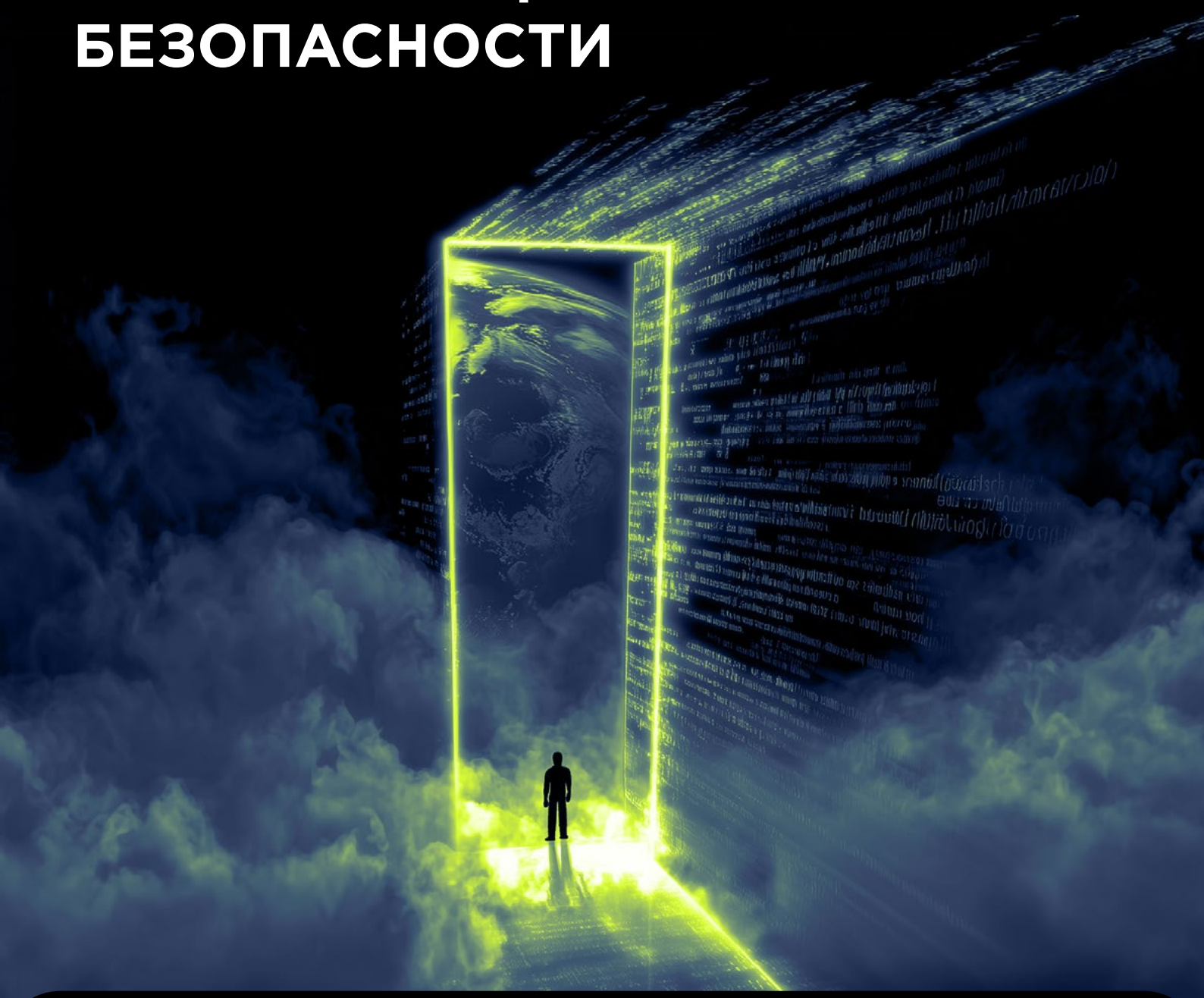
Исследование

ИБ В РОССИИ:

КАК НЕПРЕРЫВНЫЕ АТАКИ МЕНЯЮТ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Инфосистемы Джет

JET SECURITY TEAM

Александр Морковчин

Руководитель отдела развития консалтинга по информационной безопасности, «Инфосистемы Джет»

Елена Агеева

Руководитель группы аналитических исследований, «Инфосистемы Джет»

Аскар Мусаев

Эксперт по информационной безопасности, «Инфосистемы Джет»

Ирина Павлова

Эксперт по информационной безопасности, «Инфосистемы Джет»

Оглавление

КЛЮЧЕВЫЕ ВЫВОДЫ

После завершения кризисной адаптации 2022–2024 годов российский рынок ИБ в 2025 году перешел в режим **«высоконагруженной эксплуатации»**. Ключевая особенность нового этапа — наслоение разнонаправленных факторов давления. С одной стороны — рост ключевой ставки, удорожание кредитов, увеличение налоговой нагрузки привели к сокращению инвестиционных программ. С другой — рост числа и сложности инцидентов с шифровальщиками, ужесточение регуляторных требований, системное давление кадрового дефицита требовали обеспечения киберустойчивости в условиях жесткой экономии ресурсов: делать больше с меньшими ресурсами.

> **Киберустойчивость** — способность организации непрерывно предоставлять свои услуги и выпускать продукты, несмотря на любые неблагоприятные киберинциденты, путём активной подготовки к ним, планирования защитных мер, обнаружения и реагирования на киберинциденты, а также восстановления организации после кибератак

Рынок учится жить в условиях перманентного стресса, где ценность определяется не защищенностью периметра, а зрелостью процессов реагирования, восстановления и непрерывности бизнеса. Резонансные атаки на крупнейшие российские компании [1] — с развитой цифровой инфраструктурой и значительными бюджетами на ИБ — обнажили системную проблему отрасли: реальная операционная готовность к инцидентам остается низкой.

1 Резонансные атаки на крупнейшие российские компании

Разрыв между «понимаем» и «можем отреагировать» — главная угроза 2025-2026 годов

Разрыв между «понимаем» и «можем отреагировать» — главная угроза 2025–2026 годов. Без перехода от стратегии к действию компании рискуют остаться с идеальным планом, но без реальной защиты в момент атаки. Именно поэтому в этом году мы расширили раздел, посвященный поддержанию киберустойчивости и обеспечению непрерывности бизнеса, сделав акцент на отработке поведения в кризисных ситуациях.

Результаты исследования позволяют компаниям сравнить свой подход к киберустойчивости с подходом других игроков рынка. Информация будет полезна руководителям служб ИБ и ИТ, консультантам и экспертам в области ИБ и непрерывности бизнеса.

КЛЮЧЕВЫЕ ЦИФРЫ

/01 СТРАТЕГИЧЕСКИЙ МЕНЕДЖМЕНТ

стр. 8

- Вдвое увеличилась доля компаний, в которых бюджет на ИБ был сокращен — с 8% в 2024 году до 20% в 2025-м. В основном бюджеты на ИБ остались на прежнем уровне или были проиндексированы на уровень инфляции.
- Подавляющее большинство компаний, которые существенно увеличивали бюджеты ИБ в 2025 году, постинцидентные. Затраты на восстановление после атаки требуют значительных инвестиций, для которых уже не требуется обоснования, ключевая цель — быстро восстановить операционную деятельность.
- Продолжается тренд на «сужение» горизонта планирования: популярным остается трехлетнее планирование, но все больше руководителей ИБ выбирают краткосрочные тактические действия, планируя стратегию до года.

/02 ОРГАНИЗАЦИЯ СЛУЖБЫ ИБ

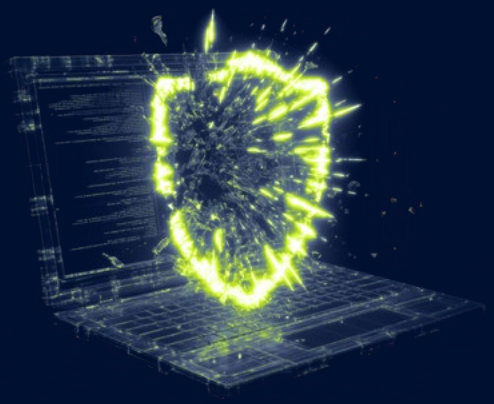
стр. 16

Большинство опрошенных компаний (80%) испытывают потребность в специалистах по ИБ. Значительная доля респондентов оценивает кадровый дефицит более чем в 10 специалистов — за последние три года потребность в таком объёме выросла до 32%.

- Увеличился разрыв между потребностями и фактическими возможностями найма специалистов по ИБ: в половине компаний открыты только 1-3 вакантные должности, 46% компаний вовсе не имеет открытых вакансий.
- Руководители ИБ концентрируются на привлечении редких и высококвалифицированных специалистов. На смену спроса на универсальных специалистов приходит запрос на архитекторов ИБ и специалистов по безопасной разработке.

/03 КИБЕРУСТОЙЧИВОСТЬ

стр. 23



Классические риски нарушения деятельности организации всё больше отходят на второй план: в 2025 году кибератаки впервые обошли ИТ-сбои в нашем рейтинге рисков прерывания бизнеса (42% против 33%).

- Реальная готовность к инцидентам большинства российских компаний остается низкой. В компаниях, в которых инцидент ИБ повлиял на операционную надежность, в 2025 году только 40% смогли достичь ожидаемого времени восстановления.
- В 37% компаний есть понимание ответственности за принятие решения о действиях в случае требований выкупа (например, при атаке шифровальщика или похищении данных).

/04 ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ, ИСПОЛЬЗОВАНИЕ СЕРВИСОВ И АВТОМАТИЗАЦИЯ

стр. 31

- Доля компаний, использующих ИИ в работе службы ИБ, выросла с 3% в 2024 году до 27% в 2025-м. Основные цели использования — интеграция ИИ в различные системы и процессы (например, ИИ для разработки правил корреляции SIEM) и классическое использование чат-ботов с целью обработки информации и получения рекомендаций по различным вопросам внутри службы ИБ.

Лидирующими сервисами аутсорсинга остаются услуги центра мониторинга и реагирования на инциденты ИБ (17%) и поддержка средств защиты информации (14%).

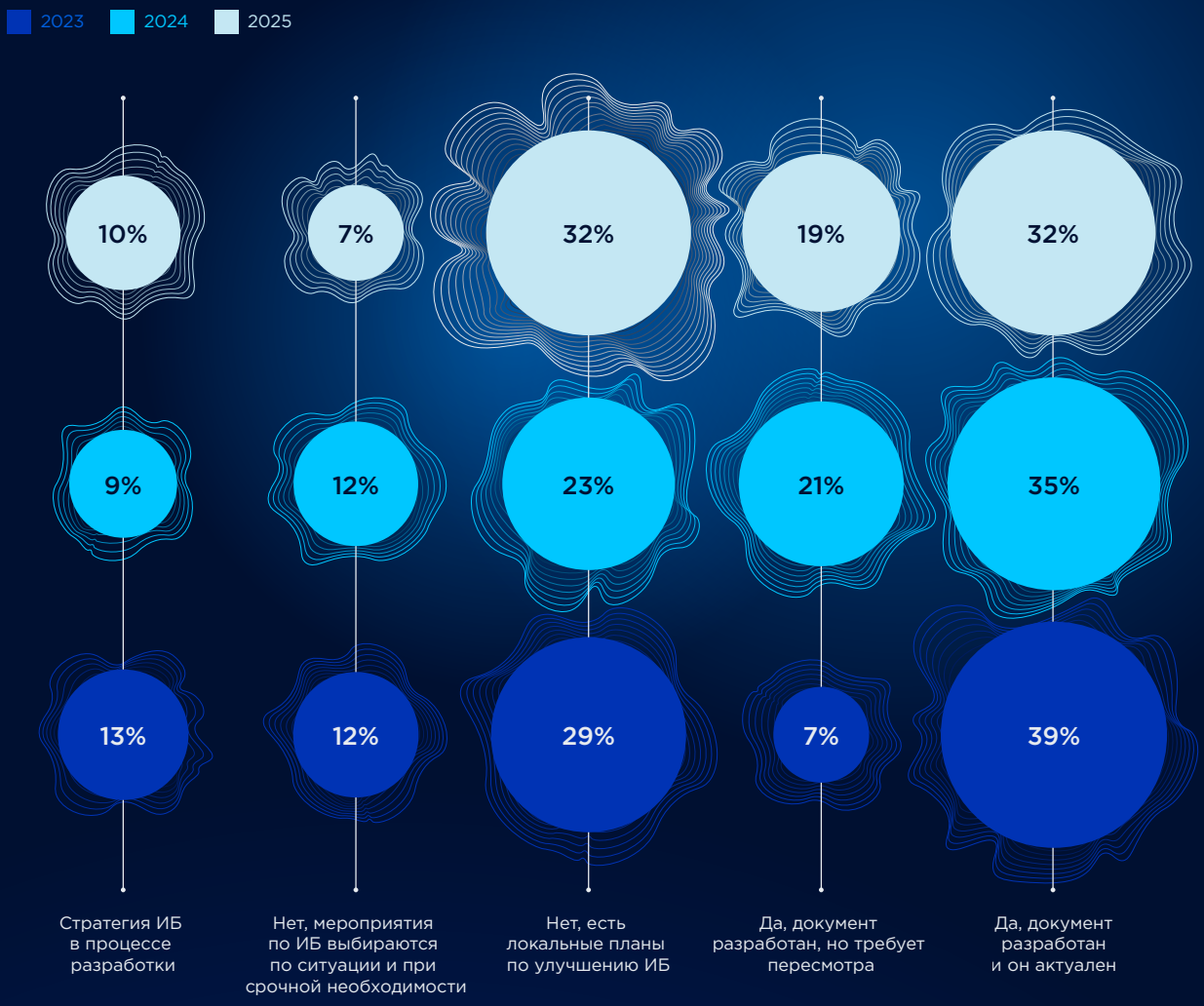
СТРАТЕГИЧЕСКИЙ МЕНЕДЖМЕНТ

Выбор вектора развития

Увеличение налоговой нагрузки на компании, вызванное ростом ключевой ставки до 21%, сокращение инвестиционных программ, заморозка найма и фокус на оптимизации привели к смене парадигмы в стратегическом менеджменте. Если ранее компании адаптировались к новым условиям и искали новые точки роста, то 2025 год отмечен возвратом бизнеса к жёсткому операционному планированию. Задача руководителя ИБ сместилась в сторону выживания в условиях ограниченных ресурсов, сохраняя устойчивость бизнеса.

Процент компаний с утверждённой стратегией ИБ остался практически на уровне 2024 года (51%), при этом доля стратегий, требующих пересмотра, выросла почти втрое с 2023 года. Такой рост обусловлен завершением первого посткризисного стратегического цикла (2022–2024). Компании, которые формировали стратегии «с нуля» в ответ на турбулентность 2022 года, подошли к этапу закономерного пересмотра утверждённых ранее планов.

Наличие стратегии ИБ в компании



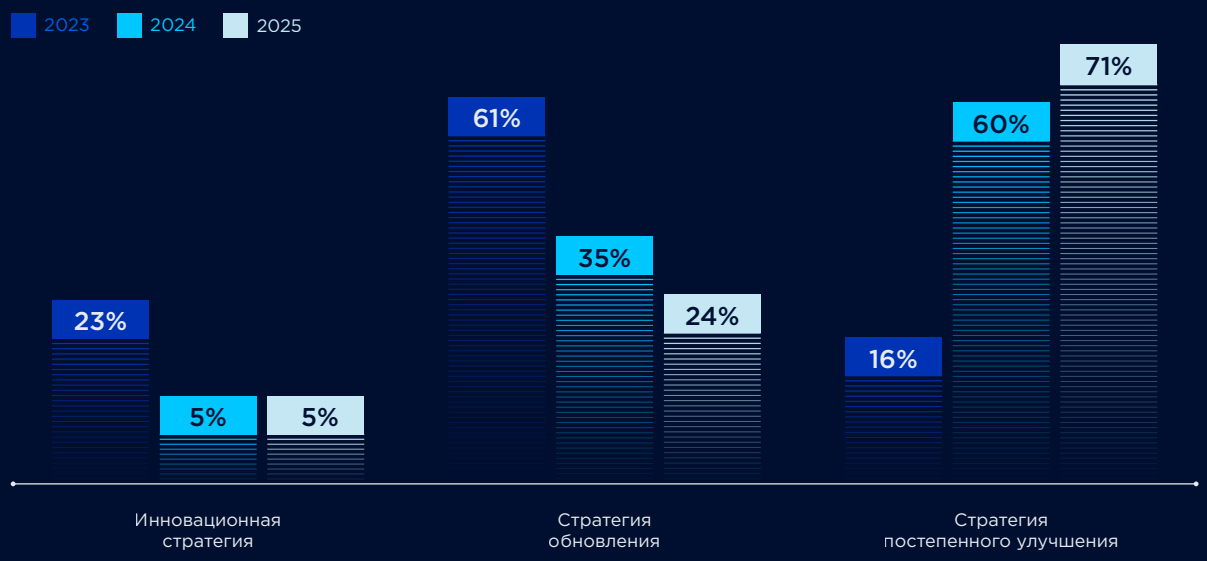
Как и годом ранее, компании продолжают выбирать «осторожный» метод стратегического планирования — стратегии постепенного улучшения[1] остаются доминирующими в российских компаниях (71%). Динамика показателей за трёхлетний период хорошо отражает реакцию компаний на внешние факторы: высокая доля инновационных стратегий (23%) в 2023 году была вынужденной мерой. Компании радикально трансформировали архитектуру ИБ, реагируя на уход зарубежных вендоров и необходимость срочного импортозамещения.

[1] Согласно ГОСТ Р 54147–2010. Стратегический и инновационный менеджмент. Термины и определения:

- Инновационная стратегия строится вокруг новых, «прорывных» продуктов или решений. Новизна стратегии охватывает все основные составляющие: масштаб, облик и цели.
- Стратегия обновления является промежуточной между инновационной стратегией и стратегией постоянного совершенствования.
- Стратегия постепенного совершенствования предполагает постепенные небольшие изменения масштаба, облика и цели: выполнение в основном прежних операций, но в больших объемах и с незначительными изменениями используемых процессов.

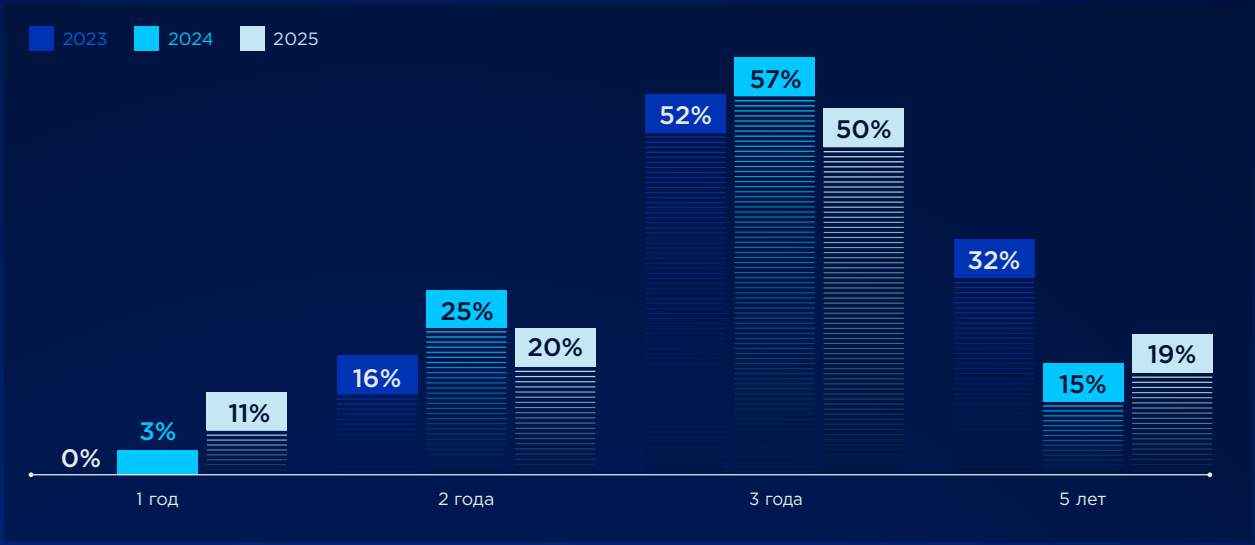
В 2025 году вектор сместился: вместо наращивания инвестиций компании вновь перешли к жёсткой приоритизации. Руководители ИБ фокусируются на планомерном улучшении и направлениях с максимальным влиянием на непрерывность бизнеса, тогда как долгосрочные инициативы откладываются.

