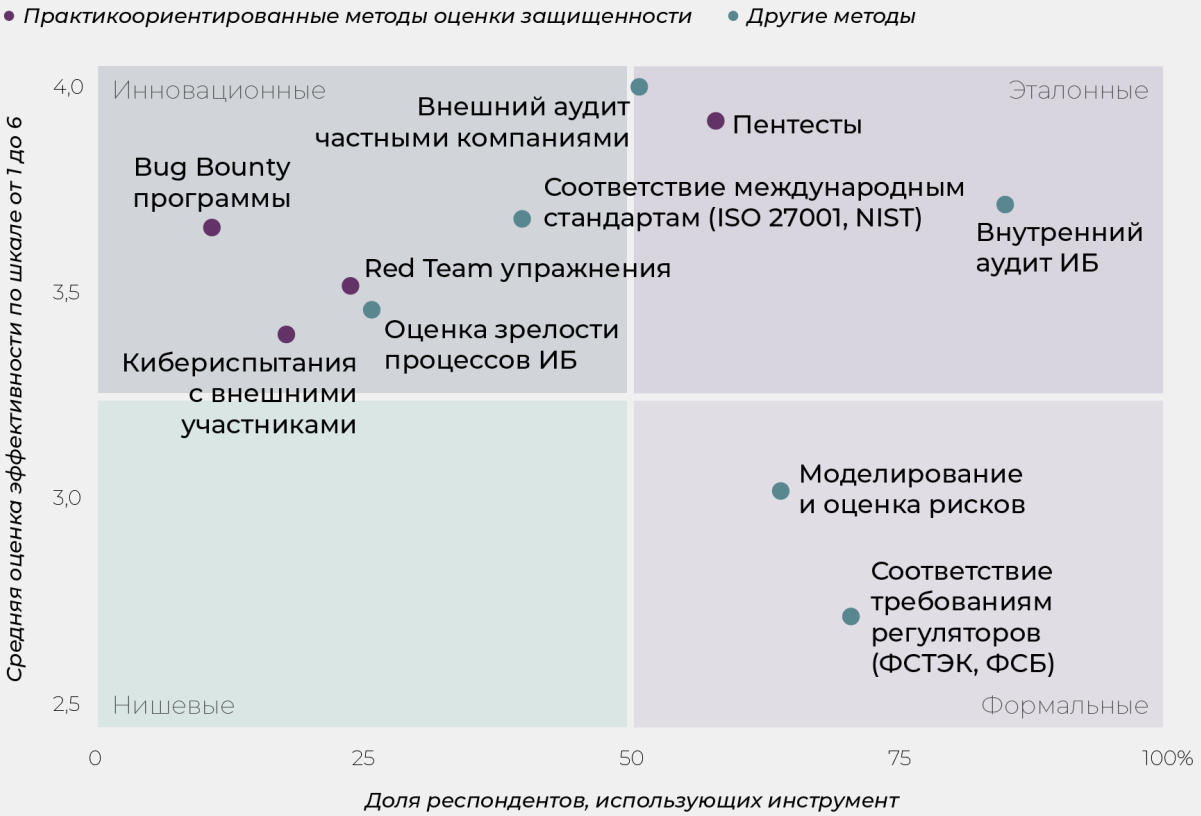


Анализ этих оценок выявил две интересных закономерности. Первая заключается в том, что компании, активно использующие практические методы оценки защищенности (пентесты и Red Team), дают в среднем в полтора раза более высокие оценки стоимости взлома по сравнению с теми, кто таких методов не использует (3,46 против 2,24 по шкале от одного до пяти). **Среди использующих практические методы 48,2% выбирают максимальную категорию «свыше 10 млн рублей», тогда как среди не использующих — только 26,7%**. Компании, которые регулярно проверяют свою защиту и должны лучше понимать реальные уязвимости, дают завышенные оценки защищенности. По результатам исследования «Недопустимое событие 2025. Цифровой краш-тест российского бизнеса» бюджета в 1 млн рублей было достаточно, чтобы реализовать недопустимое событие у 3 из 5 компаний, причем 67% были взломаны простыми атаками.

Объяснение может лежать в психологической плоскости — CISO путают техническую сложность взлома со стоимостью атаки для злоумышленников. Видя тщательно выстроенную защиту, они переоценивают экономические барьеры для атакующих, не учитывая существование специализированного рынка услуг киберпреступности и готовых инструментов.

Рост популярности проверок bug bounty и кибериспытаний, в рамках которых сторонние белые хакеры за конкретное вознаграждение готовы имитировать взлом защиты компании, мог бы исправить ситуацию. Такие практикоориентированные подходы показывают реальную стоимость взлома. Однако пока российский рынок только начинает осваивать подобные варианты проверок, которые являются распространенной общемировой практикой.

КАКИЕ ИНСТРУМЕНТЫ ВЫ ИСПОЛЬЗУЕТЕ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ? НАСКОЛЬКО ОБЪЕКТИВНЫ ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ?



Вторая закономерность связана со зрелостью процессов. **Компании с утвержденным списком критических активов (более зрелые в управлении информационной безопасностью) дают на 26% более низкие оценки стоимости взлома по сравнению с компаниями без такого списка (2,62 против 3,29)**. Это указывает на то, что детальное понимание критических активов и угроз ведет к более реалистичным оценкам. Зрелость в управлении информационной безопасностью коррелирует не с завышением оценок, а с их точностью.

