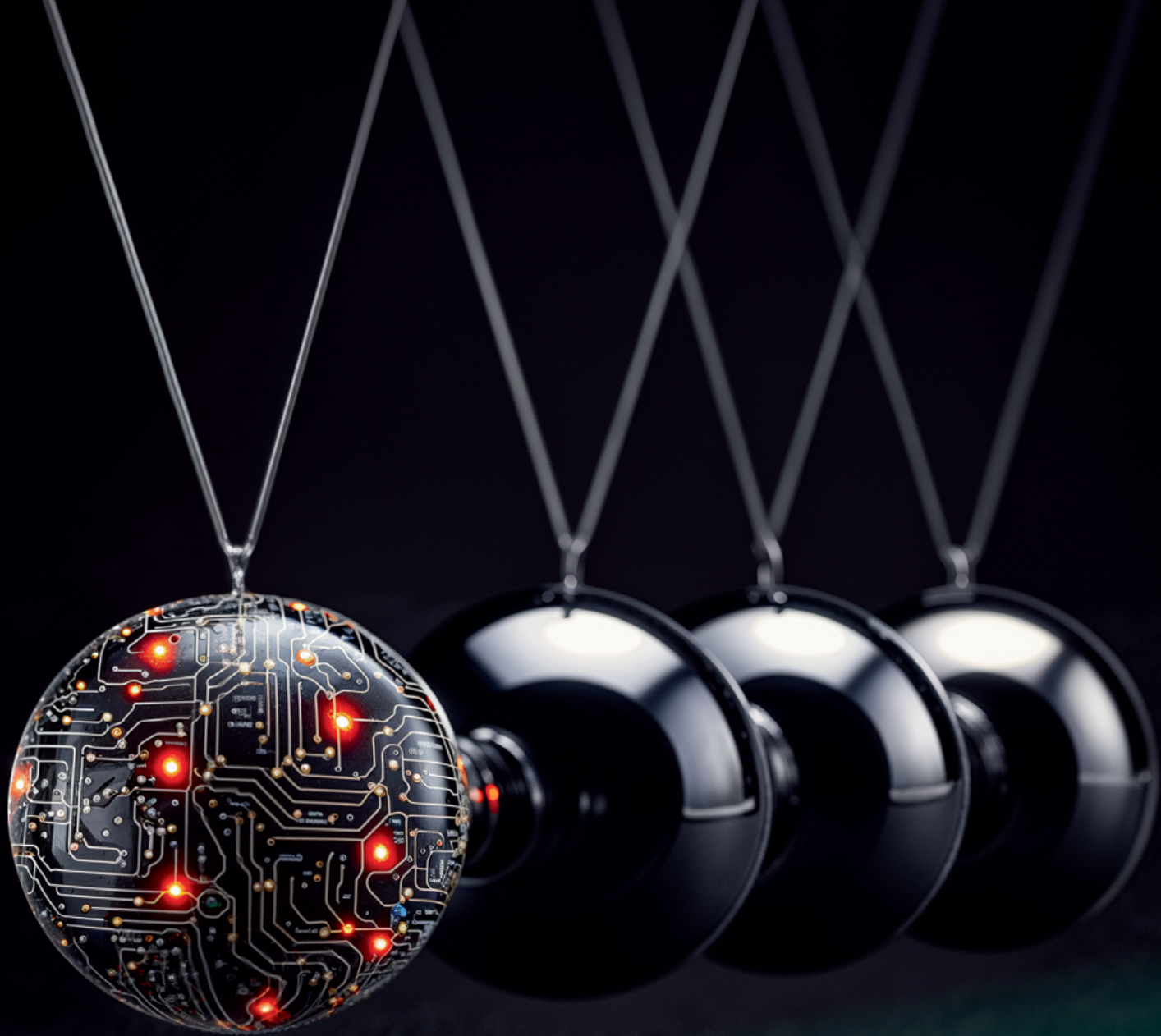




Кибербезопасность цепочек поставок

По данным глобального исследования
«Лаборатории Касперского»

kaspersky

Вступление



Анна Кулашова

вице-президент «Лаборатории Касперского»
по развитию бизнеса в России и странах СНГ



Несмотря на стремительную цифровую трансформацию экономики, усложнение киберугроз и изменения в законодательстве, риски информационной безопасности остаются крайне недооцененными в бизнесе. Внедрение решений для противодействия массовым атакам уже стало стандартом, однако сегодня этого недостаточно. Компаниям важно осознавать: уровень их информационной безопасности определяется в том числе защищенностью их подрядчиков и поставщиков, а значит необходимо менять подход к формированию стратегии кибербезопасности.

Наше исследование показало, что ИТ и ИБ специалисты объективно оценивают риски атак на бизнес через подрядчиков и поставщиков, и при этом подчеркивают нехватку инструментов мониторинга, хотя такие решения представлены на российском рынке. Более того, каждый третий специалист отметил недостаток поддержки со стороны высшего руководства.

Мы надеемся, что исследование обратит внимание руководителей на актуальные киберриски, подчеркнет важность кибербезопасности как стратегического актива и поможет наладить регулярный диалог между топ-менеджерами и техническими экспертами, ведь в современных условиях только так можно обеспечить устойчивость и конкурентоспособность бизнеса.



