РОСКОНГРЕСС
Пространство доверия

Положение ИБ в малом и среднем бизнесе: новые вызовы и отношение к аутсорсу

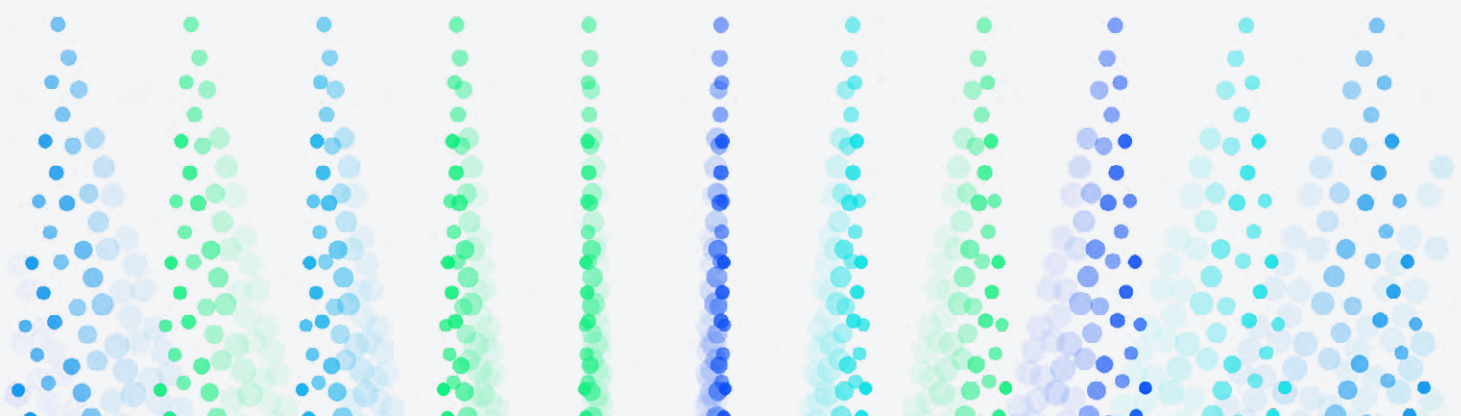
ИИМР
Институт Изучения Мировых Рынков

СОДЕРЖАНИЕ

Малый и средний бизнес (МСП) с каждым годом все чаще попадает в сферу интересов киберпреступников. По данным RED Security SOC, по итогам 2025 года **количество атак на российские компании выросло почти в 3 раза по сравнению с 2023 годом** и превысило 141 тыс. Доля успешных атак, по оценке Positive Technologies, достигла в 2025 году 47% против 31% годом ранее. Изменился и фокус: 76% критических инцидентов в 2025 году пришлись на уничтожение инфраструктуры с целью вымогательства, а размер первоначального выкупа для МСП, по данным F6, составил от 240 тыс. до 4 млн рублей.

Целью атак все чаще становятся **компании с относительно небольшим годовым оборотом — до 400 млн рублей.** Под ударом находится бизнес, который раньше не интересовал злоумышленников из-за своего скромного размера. Защитная инфраструктура МСП за изменением угроз не успела. Большинство компаний МСП находятся в уязвимом положении. С одной стороны, они преимущественно имеют корпоративную подписку на антивирусы и минимальные сетевые политики. С другой стороны, они далеки от создания полноценного центра мониторинга безопасности, к которому не готовы ни инфраструктура, ни бюджет.

Задача исследования — понять, как руководители воспринимают современные киберугрозы и принимают решения о модели защиты. Делается это собственными силами, через аутсорс или в гибридном формате? Задача состояла в реконструкции управленческой логики. Какие факторы воспринимаются как драйверы, какие — как барьеры, и как оценивается экономика решений? Отдельный фокус сделан на **отношении к аутсорсингу информационной безопасности (ИБ) как формирующемуся сегменту рынка** — насколько он понятен бизнесу и в чем расходятся ожидания заказчиков с действующим предложением поставщиков.



Описание выборки

В исследовании приняли участие **25 руководителей компаний** из секторов фармацевтики, медицины, включая стоматологию, а также ритейла, общественного питания, медиа, туризма, легкой, пищевой и обрабатывающей промышленности. Распределение размера компаний широкое: от микропредприятий с командой в десять человек, до структуры с тысячью рабочих мест. Формат — интервью продолжительностью 45–60 минут с дополнительным блиц-опросом с ответами по шкале от 1 до 5.

Состав выборки определен характером задачи. Она построена по принципу качественной репрезентативности. В нее включены руководители из отраслей с разным уровнем цифровизации и регуляторного давления, компании от микропредприятий до средних по обороту, а также представители разных уровней зрелости ИБ-функции.

Как изменилась природа угроз

В нескольких интервью независимо друг от друга респонденты отметили следующую особенность. Атаки совершаются уже не только на крупные структуры. С середины 2023 года под ударом и компании с оборотом от 150–200 млн рублей. Но этот сегмент рынка пока остается без правил. **Крупные вендоры привыкли к контрактам на сотни миллионов рублей и не перестроились к работе с малым бизнесом**.