Дополнительную проблему создает тенденция выбора «безопасного максимума». **Наибольшую категорию «свыше 10 млн рублей» выбирают 41,2% респондентов**. Такая концентрация ответов в максимальной категории свидетельствует о том, что значительная часть CISO не производит детальных расчетов, а выбирает максимально высокую оценку как наиболее безопасную с точки зрения обоснования инвестиций перед руководством.

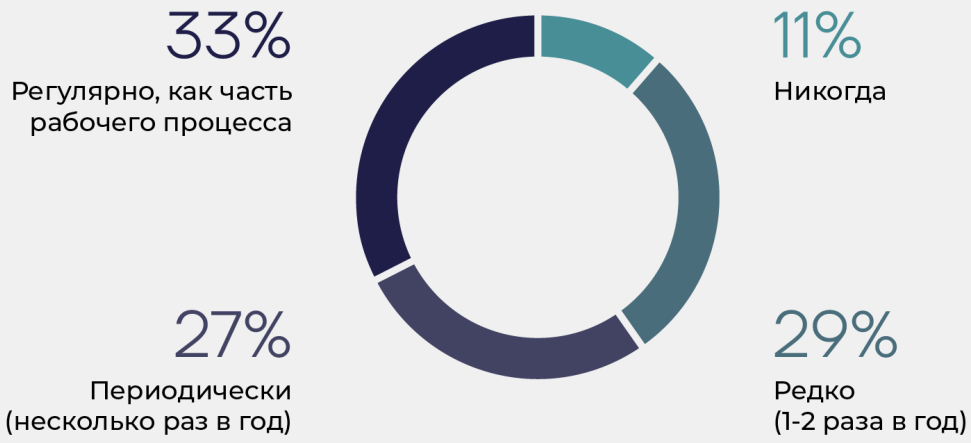
Отсутствие единой методики экономической оценки киберугроз приводит к тому, что даже опытные руководители служб ИБ, активно проверяющие защиту, систематически переоценивают стоимость взлома. Это затрудняет обоснование инвестиций перед руководством и приводит к искажению приоритетов. Топ-менеджеры в интервью подтверждают, что экономическая оценка киберрисков остается нерешенной задачей для большинства организаций при отсутствии единой методики.

Исследование подтверждает существование запроса на создание единой системы рейтинга кибербезопасности. **Подавляющее большинство CISO (86%) считают нужным появление такой системы, хотя только 12% называют ее критически необходимой**. Противников концепции среди руководителей ИБ существенно меньше — седьмая часть (14%) опрошенных считает создание единой системы рейтингов невозможным или бесполезным начинанием. Вопрос институционального устройства такой системы выявляет расхождения в предпочтениях CISO. Почти половина (47%) респондентов видит профессиональные ассоциации и сообщества наиболее подходящими разработчиками методологии рейтингования, что можно интерпретировать как стремление отрасли к саморегулированию. Почти пятая (18%) часть ответивших отдает предпочтение государственным регуляторам как институтам, обладающим необходимыми полномочиями для создания обязательной системы оценки.

ИСКЛЮЧЕНИЕ ИБ-ДИРЕКТОРОВ ИЗ ПРОЦЕССОВ ПРИНЯТИЯ БИЗНЕС-РЕШЕНИЙ

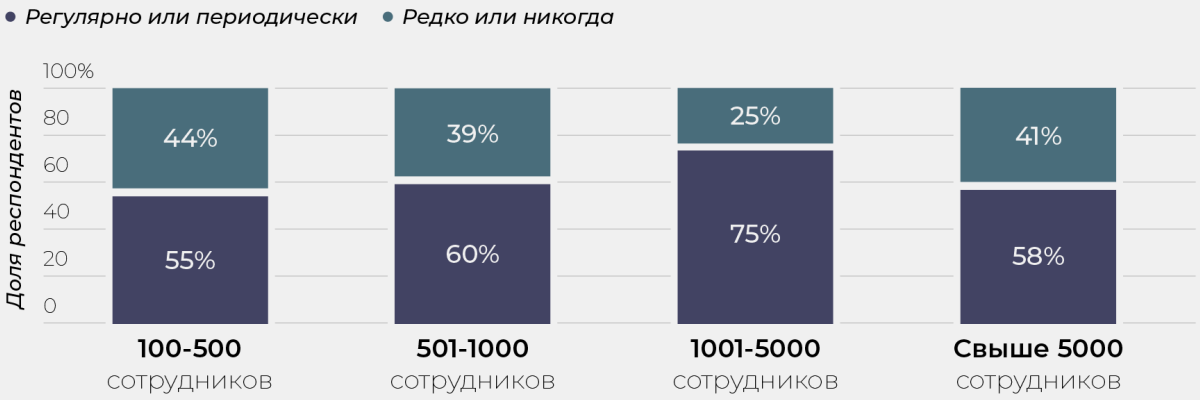
Анализ частоты привлечения служб информационной безопасности к принятию бизнес-решений, не связанных непосредственно с задачами ИБ, например, к запуску нового продукта, выявил неоднородность ситуации. Регулярное привлечение отмечают 33% респондентов, периодическое участие — 27%, редкое — 27%, никогда — 11%. Другими словами, **практически 70% CISO исключены из процесса принятия стратегических бизнес-решений или имеют крайне ограниченные возможности на них повлиять**.