Согласно данным глобального отчета Kaspersky Security Services, доля атак, когда злоумышленникам удалось проникнуть в инфраструктуру организации через доверительные отношения, продолжает расти. Среди всех инцидентов, в которых команда «Лаборатории Касперского» по реагированию на инциденты помогала компаниям в 2025 году, этот показатель составил 16%. Сегодня такой вектор проникновения в инфраструктуру организации входит в топ-3 по частоте использования атакующими.

Содержание

Вступление	2
Содержание	3
Международное исследование	5
Ключевые показатели для России	6
Ключевые выводы	7
Глава 1. Риски цепочки поставок: точная оценка и недостаточный приоритет	8
Угроза номер один	9
Угрозы, с которыми организация столкнулась за последние 12 месяцев	10
Осведомленность об уязвимостях: Россия и мир	11
Глава 2. Фрагментарная защита: три барьера в контроле подрядчиков	12
№1 — Недостаточность защитных мер	12
№2 — Недостаточная проверка подрядчиков	13
№3 — Ресурсные и структурные ограничения	14
Заключение: от осознания рисков к устойчивым действиям	15
Практические рекомендации по многоуровневой защите для организаций	16
Методология	17
Возможности портфолио «Лаборатории Касперского» для защиты от атак на подрядчиков и поставщиков	18

Современные организации зависят от десятков внешних партнеров и подрядчиков, включая поставщиков ПО, услуг и облачных сервисов. Эта цифровая взаимозависимость повышает операционную эффективность, но существенно повышает риск атак на цепочки поставок и атак на доверенные отношения. В этих случаях злоумышленники пытаются проникнуть в компанию через ее менее защищенных партнеров. В отчете [Global Cybersecurity Outlook 2026](#) Всемирного экономического форума отмечается, что растущая взаимосвязанность цифровых систем и недостаточная прозрачность в вопросах кибербезопасности третьих сторон становятся серьезным вызовом для обеспечения киберустойчивости. Для российских предприятий эти риски особенно значимы.

По данным опроса, российские компании оценивают свою уязвимость к угрозам цепочек поставок и атакам через доверенных партнеров значительно выше среднемирового уровня, а также сообщают о более широком спектре атак за последние 12 месяцев.

Уязвимость в популярном компоненте ПО или успешная атака на облачный сервис для конкретной индустрии может стать глобальным кризисом, останавливающим бизнес-процессы и приносящим огромные убытки.

Цена уязвимости*: крупные атаки на цепочки поставок

Кража \$1,4 млрд с криптобиржи ByBit

стала возможна, [благодаря компрометации ПО Safe{Wallet}](#), которое биржа использовала для работы со своими активами.

Кибератака на Jaguar Land Rover

остановила конвейер автопроизводителя почти на месяц и принесла ущерб до 500 млн фунтов. Атаку провели через [ИТ-подрядчика](#).

* Информация об атаках приведена по открытым источникам и не является частью исследования.

Международное исследование

Об угрозе

Атаки на подрядчиков и поставщиков — термин, объединяющий два типа угроз.

Атака на цепочку поставок (supply chain attack) означает компрометацию поставщика и его продукта — например, когда злоумышленники выпускают вредоносное обновление легитимного ПО.

Атака на доверительные отношения (trusted relationship attack) — это злоупотребление уже выданными доступами, когда злоумышленники проникают в сеть компании через взломанного партнера или субподрядчика.



Охват: более **1700** респондентов в **16** странах, в России были опрошены **100** специалистов по ИБ из компаний с численностью персонала от **500** человек.



Респонденты: топ-менеджеры, руководители групп и ведущие специалисты, у которых значительная часть рабочего времени посвящена вопросам информационной безопасности.



Авторы исследования: внутренний центр маркетинговых исследований «Лаборатории Касперского».

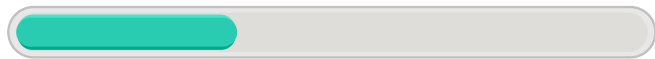


Цель исследования: узнать, как компании оценивают риски атаки на подрядчиков и поставщиков, какие пробелы в защите и организационные сложности мешают снижению этих рисков, что компании делают для защиты и как относятся к принципу общей ответственности, требующему строить защиту совместно с деловыми партнерами.