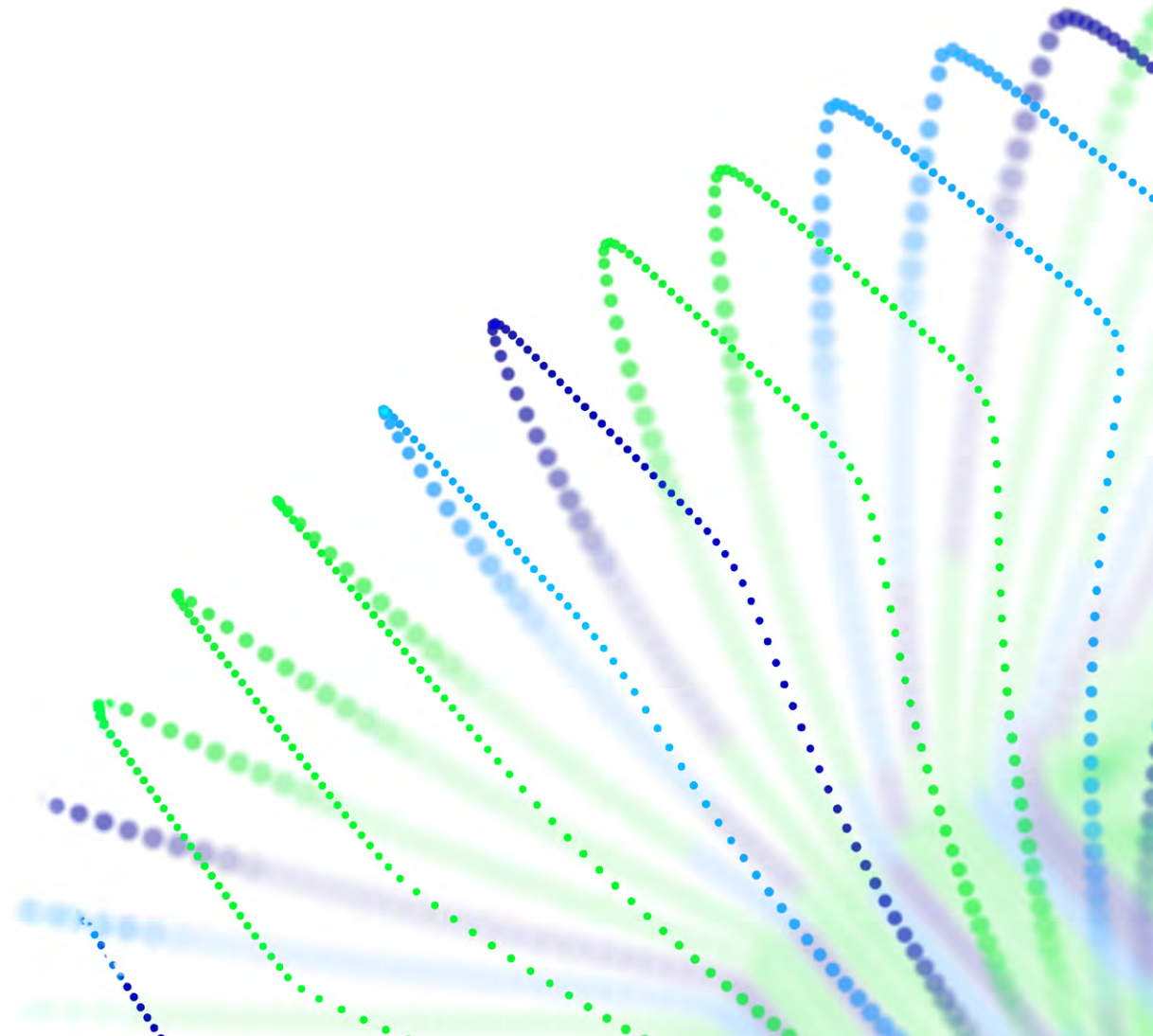
Изменился не только размер цели, но и экономика атак. Они приобрели неспецифический характер. Автоматизированные инструменты позволяют атакующим работать «по площадям». **«Хакеры бьют не прицельно, а массово: скрипты, ИИ, боты — все, что можно. И стоит это для них копейки»,** - заметил генеральный директор текстильного предприятия. Заместитель генерального директора медиахолдинга «Русская медиагруппа» Роман Лукьяненко описывает изменения в образе мысли руководителей. По его словам, компании все чаще исходят не из вопроса, произойдет ли инцидент, а из того, когда он произойдет и насколько организация к нему готова.

Наблюдается еще одна закономерность: крупные инциденты, по словам нескольких респондентов, происходят неожиданно. «Все известные мне серьезные взломы проходили в нерабочее время, а чаще всего в предпраздничное, когда уже все разъехались», — отмечает Роман Лукьяненко. Это повышает требования к защите, которая должна работать в режиме круглосуточного мониторинга, что недостижимо для большинства МСП собственными силами.

Новые источники риска

Отдельный и, по оценке ряда респондентов, недооцененный источник риска для малого и среднего бизнеса связан с зависимостью от внешних платформ. Значительная часть таких компаний работает на чужой инфраструктуре — торговых площадках, маркетплейсах, сервисах бронирования, облачных CRM и арендованном хостинге — и наследует их уязвимости. Часто если целью атаки становится один сайт или сервис, то страдает вся площадка.

Вторая зона риска — стремительный рост числа внешних цифровых сервисов и инструментов на основе искусственного интеллекта. Сотрудники и подрядчики используют множество платформ, и ключевым становится вопрос, где хранятся данные и что допустимо загружать во внешние сервисы. По словам владельца клиники «Доктор Фридман» Ильи Фридмана, для организации закрытого контура стоимость оборудования больших языковых моделей слишком высока. Опыт ИТ-директора (CIO) компании Tom Tailor Дмитрия Касаткина указывает на смежный вектор — риск цепочки поставок. Это когда компанию могут взломать не через собственную инфраструктуру, а через подрядчика.



Четыре уровня зрелости

Анализ интервью позволяет выделить четыре состояния информационной безопасности в компаниях МСП.

Нулевой уровень — слепая зона

ИБ не присутствует в управленческой повестке. На рабочих станциях стоит антивирус, этого считается достаточно. Нет отдельного ответственного, бюджет не выделяется, риски формально не оценены. Профиль таких компаний — мелкосерийное производство, b2b без онлайн-транзакций. **Чаще всего это отражает не безразличие, а ограниченность ресурсов и низкую цифровизацию основного процесса.** Сооснователь и директор производственно-методической компании «Геккон» Эльдар Губейдулин формулирует эту позицию прямо. «У нас нет возможности держать штат сотрудников или привлекать компании, которые проведут аудит нашей безопасности», – подчеркивает он.

Первый уровень — реактивный

Функция появляется после конкретного инцидента или регуляторного давления. Решения принимаются ситуативно. Ответственность концентрируется на одном человеке, а бюджет формируется под конкретные мероприятия, а не под планомерное выполнение ИБ-функции. Характерный пример приводит Александр Изюмский, директор дирекции по развитию цифрового бизнеса АСНА. Серьезная кибератака на ИТ-инфраструктуру компании стала точкой перелома. После нее была проведена реорганизация штата и пересмотрена архитектура защиты. «Благодаря оперативной работе команды удалось восстановить критические системы и предотвратить существенные потери для бизнеса. Это, конечно, стало тем самым импульсом, когда в течение 1,5 лет мы усилили компетенции в этом направлении и выстраивали новую стратегию защиты с полным карт-бланшем на изменения», — описывает он триггер трансформации.