КАК ЧАСТО РУКОВОДСТВО КОМПАНИИ ПРИВЛЕКАЕТ СЛУЖБУ ИБ К ПРИНЯТИЮ БИЗНЕС-РЕШЕНИЙ, НЕ СВЯЗАННЫХ НАПРЯМУЮ С БЕЗОПАСНОСТЬЮ?



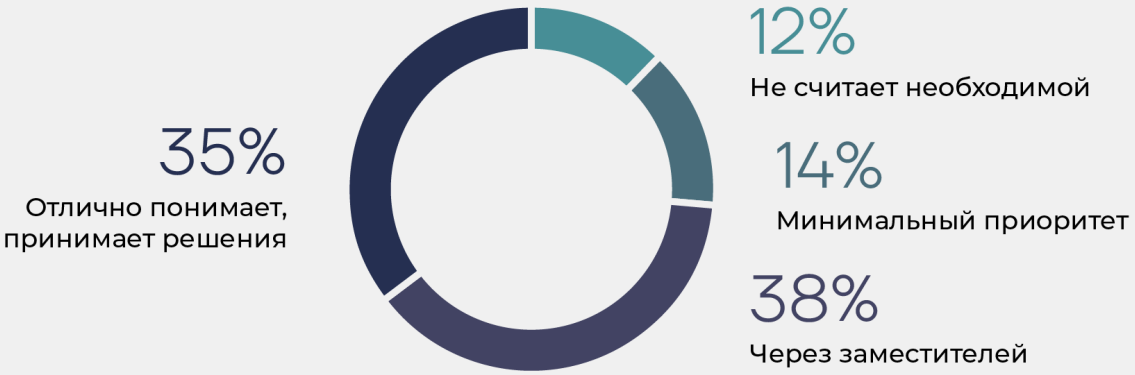
Анализ связи между размером компании и частотой привлечения служб ИБ к обсуждению бизнес-задач выявил следующую картину. Наименьшую вовлеченность в обсуждение и принятие бизнес-решений демонстрируют малые компании численностью от 100 до 500 человек, где 44% исключены из обсуждения бизнес-процессов. Пиковой вовлеченности достигают средние организации от 1001 до 5000 сотрудников (75%). **В крупных корпорациях свыше 5000 человек показатель снижается до 59%, что указывает на возникновение барьеров при многоуровневой иерархии**.

ПРИВЛЕЧЕНИЕ ИБ К БИЗНЕС-РЕШЕНИЯМ ПО РАЗМЕРАМ КОМПАНИЙ



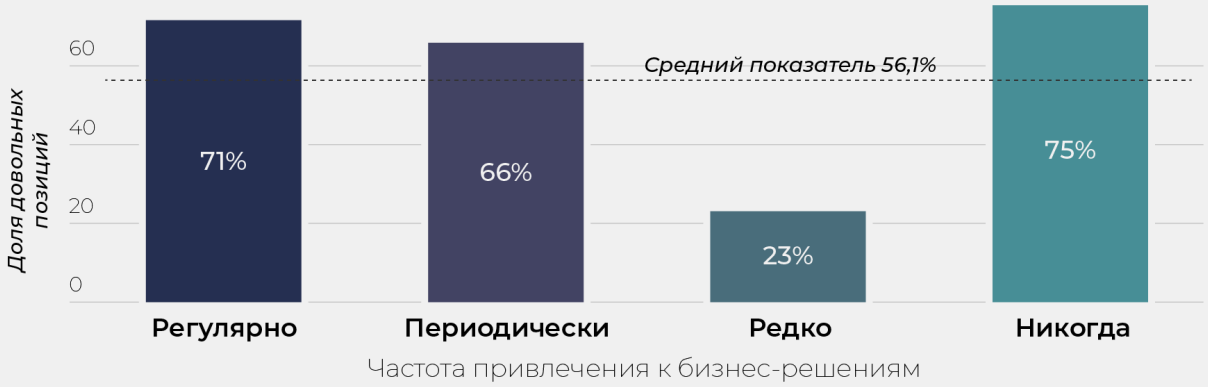
Исследование подтвердило связь между частотой привлечения руководителей ИБ к принятию бизнес-решений и их удовлетворенностью текущей позицией в компании. Общий уровень удовлетворенности составил 56%.

ВОВЛЕЧЕННОСТЬ ГЕНЕРАЛЬНОГО ДИРЕКТОРА (ОЦЕНКА CISO)



Среди CISO, регулярно участвующих в принятии решений, довольны своей позицией 71%. Периодическое привлечение ассоциируется с удовлетворенностью у 66%. Редкое привлечение снижает долю довольных до 23%. Формальное привлечение без реального влияния создает максимальную фрустрацию. Группа «Никогда» имеет самую высокую удовлетворенность (75%). У таких респондентов нет завышенных ожиданий, они не ждут вовлечения в бизнес-процессы и не разочарованы его отсутствием. Возможно, их устраивает чисто техническая функция.