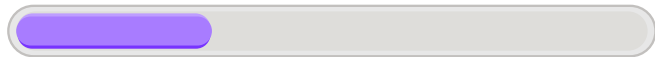
Ключевые показатели для России:

35%

российских компаний в 2025 году столкнулись с атаками на цепочки поставок

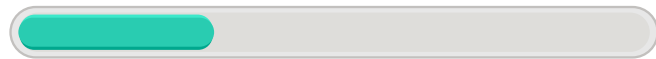


доля в мире: **31%**

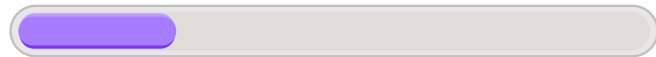


31%

пережили атаки через доверенных партнеров

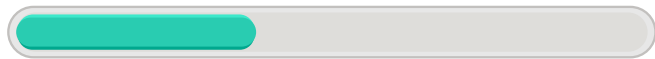


в мире: **25%**

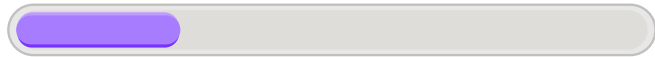


38%

оценивают свою уязвимость к этим типам атак как высокую

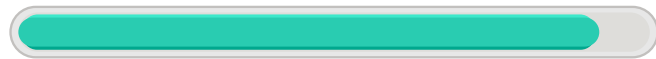


в мире: **26%**



92%

считают необходимым совершенствовать защиту компании от атак на подрядчиков и поставщиков

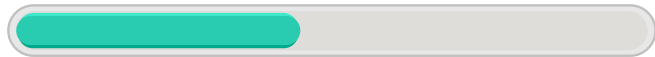


в мире: **85%**

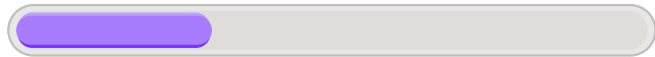


45%

называют нехватку инструментов контроля за кибербезопасностью подрядчиков в качестве ключевого барьера — в полтора раза выше среднемирового значения



в мире: **31%**



67

среднее количество поставщиков программного и аппаратного обеспечения на одну компанию. В среднем **99** подрядчиков имеют доступ к системам (в мире: **61** и **72**)

Хотя российские компании хорошо осведомлены об угрозе атак на подрядчиков и поставщиков и адекватно ее оценивают, защита от нее недостаточна и фрагментарна. Даже самые популярные меры обеспечения безопасности применяются менее чем в половине организаций.

Вместе с тем российские организации демонстрируют высокую готовность к коллективной защите: 20% разделяет с подрядчиками затраты на кибербезопасность, и 100% тех, кто еще не практикует это, выразили готовность инвестировать в безопасность партнеров ради повышения общей устойчивости.

Ключевые выводы

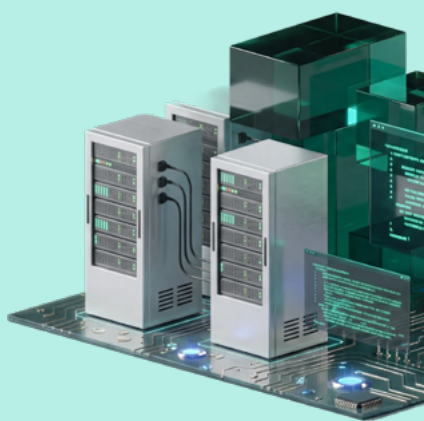
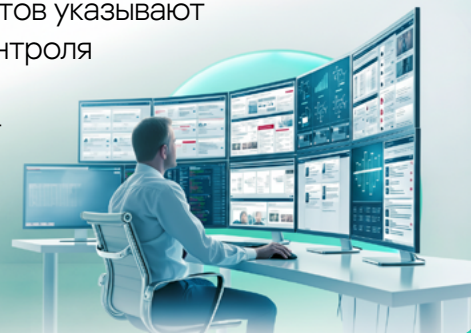
Атаки на цепочки поставок — на втором месте среди инцидентов, с которыми компании столкнулись за 2025 год. Их признали **35%** опрошенных российских компаний — выше среднемирового показателя в **31%**.

Повышенное ощущение уязвимости. **38%** российских предприятий оценивают свою уязвимость к атакам на подрядчиков и поставщиков как высокую — значительно выше глобального показателя в **26%**. Практически никто (**1%**) не считает ее низкой.

Атакам через доверенных партнеров подверглись 31% российских компаний (в мире: 25%), что делает данный тип угроз пятым по распространенности.

Широкая экосистема подрядчиков. В среднем российские компании работают с **67** поставщиками и предоставляют доступ к системам **99** подрядчикам, что расширяет поверхность атаки.

Главный барьер: нехватка инструментов мониторинга. **45%** российских респондентов указывают на нехватку решений для контроля за кибербезопасностью подрядчиков (в мире: **31%**) — это наиболее существенное отличие от общемировой картины.



Практически всеобщий запрос на улучшения. **92%** говорят о необходимости совершенствования защиты (в мире: **85%**), при этом **18%** требуют серьезных изменений.



Высокая готовность к разделению затрат. **100%** российских компаний, еще не разделяющих расходы на ИБ с подрядчиками, готовы к этому, **20%** уже практикуют подобный подход.



Рекордно низкая удовлетворенность. Лишь **8%** российских предприятий считают текущий уровень защиты цепочек поставок эффективным — один из самых низких показателей в мире, наравне с Германией (**6%**), Турцией (**7%**), Италией (**8%**), Бразилией (**8%**).

Глава 1.

Риски цепочки поставок: точная оценка и недостаточный приоритет

Российский бизнес довольно точно оценивает риски, связанные с подрядчиками и поставщиками. Атаки на цепочку поставок входят в топ-3 как среди главных воспринимаемых угроз (их назвали в **11%** опрошенных компаний), так и среди реально произошедших инцидентов. Атаки на доверенных партнёров остаются немного недооцененными — 7 место среди воспринимаемых угроз и 5 место среди фактических.