Тип действующей стратегии ИБ



Самой популярной практикой остается трёхлетнее планирование, при этом тренд на «сужение» горизонта планирования продолжает укрепляться. Все больше руководителей ИБ выбирает краткосрочные тактические действия, планируя стратегию до года (10%).

Горизонт стратегического планирования в ИБ



Успех самой стратегии ИБ во многом определяется способностью руководителя ИБ показать измеримую ценность и «продать» целевой уровень ИБ бизнесу. При этом, хотя сам формат закрепления целевого состояния адаптируется под контекст конкретной организации, существуют универсальные подходы, часто используемые в индустрии:

- рост уровня зрелости;
- достижение бизнес-ориентированных метрик;
- снижение уровня рисков.

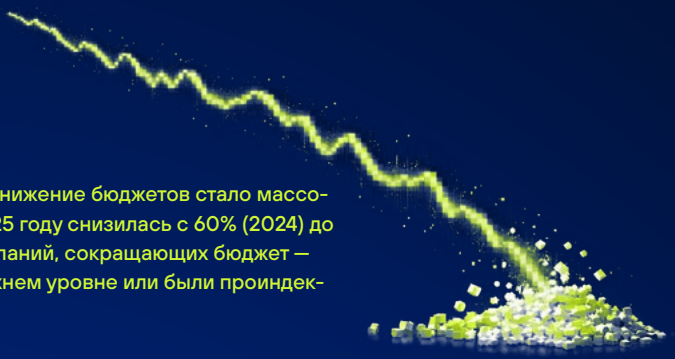
Постепенно набирает популярность подход через закрытие рисков «нулевой терпимости» (Zero Tolerance) — фокус на предотвращении недопустимых событий. Если в 2024 году практика формирования недопустимых событий была скорее исключением, то в 2025 году она была отмечена в 58% компаний. Через призму недопустимых событий бизнес-руководителям проще оценить риски в понятных критериях, например, остановка производства, утечка данных, потеря ключевых клиентов и другое. Наибольшую эффективность данный подход приобретает при подтверждении реализации недопустимых событий путем тестирования на проникновение.

Александр Танчук,

Руководитель отдела информационной безопасности, АО «Дикси Юг»

> Информационная безопасность обретает реальную ценность лишь тогда, когда говорит с бизнесом на одном языке. Язык угроз и уязвимостей должен быть переведён в язык цифр, выручки, потерь и управляемых рисков — в тот контекст, в котором топ-менеджмент живёт и принимает решения. Только в этом случае безопасность перестаёт быть абстрактной функцией и становится важным и неотъемлемым элементом стратегии бизнеса.

Бюджеты ИБ

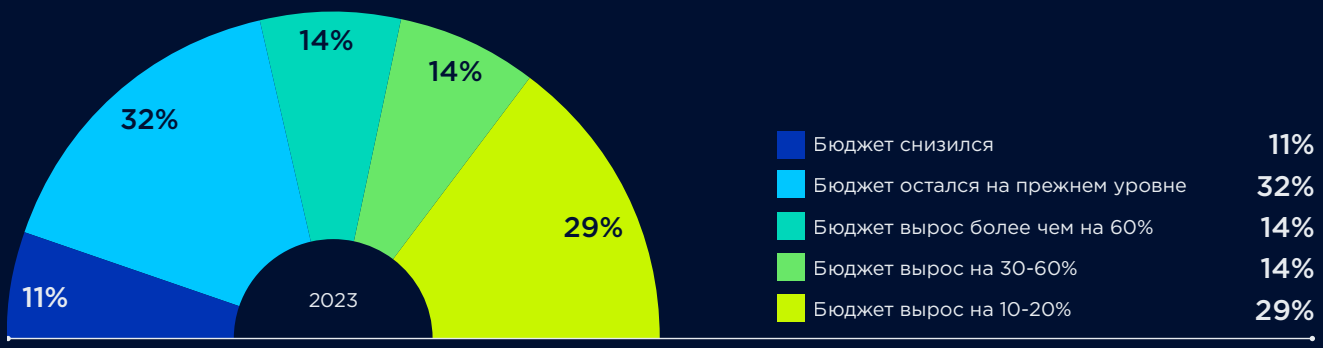


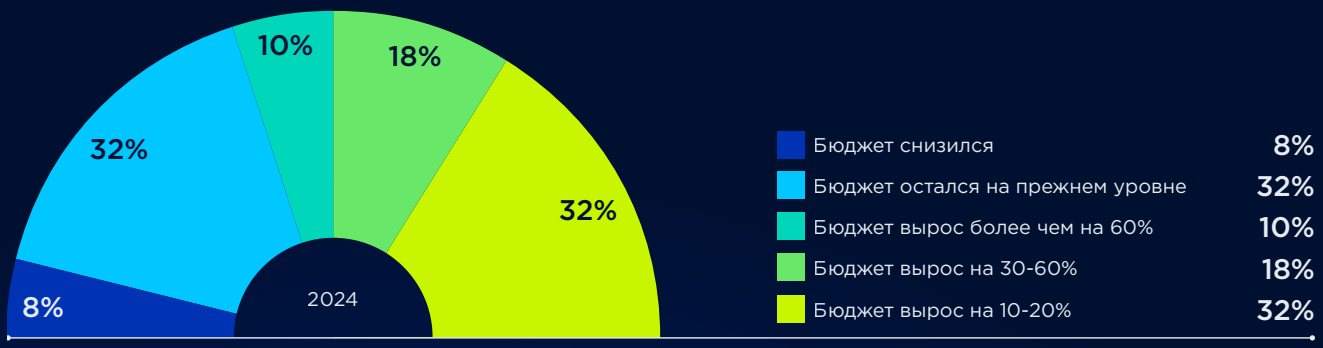
2025 стал годом бюджетного перелома — впервые снижение бюджетов стало массовым. Доля компаний с растущим бюджетом ИБ в 2025 году снизилась с 60% (2024) до 49% (2025), при одновременном удвоении доли компаний, сокращающих бюджет — с 8% до 20%. В основном бюджеты остались на прежнем уровне или были проиндексированы на уровень инфляции.

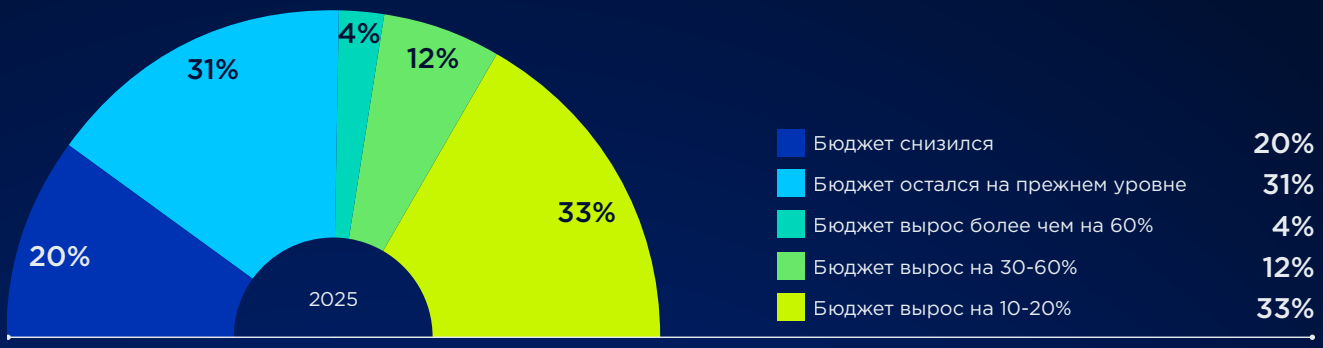
Компании, удваивающие бюджеты, практически исчезли, с 2023 года их доля снизилась с 14% до 4%. Подавляющее большинство среди таких компаний в 2025 году — постинцидентные. Затраты на восстановление после атаки требуют значительных инвестиций, для которых уже не требуется обоснования, ключевая цель — быстро восстановить операционную деятельность.

Промышленность, телеком и финансы возглавили рейтинг инвестиций в ИБ по итогам 2023–2025 годов. Это обусловлено совокупностью нескольких факторов: эти секторы входят в топ наиболее атакуемых целей [2] и попадают под жёсткие требования регуляторов как субъекты критической инфраструктуры.

Изменение бюджета на ИБ



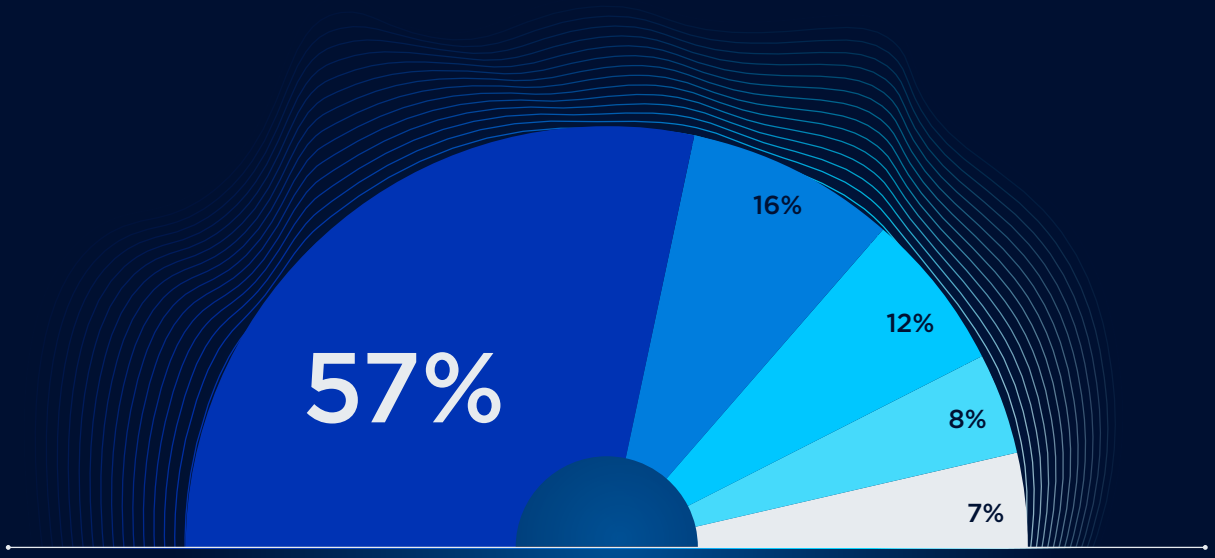




При этом даже фактор организационного подчинения службы ИБ не повлиял на рост бюджетов: службы ИБ в структуре ИТ-департаментов или служб безопасности ранее чаще сталкивались с ограничениями на финансирование, чем службы с прямым подчинением руководству. В 2025 году заморозка бюджетов затронула компании независимо от того, подчиняется ли ИБ совету директоров, ИТ-директору или руководителю службы безопасности.

Стоп-факторы при выделении бюджета (2025)

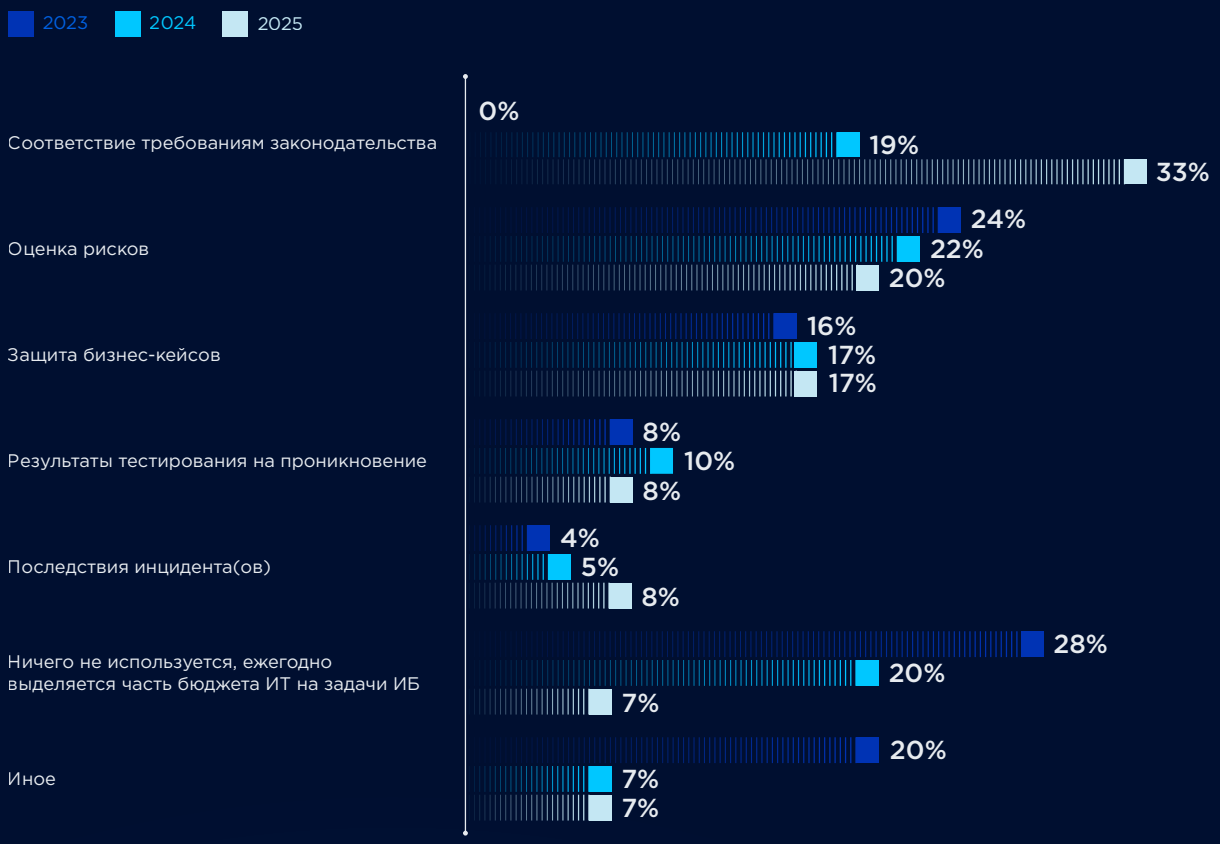
- **57%** Ограниченный бюджет компании
- **16%** Препятствия отсутствуют
- **12%** Недостаточный уровень информированности высшего руководства в вопросах ИБ
- **8%** Руководство не видит результата от ИБ
- **7%** Возможные потери в результате ИБ-рисков руководство считает меньшими по сравнению с затратами на развитие системы ИБ



Накопленные данные за три года наблюдения отражают значительную трансформацию подходов к обоснованию бюджета ИБ. Доля компаний, которые возвращаются к комплаенсу (включая требования по импортозамещению) как к основному аргументу для получения бюджета, выросла в 4 раза, ссылки на требования законодательства в 2025 году были весомым аргументом при общении с бизнесом.

Оценка рисков и формат через защиту бизнес-кейсов сохранили позиции в тройке лидеров (17% в 2025 году). При этом мы фиксируем исчезновение модели защиты бюджета «по остаточному принципу». В 2023 году каждый четвертый руководитель ИБ «отщипывал» кусок от ИТ-бюджета, к 2025 году таких компаний осталось всего 7%. Это во многом маркер зрелости рынка — функция ИБ всё чаще выделяется в отдельное структурное подразделение с прямым подчинением руководству и своей статьей расходов.

Основной инструмент обоснования бюджета на ИБ



Медианная доля бюджета на информационную безопасность в структуре ИТ-бюджета составила 10%

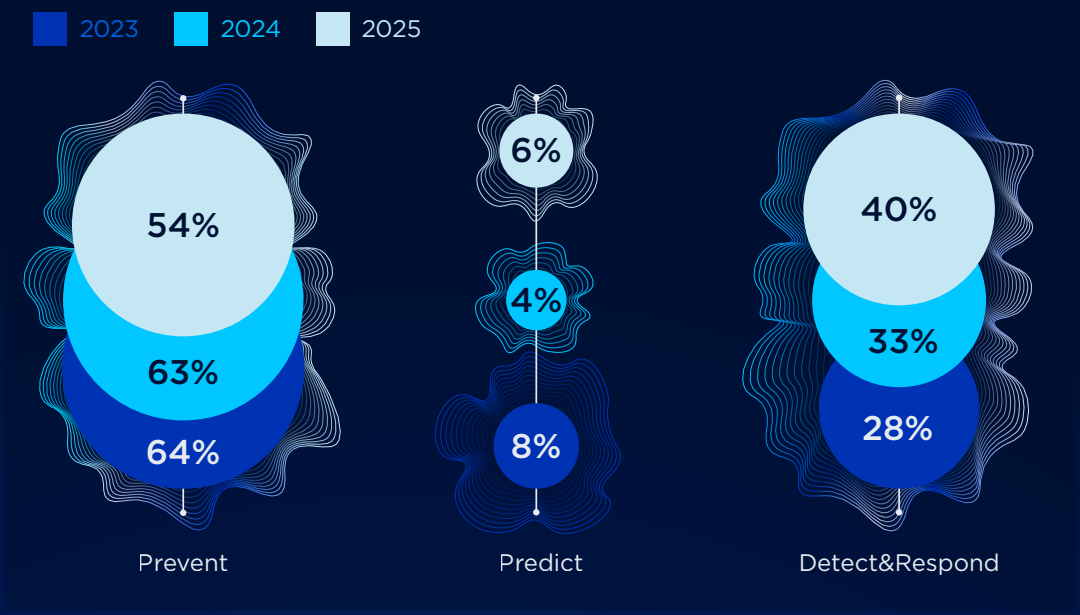
Показатель практически идентичен глобальному тренду: согласно отчету ENISA «NIS Investments 2025», международная медиана находится на уровне 9%.

Фокус бюджетирования на ИБ в 2025 году

В 2025 году мы фиксируем ускорение тренда, обозначенного ранее — рост бюджетирования функции Detect & Respond (обнаружение и реагирование). Компании постепенно переходят к сбалансированной модели бюджетирования обнаружения и предотвращения.

Хотя функция предотвращения остаётся крупнейшей статьей расходов, её доля постепенно снижается относительно других функций (64% -> 54%), однако растёт в абсолютном выражении. Доля обнаружения и реагирования выросла с 28% до 40%, что напрямую коррелирует с увеличением запросов на зрелые сервисы — SOC, киберучения, Threat Hunting. Доля прогнозной аналитики (Predict) колеблется на уровне 4–8%.

Наиболее финансируемый сегмент ИБ в компании



Наибольший спрос в 2025 году наблюдался по следующим направлениям:

- сетевая безопасность остаётся крупнейшим сегментом рынка: спрос на NGFW и сетевое шифрование продолжается на фоне импортозамещения, также повышается спрос на решения класса NTA и NAC — они активно используются не только для ИБ, но и для задач ИТ;
- защита от вредоносных кодов и целенаправленных атак развивается на фоне роста количества атак вирусов-шифровальщиков. Решения класса EDR постепенно становятся базовым элементом защиты и всё чаще интегрируются в SOC;
- мониторинг и реагирование. Всё больше компаний приходят к пониманию того, что без постоянного контроля и своевременной реакции средства защиты работают не в полную силу, поэтому SOC (собственный или аутсорсинговый) становится необходимой частью ИБ.

Отчёт по обзору рынка 2025

ОРГАНИЗАЦИЯ СЛУЖБЫ ИБ

Поиск кадров

В 2025 году рынок труда начал смещать фокус с оперативного реагирования, гиперспроса и массового найма на заморозку найма и оптимизацию. Многие компании сократили расходы и ушли в режим сохранения эффективности.