СВЯЗЬ МЕЖДУ ПРИВЛЕЧЕНИЕМ И УДОВЛЕТВОРЕННОСТЬЮ



Частота привлечения к бизнес-решениям

Отметим, что атмосфера, которая сформировалась на российском рынке ИТ и кибербезопасности после событий 2022 года, может превратить подобную инертность в бомбу замедленного действия.

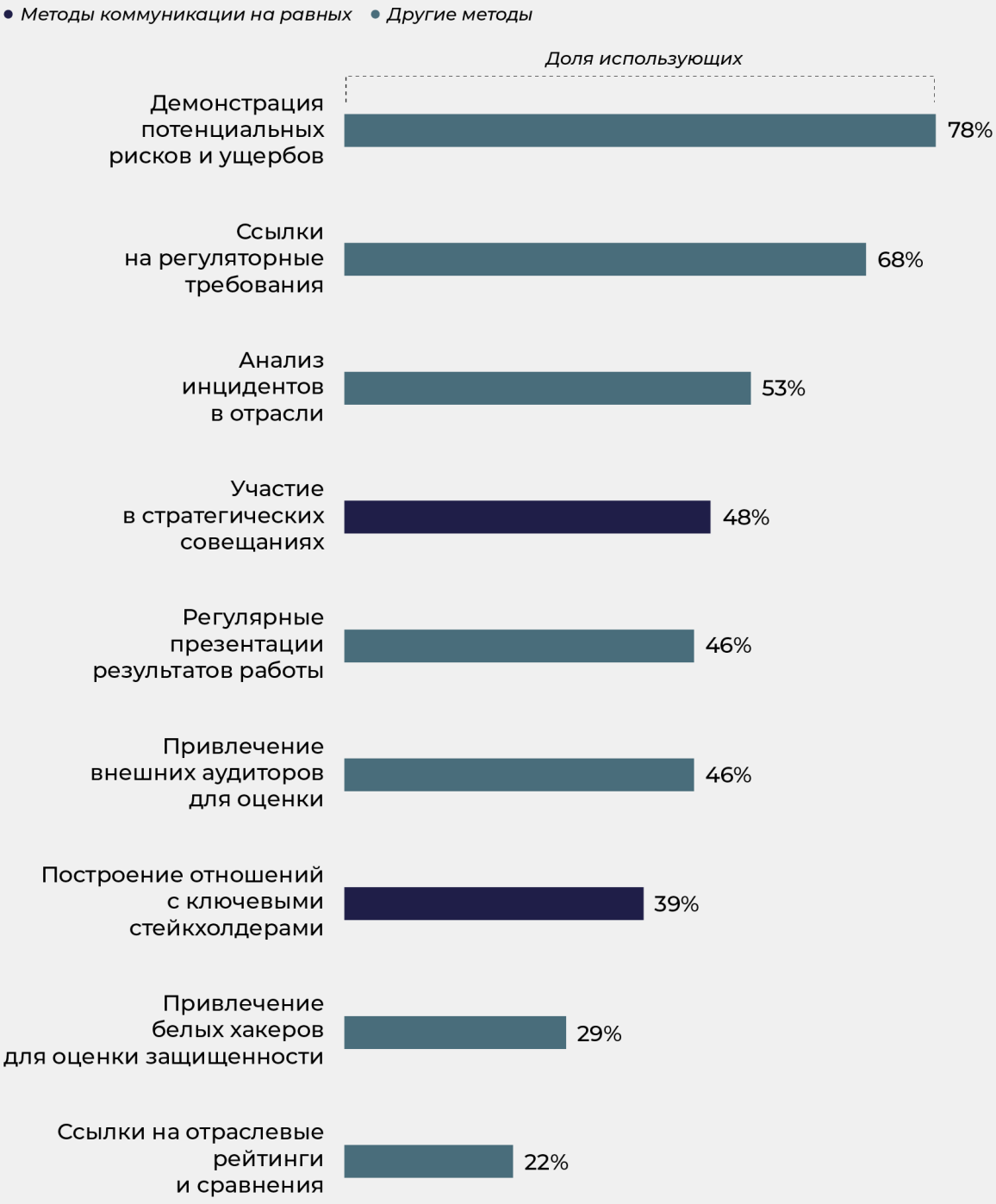
Прежний подход, «если работает, не трогай» теряет актуальность, так как ландшафт угроз изменился как и их интенсивность. Это показали результаты наших предыдущих исследований.

Консервативный подход к формированию бюджетов и опора на западные решения, которые «как-то сами все сделают», приводит к зависимости от ненадежных на фоне действий недружественных стран бизнес-связей.

Интересно, что в последующих ответах руководители служб ИБ говорили о важности импортозамещения, однако не всегда это понимание способствует преодолению инертности и активизации участия в бизнес-процессах.

Две трети респондентов (67%) используют хотя бы один метод коммуникации на равных, включая участие в стратегических совещаниях (48%) и построение отношений с ключевыми стейкхолдерами (39%). Однако эффективность этих методов оказывается ограниченной. Среди использующих стратегические подходы только 56% ометили, что существенно влияют на принимаемые решения.

КАКИЕ МЕТОДЫ ВЫ ИСПОЛЬЗУЕТЕ ДЛЯ ПРОДВИЖЕНИЯ ИНТЕРЕСОВ ИБ В КОМПАНИИ?



Проблема заключается не столько в отсутствии попыток выстроить равноправный диалог, сколько в низкой эффективности этих попыток и в том, что почти половина специалистов остается за пределами полноценного участия в бизнес-процессах.