Если в мире основным следствием атак на подрядчиков и поставщиков считают операционные сбои (**52%**), то российский

бизнес больше сфокусирован на прямых убытках: на первом месте финансовый ущерб (**61%** против **48%** в мире), за ним следуют операционные нарушения (**49%**) и кража интеллектуальной собственности (**44%** против **33%**).

Хотя компании понимают, что ущерб от атак на цепочку поставок и атак через партнеров может быть большим, они все равно не ставят эти угрозы на первые места в своих оценках рисков. Как следствие, выделение бюджетов и внедрение конкретных мер защиты также не становятся приоритетом.



Угроза номер один

Угроза	Место в рейтинге	Доля респондентов, считающих эту угрозу самой опасной	
		Россия	Мир
Вредоносные программы как услуга (MaaS)	1	12%	7%
	7		
Разведка ИТ-инфраструктуры, проводимая злоумышленниками (Reconnaissance)	1	12%	7%
	7		
Атаки на цепочки поставок	3	11%	9%
	3		
Сложные целевые атаки (APT)	3	11%	14%
	1		
DDoS-атаки	5	10%	8%
Программы-вымогатели (Ransomware)	6	8%	11%
	2		
Инсайдерские (внутренние) угрозы	7	7%	9%
	3		
Атаки через доверенных партнеров	7	7%	8%
	5		
Атаки с применением искусственного интеллекта	9	6%	8%
	5		
Кибершпионаж	9	6%	7%
	7		
Фишинг / социальная инженерия	11	5%	6%
	10		
Атаки нулевого дня (Zero-day)	11	5%	6%
	10		

Угрозы, с которыми организация столкнулась за последние 12 месяцев

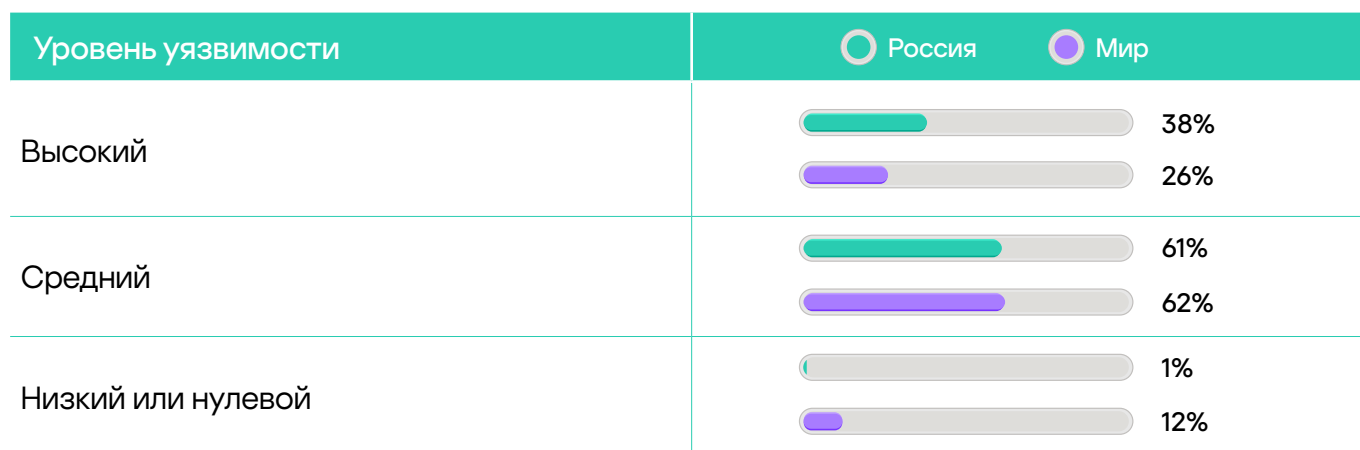
Угроза	Россия	Мир
Разведка ИТ-инфраструктуры, проводимая злоумышленниками (Reconnaissance)	36%	19%
Атаки на цепочки поставок	35%	31%
Атаки с применением искусственного интеллекта	34%	30%
Фишинг / социальная инженерия	32%	28%
Атаки через доверенных партнеров	31%	25%
Вредоносные программы как услуга (MaaS)	31%	23%
DDoS-атаки	31%	23%
Инсайдерские (внутренние) угрозы	30%	24%
Программы-вымогатели (Ransomware)	29%	25%
Атаки нулевого дня (Zero-day)	25%	19%
Кибершпионаж	19%	26%
Сложные целевые атаки (APT)	14%	20%

Самой частой реальной угрозой в России стала разведка — попытки злоумышленников изучить инфраструктуру для будущего взлома. При этом о сложном кибершпионаже (APT) российский бизнес сообщает реже, чем в среднем по миру. Но общий спектр реальных угроз российскому бизнесу шире: за год отечественные компании столкнулись в среднем с **3,5** типами атак против **2,9** в мире.