Работодатели вынуждены пересматривать бюджеты, оптимизировать штаты и фокусироваться на сохранении текущих сотрудников, при этом кадровые потребности большинства компаний так и остались не закрыты.

Большинство организаций (80%) испытывают потребность в специалистах по ИБ

Значительная доля респондентов оценивает кадровый дефицит более чем в 10 специалистов — за последние три года потребность в таком объёме выросла с 17% до 32%. За три года наблюдений насыщения рынка так и не произошло — медианное значение требуемых специалистов зафиксировано на уровне 8. Полностью укомплектован штат только у 11% компаний.

Зависимость количества специалистов ИБ, необходимых компании для полноценного покрытия операционных задач и развития функции ИБ, от общего количества работников в компании (2025)

Количество необходимых специалистов ИБ	Меньше 100 работников	от 100 до 500 работников	от 500 до 1000 работников	от 1000 до 2000 работников	Больше 2000 работников
1-3 специалиста	37%	89%	26%	25%	13%
4-10 специалистов	18%		8%	44%	23%
Больше 10 специалистов	16%	11%	33%	13%	45%
Дополнительные специалисты не требуются, штат ИБ полностью укомплектован	29%		25%	5%	9%
Сейчас нет понимания, сколько и каких специалистов нужно			8%	13%	10%

Наименьшее количество ответов — Наибольшее количество ответов

При этом с 2024 года сохраняется устойчивая отрицательная динамика количества открытых позиций. В половине компаний открыты только 1-3 вакантные должности, 46% компаний не имеют открытых вакансий вовсе, что отражает заметный разрыв между потребностями и фактическими возможностями найма.

В 2025 году рынок ИБ-кадров расслоился на два сегмента. Крупные компании (с численностью более 2000 сотрудников) продолжают вести точечный набор в пределах 1-3 вакансий, тогда как организации меньшего масштаба (менее 500 сотрудников) во многих случаях практически приостановили найм. Массовый подбор (более 4 вакансий) практически сошёл на нет.

Зависимость количества открытых вакансий специалистов ИБ от общего количества работников в компании (2025)

Количество вакансий	Меньше 100 работников	от 100 до 500 работников	от 500 до 1000 работников	от 1000 до 2000 работников	Больше 2000 работников
1-3 вакансии			57%	75%	52%
4-10 вакансий					5%
Больше 10 вакансий					
Открытых вакансий нет	100%	100%	43%	25%	43%

Наименьшее количество ответов — Наибольшее количество ответов

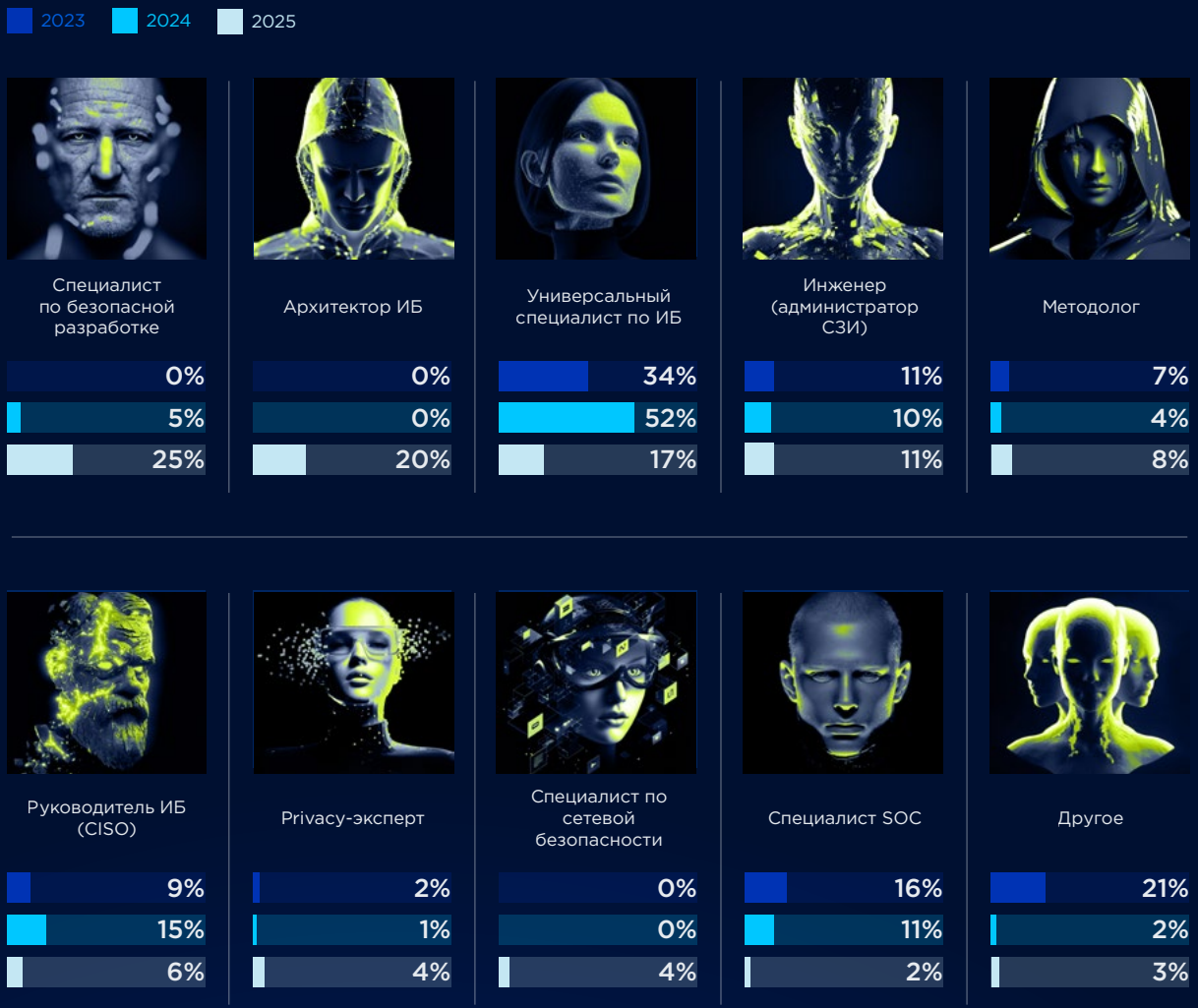
Ольга Ковардакова,

директор по работе с персоналом, «Инфосистемы Джет»

Рынок ИБ по-прежнему характеризуется дефицитом кадров, хотя в 2025 году мы наблюдали увеличение доступных для найма специалистов за счёт перераспределения кадров между крупными игроками рынка. При этом кандидаты, включая новичков, всё чаще приходят с ожиданиями быстрого карьерного роста, вовлечённости в сложные задачи уже на старте и высокими зарплатными ожиданиями. Работодатели, в свою очередь, подходят к расширению штата ИБ сдержанно и вынуждены искать баланс между потребностью в кадрах и требованиями к качеству.

В условиях оптимизации сместились и приоритеты работодателей — вместо количественного наращивания команд руководители ИБ концентрируются на привлечении редких и высококвалифицированных специалистов. На смену популярности универсальных специалистов приходит запрос на архитекторов ИБ и специалистов по безопасной разработке. Этот тренд напрямую связан с усложнением ИТ-ландшафта: ростом объёмов разработки, распространением контейнеризации и активным внедрением ИИ.

ИБ-специалисты, которых чаще всего искали

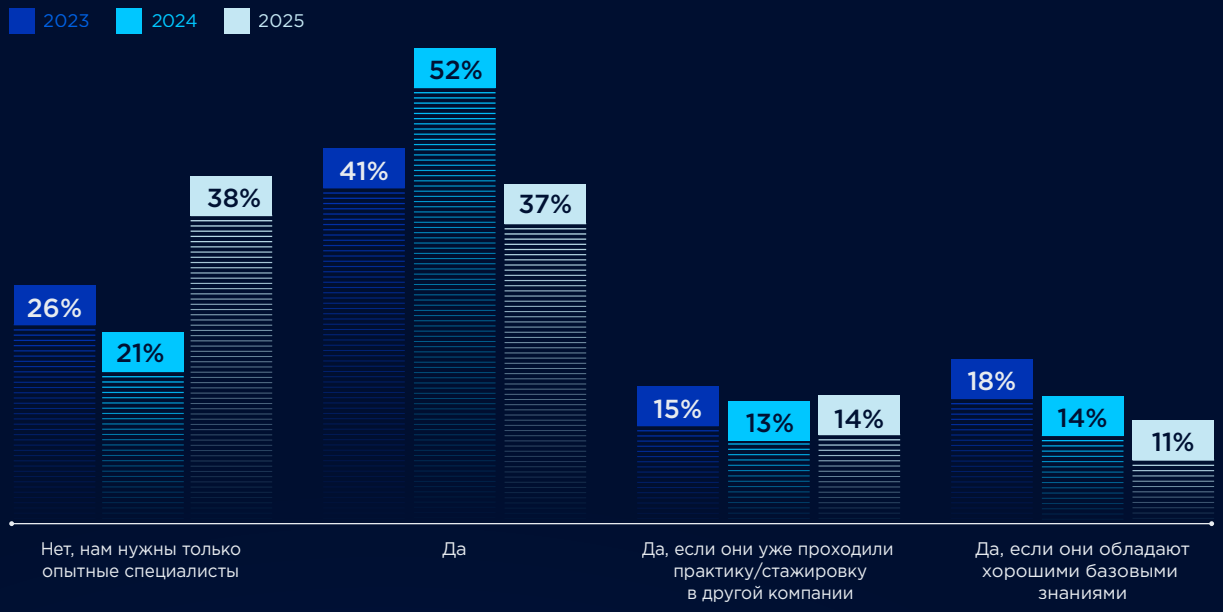


На фоне растущего спроса на узкопрофильных специалистов сместилась и ключевая проблематика найма: в 2025 году она была связана не столько с неконкурентоспособностью условий, сколько с нехваткой подходящих кандидатов на рынке. В ответ на дефицит экспертов выросли и сроки подбора: для специалистов по безопасной разработке, архитекторов ИБ поиск занимает около 6 месяцев, для специалистов по сетевой безопасности — 9 месяцев, поиск CISO зачастую превышает 1 год. Быстрее всего закрываются операционные позиции (SOC-специалисты первой линии, методологи, privacy-эксперты): минимальные сроки начинаются от 3 месяцев и редко превышают полгода.

Для большинства ИБ-ролей средний срок закрытия вакансий удерживается на уровне 5 месяцев

Из-за сдержанной политики найма компании всё меньше готовы брать студентов и предпочитают «готовых» специалистов, которых можно сразу включать в работу (38% против 21% в 2024 году). И если в 2023–2024 годы от работы со студентами чаще отказывались небольшие организации, в 2025 году практика распространилась и на крупный бизнес.

Готовность компаний брать в штат выпускников по ИБ-специальностям



Формирование команд

Масштаб компании, стадия её развития и размер штата ИБ соотносятся почти линейно. На компании с малым штатом (до 500 работников) приходится в среднем 1-2 специалиста по ИБ. В средних компаниях (от 500 до 1000 работников) штат специалистов по ИБ в среднем составляет 6-7 специалистов, а для крупных компаний — 17-18 специалистов.

9%

Доля ИБ-специалистов от количества специалистов ИТ-блока в 2025 году

На этапах «Юность» и «Расцвет» по модели Ицхака Адизеса команды ИБ минимальны или отсутствуют, что отражает приоритет бизнеса на рост и развитие над инвестициями в безопасность. Основная концентрация ИБ-специалистов наблюдается на стадии «Стабильность» — именно такие компании постепенно наращивают кадровый потенциал.

Зависимость размера команды ИБ от стадии развития компании по модели Ицхака Адизеса (2023–2025 годы)

Число работников ИБ	Юность	Расцвет	Стабильность
В компании нет работников ИБ	60%	39%	5%
От 1 до 3	40%	47%	7%
От 3 до 5		8%	6%
От 5 до 10		6%	8%
От 10 до 15			18%
От 15 до 20			22%
От 20 и больше			34%

В динамике трёх лет мы наблюдаем постепенное расширение ИБ-команд: более 5 специалистов в штате уже имеют 67% компаний, а доля компаний с более чем 20 специалистами по ИБ выросла с 22% до 31%. Полное отсутствие штата уже почти не встречается и составляет всего 4%, что является важным индикатором зрелости рынка в целом.

Количество небольших команд (1-3 специалиста) уменьшилось в два раза и составило 13%. Средний бизнес практически полностью ушёл от модели одного универсального специалиста на все задачи

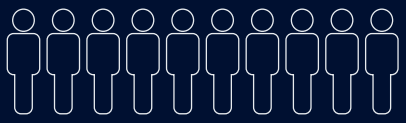
Финансовый сектор и ИТ сохраняют стабильно высокий уровень команды ИБ, подтверждая статус лидеров по штатной численности в ИБ[2].

[2] Данные по размеру штата ИБ в разных сферах бизнеса в 2025 году приведены в приложении.

Среднее число ИБ-специалистов в разных сферах бизнеса (2025)

>20

Финансовый сектор, ИТ и ритейл



5—10

Топливно-энергетический комплекс, промышленность, здравоохранение

10—15

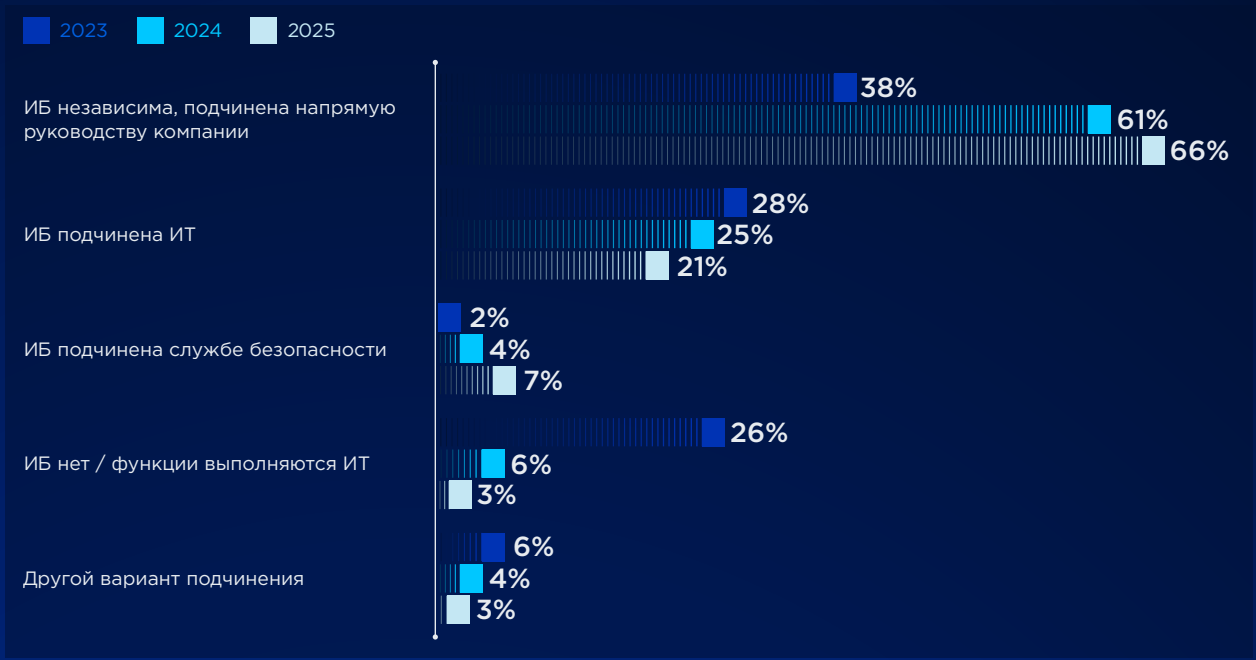
Промышленность

Структурная подчинённость

Подчинённость CISO остаётся ключевым фактором, определяющим бюджетные возможности и скорости принятия решений. В 2025 году доля прямого подчинения руководству стабилизировалась на уровне в 66%. В динамике трёх лет наблюдается небольшое перераспределение подчинённости от ИТ к службе безопасности (4% в 2024 году к 7% в 2025 году).

Отраслевой характер подчинения ИБ в целом сохранился. Финансовый сектор по-прежнему демонстрирует устойчивую практику прямого подчинения руководству. В остальных отраслях динамика подчинённости сохранилась на уровне прошлых годов.

Подчинённость подразделения ИБ



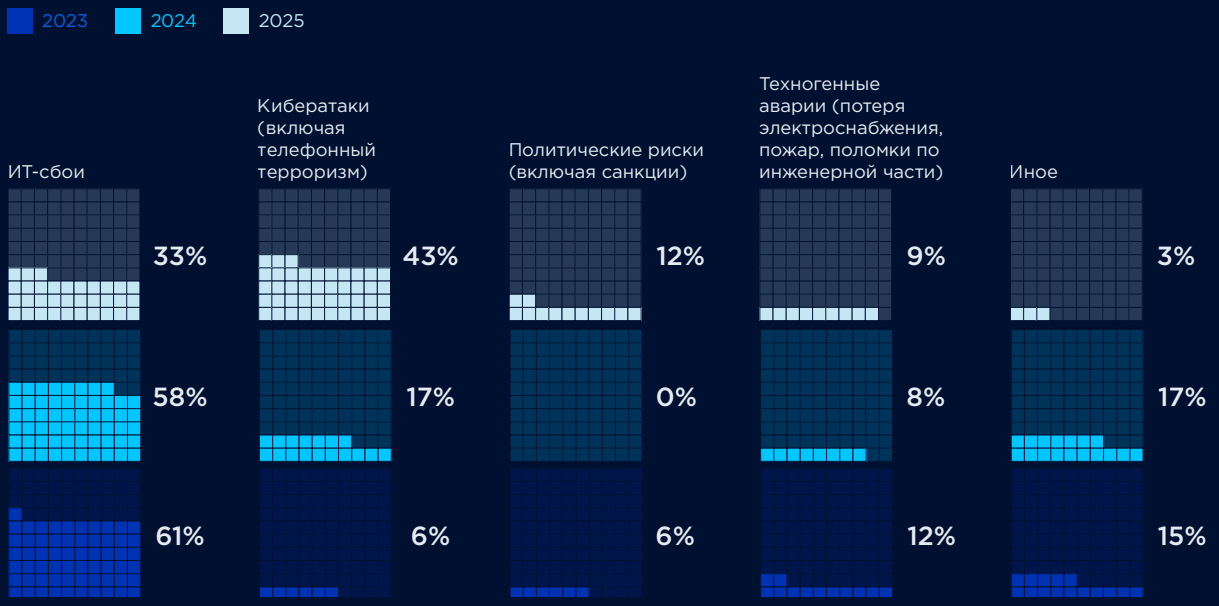
КИБЕРУСТОЙЧИВОСТЬ

Неизбежность кибератак и сбоев в работе ИТ-систем меняет подходы руководителей служб ИБ: смещается фокус на смягчение финансовых, операционных и репутационных последствий и быстрое восстановление. С практической точки зрения это требует зрелых практик управления непрерывностью бизнеса, кризисного реагирования, устойчивой архитектуры, проактивной проверки защищённости — того, что в совокупности формирует киберустойчивость. Именно эти компоненты станут фокусом данного раздела.

Классические риски нарушения деятельности организации всё больше отходят на второй план: в 2025 году кибератаки впервые обошли ИТ-сбои в нашем рейтинге рисков прерывания бизнеса (42% против 33%).

Динамика показывает практически двукратный рост с 2023 года и во многом обусловлена сменой тактики злоумышленников на деструктивные атаки (тактика «выжженной земли») и ростом медийного внимания к инцидентам: громкие кейсы активно обсуждаются в СМИ, повышая восприятие угрозы. Всё это даёт руководителям ИБ «окно возможностей» для диалога с бизнесом и обоснования инвестиций в ИБ как в гарантию выживания компании.

Каких рисков прерывания бизнеса больше всего опасается компания?



Мы наблюдаем ограниченность практик непрерывности бизнеса[3] на рынке: как правило компании подходят к их точечной реализации для ограниченной области. В половине опрошенных за три года компаний практики внедрены только для критичных бизнес-процессов (функций / услуг) или для некоторых ресурсов. В 40% компаний такой процесс либо не внедрён, либо только планируется к реализации.