Второй уровень — осознание без системы

Руководители понимают риски, изучают рынок, формулируют требования к будущему партнеру, но не переходят к структурным изменениям. Большинство опрошенных относится именно к этой категории.
«Я к аутсорсингу отношусь положительно. Если компания действительно занимается этой функцией, она может быть максимально прокачанной. Другое дело, что мы сами должны разбираться, что это такое и что мы хотим, иметь представление, как это должно выглядеть и сколько должно стоить», — комментирует Евгения Ламина, коммерческий директор ООО «Геомед».
Именно здесь обнаруживается явление, которое можно условно назвать «петлей недоверия». Желание привлечь внешнего исполнителя сталкивается с невозможностью верифицировать его работу собственными силами. Все упирается в закономерный вопрос о том, что **если для проверки вендора нужно нанимать отдельного эксперта, то зачем тогда вендор.**

Третий уровень — системный

Есть дорожная карта, аутсорсинговый центр мониторинга или собственная служба. Аутсорс используется точечно как усиление, а не замещение. ИТ-директор ООО «Латео» Иван Козлов отмечает, что эффективность ИБ-функции оценивается по дорожной карте развития компании, а внешние пентесты проводятся ежегодно с привлечением разных подрядчиков.

Стоит отметить, что переход между уровнями происходит не плавно, а скачкообразно.

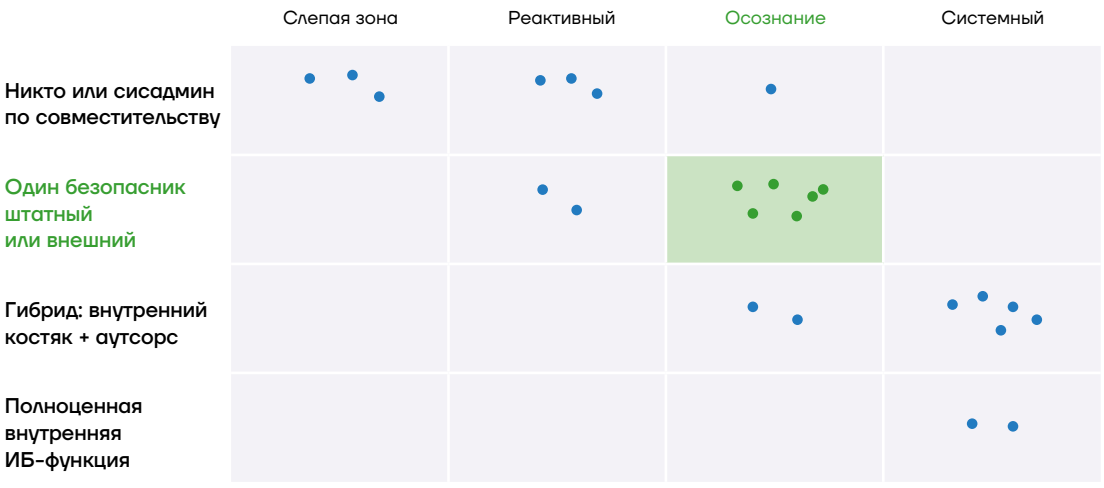
Триггером часто становится инцидент или прямое предписание регулятора. Вместе с тем триггерная модель не универсальна: часть компаний выстраивала защиту заблаговременно, исходя из оценки рисков, а не после потерь. Дмитрий Рыжиков - «Лагонаки.ру», товарный знак «itmode.» – отмечает, что закладывал требования к защите еще на этапе создания бизнеса. «**Думал об этом изначально.** Даже компанию строил так: выбирал защищенную CRM-систему, связывал с сайтами, с соцсетями. Всё делал сразу», – отметил он.

Схожую логику — выстраивать защиту до, а не после потерь — демонстрируют и другие респонденты. Исполнительный директор крупного производителя одежды подошел к ИБ системно еще до серьезных инцидентов. Аналогичную позицию занимает основатель консалтинговой компании HeadExpert Александр Абрамкин, для которого зрелое отношение к безопасности сложилось из общего усложнения цифровой среды, а не из конкретного происшествия.

Зрелость может выражаться и в осознанном ограничении периметра. Илья Фридман описывает свой подход как закрытый контур. Наружу данные либо не передаются вовсе, либо обезличиваются, а работа ведется через сертифицированных отраслевых операторов, гарантирующих защиту. **Для него критический инцидент — это появление медицинских данных своего пациента в открытом доступе — и именно для предотвращения такого риска выстроена его модель.**

Уровень зрелости × модель организации ИБ

где какие компании концентрируются (точка респондент N=24)



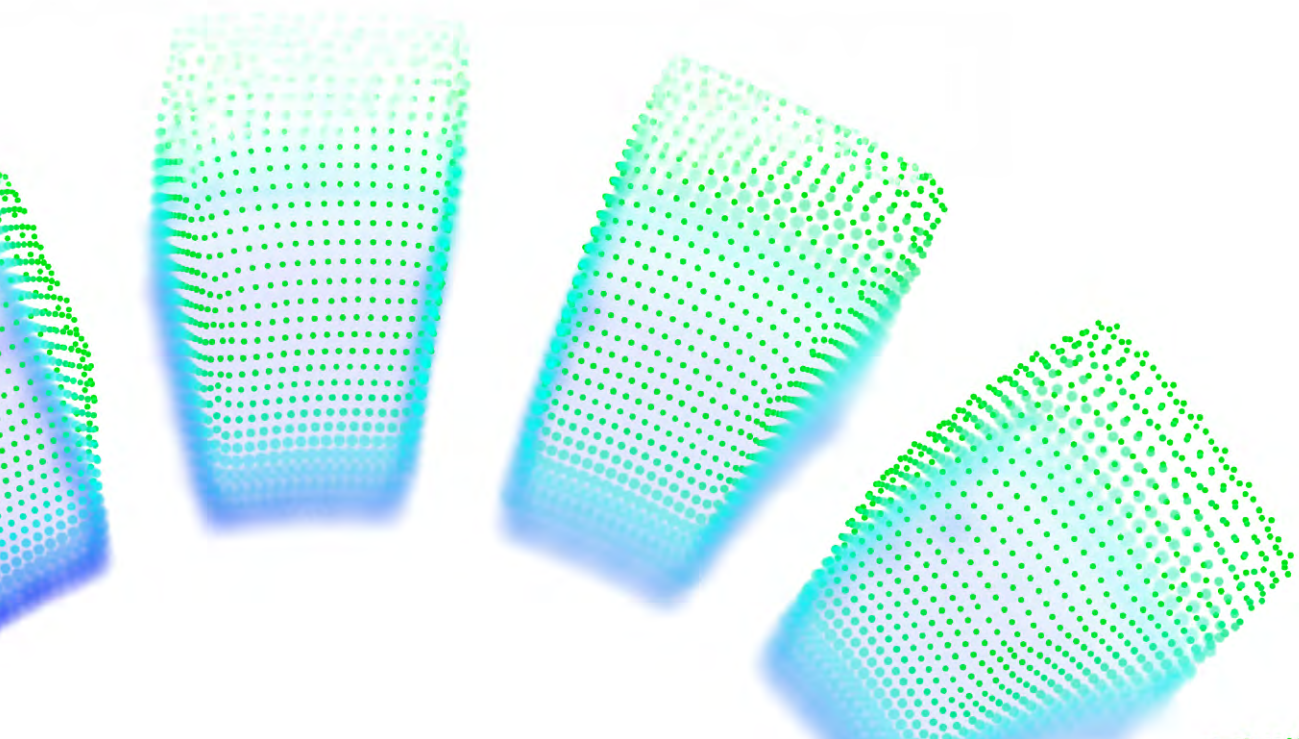
Большинство выборки - на пересечении 2-го уровня и модели «один безопасник» либо «гибрид». Левая нижния зона (0 уровень х полноценная служба) и правая верхняя (3 уровень х никто) в выборке не встречаются, Полный аутсорс ИБ ни один респондент не рассматривает.