Такая высокая активность отчасти объясняется масштабом бизнеса. Мировая статистика показывает, что чаще всего цепочки поставок атакуют в крупных корпорациях от 2500 сотрудников (**36%** инцидентов), так как у них больше контрагентов. В нашем опросе к этой категории относятся **46%** российских респондентов. Именно сложная экосистема поставщиков делает крупный бизнес более привлекательной и вероятной мишенью для атак.

Осведомленность об уязвимостях: Россия и мир

Российские компании чаще осознают свою уязвимость перед атаками на цепочки поставок и через партнеров:



Повышенное чувство уязвимости оправдано большим количеством партнеров. Российские участники опроса работают в среднем с 67 поставщиками ПО и оборудования (в мире — 61) и предоставляют доступ к системам 99 подрядчикам (в мире — 72).

При этом глобальные данные показывают, что низкая оценка рисков часто связана

с недостаточным знанием своей инфраструктуры. Так, **21%** мировых компаний, заявляющих о нулевой уязвимости, не могут назвать число своих поставщиков. В России эта проблема менее выражена (свою уязвимость считают низкой лишь **1%**), но **9%** компаний по-прежнему затрудняются оценить количество своих партнеров. Это указывает на нехватку прозрачности и контроля над активами.

Глава 2.

Фрагментарная защита: три барьера в контроле подрядчиков

Несмотря на четкое осознание угроз, связанных с цепочкой поставок, защита российских компаний остается фрагментарной — эта проблема актуальна для всего мира. Ни одна из базовых мер безопасности не применяется большинством организаций. Практические сложности бизнеса можно разделить на три основные категории.

92%

нуждаются в более эффективной защите

45%

не хватает инструментов контроля подрядчиков

№1 — Недостаточность защитных мер

Как в России, так и во всем мире, нет ни одной защитной меры, которая была бы внедрена большинством опрошенных компаний.

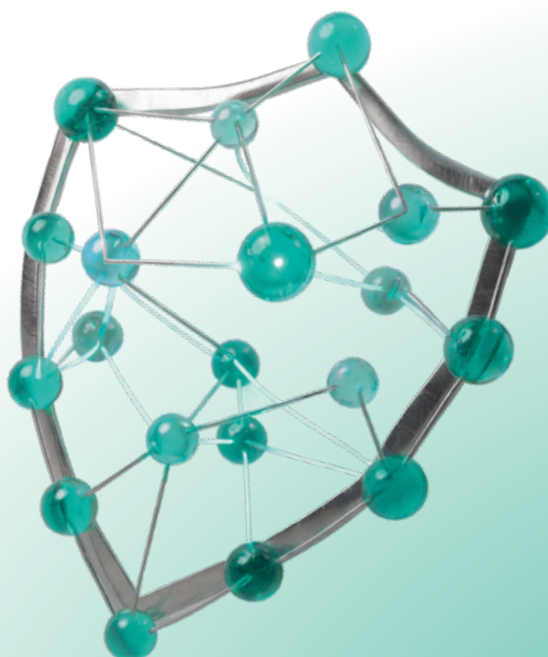
Даже самые популярные меры — включение требований ИБ в договоры и двухфакторная аутентификация (2FA) для поставщиков — используют лишь **37–38%** компаний.

То, что даже эти базовые практики не стали повсеместными, показывает незрелость процессов защиты цепочки поставок.

Российский бизнес чаще глобального проверяет подрядчиков до начала работы

(**36%** против **28%**), но меньше компаний регулярно проверяет ИБ действующих подрядчиков (**27%** против **35%** в мире). В результате большинство компаний не знают, как меняются риски ИБ у их постоянных партнеров и поставщиков.

Лишь **8%** российских предприятий считают, что не требуются изменения в системе их защиты от атак на подрядчиков и поставщиков (в мире: **15%**). Это один из самых низких показателей в мире, наряду с Германией (**6%**), Турцией (**7%**), Италией (**8%**) и Бразилией (**8%**).