Внедрение BCM без внешнего стимула, регуляторного давления или опыта реальных инцидентов, как правило, остаётся «бумажным» процессом. Только компании финансового сектора демонстрируют самую высокую практическую зрелость, что является следствием требований Банка России в части непрерывности и операционной надёжности. Также зрелые практики непрерывности бизнеса частично внедрены в промышленности и ИТ-компаниях.

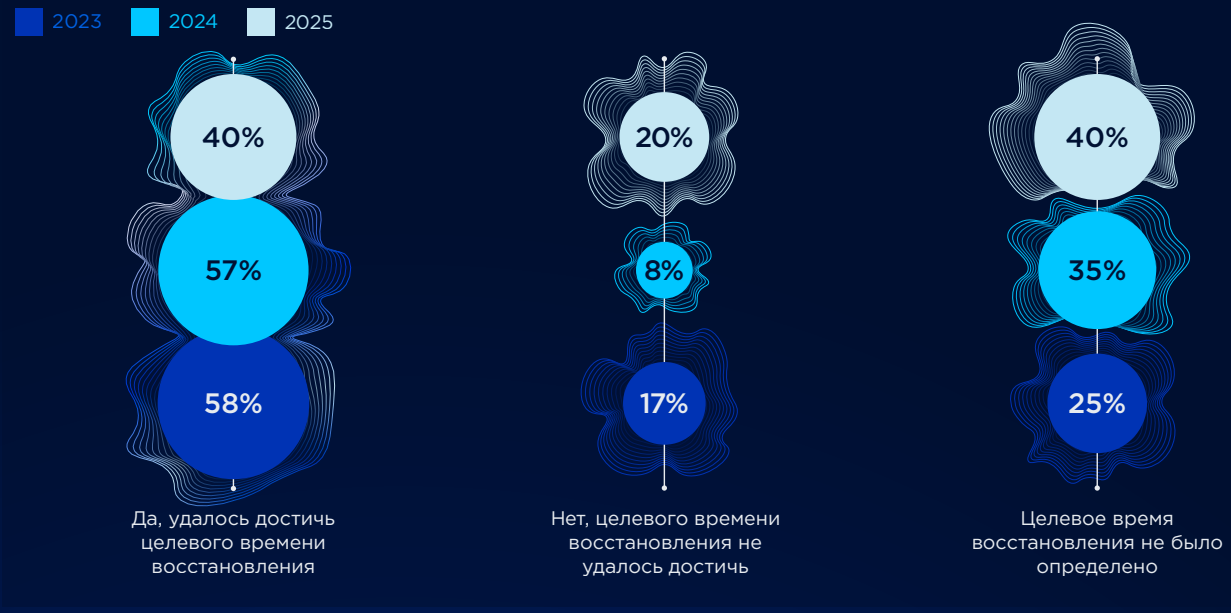
Область действия процессов обеспечения непрерывности бизнеса (данные по годам, 2023–2025 годы)

[3] BCM (Business Continuity Management) — управление непрерывностью бизнеса

При этом реальная операционная готовность к инцидентам большинства российских компаний остается низкой. В компаниях, в которых инцидент ИБ повлиял на операционную надёжность, в 2025 году только 40% смогли достичь ожидаемого времени восстановления. При этом в трети всех опрошенных за три года компаний такое целевое время так и не было определено, поэтому реальная цифра значительно ниже.

Снижение показателя достижения целевого времени восстановления по сравнению с 2023 годом связано с усложнением характера атак — от массовых к более целенаправленным, повышающим требования к реагированию.

Была ли компания готова к реализации рисков, связанных с непрерывностью?



Владимир Лапшин,

Руководитель службы внутренней информационной безопасности, АО «Инфосистемы Джет»

Киберустойчивость для нас — это про ответственность перед нашими клиентами. Выстроить равномерную защиту от компьютерных атак для всей сети — недостаточно: важно понимать, какие сценарии являются самыми опасными, и быть готовыми к любому из них. В 2025 году мы сосредоточились на практических мерах: мы выстроили защиту таким образом, чтобы снизить вероятность и степень влияния потенциального инцидента на наших заказчиков. Мы построили у себя отделённую от основной инфраструктуры систему, назначение которой — обеспечить чистую среду для защищённой удалённой работы с системами заказчиков.

Отдельной задачей для усиления антихрупкости было улучшение механизмов восстановления — от защиты резервных копий до полноценных учений по восстановлению без серьёзных последствий.

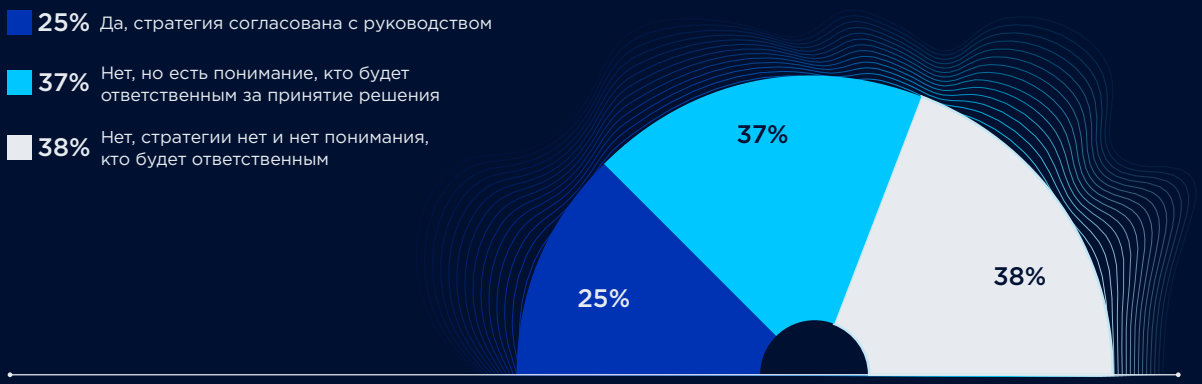
Владение процессом BCM, ранее традиционно закрепленным за ИТ, кардинально поменяло свою картину в 2025 году. Там, где BCM и инцидент-менеджмент управляются разными подразделениями без координации или исключительно ИТ, время восстановления после кибератаки значительно увеличивается. Понимая это, компании начали выстраивать синергию систем управления ИБ и непрерывностью бизнеса: доля компаний с совместной ответственностью ИТ и ИБ выросла в 5 раз с 2024 года и составила 30%.

Какое подразделение в компании ответственно за обеспечение непрерывности бизнеса?

Основным пробелом в реализации киберустойчивости остаётся отсутствие процесса сквозного реагирования и кризис-менеджмента — зрелость кризисного управления остается невысокой, и реагирование, как правило, происходит ситуационно. Только 35% компаний за все три года анализа имеют формализованный план кризисного реагирования, включающий роли, эскалацию и планы коммуникации.

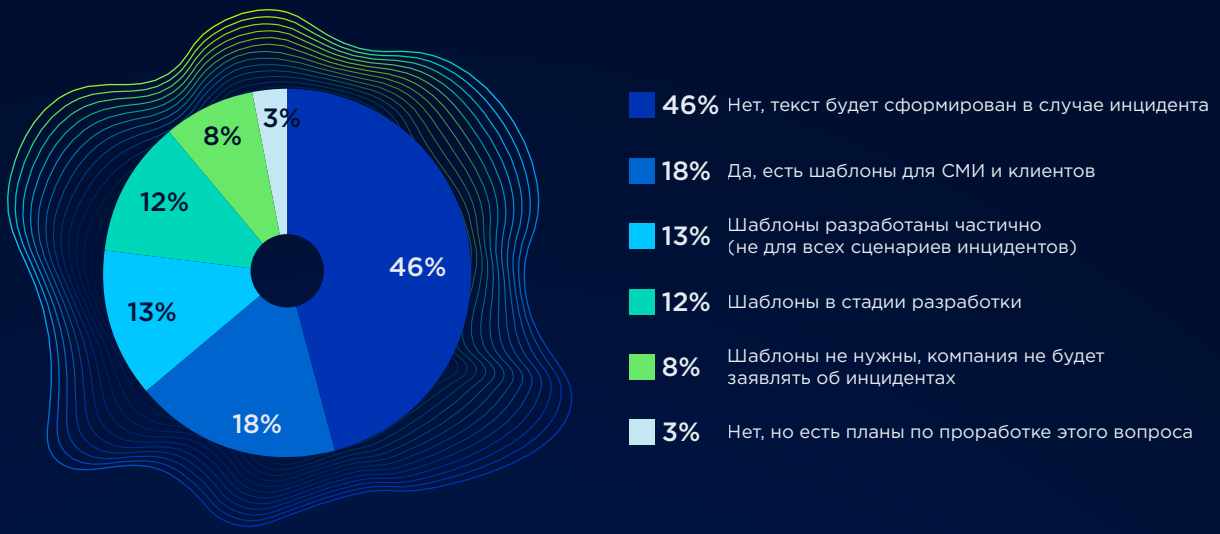
В 37% компаний есть понимание ответственности за принятие решения о действиях в случае требований выкупа (например, при атаке шифровальщика или похищении данных). При этом у 25% опрошенных такая стратегия уже формализована и согласована с руководством, что чаще всего характерно для компаний с наличием зрелого кризисного управления.

Есть ли в компании согласованная с топ-менеджментом стратегия действий на случай требования выкупа (2025)?



Начиная с 2022 года компании постепенно меняют отношение ко внешним коммуникациям: практика умалчивания инцидентов постепенно сходит на нет. Доля компаний, в которых шаблоны публичных заявлений находятся на стадии разработки или уже согласованы с PR-службой, составляет 43%.

Есть ли в компании согласованные шаблоны публичных заявлений на случай киберинцидентов (2025)?



Ещё одним ключевым фактором устойчивости является резервное копирование и восстановление данных. Под влиянием эпидемии шифровальщиков подходы к резервному копированию превратились в элемент управления киберрисками: создание отказоустойчивых, изолированных, защищённых от компрометации систем резервного копирования становится базовым элементом ИТ-архитектуры компании.

С начала 2025 года устойчиво формируется тренд на защищённые резервные копии: сами системы СРК в 2025 году стали ключевой целью злоумышленников. Компрометация таких систем позволяет саботировать процесс восстановления, получить доступ к критичным данным компании и уничтожить их. Создание защищённых хранилищ становится стандартным требованием при внедрении или модернизации СРК.

Наиболее распространёнными практиками по защите СРК и резервных копий в 2025 году стали следующие:

- использование ленточных библиотек для размещения изолированных копий, с обязательным регламентом ротации носителей;
- физическое изъятие лент из библиотеки и хранение их в местах с ограниченным доступом;
- формализованная процедура обмена, транспортировки и учёта носителей;
- применение системы хранения, где часть копий хранится в оперативных репозиториях, а критичные и долгосрочные — в более защищённых.

Кирилл Назаров,

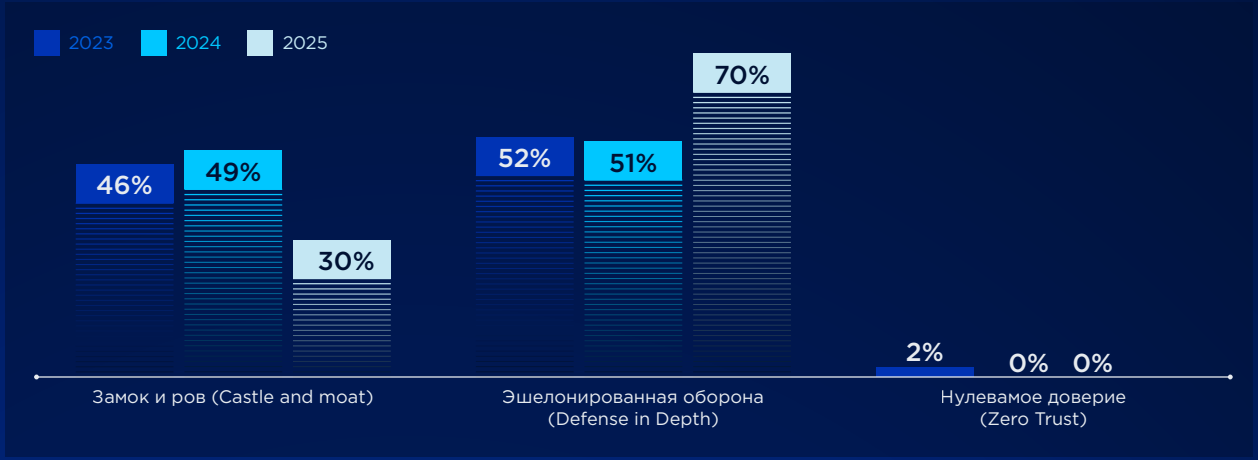
Руководитель отдела информационной безопасности,
ООО «ППР»

До 2022 года информационная безопасность во многом воспринималась бизнесом как теоретическая дисциплина — набор рекомендаций о том, как следует защищаться от потенциальных угроз. Сегодня ситуация принципиально иная: ежедневная работа в условиях постоянных атак, где каждое решение проверяется практикой, экспертиза формируется под давлением инцидентов, а потенциальные угрозы перешли в разряд вполне реальных. К этим вызовам добавляется ключевая задача — выстроить защиту, которая будет не только эффективной, но и экономически оправданной.

Рынок продолжает искать «серебряную пулю», способную разом снять все риски ИБ, однако такого универсального решения не существует. Устойчивость бизнеса достигается лишь через взвешенный баланс стратегий, инструментов, методов, правильно подобранных людей и выстроенных процессов.

Устойчивость организации также напрямую зависит от зрелости процессов управления архитектурой ИБ. Критически важно, чтобы она проектировалась с учётом особенностей бизнеса и ландшафта угроз и являлась неотъемлемой частью общей архитектуры организации. Начиная с 2023 года модель «Эшелонированной обороны» укрепила доминирование: 70% (2025) против 52% (2023). Российский бизнес постепенно уходит от устаревшей, основанной на превентивных периметровых мерах модели безопасности «Замок и ров».

Какая архитектурная модель лучше всего описывает подход к защите в компании?



При этом концепция Zero Trust не исчезла из фокуса, изменился горизонт её внедрения. В условиях технологического барьера (российский рынок не предлагает полноценных ZT-платформ), кадрового и бюджетного дефицита компании переориентировались на точечное внедрение отдельных принципов (ZTNA, микросегментация) и постепенное закрытие технического долга. Реалистичная оценка рынка: горизонт следующего десятилетия, а не тактическая задача на 2026 год.

Zero Trust невозможен без зрелого управления идентичностью, аналитики поведения пользователей, оркестрации политик и перестройки приложений. Пока компания не достигнет необходимой технологической зрелости, переход к ZT преждевременен.

Ещё одним ключевым фактором повышения устойчивости является харденинг. Для реализации базовой гигиены ИБ не всегда требуется внедрение большого числа средств защиты — грамотная настройка систем и ИТ-инфраструктуры создаёт дополнительные барьеры для злоумышленника, затрудняя его продвижение по сети. Это напрямую влияет на две критические метрики: растёт время успешной атаки (TTA), а время на реагирование и локализацию (TTR) — сокращается.

Лидером по использованию харденинга остаётся финансовая отрасль как одна из самых зарегулированных. Высокую зрелость также демонстрируют ИТ-компании: в этой отрасли технологии исторически являются ядром бизнеса. Для остальных отраслей картина с 2024 года практически не изменилась — только в четверти компаний утверждены стандарты конфигурирования и проводятся регулярные аудиты.

Существует ли в компании практика настройки компонентов ИТ-инфраструктуры в соответствии с лучшими практиками по безопасности?

Обеспечение киберустойчивости не ограничивается укреплением внутреннего периметра. Важным элементом становится проактивное управление безопасностью за периметром инфраструктуры. Примером таких практик служит мониторинг даркнета, позволяющий выявлять утечки данных, скрытые угрозы и информацию о готовящихся атаках до нанесения ущерба.

Начиная с 2024 года мы фиксируем рост интереса к кибервразведке и другим методам защиты вне ИТ-периметра: около 32% компаний уже используют такие сервисы для защиты своих активов, 20% пилотировали такой сервис.

Используется ли в вашей компании сервис кибервразведки?

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ, ИСПОЛЬЗОВАНИЕ СЕРВИСОВ И АВТОМАТИЗАЦИЯ

Управление по процессам

В компаниях с описанными и контролируемыми корпоративными процессами переход на процессное управление в ИБ постепенно становится базовой практикой. При этом всё ещё остаётся разрыв между «формализацией» и «эффективностью» — процессы ИБ описываются, но не автоматизируются и не измеряются.

Лидерами использования процессного подхода в ИБ являются финансовая отрасль и ритейл (более 70% опрошенных компаний этих сфер уже выстроили процессы). Для финансового сектора это объясняется ориентацией всей регуляторной базы (например, Положение 716-П ЦБ РФ) на процессный подход. Для ритейла высокий уровень вызван бизнес-необходимостью: он позволяет быстро масштабировать защиту при открытии новых точек.

Осуществляется ли управление ИБ при помощи процессного подхода?

Сервисное управление

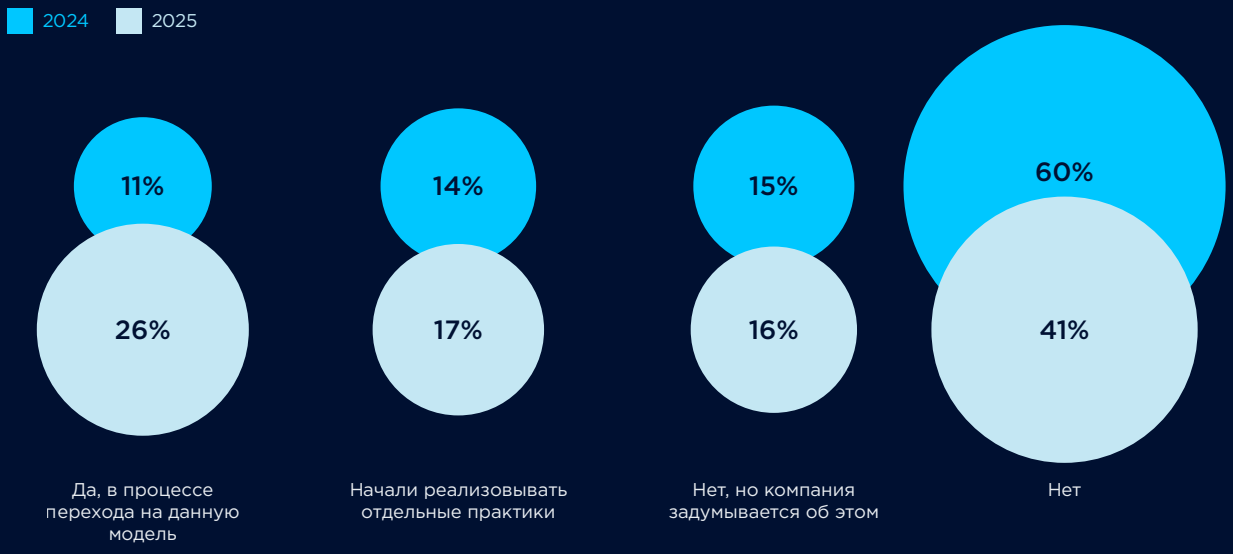
В условиях перехода крупного бизнеса и холдингов к централизованному управлению дочерними обществами и создания единой информационно-технологической архитектуры с системой планирования и контроля наблюдается рост популярности сервисного подхода в ИБ. Компании стремятся создать единую ИТ- и ИБ-архитектуру для снижения операционных и капитальных затрат, трансформируя подразделение ИБ во внутреннего поставщика услуг.

Подход «Безопасность как сервис» предоставляет бизнесу определённый каталог сервисов с фиксированными параметрами качества (SLA) на базе централизованного провайдера. Как правило, централизация функций осуществляется на уровне головной компании или выделенной ИТ-сервисной организации.

Ключевым фактором внедрения сервисного подхода является масштаб компании

Доля крупных компаний, постепенно внедряющих сервисный подход, выросла до 26% за два года наблюдений.