Главный мотиватор — предсказуемость

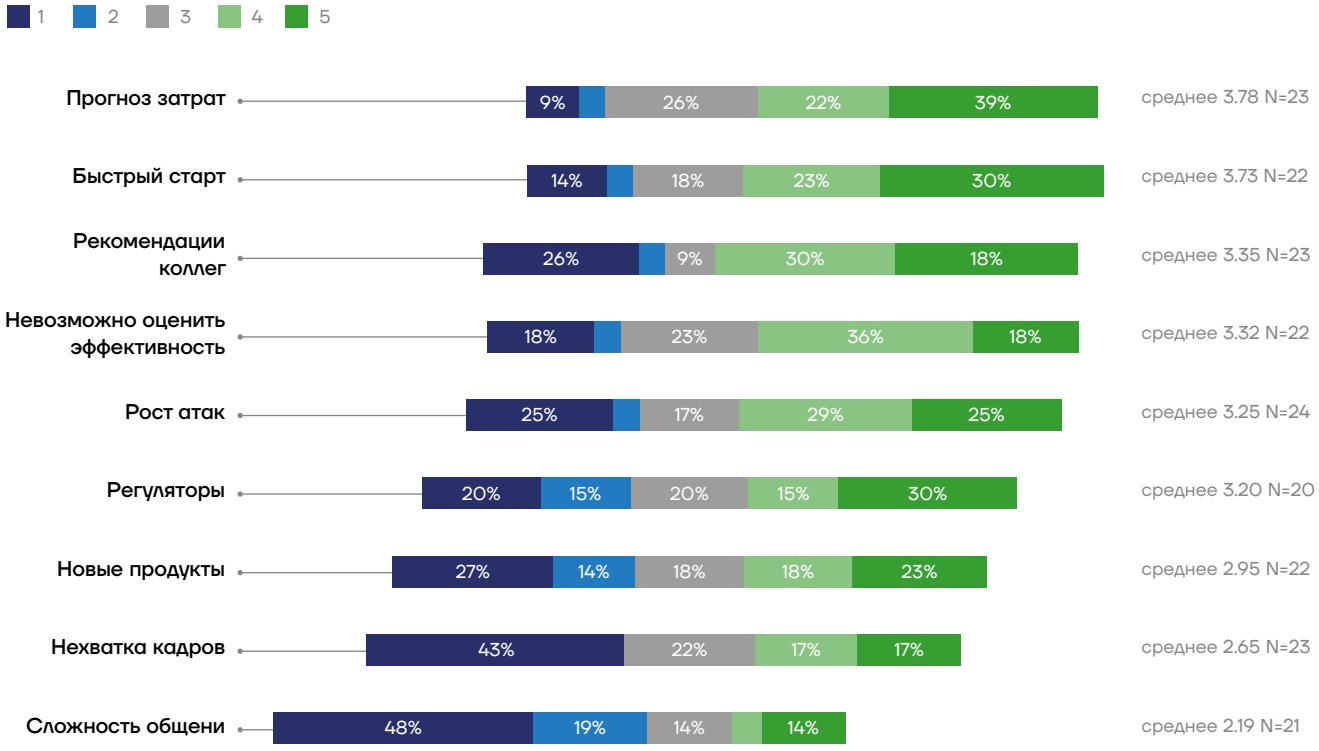
В блиц-опросе фактор «прогнозируемость затрат на ИБ» (средняя 3,78) уверенно лидирует среди драйверов интереса к аутсорсу. Следом идут «быстрая организация защиты» (3,73) и «рекомендации коллег из других компаний» (3,35). «Рост числа и сложности атак» (3,25) занимает четвертое место. «Нехватка кадров и сложность найма» (2,65) опустилась в нижнюю часть рейтинга. Этот результат корректирует представление о том, что главный двигатель аутсорса — кадровый голод. Данный вопрос остается значимым для среднего бизнеса с собственной ИТ-командой, но в целом по выборке его заметно опережают финансовый и операционный факторы.

Логика проста, при ограниченном бюджете и неровной выручке компании готовы выбрать предсказуемую операционную статью расходов вместо капитальных вложений с неопределенной отдачей. Один из респондентов описывает это через арифметику. Подписка на сервис ИБ за 1–1,5 млн рублей в год выгоднее, чем наём в штат специалиста с фондом оплаты труда в 3 млн рублей.

Финансовый вопрос важен и для более крупных компаний. Они активно рассматривают аутсорс или уже пользуются им, предпочитая облачные – масштабируемые – решения оплате работы центров реагирования на угрозы. Говоря про постройку собственной инфраструктуры, эффект описывает Роман Лукьяненко. «Ты вынужден брать такие же решения, как компании на десятки тысяч сотрудников, и переплачивать за размер, который тебе не нужен», – сказал он.