КУЛЬТУРА БЕЗОПАСНОСТИ И ДИАЛОГ С ДРУГИМИ ОТДЕЛАМИ

В этом сегменте задавались вопросы об эффективности диалога между ИБ-отделом и другими подразделениями компании уже не с точки зрения формирования бюджетов: речь шла о внутрикорпоративной культуре и информационной гигиене.

Большинство ответивших (63%) отмечают конструктивный формат работы, при котором риски обсуждаются совместно с бизнес-подразделениями и требования ИБ формируются с учетом операционных приоритетов. Четверть респондентов указывает на подчиненное положение, когда требования информационной безопасности имеют более низкий приоритет по сравнению с потребностями бизнеса, но в определенной мере учитываются. Крайние позиции занимают небольшие доли — полное отсутствие диалога фиксируют 5%, доминирование требований ИБ над бизнес-приоритетами отмечают 7%.

КАК ПОСТРОЕН ДИАЛОГ МЕЖДУ ИБ И ДРУГИМИ ПОДРАЗДЕЛЕНИЯМИ В ВАШЕЙ ОРГАНИЗАЦИИ?

Данные интервью с топ-менеджерами подтверждают фундаментальное противоречие между задачами безопасности и эффективностью бизнеса.

Службы ИБ стремятся максимально ограничить доступы и изолировать критические системы, тогда как бизнес не может работать конкурентоспособно в условиях жестких ограничений.

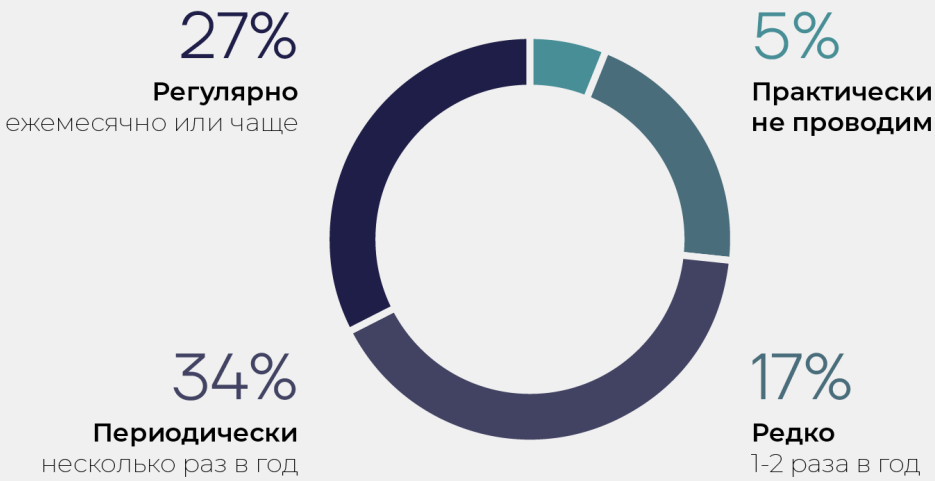
По словам руководителям компаний, новое поколение руководителей служб безопасности демонстрирует большую готовность к компромиссам, понимая необходимость баланса между защитой и операционной эффективностью. Однако конфликт интересов остается системной проблемой, требующей постоянного согласования приоритетов.

Формирование культуры безопасности в компаниях происходит с умеренным успехом. Только 9% опрошенных оценивают процесс как очень успешный с активным вовлечением сотрудников. Половина респондентов (51%) отмечает в целом успешное развитие культуры с заметным прогрессом, четверть констатирует медленный прогресс. Неудовлетворительную ситуацию фиксируют 15% — либо слабое продвижение с сопротивлением сотрудников (10%), либо полную незаинтересованность персонала в вопросах безопасности (5%).

НАСКОЛЬКО ОСТРО СТОИТ ПРОБЛЕМА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ВАШЕЙ КОМПАНИИ?

Острота проблемы социальной инженерии как вектора атак получает высокую оценку у большинства компаний. Серьезной или критической проблемой ее считают две трети опрошенных. Однако только 9% называют социальную инженерию главным вектором атак и основной угрозой, тогда как 58% рассматривают ее как серьезную, но не единственную проблему. Пятая часть компаний (21%) не сталкивается с заметными проявлениями социальной инженерии, что может объясняться как эффективной защитой, так и недостаточным выявлением таких инцидентов.

КАК ЧАСТО СЛУЖБА ИБ ПРОВОДИТ РАБОТУ С СОТРУДНИКАМИ КОМПАНИИ (ОБУЧЕНИЕ, ТРЕНИНГИ, ИНФОРМИРОВАНИЕ)?



Частота работы с сотрудниками по вопросам информационной безопасности демонстрирует недостаточную системность. Регулярное обучение на ежемесячной основе или чаще проводят лишь 27% компаний. Периодические мероприятия несколько раз в год организуют 34%. Редкие тренинги один-два раза в год или только при инцидентах характерны для 34% организаций. Практически не проводят работу с персоналом 5% компаний.

ИМПОРТОЗАМЕЩЕНИЕ

Более половины организаций завершили переход на российские продукты, и еще четверть находится в фазе трансформации. **Пятая часть компаний принципиально отказывается от импортозамещения**, что может объясняться спецификой деятельности или технологическими ограничениями.