Используется ли в компании сервисный подход для обеспечения ИБ?



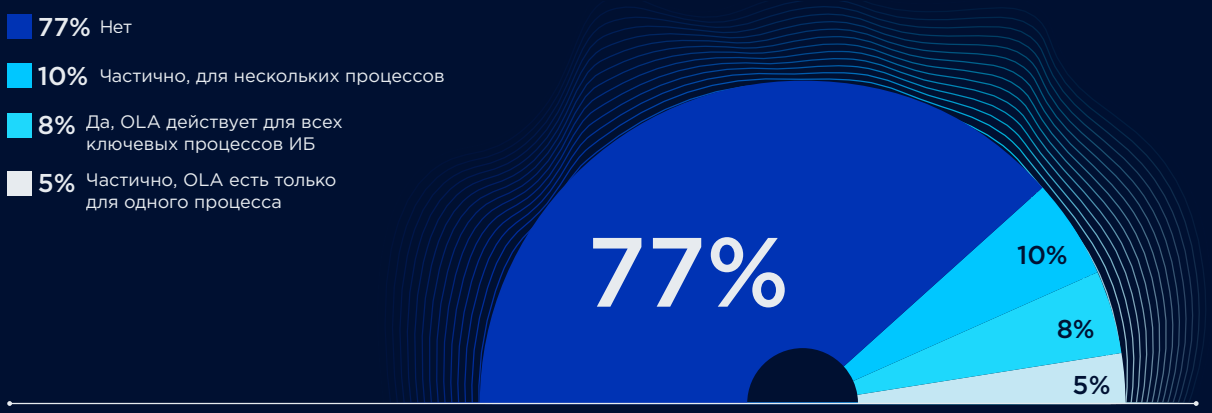
Александр Данченков,

Руководитель дирекции информационной безопасности, Группа Компаний «Русагро»

Когда информационная безопасность выстраивается как сервис, она перестаёт восприниматься как набор запретов и становится частью бизнес-системы, которая помогает компании безопасно развивать бизнес-инициативы. Вместо абстрактных требований бизнес получает понятные услуги с прозрачными метриками и ответственностью за результат. Такой подход превращает информационную безопасность в предсказуемый инструмент для поддержки и развития ИТ-систем с измеримой ценностью для бизнеса.

В этом случае важным инструментом является OLA (Operational Level Agreement), который описывает взаимодействие между подразделением и определяет конкретные условия предоставления услуг ИБ. Практика заключения OLA остаётся редкой для российского рынка в целом, чаще всего встречается в финансовом секторе и используется только в рамках некоторых конкретных процессов, например, в управлении уязвимостями.

Есть ли между подразделениями ИБ и ИТ зафиксированные OLA (накопительные данные за 2023–2025 годы)?



Использование MSSP

Отдельно необходимо выделить практику использования компаниями услуг по модели Managed Security Service Provider (MSSP). Лидирующими сервисами, отданными на аутсорсинг, по-прежнему остаются услуги центра мониторинга и реагирования на инциденты ИБ, поддержка СЗИ (средства защиты информации) и защита от DDoS. При этом впервые в выборку вошла и услуга выделения специалистов по ИБ, подтверждая пик кадрового дефицита в ИБ в 2025 году.

Используя управляемый сервис, компания переводит постоянные затраты в переменные. За счёт использования готовой инфраструктуры внешнего провайдера сокращаются накладные расходы на обеспечение деятельности собственных подразделений (например, затраты на закупку средств защиты информации, оплата труда специалистов).

Использование MSSP-сервисов (2025)

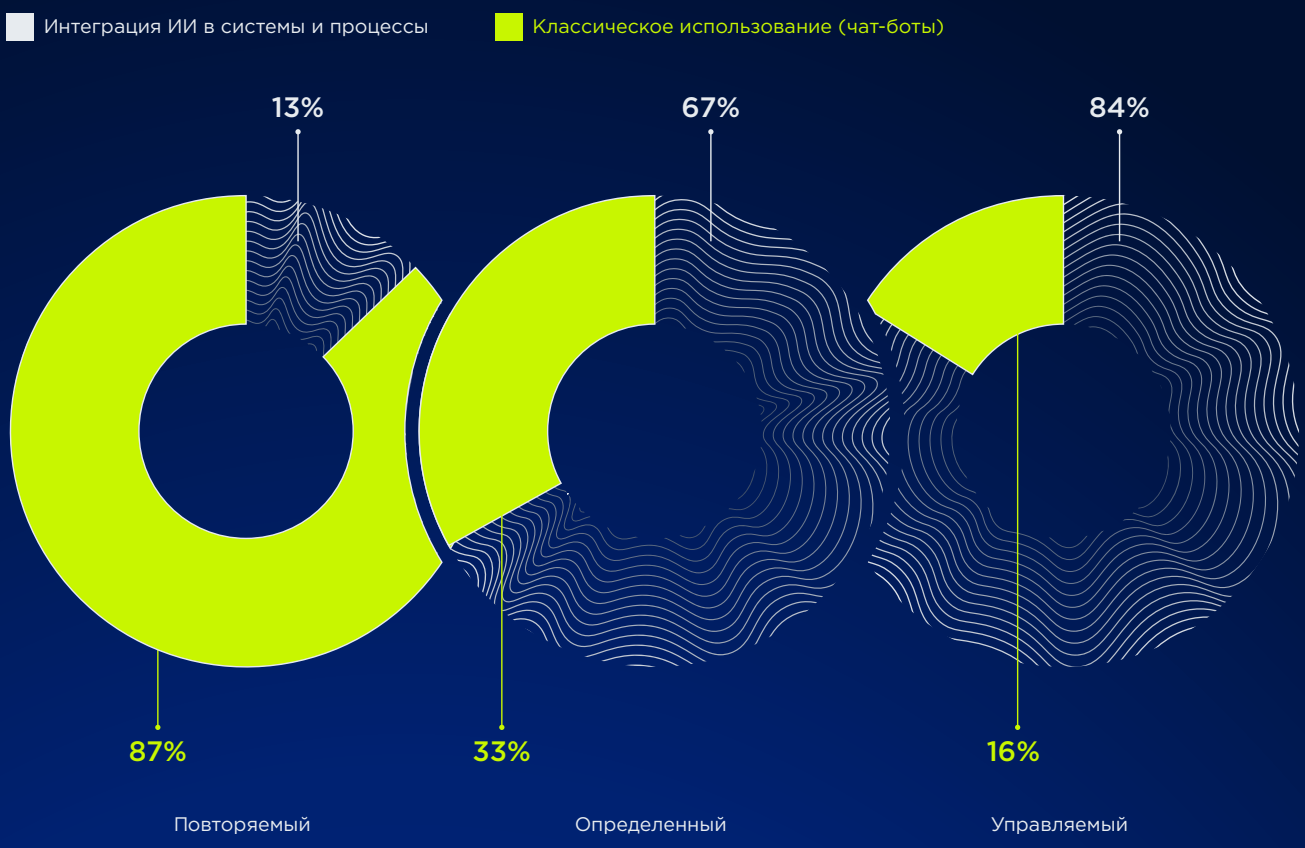
(Респондентам были доступны несколько вариантов ответа)

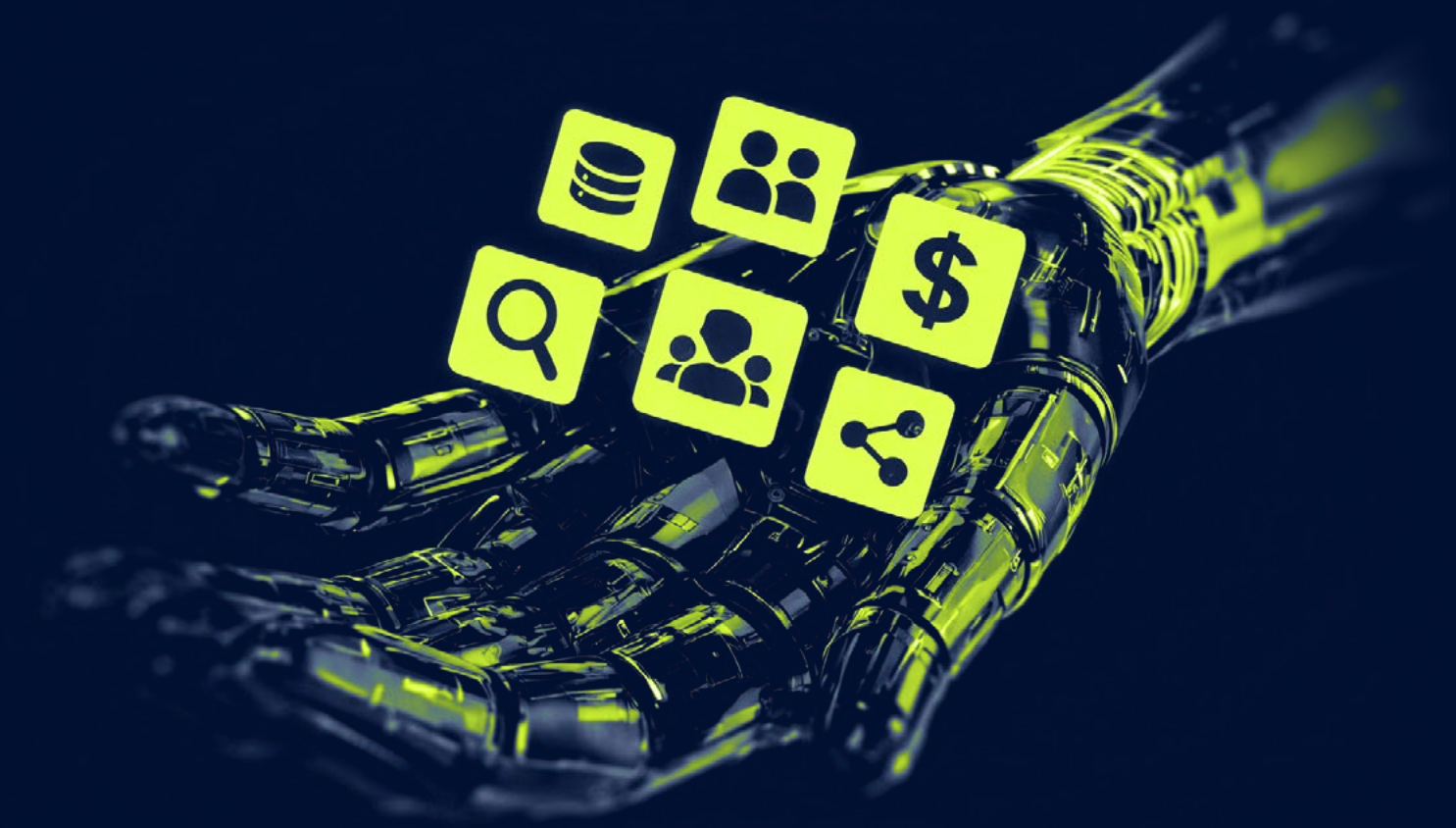
Автоматизация и ИИ

Тренд на использование генеративного искусственного интеллекта распространяется в том числе и на ИБ-отрасль. Доля компаний, использующих ИИ в работе, выросла с 3% в 2024 году до 27% в 2025-м. Основные цели использования можно разделить на два блока: решения по интеграции ИИ непосредственно в различные системы и процессы (например, ИИ-агенты по анализу кода, разработке правил корреляции для SIEM, приоритизации уязвимостей и так далее), а также классическое использование чат-ботов с целью обработки информации и получения рекомендаций по различным вопросам внутри службы ИБ. При этом цель использования ИИ напрямую коррелирует с уровнем зрелости: на повторяемом уровне ИИ больше используется как ассистент, а с определённого уровня зрелости — как инструмент автоматизации отдельных задач.

Доля компаний, использующих ИИ в работе, выросла с 3% в 2024 году до 27% в 2025-м.

Использование инструментов ИИ на различных уровнях зрелости процессов ИБ по модели CMMI (накопительные данные за 2024–2025 годы)



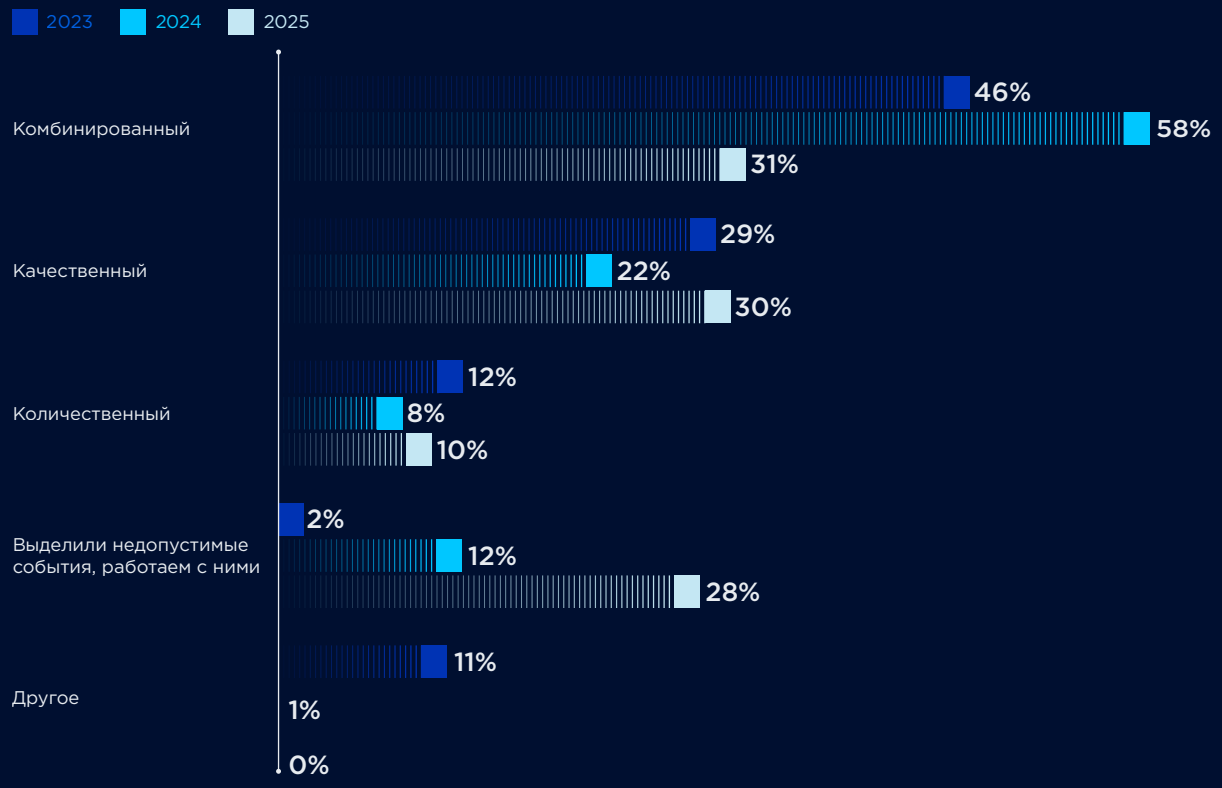


УПРАВЛЕНИЕ РИСКАМИ

Методологии оценки рисков ИБ

Выбор подходящей системы оценки рисков помогает руководителям ИБ обоснованно расставлять приоритеты, а топ-менеджменту — принимать взвешенные решения. Экономические аргументы остаются самой понятной для бизнеса формой обоснования инвестиций в ИБ, поскольку позволяют наглядно показать реальную стоимость инцидентов и бездействия при защите от них. Однако количественные методы оценки рисков ИБ применяются редко (только 10% компаний в 2025 году использовали количественную оценку рисков ИБ) из-за сложности расчёта потерь.

Метод оценки рисков ИБ



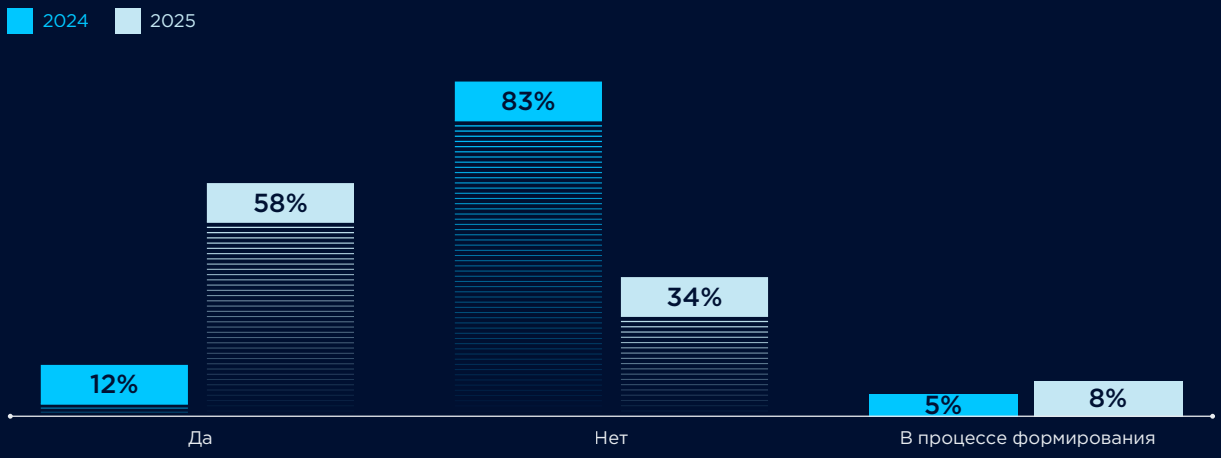
Сложные комбинированные методологии оценки рисков часто оказываются непонятны для бизнеса, поэтому всё чаще команды ИБ отходят от громоздких моделей риск-анализа к более бинарным форматам — сценарному анализу или определению недопустимых событий[4].

Процесс определения недопустимых событий позволяет фокусироваться не на технических деталях, а на наиболее критичных сценариях, способных нанести компании максимальный ущерб.

Больше половины опрошенных в 2025 году организаций (58%) уже определили недопустимые события для своего бизнеса.

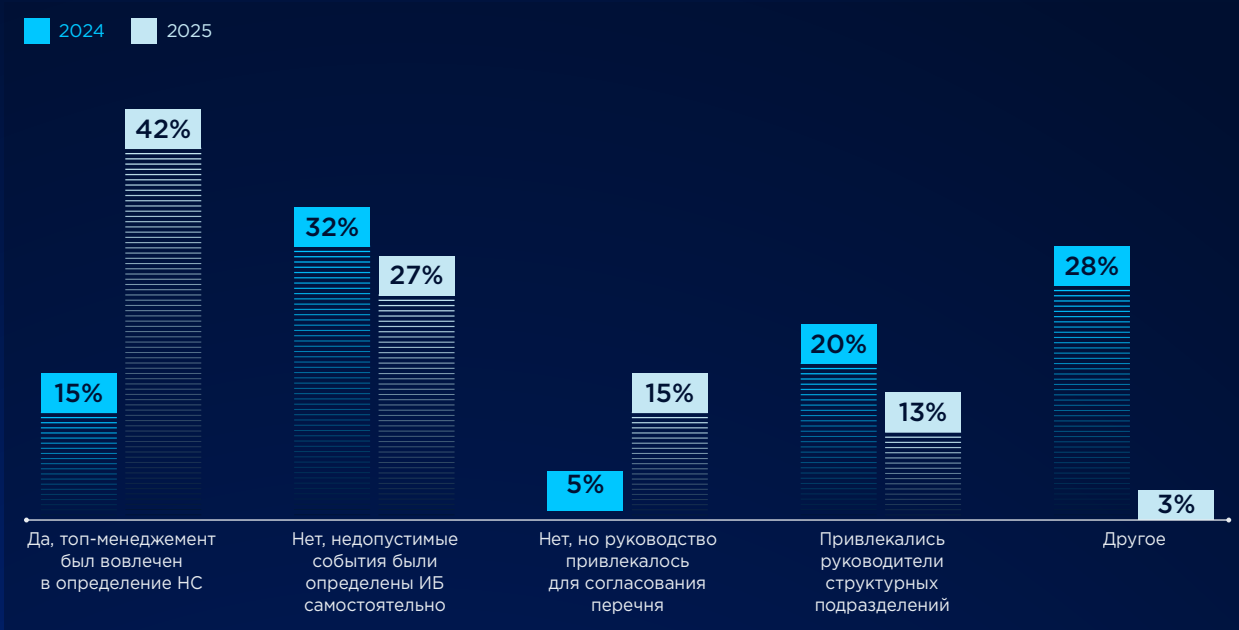
[4] Недопустимое событие — событие в результате кибератаки, делающее невозможным достижение операционных и (или) стратегических целей организации или приводящее к значительному нарушению её основной деятельности.