Драйверы интереса к аутсорсу ИБ



1 — совсем не актуально, 3 — нейтрально, 5 — максимально актуально

N=24 респондента, пропущенные оценки исключены из расчета. Полосы упорядочены по среднему (сверху - самые значимые факторы).

Респонденты стремятся перевести коммуникацию с поставщиками услуг ИБ в понятную экономическую плоскость с предсказуемым ежемесячным платежом и измеримым результатом. Для руководителя МСП предсказуемость — необходимое условие принятия положительного решения. Прогнозируемость расходов и снижение времени на восстановление нормального режима работы после инцидентов являются факторами, которые повышают финансовую устойчивость предприятий МСП.

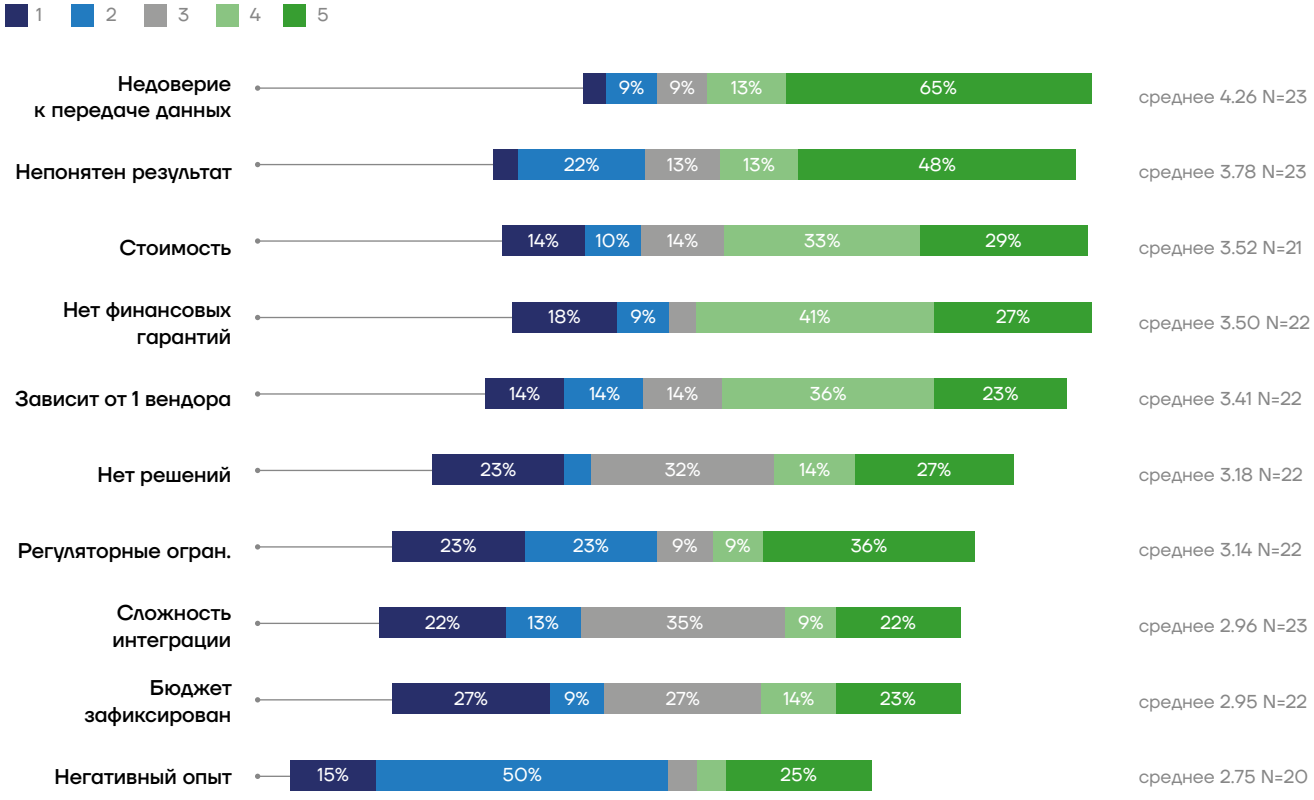
Главный барьер — недоверие и непрозрачность

В блиц-опросе по барьерам использования аутсорса первое место занимает «недоверие к передаче чувствительных данных вовне» (средняя 4,26), второе — «непонятно, как оценить результат работы вендора» (3,78). Эти два барьера составляют верхний эшелон, оба относятся к информационной асимметрии между заказчиком и поставщиком. Третий — «стоимость» как барьер (3,52), далее с минимальным отрывом «отсутствие финансовых гарантий» (3,50) и «зависимость от одного вендора» (3,41).

Иван Козлов, ИТ-директор (CIO) ООО «Латео», описывает первый из них. **«Когда мы отдаем аутсорсеру весь периметр, то теряем контроль и не знаем, что там происходит и делают ли они что-то реально.** Может взяли деньги — сделали видимость «что у нас все хорошо», а дальше сидят и ничего не делают», — отмечает он.

Второй барьер — непрозрачность предмета услуги — формулирует основатель консалтинговой компании HeadExpert Александр Абрамкин. **«Бизнесу важно понимать, что именно он покупает**: аудит, мониторинг, сопровождение, реагирование, снижение риска, соответствие требованиям или просто «пакет услуг». **Если предмет услуги размыт, решение принимать сложно»**, – говорит он. Для компании, у которой доверие клиентов является ключевым активом, любая непрозрачность защиты этого актива воспринимается как недопустимый риск. Дополнительное, репутационное и регуляторное измерение данная тема приобретает для медицинских организаций, оперирующих чувствительными персональными данными пациентов. Медицинский директор клиники иммунной диетологии «Иммунохелс Рус» Ольга Посвянская подчеркивает, что **привычные неформальные практики несовместимы с цифровой средой**. Данные пациентов передаются только по защищенному каналу, со всех сотрудников взяты обязательства о неразглашении, а свободное обращение с клиентской базой недопустимо. «Кибербезопасность — это вопрос цифровой среды», — формулирует она.

Барьеры использования аутсорса ИБ



1 — совсем не актуально, 3 — нейтрально, 5 — максимально актуально

N=24 респондента, пропущенные оценки исключены из расчета: Полосы упорядочены по среднему (сверху - саные значиные факторы).