ВЫ УЖЕ МИГРИРОВАЛИ НА ОТЕЧЕСТВЕННЫЕ РЕШЕНИЯ В СФЕРЕ ИБ?

КАК ВЫ ОТНОСИТЕСЬ К ВОЗМОЖНОМУ ВОЗВРАЩЕНИЮ ЗАПАДНЫХ ВЕНДОРОВ?

Отношение к потенциальному возвращению западных вендоров на российский рынок демонстрирует практически равное разделение мнений CISO. Незначительное большинство выражает приверженность отечественным решениям вне зависимости от изменения внешних условий, тогда как сопоставимая доля респондентов готова вернуться к проверенным западным продуктам при возникновении такой возможности.

Отношение к возможному возвращению зарубежных поставщиков опрошенных руководителей ИБ контрастирует с позицией топ-менеджмента. Две трети руководителей выступают против возобновления сотрудничества, ссылаясь на ненадежность таких партнеров. Каждый пятый руководители готов обсудить частичное возвращение, преимущественно в аппаратном сегменте, где отечественные производители еще не достигли технологического паритета. И лишь 1 из 10 топ-менеджеров готов на полное возвращение при условии демонстрации надежности и качества решений.

Отметим, что такие результаты подтверждают: в данный момент уровень вовлеченности ИБ-специалистов в стратегическую финансовую конъюнктуру в ряде компаний остается слишком низким. Это мешает видеть риски от импортозависимости в сфере информационной безопасности, в то время как опора на проверенные решения или возврат к ним при первой возможности видится более привлекательным вариантом.

В КАКИХ КЛАССАХ РЕШЕНИЙ ИБ НАИБОЛЕЕ ОСТРО ОЩУЩАЕТСЯ НЕДОСТАТОК КАЧЕСТВЕННЫХ РОССИЙСКИХ ПРОДУКТОВ?

Недостаток российских решений ощущается в области систем управления политиками сетевой безопасности, межсетевых экранов нового поколения, средств защиты облачных инфраструктур и автоматизированных инструментов оценки безопасности — каждую из этих категорий отметила половина. Средства криптографической защиты и комплексной защиты почты выделили меньше 20% респондентов.

АУТСОРСИНГ ФУНКЦИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ответы на вопрос о готовности к передаче функций информационной безопасности внешним провайдерам демонстрируют **существенное расхождение между руководителями служб ИБ и топ-менеджерами**. Среди руководителей технических служб 43% категорически против аутсорсинга безопасности, 39% уже используют или намерены использовать внешних провайдеров, 18% хотели бы передать функции на аутсорсинг, но не могут из-за регуляторных ограничений или внутренних регламентов.

РАССМАТРИВАЕТ ЛИ ВАША КОМПАНИЯ ВОЗМОЖНОСТЬ АУТСОРСИНГА ФУНКЦИЙ ИБ?

Данные интервью с топ-менеджерами показывают более консервативный подход — **60% руководителей выступают против аутсорсинга функций ИБ, только 30% готовы рассматривать такую возможность, еще 10% допускают частичную передачу отдельных функций** внешним провайдерам.

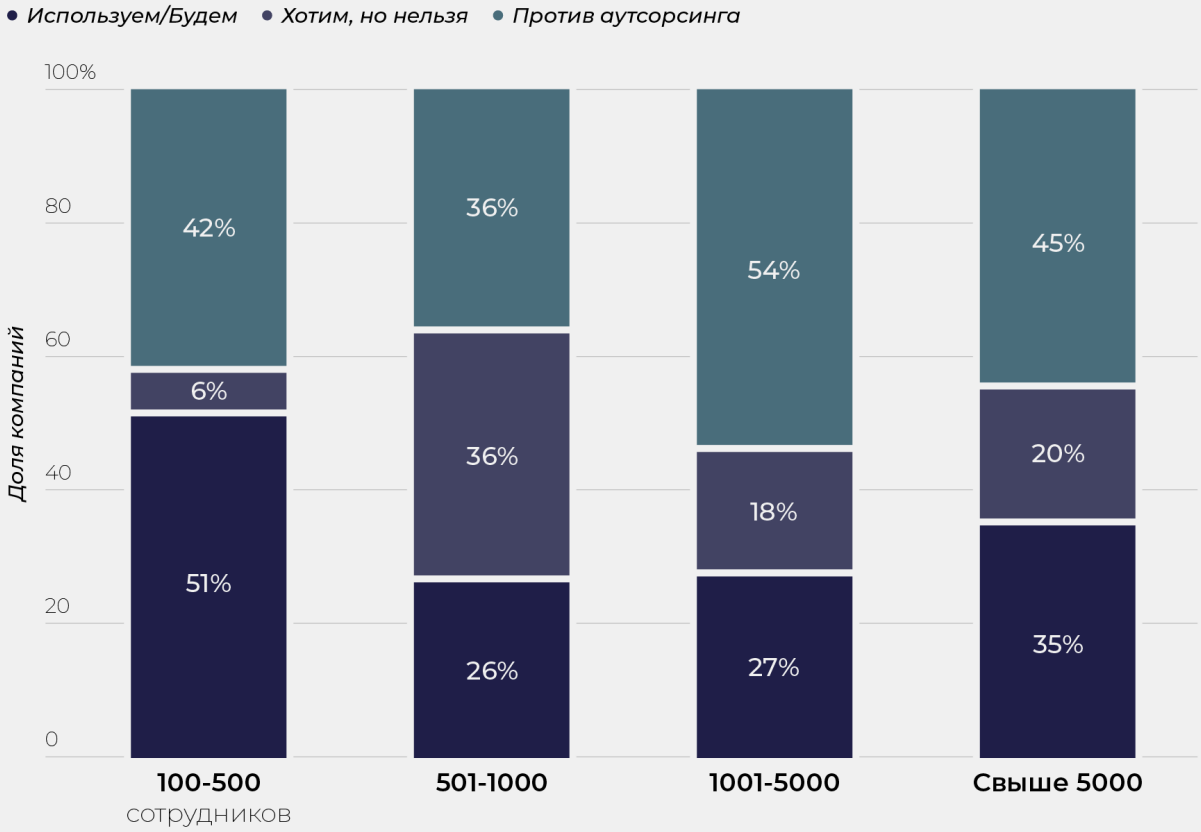
С точки зрения CISO, если функции информационной безопасности передаются на аутсорс, ключевым фактором при заключении договора должна быть финансовая ответственность поставщика услуг. Другим вариантам гарантий, таким как SLA (соглашение об уровне обслуживания), присваивается меньший приоритет.