Доля компаний, которые определили для себя недопустимые события



В соответствии с методологией недопустимых событий, к процессу их определения должно привлекаться высшее руководство организации, поскольку оно имеет широкое понимание целей организации и знает, какие события могут нанести критический ущерб. По сравнению с прошлыми периодами, в 2025 году заметно выросло число компаний, вовлекающих руководство на этапе определения недопустимых событий (42%) или согласования (15%).

Привлекалось ли руководство компании для определения недопустимых событий?



Чтобы перейти от абстрактных рисков «потери данных» к практической защите, в мировой практике широко распространён подход, основанный на угрозах (Threat-Driven Security). Здесь ключевым инструментом становится MITRE ATT&CK: анализ тактик и техник противника позволяет выйти за рамки гипотетических сценариев.

MITRE ATT&CK — база знаний о тактиках и техниках злоумышленников, разработанная некоммерческой организацией MITRE Corporation.

Проект можно использовать в различных процессах обеспечения безопасности, таких как моделирование угроз, оценка уязвимостей, тестирование на проникновение, учения Red Team и другие.

В 2025 году мы спросили респондентов, в каких сценариях они применяют матрицу MITRE ATT&CK. Четверть респондентов используют проект для оценки текущих возможностей по обнаружению распространённых тактик и техник атакующих. Как правило, такая аналитика уже существует в правилах обнаружения по умолчанию, часть (11% опрошенных) использует проект для выбора контрольной среды против актуальных методов атакующих.

Используется ли вами матрица MITRE ATT&CK (2025)?

Ещё одним методом, позволяющим управлять рисками ИБ, является киберстрахование. Страхование закрывает вопрос финансовых последствий, когда инцидент всё же произошёл.

В 2025 году в бюджетах на ИБ появились принципиально новые статьи расходов. Одним из заметных изменением стало киберстрахование: около 4% опрошенных компаний уже приобрели полисы страхования, а 22% компаний задумаются об этом.

Всё больше страховых компаний предлагают продукты для защиты от киберрисков, а спрос подогрели атаки шифровальщиков и массовые утечки клиентских данных. Для бизнеса страхование становится способом снизить финансовые потери.

Киберстрахование в России пока остаётся инструментом, доступным преимущественно для крупного бизнеса, прежде всего в финансовом и промышленном секторах. До массового спроса пока далеко — полисы остаются дорогими, андеррайтинг — сложным и непрозрачным.

Риски третьих сторон

Риски взаимодействия с подрядчиками часто недооцениваются из-за сложившихся доверительных отношений. На практике именно это приводит к отсутствию контроля за действиями внешних специалистов и игнорированию рисков ИБ. Компании, оказывающие аутсорсинговые услуги, зачастую ограничены в ресурсах и не имеют зрелых практик ИБ, поэтому становятся удобной точкой входа для атак через цепочку поставок.

По итогам нашего исследования, в 2025 году именно компрометация подрядных организаций стала одним из наиболее распространённых векторов проникновения в инфраструктуру компании (23% от всех сценариев) и получения злоумышленниками критичных данных.

Максим Осипов,

Начальник отдела по информационной безопасности, Светогорский ЦБК

Для нас при работе с подрядчиками принципиально важно видеть системные инвестиции будущего партнёра в кибербезопасность. Сегодня это не просто формальность, а жизненная необходимость, позволяющая избежать значительных рисков и финансовых потерь. Мы наблюдаем позитивную динамику: растёт понимание важности контроля за подрядчиками на рынке, усиливается внимание к соответствию стандартам и лучшим практикам. Рынок активно развивается, предлагая всё новые специализированные сервисы — от мониторинга цифрового периметра до углублённой оценки уровня информационной безопасности контрагентов. Это позволяет нам не только повышать собственную защищённость, но и формировать надёжную экосистему сотрудничества.

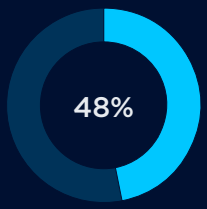
Важным этапом безопасной работы с подрядчиками является их предварительная оценка ещё на стадии выбора. Такая оценка помогает заранее выявить возможные риски и определить дополнительные меры защиты собственной инфраструктуры.

Результаты опроса показывают небольшой рост доли компаний, которые используют анкеты для предварительной оценки подрядчиков (с 16% до 20%), и компаний, которые проводят аудиты для наиболее критичных подрядчиков (с 36% до 38%).

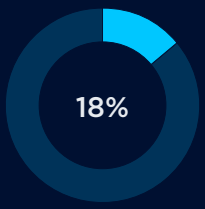
Большая часть опрошенных компаний имеет комбинированный подход, состоящий из нескольких мер, направленных на снижение риска взаимодействия с подрядными организациями. Наиболее распространённой практикой является закрепление правил безопасного взаимодействия — заключения NDA (48%), включения в договор требований по ИБ (10%) и процедур оповещения об инцидентах (10%). При этом наиболее строгие требования к взаимодействию с подрядчиками, как правило, устанавливают холдинговые компании, имеющие большое количество дочерних структур.

Какие меры принимаются в компании по безопасному взаимодействию с третьими лицами (2025)?

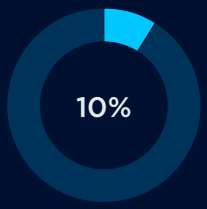
(Респондентам были доступны несколько вариантов ответа)



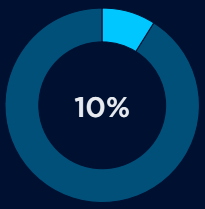
Заключение NDA с третьими лицами (не персонифицированный)



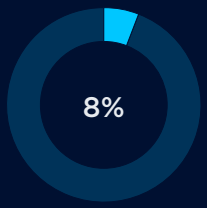
Контроль блокировки доступа по истечении срока договора



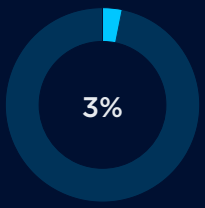
В договора с третьими лицами включены требования по ИБ (помимо NDA)



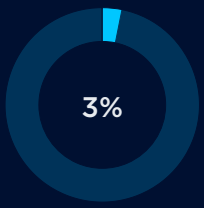
В договора с третьими лицами включаются процедуры оповещения об инцидентах



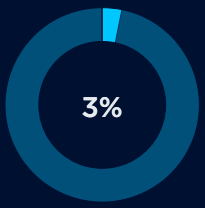
Осуществляется контроль действий подрядчиков с помощью PIM/PAM



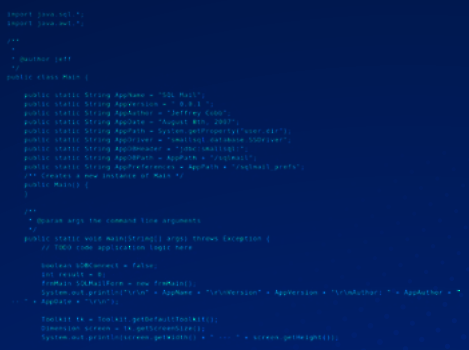
Персональных NDA для работников подрядных организаций

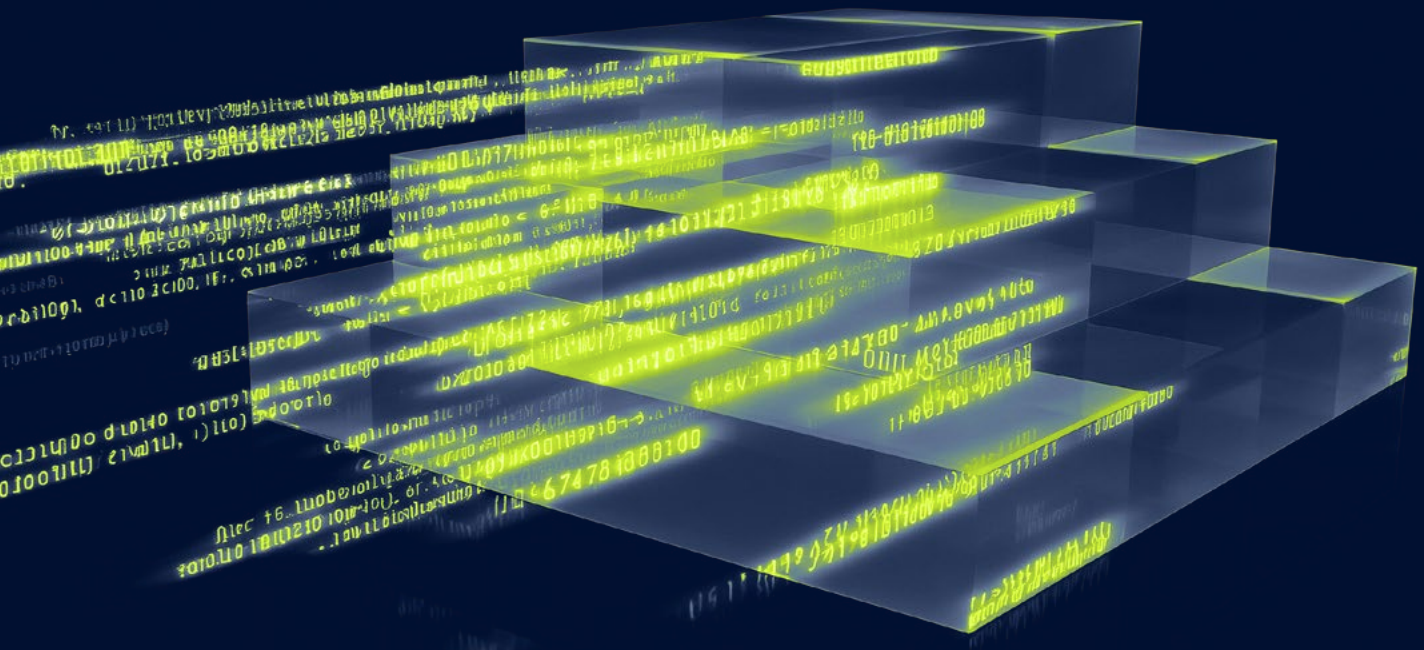


В договорах предусмотрены штрафные санкции за нарушение требований ИБ



Меры не принимаются





ОЦЕНКА СВОЕГО УРОВНЯ ИБ И ОТЧЁТНОСТЬ

Отчётность по ИБ обычно дифференцируется в зависимости от аудитории и уровня принятия решений. Мы будем рассматривать три уровня: операционный, тактический и стратегический.

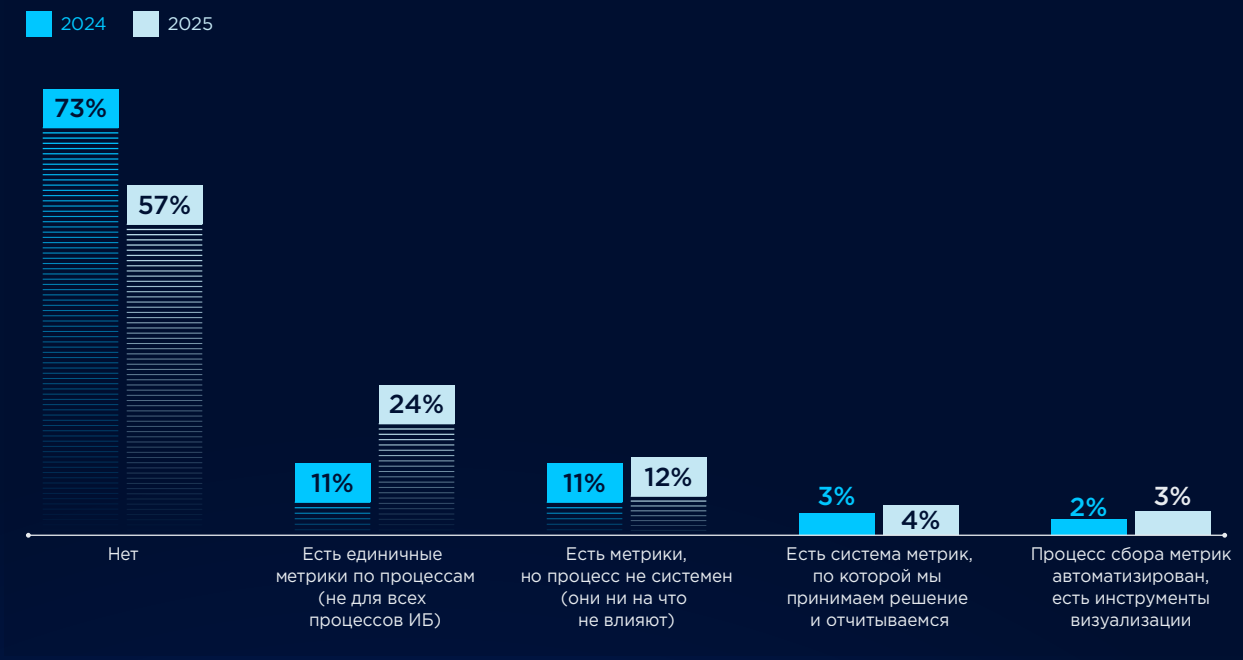
Операционный уровень

Для получения оперативной информации о состоянии процессов, как правило, используются систематизированные качественные или количественные индикаторы — метрики. Анализ данных опроса за три года отражает поступательное движение организаций от полного отсутствия каких-либо метрик к их единичному внедрению.

Доля компаний, у которых система метрик ИБ отсутствует, сократилась в сравнении с 2024 годом — с 73% до 57%. При этом процент компаний, которые используют полноценную систему метрик для принятия решений о функционировании ИБ, остается низким (4%).

Набор метрик всё ещё фрагментарный: компании начинают с внедрения простых изолированных показателей (24%), которые собираются вручную. Ручной сбор метрик и их анализ ведут к быстрому устареванию собранных данных и требуют ресурсов для их сбора и обработки, однако автоматизация сбора остаётся наиболее сложным этапом и также не стала массовой — остаётся уделом небольшого числа зрелых компаний (3% в 2025 году).

Используется ли в компании единая система метрик для отслеживания эффективности ИБ?



Тактический уровень

На данном уровне информация о состоянии процессов и результаты контрольных процедур, как правило, агрегируются в сводную периодическую отчётность для предоставления руководству.

К 2025 году отчётность перед C-level стала де-факто стандартом для российского рынка: доля таких компаний выросла с 72% до 88% с 2023 года. Одновременно сократилась доля организаций, где отчётность отсутствует или остаётся на уровне подразделения: с 28% до 11%.

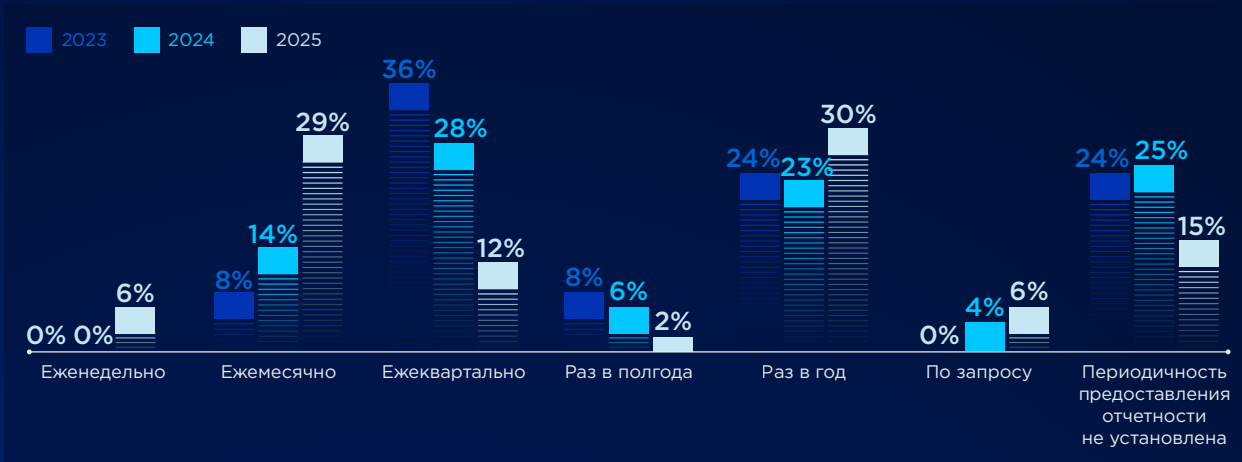
Полученные цифры подтверждают тренд, отмеченный Всемирным экономическим форумом в своём исследовании «Elevating Cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs»: переход службы ИБ из категории «технаря в подвале» в сторону бизнес-партнёра.

Для кого подготавливается отчётность по результатам работы ИБ?

Предоставление отчётности руководству становится более регулярным и частым. В 2025 году ежемесячная отчётность (29%) впервые обогнала ежеквартальную (12%). Руководители хотят видеть ситуацию в моменте, и месяц — идеальный горизонт для контроля эффективности тактических задач и повышения скорости принятия решения. При этом сохраняется стабильный спрос на ежегодные сводки (30%).

Мы впервые зафиксировали долю еженедельной отчётности (6%). Как правило, это постинцидентные компании или организации из регулируемых отраслей, где руководство держит «руку на пульсе», а сам формат носит временный характер.

Как часто осуществляется отчётность ИБ для руководства?



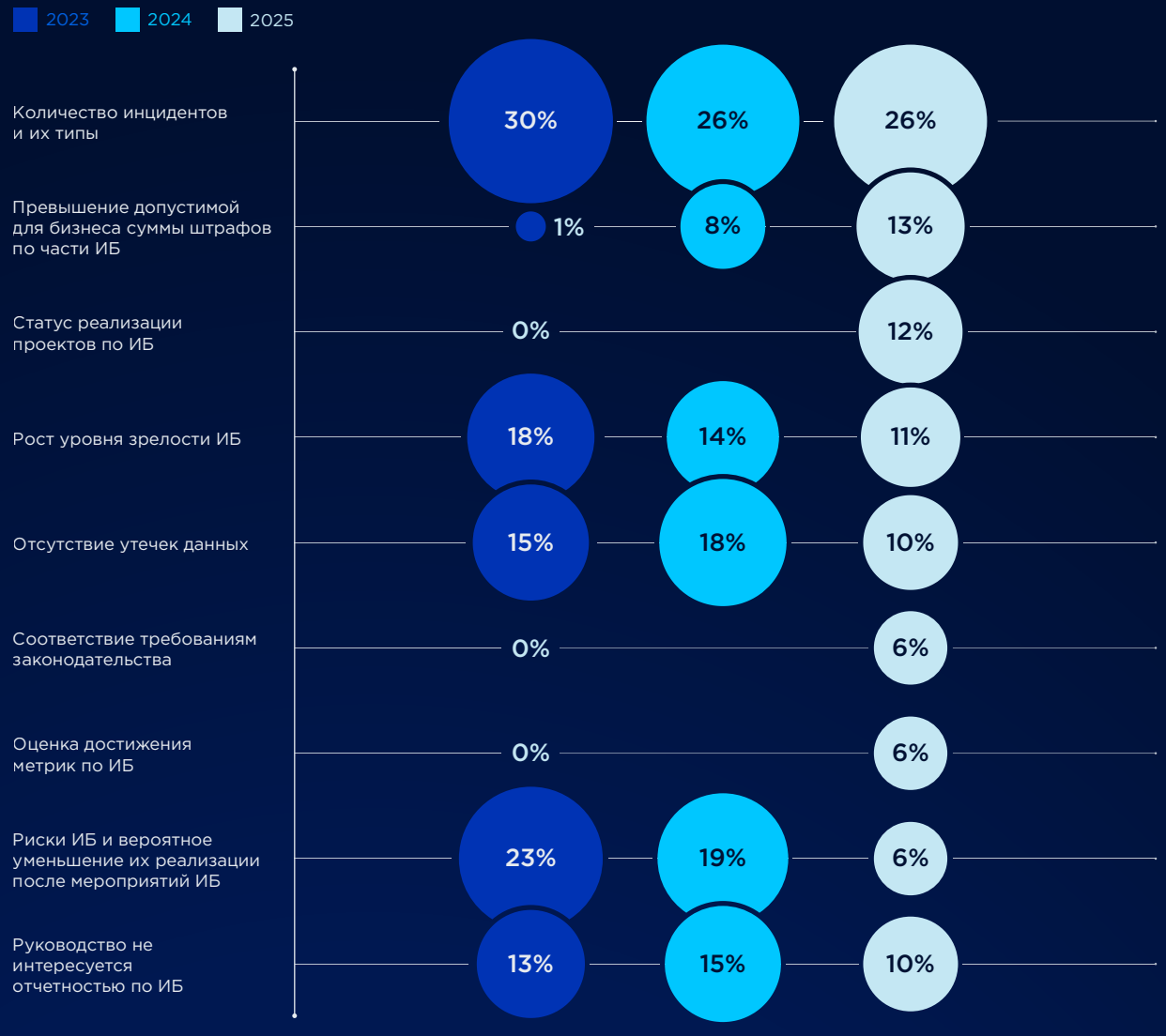
Денис Соколов,

Руководитель информационной безопасности, ООО «Нордголд Менеджмент»

> В структуре крупного холдинга регулярная отчётность помогает структурировать работу ИБ и увидеть её развитие в динамике. Отчётность помогает системно фиксировать достигнутые результаты (от внедрения новых средств защиты до повышения уровня зрелости процессов), продемонстрировать руководству реальные изменения в безопасности и определить, какие шаги уже дали результат, а какие — остаются в фокусе внимания на следующий период.