Концентрация рисков на одном сотруднике

Самая распространенная модель организации ИБ-функции в МСП, если она есть, — единственный специалист, штатный или внешний на неполной занятости, отвечающий одновременно за поддержку пользователей, инфраструктуру и собственно безопасность. Преимущества для CEO очевидны: простота управления, низкая стоимость, личная доступность. Системные риски — концентрация знаний и компетенций на одном человеке, отсутствие у руководства возможности оценить качество его работы, ограничение защиты тем, что специалист помнит и успевает, невозможность круглосуточного мониторинга.

Сами руководители понимают данную уязвимость. Характерный признак этой осознанности — то, как именно она формулируется. Один из участников опроса, говоря о главном беспокоящем факторе в текущей организации ИБ, формулирует его через имя конкретного человека: **«Не дай бог с Владимиром что-то случится», — заявил он.** В этой реплике обнаруживается структурный факт: для управленца ИБ-функция фактически слилась с конкретным сотрудником и существует в его сознании не как процесс, а как личность. При потере единственного исполнителя компания не может даже инвентаризировать собственный парк машин. Концентрация риска при этом систематически недооценивается. Владельцы, несмотря на осознание реальности ИБ-рисков, оценивают вероятность наступления инцидента в ближайшее время как низкую и не закладывают в бюджет длительный сбой ИТ-функции.

В нескольких компаниях выборки эта же фигура — привычный системный администратор, обслуживающий бизнес годами — оказывается одновременно главным препятствием на пути к профессиональному решению. От его услуг сложно отказаться, не теряя накопленных знаний об оборудовании, конфигурациях и контуре. На уровне принятия решений этот момент часто оказывается весомее экономических выкладок. «Для локального офлайн-бизнеса в сфере услуг, у которого нет значимых онлайн-сервисов и критичных данных в открытом контуре, серьезная внешняя система ИБ пока избыточна», — описывает логику соразмерности мер профилю бизнеса владелец сети стоматологических клиник «Денталь Профи» Александр Хан.

Человеческий фактор

Отдельная тема, к которой независимо возвращались многие респонденты, — человеческий фактор. Какой бы ни была техническая защита, источником инцидента чаще оказывается не отсутствие технологии, а действие сотрудника. Александр Хан называет этот фактор основным риском для своей организации. «На корпоративную почту пришло письмо с вложением, файл открыли — компьютер заразили шифровальщиком и потребовали выкуп. Данные восстановили из ночной резервной копии, но рабочий день был потерян», — рассказал он.

Несколько респондентов отмечают, что значительная часть атак начинается с фишинга, поэтому акцент делается на обучении сотрудников действиям при получении подозрительных писем. Вице-президент по развитию нефтесервисной компании добавляет еще один риск, связанный с человеческим фактором. Уволившийся сотрудник может унести с собой наработки компании — ее интеллектуальную собственность.

От обороны — к восстановлению

Одно из наблюдений касается управленческой логики, которая обнаруживается у респондентов с наибольшим опытом. Они отказываются от попытки построить непробиваемую защиту и переориентируются на способность быстро восстановиться после инцидента.

Александр Изюмский, директор дирекции по развитию цифрового бизнеса АСНА, описывает выбранную стратегию. «Мы провели базовые работы, но главные усилия сосредоточили на создании надежной системы резервного копирования, географически распределенной, с изолированным офлайн-компонентом и регулярными учениями по восстановлению. Цель была в том, чтобы сделать стену непробиваемой и иметь все возможности быстро «подняться» после любого инцидента», — отметил он. По его словам, **резервное копирование построено по стратегии «3-2-1»** — три копии в двух разных местах, одна из которых вынесена за пределы ЦОДа.

ИТ-директор АО «Фирма Евросервис» Виктор Чуваев формулирует свой принцип: «Персонал и инфраструктура должны быть готовы к оперативному восстановлению». По его словам, именно экономическая нецелесообразность содержания круглосуточной внутренней службы мониторинга подталкивает бизнес к переходу на аутсорсинг SOC.

Сдвиг важен, поскольку он может влиять на приоритеты при бюджетировании. Вместо увеличения расходов на превентивные средства защиты ресурсы будут направлены на резервное копирование, планы обеспечения непрерывности исполнения ИТ-функций и способность усиливать защиту в кризисные моменты. **Быстрое реагирование при наступлении инцидента у респондентов с высокой зрелостью ИБ ценится выше, чем скорость развертывания средств защиты.**

Логику принятия решений и оценку рисков ИБ раскрывает главный экономист ЗАО «Хлеб» Светлана Шилова. Она указывает, что физический процесс выпечки «можно восстановить руками», тогда как потеря ERP-системы означает остановку приема заказов и отгрузки. Такое деление активов характерно для производственных компаний с невысокой долей цифрового компонента в основном бизнес-процессе.

«Хлеб — продукт социальный, с невысокой долей маржинального дохода. В таких условиях любая внеплановая затрата, включая внедрение систем защиты информации, становится чувствительной. Физически люди смогут выпечь хлеб, обладания умениями и навыками, но процессы приемки заказов и отгрузки продукции полностью зависят от работоспособности информационной системы. Без нее физическая способность испечь хлеб не имеет экономического смысла», – говорит она.

Недоинвестирование в ИБ ведет к риску полной остановки бизнеса. Расходы на кибербезопасность снижают рентабельность, однако потенциальный ущерб от простоя из-за киберинцидента гораздо больше.

Предпочитаемая модель — партнерство

Модель обоюдных обязательств получила широкое признание. Готовность принять симметричную ответственность, когда вендор отвечает за защиту, а заказчик — за выполнение базовых требований гигиены, выражена независимо от размера компании и отрасли. **«Поставщик имеет такое право. Более того, это правильно. Нельзя требовать от вендора полной ответственности, если компания сама не выполняет базовые меры:** не обновляет системы, не использует двухфакторную аутентификацию, не контролирует доступы, не обучает сотрудников», — формулирует условие основатель компании

HeadExpert Александр Абрамкин. Сходная логика прослеживается у многих других респондентов и не оспаривается даже аутсорс-скептиками.

Несколько участников подчеркивают: **ни одно техническое решение не дает стопроцентной гарантии, сколько ни вложи в защиту, остается риск взлома**. А значит открытым остается вопрос, как покрыть киберриски. Эту проблему развернуто описывает CIO компании Tom Tailor Дмитрий Касаткин. «Я хочу застраховаться, но не могу застраховаться. Такие услуги на рынке есть, но они неполноценные, много ограничений», — поясняет он. Именно поэтому барьер «отсутствие финансовых гарантий» он оценивает максимально высоко, хотя сам близок к полной передаче функции на аутсорс.