ПРИОРИТЕТЫ ГАРАНТИЙ ОТ ПРОВАЙДЕРА АУТСОРСИНГА ИБ (ПО УБЫВАНИЮ ВАЖНОСТИ)

Руководители ИБ из малых компаний (100-500 сотрудников) чаще всего готовы к аутсорсингу и демонстрируют результат 52% — это максимальный показатель среди всех категорий. Средние компании (501-1000 и 1001-5000 сотрудников) показывают минимальную готовность к аутсорсингу. Именно в этом сегменте максимальна доля противников аутсорсинга — 55% у компаний с 1001-5000 сотрудников. Крупные компании (свыше 5000 сотрудников) демонстрируют 35% готовности — промежуточное значение.

Можно предположить, малые компании используют аутсорсинг из-за нехватки ресурсов, средние компании активно строят собственные команды ИБ, а крупные компании готовы рассматривать аутсорс как вариант масштабирования.

ОТНОШЕНИЕ К АУТСОРСИНГУ ИБ ПО РАЗМЕРУ КОМПАНИЙ (ПРОЦЕНТНОЕ РАСПРЕДЕЛЕНИЕ)



Данные также указывают на возможную связь готовности к аутсорсу со зрелостью процессов ИБ в компании. Отсутствие списка критических активов ассоциируется с максимальной готовностью передать функции ИБ внешним провайдерам. 63% компаний без списка критических активов выступают за аутсорс.

ПРИОРИТЕТЫ ПРОБЛЕМ РАЗВИТИЯ ИБ

Анализ оценок факторов, мешающих развитию сферы информационной безопасности в России, выявил характерную расстановку приоритетов. По шкале от 1 до 10 наивысшую оценку значимости получили операционные проблемы, а организационным факторам был присвоен более низкий приоритет.

НАСКОЛЬКО СИЛЬНО МЕШАЮТ РАЗВИТИЮ СФЕРЫ ИБ В РОССИИ СЛЕДУЮЩИЕ ФАКТОРЫ?

Фокусируясь на операционных проблемах — стоимости решений, дефиците кадров и качестве продуктов — CISO уделяют меньше внимания факторам, определяющим позиции структур информационной безопасности в их организациях. Между тем, именно организационные проблемы — слабая интеграция в бизнес-процессы, непонимание руководством, отсутствие четких целей — создают контекст, в котором решение операционных задач не приводит к повышению роли служб ИБ и признанию их вклада в работу компаний.

РАЗЛИЧИЯ ПОЗИЦИЙ ТОП-МЕНЕДЖЕРОВ И CISO В ВОПРОСАХ ИБ

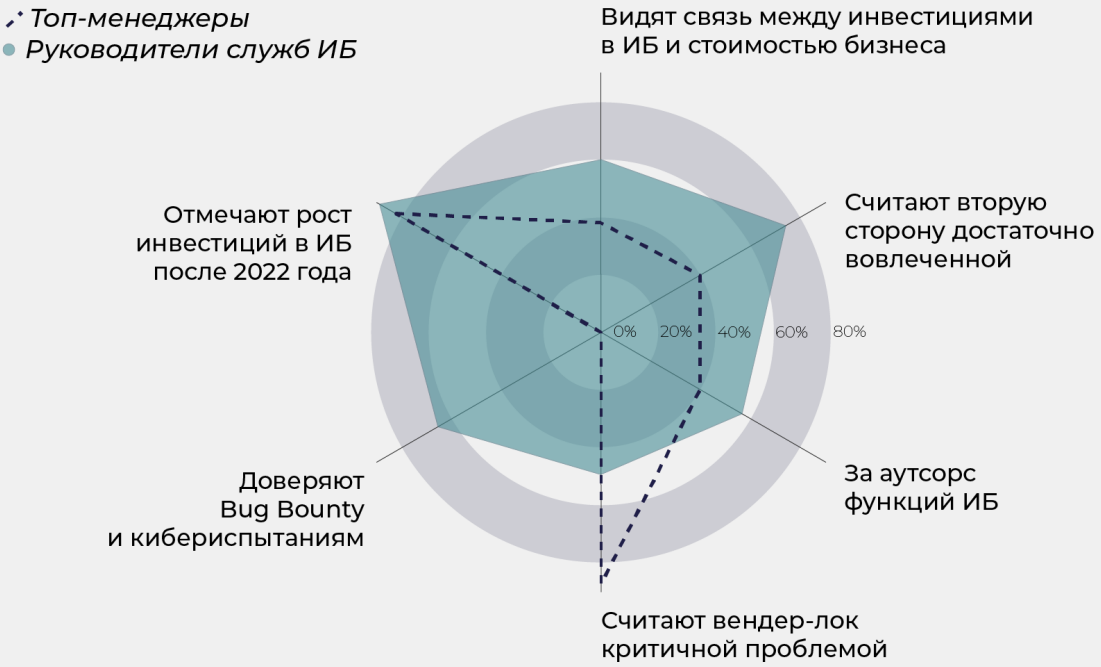
Сопоставление результатов опроса руководителей служб ИБ и интервью топ-менеджеров выявило расхождения по ряду ключевых параметров.