В части содержания отчётности в 2025 году мы отмечаем появление новых категорий, которые отсутствовали в предыдущие годы: оценка достижения метрик, статус проектов и регуляторный комплаенс. Накопительные данные за три года отражают снижение интереса к «технической» отчётности и сложным рискам, которые зачастую непонятны бизнесу.

Какой показатель больше всего интересует руководство компании?



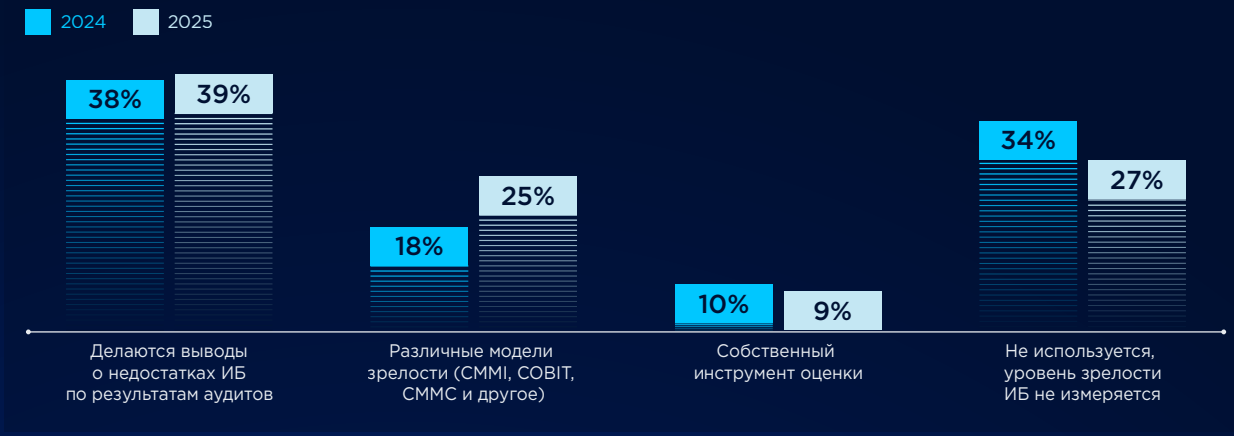
Стратегический уровень

В рамках стратегического уровня компании используют различные инструменты измерения существующего уровня ИБ в качестве консолидированного показателя для верхнеуровнего измерения прогресса и сравнения себя с рынком.

Ключевыми инструментами оценки эффективности ИБ остаются упрощённые западные модели зрелости (CMMI, COBIT) (27%), большая же часть (39%) компаний делает выводы о недостатках ИБ по результатам аудитов.

Растущий интерес к моделям зрелости отражает запрос рынка на объективность и сравнимость. При этом на рынке существует дефицит адаптированных, локализованных «линеек» для оценки зрелости. Собственные же инструменты оценки используют ограниченно только зрелые компании (9%).

Какой инструмент используется в компании для измерения существующего уровня ИБ?



Для оценки уровня зрелости процессов опрашиваемых нами компаний мы используем упрощённую качественную шкалу CMMI. Подавляющее большинство компаний (64%) находятся на стадиях «Начальный» (32%) и «Повторяемый» (32%), где процессы ИБ либо хаотичны, либо стандартизированы частично и зависят от конкретных исполнителей. Бюджетная оптимизация и заморозка найма тормозят переход на более высокие уровни зрелости.

Оценка текущего уровня ИБ по модели CMMI (средний показатель на основе накопленных данных за 2023–2025 годы)

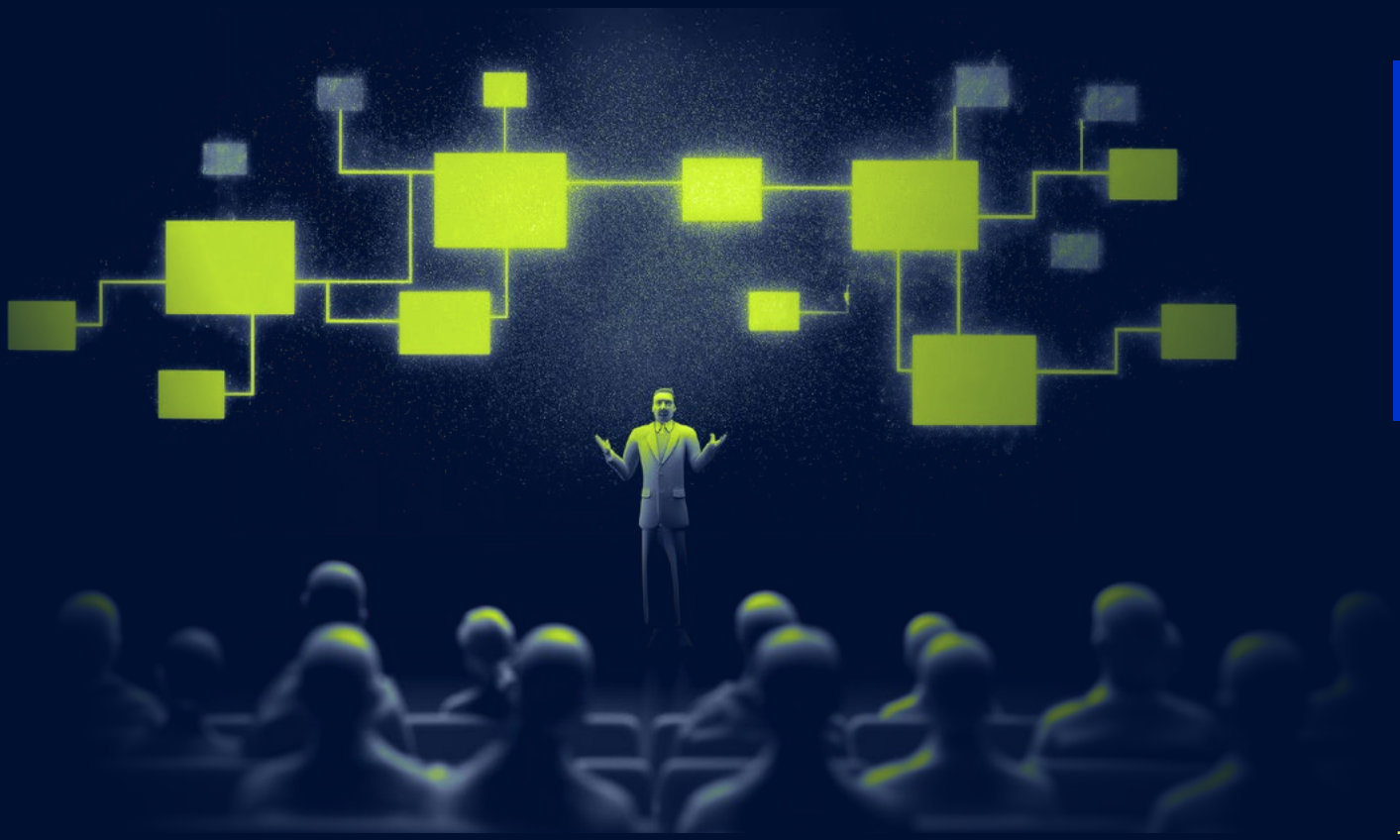
Совместный анализ данных по уровню зрелости и численности штата выявляет прямую связь: уровень зрелости ИБ растёт вместе с размером команды.

Небольшие команды до 5 человек, как правило, обеспечивают начальный и повторяемый уровень ИБ. Коллективы численностью 10-20 специалистов способны повысить ИБ до определённого уровня. Порог масштаба команды ИБ для устойчивой зрелости — минимум 20 ИБ-специалистов.

Зависимость зрелости процессов ИБ (по модели CMMI) от размера команды ИБ (накопленные данные за 2023–2025 годы)

Число работников ИБ	Нулевой	Начальный	Повторяемый	Определённый	Управляемый
От 1 до 3					
От 3 до 5					
От 5 до 10					
От 10 до 15					
От 15 до 20					
От 20 и больше					

Наименьшее количество ответов — Наибольшее количество ответов



КИБЕРКУЛЬТУРА

Для оценки уровня зрелости повышения осведомленности мы используем упрощённую модель зрелости на базе SANS, которая является адаптацией международных практик. Данная модель является инструментом оценки развития процесса.

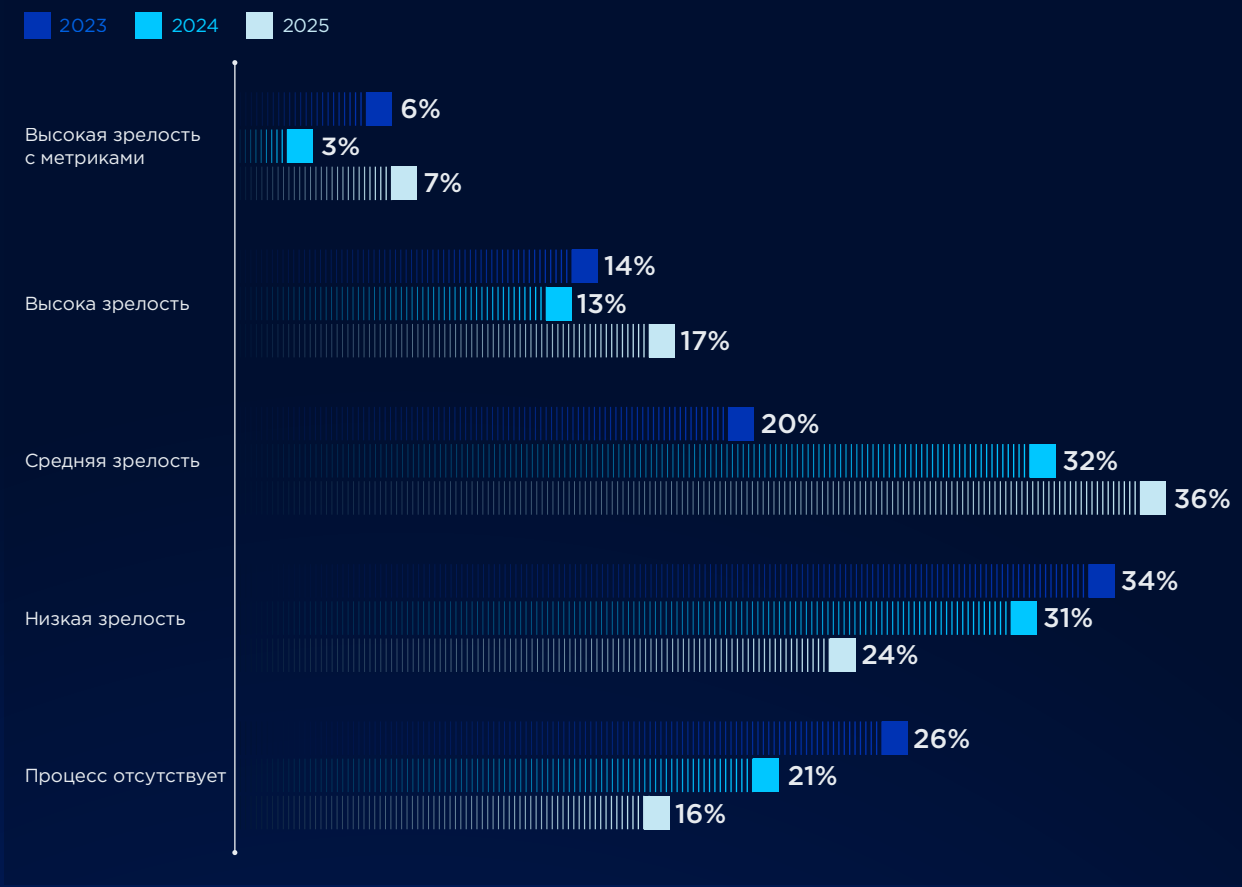
Общепризнанные модели оценки зрелости (Metacompliance[5] 3, SANS[6] 4 и KnowBe4[7] 5), как правило, характеризуются схожими уровнями роста зрелости процесса: от формального обучения «для галочки» к устойчивой культуре безопасности.
На начальных уровнях зрелости обучение по ИБ носит эпизодический характер и чаще связано с выполнением требований регуляторов. По мере развития процесс становится системным — появляются регулярные тренинги, сегментация контента и практические проверки знаний (например, антифишинговые учения).
На более высоких уровнях фокус смещается с обучения на управление поведением сотрудников: используются метрики, анализируются риски человеческого фактора, усиливается поддержка со стороны руководства. На максимальной стадии безопасность становится частью корпоративной культуры, а программы осведомлённости превращаются в постоянный управляемый процесс.

[5] Cyber Security Behavioural Maturity Model
[6] Security Awareness & Culture Maturity Model
[7] Security Culture Maturity Model

С 2023 года заметно увеличилась доля организаций со средним и высоким уровнями зрелости процесса — с 40% до 60% суммарно по нескольким уровням зрелости.

Одновременно сократилась доля компаний с низким уровнем зрелости и его отсутствием (с 60% до 41%), что указывает на постепенный переход организаций от базовых и фрагментарных практик к более системному развитию программ повышения осведомлённости.

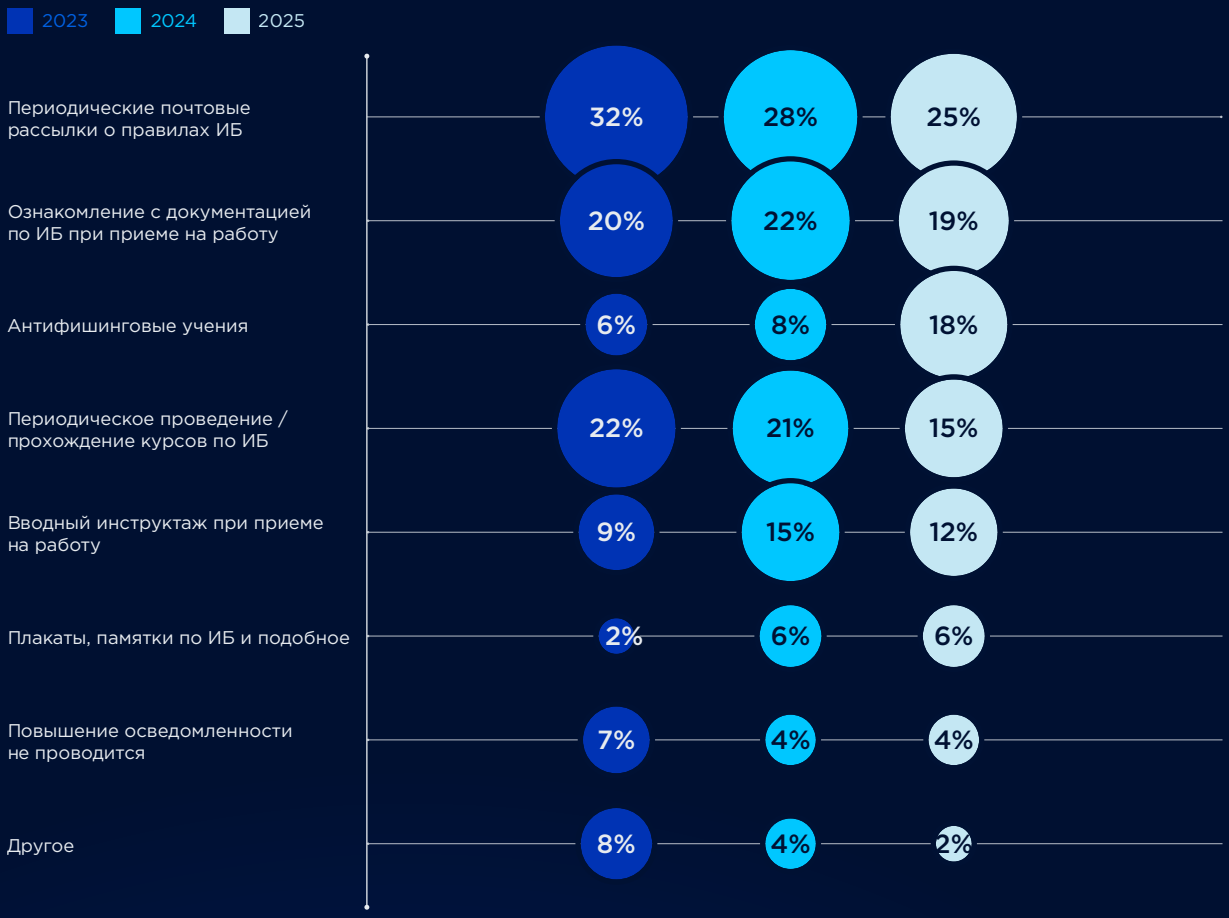
Оценка уровня зрелости процесса повышения осведомлённости



Наиболее распространёнными методами повышения осведомлённости остаются базовые практики — рассылки о правилах ИБ в почте (25%) и ознакомление с документацией по ИБ (19%). Мы отмечаем рост системности проведения обучающих мероприятий и их сегментирование под конкретные риск-группы работников. При этом доля организаций, в которых повышение осведомлённости не проводится, остаётся на уровне 4%.