№2 — Недостаточная проверка подрядчиков

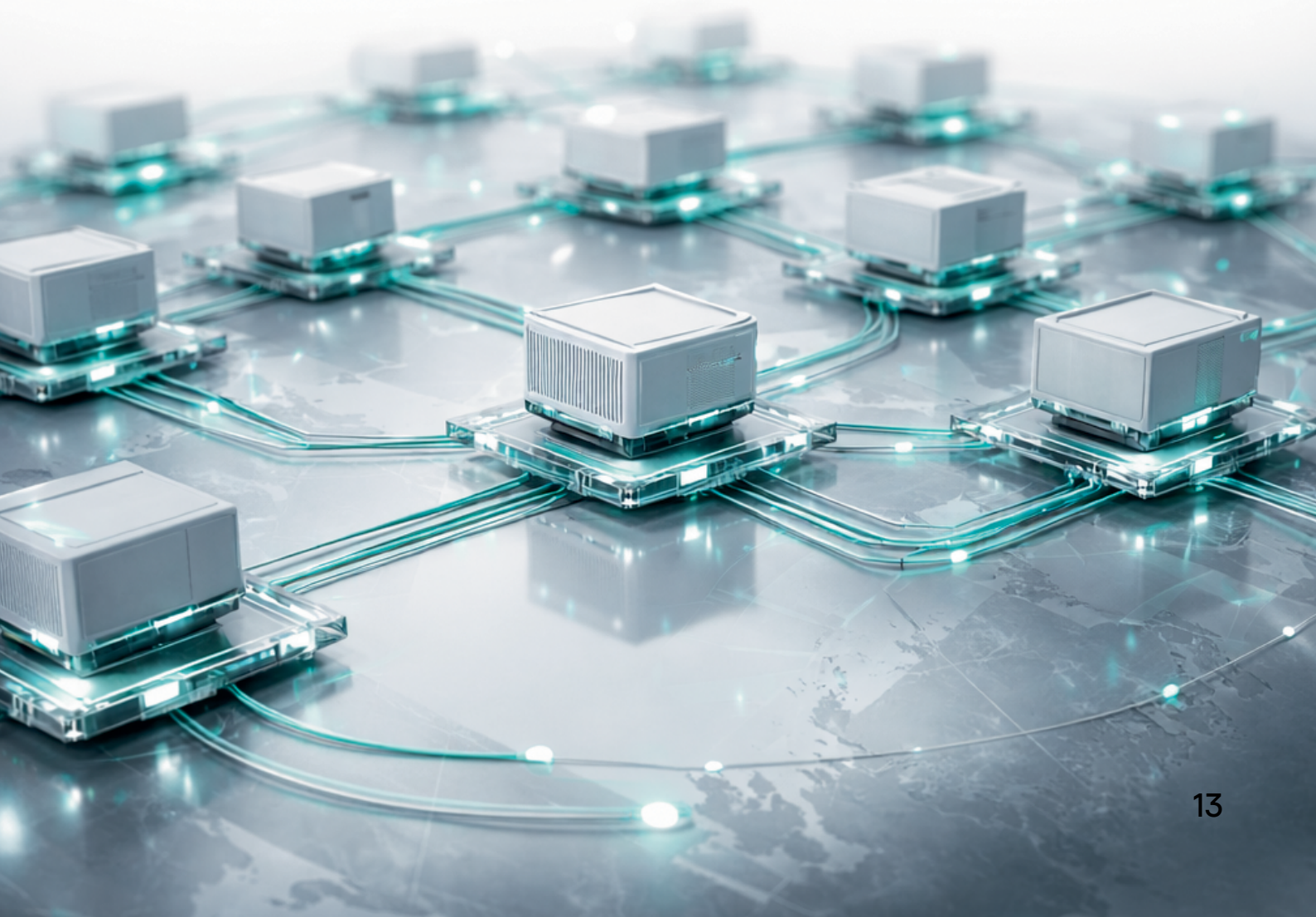
Даже когда российские компании проверяют ИБ контрагентов, аудит получается несбалансированным.** Более половины изучает планы реагирования на инциденты. Однако историю реальных инцидентов у партнера запрашивают лишь треть (в мире — **51%**), а регламенты кибербезопасности — только около **40%** (в мире — **53%**).

При оценке надежности подрядчика менее половины российских компаний, у которых есть эта практика, вообще включают в оценку критерии ИБ (в мире — **62%**). Большинство организаций по-прежнему смотрит исключительно на финансы, юридическую чистоту и репутацию, воспринимая

кибербезопасность как второстепенный компонент надежности.

Мировая статистика показывает, что компании учатся на горьком опыте. Организации, пострадавшие от атак на цепочки поставок, значительно чаще запрашивают у поставщиков результаты тестирования на проникновение (**56%** среди тех, кто проверяет ИБ поставщиков), а жертвы атак через доверенных партнеров уделяют внимание проверке соответствия отраслевым стандартам (**56%**) и анализу собственных политик безопасности цепочек поставок у подрядчиков (**53%**).

** — В эту часть выборки вошло 15 компаний.



№3 — Ресурсные и структурные ограничения

Что мешает выстроить надежную защиту цепочек поставок:

Препятствие	Россия	Мир
Нехватка инструментов контроля за ИБ подрядчиков	45%	31%
Отсутствие договорных требований по безопасности	44%	39%
Нехватка квалифицированных специалистов по ИБ	42%	42%
Приоритет других задач в области ИБ	41%	42%
Недостаточное понимание проблемы нетехническими сотрудниками	37%	32%
Недостаточная поддержка со стороны высшего руководства	30%	27%
Недостаточное финансирование	26%	29%

Главное отличие российского рынка — острая нехватка инструментов для мониторинга подрядчиков (**45%** против **31%** в мире). Этот дефицит отчасти объясняет, почему отечественные компании редко проверяют действующих партнеров (**Проблема №1**). Кроме того, российский бизнес чаще жалуется на отсутствие ИБ-требований в контрактах (**44%**). Это значит, что нормативно-договорная база

для защиты цепочек поставок на нашем рынке все еще находится на стадии формирования.

Чтобы улучшить свою защиту, организации готовы рассматривать затратные подходы, такие как разделение расходов на ИБ с подрядчиками. **20%** опрошенных уже делают это, демонстрируя прагматичное понимание, что уровень безопасности системы определяется ее самым слабым звеном.