Наиболее выраженное различие связано с восприятием экономической ценности информационной безопасности. CISO значительно чаще видят связь между инвестициями в защиту и стоимостью бизнеса: 60% против 38% у руководителей компаний. Разрыв в 22 п.п. указывает на проблему коммуникации между техническими службами и руководством.

Оценки взаимной вовлеченности также серьезно отличаются. Большинство руководителей ИБ (74%) формально отмечают высокую вовлеченность генерального директора в вопросы информационной безопасности. Из них 36% указывают, что первое лицо отлично понимает вопросы ИБ и принимает решения самостоятельно, тогда как 38% говорят о регулярных докладах через доверенных заместителей или советников. Низкую вовлеченность фиксируют 26% респондентов: 14% отмечают поддержку информационной безопасности с минимальным приоритетом, а 12% констатируют, что генеральный директор не считает ИБ необходимой функцией. При этом только 40% топ-менеджеров считают директора по кибербезопасности достаточно вовлеченным в бизнес-процессы. Разрыв в 34 п.п. может указывать на то, что CISO переоценивают реальную вовлеченность руководства.

Анализ изменений после 2022 года показал различия восприятия проблем ИБ. Интервью с топ-менеджерами выявили, что 64% организаций изменили понимание защищенности, а 83% увеличили инвестиции в кибербезопасность. Однако лишь четверть руководителей ИБ (24%) отметила повышение вовлеченности генерального директора за последние три года. При этом две трети CISO зафиксировали усиление внимания ИТ-направления к вопросам кибербезопасности. Это указывает на то, что **рост финансирования и осознание угроз не повлекли за собой изменения роли службы информационной безопасности в глазах первых лиц компаний**.

ВОСПРИЯТИЕ КИБЕРБЕЗОПАСНОСТИ: ПОЗИЦИИ ТОП-МЕНЕДЖМЕНТА И РУКОВОДИТЕЛЕЙ СЛУЖБ ИБ



Отношение к зависимости от единственного вендора демонстрирует противоположные приоритеты. Среди топ-менеджеров 88% считают вендор-лок критичной проблемой, тогда как эту позицию разделяют лишь 50% руководителей служб ИБ. Разрыв в 38 п.п. объясняется различием в перспективах: CISO более прагматично оценивают компромисс между экосистемностью решений и рисками зависимости, понимая операционные преимущества интегрированных платформ. Топ-менеджеры фокусируются на стратегических рисках утраты контроля над технологической инфраструктурой.

Готовность к возвращению западных вендоров на российский рынок также выявила существенные расхождения. Среди CISO мнения разделились практически поровну между сторонниками отечественных решений и готовыми вернуться к зарубежным продуктам. Топ-менеджеры занимают более консервативную позицию: две трети (67%) выступают против возобновления сотрудничества, ссылаясь на ненадежность таких партнеров. Каждый пятый руководитель готов обсуждать частичное возвращение, преимущественно в аппаратном сегменте, и лишь 11% рассматривают полное возвращение при условии демонстрации надежности и качества решений.

Отношение к аутсорсингу функций информационной безопасности показывает схожую картину. Среди ИБ-руководителей 43% категорически против передачи функций внешним провайдерам, 39% уже используют или намерены использовать аутсорсинг, 18% хотели бы это сделать, но не могут из-за регуляторных ограничений. Топ-менеджеры более осторожны: 60% выступают против аутсорсинга, только 30% готовы рассматривать такую возможность.

Доверие к методам оценки защищенности выявило крупный разрыв. Руководители ИБ высоко оценивают объективность практических методов: пентесты получили 4,02 балла из 5, Red Team — 3,94 балла. Соответствие регуляторным требованиям оценивается существенно ниже — 2,74 балла. При этом 74,8% CISO готовы продемонстрировать защищенность компании с привлечением белых хакеров, 66% готовы рекомендовать руководству участие в кибериспытаниях. Однако интервью с топ-менеджерами показали нулевое доверие к bug bounty и кибериспытаниям. Барьер принятия практических методов оценки находится не на уровне технических служб, а на уровне высшего руководства.