ИТ-директор АО «Фирма ЕВРОСЕРВИС» Виктор Чуваев упоминает обсуждаемый на рынке лимит ответственности в 1 млн долларов. И хотя вряд ли дело дойдет до выплат, такие гарантии — это маркер взаимных обязательств, которые побуждают обе стороны действовать слаженно ради минимизации рисков. Именно поэтому наличие подобных условий может стать решающим фактором при выборе поставщика. В качестве жизнеспособной альтернативы эксперт приводит встроенное страхование от операторов связи в рамках защиты от звонков мошенников, которое автоматически активируется вместе с услугой.

Конструкция, которая в материалах интервью прозвучала как наиболее заслуживающая доверия — независимая страховая компания как третья сторона договора между вендором и заказчиком. «Такой подход мне нравится. Здесь здоровый интерес: они растут за счет нас, проверяя собственную защиту, которую нам же и предоставляют. В итоге я защищена, так как заплатила за услугу — и ничего не теряю», – комментирует владелец кафе «Городок» из Самарской области Елена Деревяга.

Преобладание гибридной модели

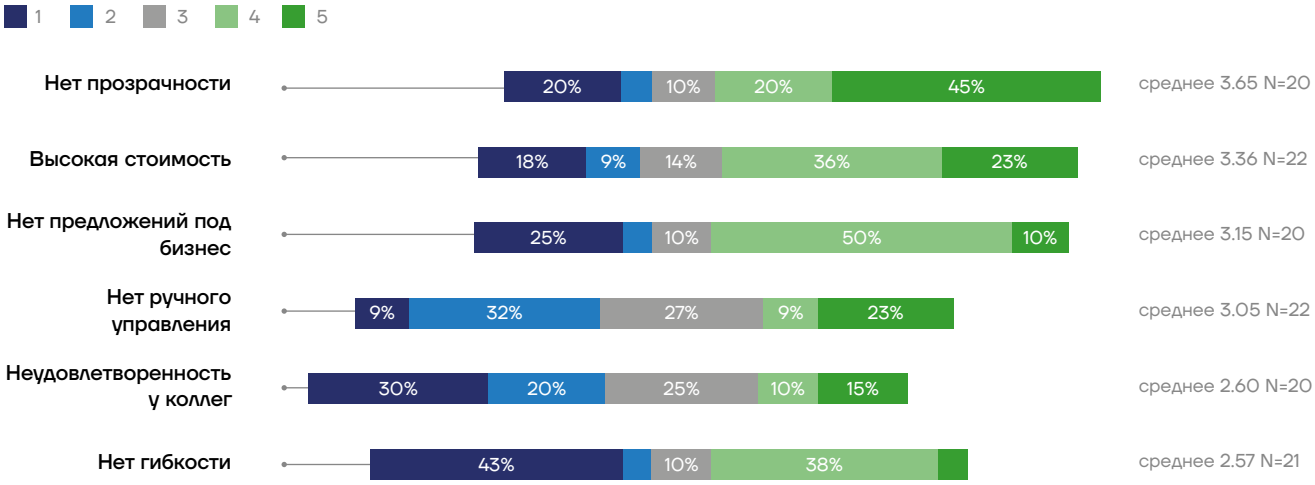
Большинство респондентов, рассматривающих аутсорс, предпочитают гибридную конструкцию, при которой внешний партнер выполняет мониторинг, реагирование и экспертизу, а внутри компании остаются регламентирование, контроль, управление доступами, физическая инфраструктура и принятие решений по рискам. Эта модель воспринимается как реалистичная и зрелая.

Распределение ролей чаще описывают в логике, при которой стратегию компания определяет сама, а подрядчиков привлекает на конкретные задачи. «Тендер проводим. По техническому заданию подрядчики присылают коммерческие предложения, и дальше мы их выбираем», — описывает процесс ИТ-директор ООО «Латео» Иван Козлов.

К полной передаче информационной безопасности на аутсорс были готовы только несколько компаний. По оценке Дмитрия Касаткина, внешними подрядчиками можно закрыть порядка 90–95% задач ИБ в компании. За внешними партнерами — документооборот, работа с персональными данными и защита внешнего контура, внутри остается управление правами доступа. **«Какая разница, кто исполнитель? Мне важно, чтобы были метрики, которые выполняются»**, – отмечает он. Самым сложным в переходе он называет не выбор продуктов, а договорную работу — порядок передачи и использования персональных данных.

Скепсис в отношении полного аутсорса отчасти объясняется тем, что предложение, которое сегодня видят в сегменте МСП, не совпадает с представлениями о приемлемой услуге. В блиц-опросе о недостатках аутсорса ИБ на рынке первое место занимает «отсутствие прозрачности результатов» (3,65). Вплотную за ним — «высокая стоимость» (3,36). Следом — «отсутствие предложений, закрывающих потребности бизнеса» (3,15) и «отсутствие ручного управления» (3,05).