Заключение: от осознания рисков к устойчивым действиям

Российский бизнес осознает риски в цепочках поставок лучше многих зарубежных коллег, но одной осведомленности мало. Лишь **8%** компаний полностью удовлетворены внедренными мерами защиты, тогда как **92%** признают необходимость ее усилить. Этот колоссальный разрыв между пониманием угрозы и реальной защищенностью требует решительных действий.

Данные указывают на четыре стратегических приоритета для российских организаций:



Интеграция кибербезопасности в процессы закупок. При выборе подрядчика **58%** российских компаний, которые вообще оценивают благонадежность партнера, учитывают только его финансы, юридическую чистоту и репутацию, вообще игнорируя критерии ИБ. Защита цепочки поставок не может быть задачей исключительно отдела ИБ, она должна начинаться на этапе тендера. Бизнесу необходимо внедрить критерии кибербезопасности (аудит политик, результаты пентестов, проверка истории взломов) как обязательный блокирующий фактор при выборе любого контрагента, имеющего доступ к инфраструктуре.



Отказ от иллюзии безопасности. Сейчас подход российского бизнеса к проверке партнеров носит формальный характер. Компании полагаются на то, что легко проверить: договоры и наличие плана реагирования на бумаге. При этом реальную техническую защищенность и историю прошлых инцидентов подрядчика изучают в меньшинстве случаев. Стратегическим приоритетом должен стать переход от проверки документов к проверке фактической ИТ-инфраструктуры партнера.



Преодоление «инструментального голода». Главным барьером на пути к безопасности российские компании назвали нехватку инструментов для контроля подрядчиков (**45%**, в полтора раза выше, чем в мире). Именно этот дефицит объясняет, почему бизнес вручную проверяет партнеров на старте, но прекращает проверки в процессе совместной работы, где нужна автоматизация. Инвестиции компаний должны быть направлены на внедрение специализированных платформ управления рисками третьих сторон и систем класса XDR и NDR, обеспечивающих глубокую видимость ИТ-инфраструктуры. Без автоматизированных инструментов мониторинга контролировать доступ 99 подрядчиков физически невозможно.



Проактивная стратегия: расширение периметра. **100%** российских компаний, которые пока не делят затраты на ИБ с подрядчиками, готовы к такому шагу. Эту готовность пора переводить в практику: вместе с ключевыми поставщиками разрабатывать планы реагирования, обмениваться данными об угрозах и проводить совместные киберучения.

Компании, которые смогут решить эту проблему и выстроить киберустойчивую цепочку поставок, получают конкурентное преимущество. Вместе с подрядчиками и партнерами они улучшат непрерывность бизнеса, усилят репутацию и создадут более прочные деловые партнерства. Они станут надежными узлами в глобальной сети, привлекающими клиентов и партнеров, ценящих стабильность.

Практические рекомендации по многоуровневой защите для организаций:

1. Тщательно оценивайте поставщиков. Оценивайте уровень кибербезопасности до начала сотрудничества — анализируйте политики безопасности, историю инцидентов, соответствие требованиям и результаты тестирования на проникновение.

2. Закрепляйте требования безопасности в договорах. Включайте в договоры с поставщиками конкретные обязательства в области ИТ-безопасности, права на проведение аудита и порядок уведомления об инцидентах.

3. Внедряйте превентивные технические меры. Применяйте принцип наименьших привилегий, архитектуру нулевого доверия (Zero Trust) и зрелые процессы управления идентификацией для всех подключений подрядчиков.

4. Обеспечьте непрерывный мониторинг. Внедрите решения класса XDR для обеспечения видимости инфраструктуры в режиме реального времени и выявления аномалий в сетевой активности, связанной с подрядчиками.

5. Улучшайте видимость сети. Применяйте инструменты NDR для анализа как внешнего, так и внутреннего трафика с целью выявления признаков компрометации цепочки поставок.

6. Развивайте аналитику рисков третьих сторон. Используйте мониторинг цифрового следа для выявления скомпрометированных учетных записей поставщиков и инцидентов, связанных с партнерами.

7. Разрабатывайте планы реагирования на инциденты, специфичные для цепочек поставок. Обеспечьте оперативную изоляцию скомпрометированных подключений поставщиков и четкий порядок эскалации.

8. Выстраивайте активное взаимодействие с поставщиками по вопросам безопасности. Обменивайтесь экспертизой, совместно инвестируйте в защиту и сделайте взаимную безопасность приоритетом партнерства.

Методология

В основе данного отчета лежит глобальное исследование, проведенное внутренним исследовательским центром «Лаборатории Касперского». В опросе приняли участие более **1700** специалистов по информационной безопасности из **16** стран Азиатско-Тихоокеанского региона, Европы, региона МЕНА (Ближний Восток, Турция, Африка) и Латинской Америки. Среди респондентов — топ-менеджеры (C-suite), вице-президенты, руководители групп и ведущие специалисты, значительная часть рабочего времени которых посвящена вопросам ИТ-безопасности. Все обследованные компании насчитывают не менее **500** штатных сотрудников и имеют достаточно зрелую службу ИБ — у них внедрение SOC запланировано на ближайшие два года.