Способы повышения осведомлённости работников в области ИБ

(Респондентам были доступны несколько вариантов ответа)



Владимир Лапшин,

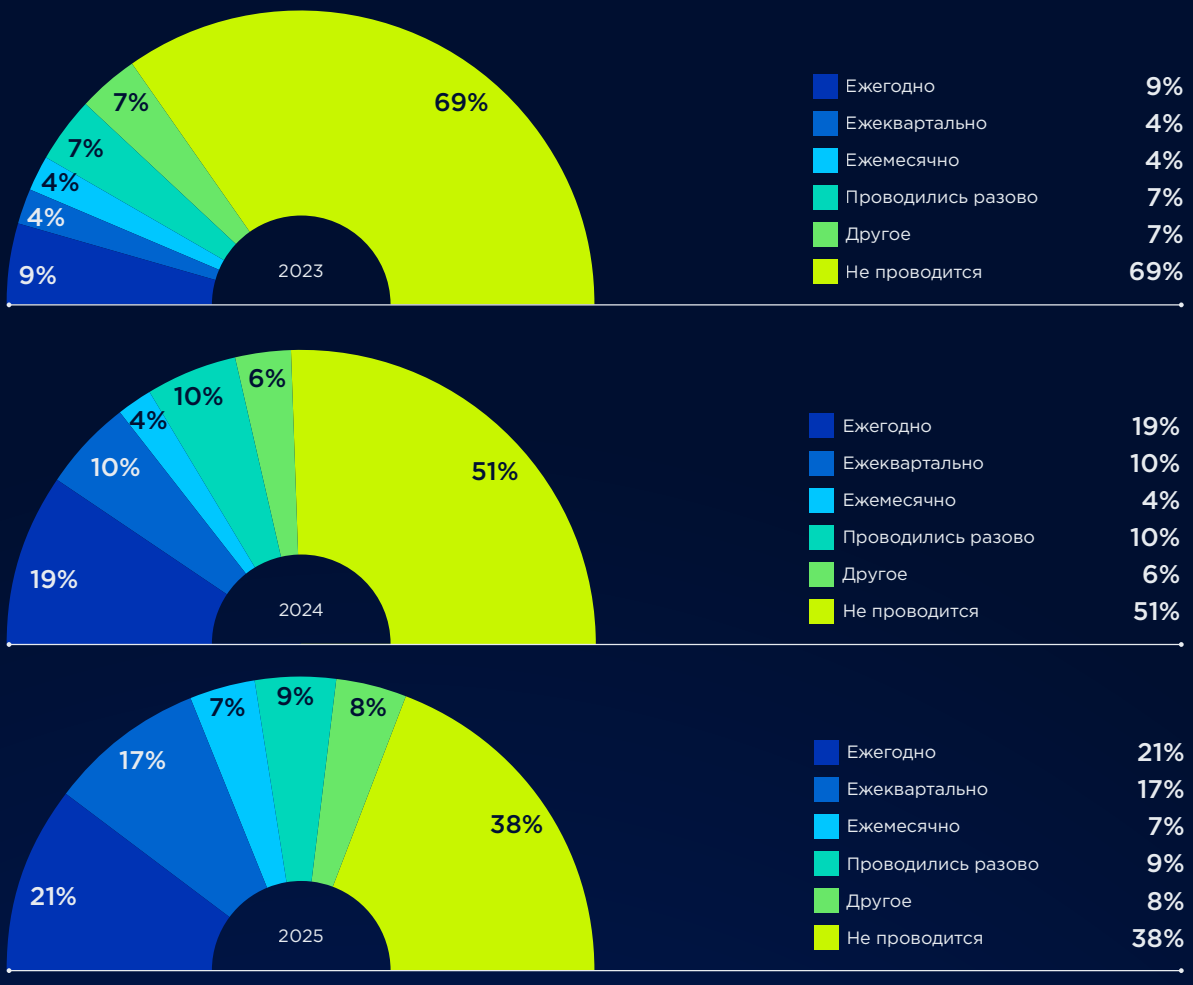
Руководитель службы внутренней информационной безопасности, АО «Инфосистемы Джет»

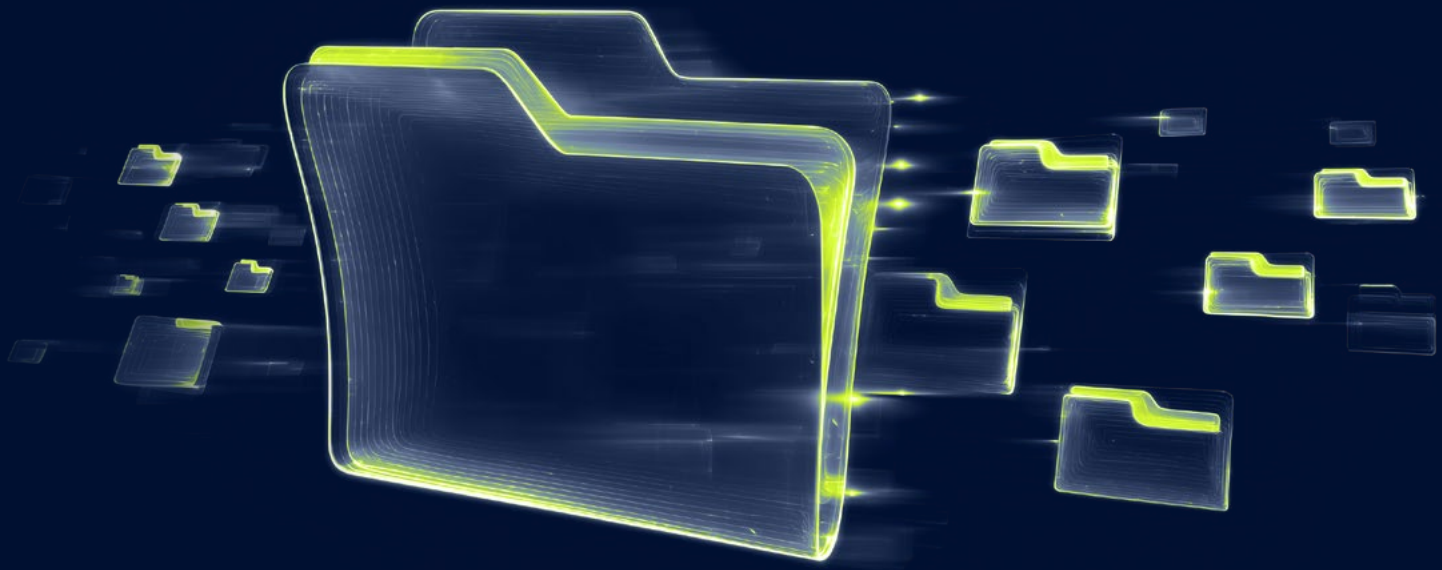
Фишинговые учения действительно помогают понять, насколько сотрудники готовы распознавать социальную инженерию. Но обратной стороной может стать избыточное недоверие пользователей к любым письмам, включая легитимные. Чтобы превратить избыточный страх в разумную осмотрительность, важно выстроить культуру коммуникаций — чётко определить, через какие каналы и в каком формате компания взаимодействует с сотрудниками.

В трёхлетней динамике мы наблюдаем рост использования практики регулярных фишинговых учений.

Чаще всего компании проводят такие учения на ежегодной (21%) и ежеквартальной (17%) основах, что указывает на выстраивание регулярных тренировок пользователей. Также мы наблюдаем, что в компаниях с более высоким уровнем зрелости всё чаще используются игровые элементы — компании внедряют балльную систему обучения, где баллы работникам начисляются за распознание фишинга и уведомление ИБ, а при переходе по фишинговым ссылкам или вводе учётных данных баллы снимаются.

Частота проведения эмуляции фишинговых атак





ПРИЛОЖЕНИЯ

Методология и охват исследования

Исследование основано на анализе данных более чем 255 компаний из 9 отраслей за три последовательных периода наблюдений (2023, 2024, 2025). Трёхлетний период наблюдений позволил минимизировать статистические погрешности и обеспечил высокую достоверность результатов текущего состояния и тенденций рынка ИБ.

Источниками данных для исследования послужили результаты опроса руководителей служб ИБ (полученные посредством очных интервью и анкетирования), а также материалы экспертных аудитов ИБ, проведённых за три года измерений.

Ключевые направления анализа:

- Стратегический менеджмент (выбор вектора стратегического развития, формирование и защита бюджета на ИБ).
- Организация службы ИБ (поиск кадров, формирование команд по ИБ и структурная подчиненность).
- Киберустойчивость (развитие аспектов киберустойчивости и обеспечение непрерывности бизнеса).
- Эффективное управление, использование сервисов и автоматизация (процессное управление, использование сторонних сервисов, автоматизация и использование искусственного интеллекта).
- Управление рисками ИБ (методологическая основа управления рисками и риски третьих сторон).
- Оценка своего уровня ИБ и отчётность.
- Киберкультура.

В отчёте рассмотрены более 40 аналитических зависимостей и тестирований гипотез на основе данных за три года наблюдений.

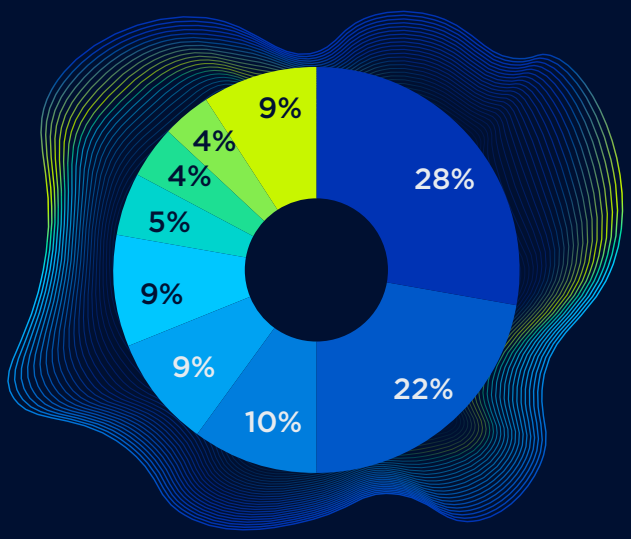
Тестирование гипотез — статистический метод, используемый для проверки утверждений или предположений на основе сопоставления и комбинированного анализа данных. Этот процесс помогает определить, есть ли достаточные доказательства для поддержки или опровержения определённой гипотезы. Примеры гипотез, которые были проверены в рамках анализа:

- архитектурная модель построения ИБ зависит от зрелости компании;
- компании, в которых бюджет обосновывают через риски, получают больше бюджета, чем остальные;
- величина выделяемого бюджета коррелирует со схемой подчинения подразделения ИБ;
- компании с регулярной отчётностью для C-level имеют больший рост бюджета ИБ;
- отчётность по ИБ свойственна более зрелым компаниям;
- компании, которые жалуются на сложность поиска специалистов, сами не готовы растить кадры;
- и другие.

Участники исследования

В исследовании приняли участие компании из пяти отраслей: финансового, промышленного и топливно-энергетического секторов, ИТ-индустрии и транспорта. На их долю приходится почти 80% всех участников **за три года** исследования.

Сфера деятельности опрошенных компаний (накопительные данные за 2023–2025 годы)

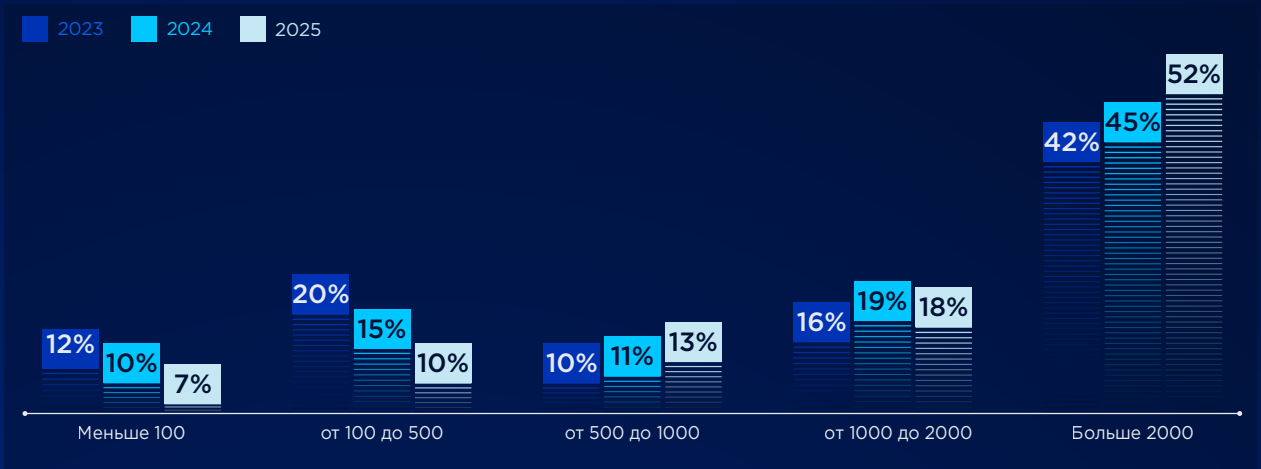


- 28% Финансовый сектор
- 22% Промышленность
- 10% Транспорт
- 9% Топливно-энергетический комплекс
- 9% IT, информационные технологии
- 5% Телеком
- 4% Государственные учреждения
- 4% Ритейл
- 9% Иные коммерческие организации

В 2025 году выборка компаний обновилась на 60% (40% компаний участвовали повторно), при этом её структура сместилась в сторону крупного бизнеса.

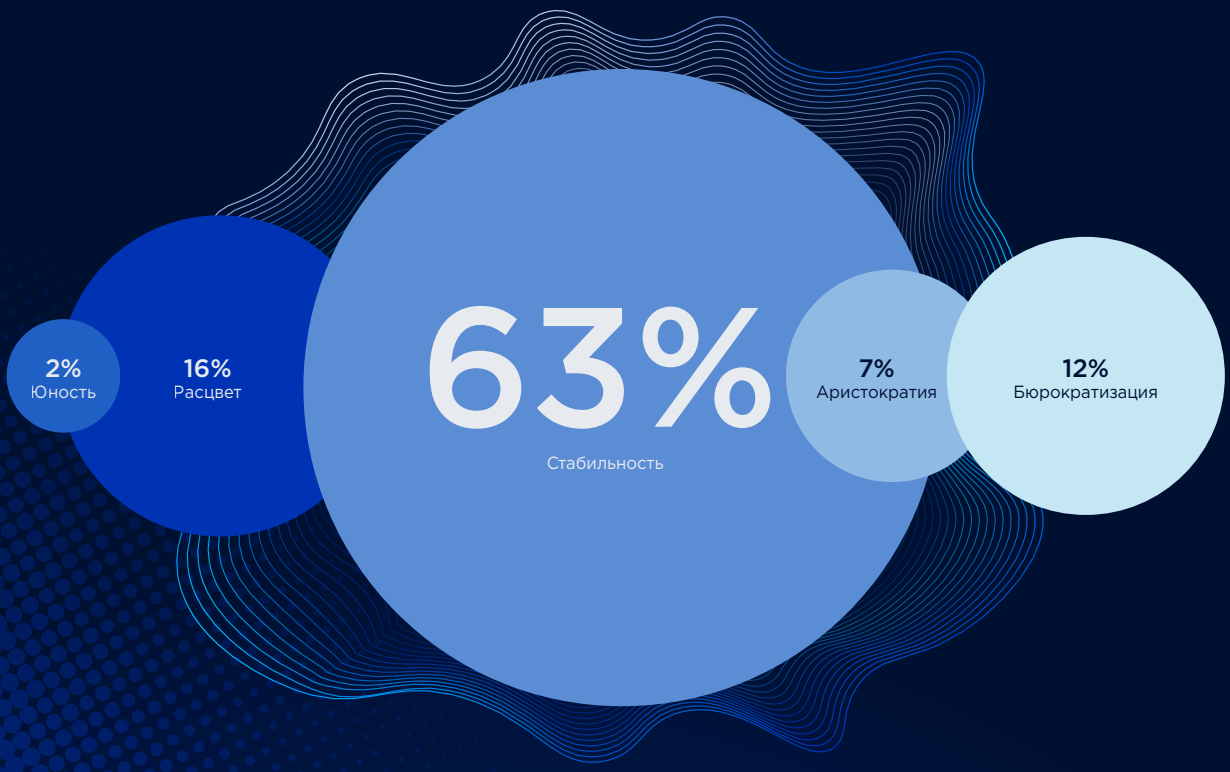
Доля компаний с численностью более 2000 человек выросла с 42% (2023) до 52% (2025), это основные респонденты исследования. Малый бизнес (менее 100 сотрудников) сократил присутствие с 12% до 7%. При этом в разрезе организационной структуры большую часть (44% респондентов) представляют дочерние компании, 21% — головные офисы холдингов и 35% — самостоятельные организации.

Количество работников в опрашиваемых компаниях



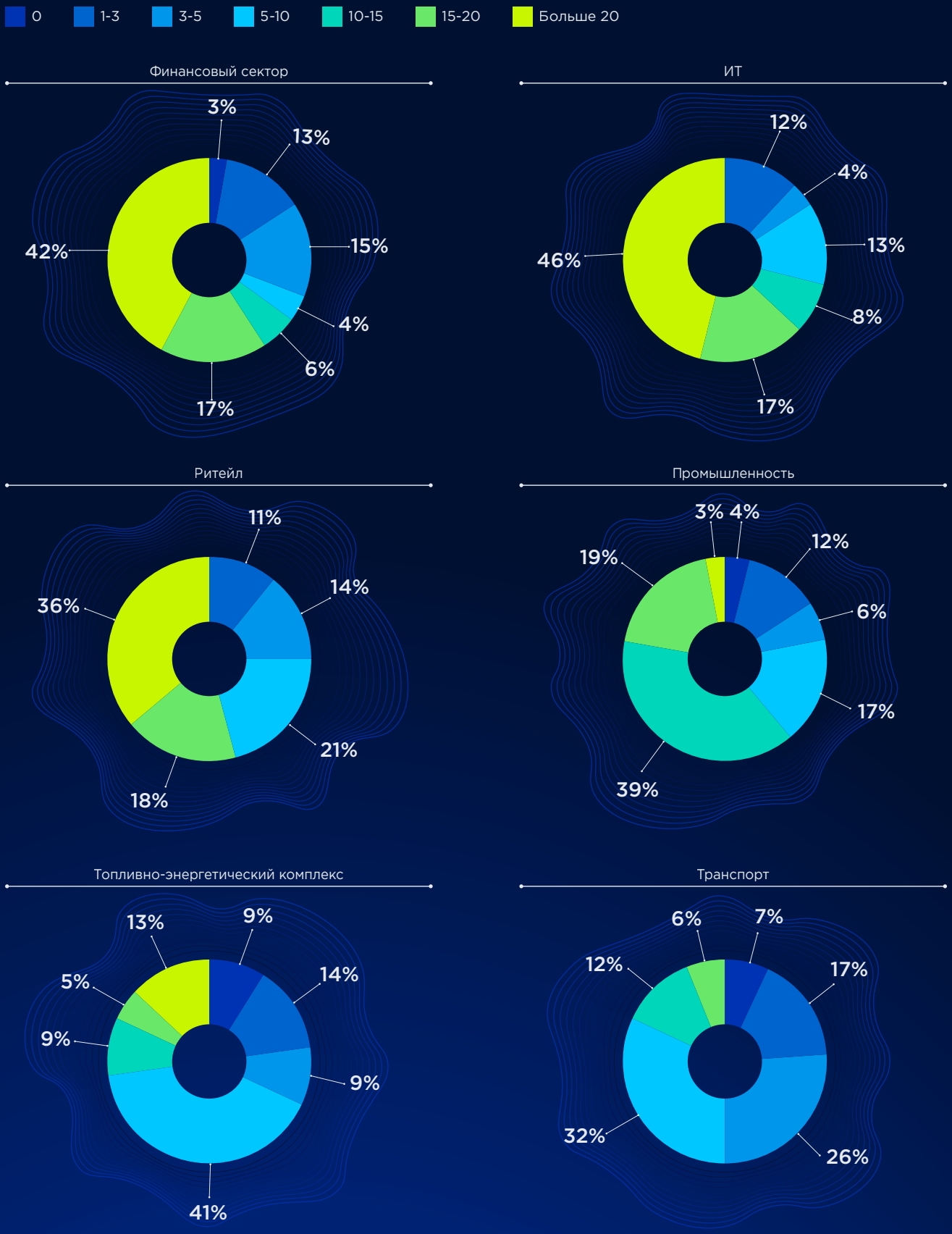
Распределение респондентов по модели Адизеса[8] напрямую коррелирует с размером исследованных компаний: ядро выборки составляют компании на пике зрелости («Расцвет») и в начале стабилизации («Стабильность»).

Модель жизненного цикла Ицхака Адизеса (2025)



[8] Модель жизненного цикла Ицхака Адизеса используется для определения уровня развития компаний. Согласно этой модели, организации, как и живые организмы, проходят несколько стадий развития и демонстрируют прогнозируемые и повторяющиеся модели поведения. На каждой стадии существуют свои вызовы и сложности. Успех организации на рынке определяется способностью менеджеров управлять переходом от одной стадии к другой.

Размер штата ИБ в разных сферах бизнеса (2025)



JET

SECURITY
TEAM

security@jet.su
jetcsirt.su