Ключевые недостатки аутсорсинга ИБ на рынке

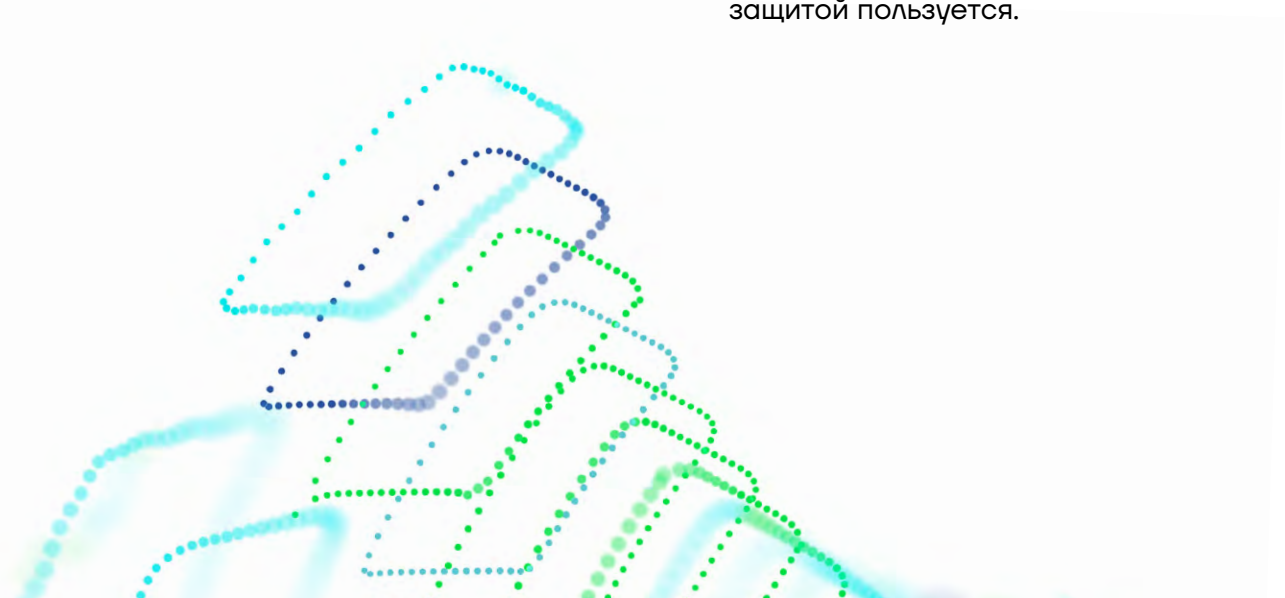


1 — совсем не актуально, 3 — нейтрально, 5 — максимально актуально

N 24 респондента, пропущенные оценки исключены из расчета, Полосы упорядочены по среднему (сверху - самые значимые факторы).

Вместе эти оценки указывают на то, что **рынок ИБ-услуг для МСП только формируется.** Большинство предложений изначально рассчитано на крупных корпоративных заказчиков с соответствующими бюджетами и инфраструктурой. Продукты и услуги зачастую не адаптированы под потребности МСП, которые, если решают им воспользоваться, переплачивают за функциональность, которой не пользуются, и не получают ни понятного отчета, ни возможности влиять на ход услуги. Предложения, построенные по принципу полного перекладывания ответственности, малым и средним бизнесом воспринимаются как маркетинговая абстракция.

Запрос МСП — **ясное разделение ролей, формализованные обязательства каждой стороны и предсказуемое ценообразование.** Дмитрий Рыжиков предлагает рассматривать ИБ для микропредприятий как объект совместной с государством работы. **«Если безопасность будет у небольших компаний стоить половину от стоимости CRM, это будет отличное решение**. Сделайте совместно с Минцифрой, выбейте денег — у бизнеса действительно будет мини-щит», – подчеркивает он. По его мнению, при стоимости такого щита в пределах нескольких тысяч рублей в месяц малый бизнес массово согласился бы на подобный продукт. Рынок находится в точке, где необходим диалог между теми, кто предоставляет защиту, и теми, кто этой защитой пользуется.



Что это значит для руководителя МСП

Приведем несколько практических следствий, которые могут быть полезны при пересмотре подхода к информационной безопасности.

- **Привычное предположение о том, что компании среднего размера интересны атакующим в меньшей степени, уже не подтверждается.** С середины 2023 года порог интереса атакующих существенно сместился вниз, из-за чего базовая оценка периметра обретает смысл независимо от размера бизнеса.

- **Значимая часть риска приходится не на технологии, а на человеческий фактор.** Обучение сотрудников распознавать фишинг, аккуратность с доступами и каналами передачи данных, а также порядок действий при уходе ключевых людей дают эффект, сопоставимый с вложениями в инструменты.

- **В вопросах безопасности на первый план может выходить зависимость от внешних платформ.** Если бизнес работает на маркетплейсе, в облачной CRM или на арендованной площадке, часть рисков он наследует от инфраструктуры, которой не управляет. Полезно понимать, где хранятся данные и что допустимо загружать во внешние сервисы, включая инструменты на основе ИИ.

- **Концентрация всех ИТ- и ИБ-функций на одном человеке создает скрытый риск, который обычно недооценивается.** План обеспечения непрерывности на случай его ухода — отдельная задача, которая в большинстве компаний выборки не стоит.

- **При выборе между капитальными вложениями в собственную инфраструктуру и подпиской на внешний сервис основной критерий — не экономия, а предсказуемость и измеримость.** Понятный ежемесячный платеж и регулярная отчетность на уровень директоров в текущей рыночной конфигурации работают эффективнее, чем единовременные крупные инвестиции в инструменты, которые потом нужно содержать.

- **Стратегия защиты, ориентированная на быстрое восстановление, для значительной части МСП оказывается рациональнее стратегии превентивной обороны и при этом дешевле.** Резервное копирование, план реагирования на инцидент и способность эскалировать защиту в кризис в этом смысле важнее набора средств предотвращения угроз.

- **При выборе внешнего партнера ключевые маркеры зрелости — четкое разделение зон ответственности, формализованные обоюдные обязательства, отчетность на управленческом языке и независимая верификация результата.** Декларативные финансовые гарантии без их понятного механизма воспринимаются как исключительно маркетинговые утверждения.

Продолжение эволюции рынка

На рынке кибербезопасности для МСП в России появляются новые возможности. Атаки участились и теперь затрагивают большинство предприятий. Руководители бизнеса это понимают и формулируют запрос на повышение уровня защиты.

Пересечение запроса МСП и предложения на рынке ИБ

наблюдение по результатам интервью с 25 руководителями МСП

Однако пока представители МСП отмечают, что **еще не сложилось взаимопонимания между защищаемыми и защитниками.** С одной стороны, предложение на рынке либо построено под крупный корпоративный сегмент, либо ограничено базовыми инструментами. С другой стороны, **бизнес только начинает овладевать языком, который позволяет ему формулировать свои потребности.** Построение успешного диалога потребует от обеих сторон шагов навстречу друг другу. Поставщикам предстоит **подготовить предложения на языке МСП.** С понятной экономикой, прозрачной отчетностью, четкими взаимными обязательствами. Самим компаниям будет лучше пересмотреть подход к ИБ и перестать думать о ней, как о разовой покупке продукта. В современных реалиях это отдельное постоянное направление работы, включающее **мониторинг и готовность быстрого восстановления после инцидента.**

В таком контексте **модели аутсорса кибербезопасности могут стать приемлемым для МСП решением.** Но доверие к ним еще предстоит вырастить на почве **прозрачности требований, измеримости результата и совместной ответственности.** Во многом развитие рынка ИБ для МСП будет зависеть от того, как пойдет построение этого диалога.