Российская подвыборка включает **100** респондентов.

Отраслевой состав смещен в сторону розничной и оптовой торговли (**27%**), энергетики и коммунального хозяйства (**18%**), телекоммуникаций (**12%**) и финансовых услуг (**12%**).

По сравнению с глобальной выборкой в ней преобладают крупные предприятия (**46%** с численностью сотрудников свыше **2500** человек против **19%** в мире) и более высокие должностные позиции (**39%** вице-президентов и **15%** топ-менеджеров уровня C-suite).

Эти особенности состава выборки следует принимать во внимание при интерпретации российских данных.

Все процентные значения в отчете округлены до целых чисел. Под «глобальными» показателями подразумеваются данные по полной выборке из **1714** респондентов из **16** стран.

Возможности портфолио «Лаборатории Касперского» для защиты от атак на подрядчиков и поставщиков



Kaspersky Symphony XDR

Платформа комплексной безопасности для многоуровневого обнаружения атак, мониторинга, расследования, проактивного поиска угроз и реагирования на сложные инциденты.



Kaspersky Unified Monitoring and Analysis Platform

SIEM-платформа, которая обеспечивает централизованный сбор, ускоренный анализ и корреляцию событий безопасности из различных источников данных. Новая версия решения позволяет обнаруживать DLL Hijacking с помощью технологий ИИ.



Kaspersky Container Security

Специализированное решение для сред разработки на всех уровнях жизненного цикла приложений. Решение поддерживает 30+ угрозных баз данных для эффективного реагирования, в т.ч. Open Source Software Threats Data Feed.



Kaspersky Threat Intelligence

Комплекс сервисов информирования об угрозах. Тактические, операционные и стратегические данные о динамично меняющемся ландшафте угроз для обогащения защитных решений и повышения экспертизы ИБ-команд.



Kaspersky Managed Detection and Response

Экспертный сервис для круглосуточного мониторинга, обнаружения и расследования сложных кибератак и быстрого реагирования на них.



Kaspersky Endpoint Detection and Response Expert

Мощная система класса EDR (Endpoint Detection and Response), которая предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает ее эффективную защиту от сложных угроз и APT-атак.

ЧЕК ЛИСТ

Снижение рисков атак на организацию через подрядчиков и поставщиков



Атаки через доверительные отношения



Атаки через цепочки поставок

- ☐ Оцениваются ли риски информационной безопасности в управлении бизнес-рисками?
- ☐ Кто владелец риска и каков риск-аппетит?

Что предусмотреть: ввести в карту рисков риски информационной безопасности, назначить ответственного с правом вето при выборе поставщиков (CISO / директор по рискам), утвердить пороговые значения (рейтинг безопасности, критичность уязвимостей), при которых поставщик или подрядчик не допускается или отключается.



- ☐ Разработан ли стандарт безопасности для поставщиков и подрядчиков?
- ☐ Распространяется ли он на субподрядчиков (4 и 5 уровня)?

Что предусмотреть: утвердить обязательные требования (например соблюдение требований ISO 27001 или SOC2) как условие допуска к тендерам и заключения договоров.



- ☐ Отражена ли в юридических документах с подрядчиками ответственность за возникновение рисков информационной безопасности?

Что предусмотреть: включить обязательства уведомлять об инцидентах в компании или у субподрядчиков, предусмотреть ответственность подрядчика при компрометации через его процессы, в том числе материальную.



- ☐ Внедрены ли регулярные (не менее 1 раза в год) аудиты для текущих поставщиков?

Что предусмотреть: аудиты соответствия процессов поставщиков и подрядчиков лучшим практикам обеспечения ИБ, технические аудиты (тестирование на проникновение, редитиминг), в т.ч. со сценариями развития атаки из сети поставщика и подрядчика.



- ☐ Внедрены ли процедуры безопасного завершения сотрудничества?

Что предусмотреть: утвердить обязательную процедуру аннулирования доступов и возврата данных при расторжении контракта, которая должна включать отзыв прав доступа, управление учетными данными, подписание NDA, оценку рисков.



- ☐ Утвержден ли план реагирования на инциденты?

Что предусмотреть: Разработать руководство (play-book) на случай киберинцидента через подрядчика или поставщика. Проводить учения по сценариям. Назначить ответственных за предоставление доступа для команды реагирования на инциденты



Технические мероприятия

- ☐ Тестирование обновлений в изолированной среде (песочнице) перед распространением в инфраструктуре

Все обновления, прежде чем распространяются на продуктивные среды проходят тестирование в песочнице на предмет аномального поведения и совместимости с программным окружением.



- ☐ Нулевое доверие (Zero trust)

Утвердить принцип минимальных привилегий: доступ приложений только к необходимым сегментам, изоляция критических активов, многофакторная аутентификация.



- ☐ Непрерывный мониторинг, анализ данных об угрозах (Threat intelligence) и проактивный поиск угроз (Threat hunting)

Внедрить непрерывный расширенный (XDR/EDR) мониторинг инфраструктуры, включая поведенческий, мониторинг действий подрядчиков, и анализ релевантных данных об угрозах, контроль уязвимостей.

