



Октябрь 2026

Оценка отраслевого киберприоритета малого и среднего бизнеса

Содержание

От авторов	3
1. Ключевые выводы	4
2. Актуальность проблемы.....	7
3. Меры поддержки киберустойчивости МСП.....	9
3.1. Международная практика	9
3.2. Российская практика	10
4. Методология оценки киберприоритета	11
4.1. Отраслевой индекс киберкритичности	12
4.2. Отраслевой индекс доступности киберустойчивости МСП	13
4.3. Отраслевой индекс влияния МСП	13
4.4. Итоговый показатель — Отраслевой индекс киберприоритета МСП	14
5. Результаты пилотного расчёта	16

От авторов

Обеспечение киберустойчивости малого и среднего бизнеса требует решений, соразмерных его финансовым, кадровым и управленческим возможностям. При этом положение МСП существенно различается по отраслям: неодинаковы зависимость от цифровых технологий, стоимость защиты и экономическая роль небольших предприятий.

В исследовании предложена методика, которая призвана помочь определить, в каких отраслях повышение доступности киберустойчивости МСП требует первоочередного внимания. Она объединяет три составляющие: киберкритичность отрасли, экономическую доступность защиты для типовых предприятий и влияние МСП на отрасль. Доступность оценивается через сопоставление расчётного бюджета предприятия на информационную безопасность (киберустойчивость) со стоимостью достаточного (эффективного) профиля защиты.

Практическая задача исследования — дать государству, поставщикам ИБ-решений и услуг, крупным заказчикам и отраслевым объединениям ориентир для заблаговременного принятия решений. Результаты могут использоваться при разработке мер поддержки, развитии доступных продуктов и сервисов, подготовке кадров и повышении киберустойчивости поставщиков крупного бизнеса. В дальнейшем отдельные показатели методики могут дополнить составляющую кибербезопасности в «Индексе цифровой зрелости субъектов МСП» Корпорации МСП.

Работа опирается на отраслевую статистику, открытые рыночные данные и экспертные оценки. Она не предполагает сравнительного рейтинга предложений поставщиков или проверки фактической защищённости отдельных организаций или отраслей. Полученный отраслевой индекс киберприоритета МСП следует рассматривать как ориентир для распределения внимания и усилий с учётом принятых допущений.

Пилотный расчёт фиксирует исходное положение для дальнейшего мониторинга. Повторные измерения по сопоставимой методике позволят оценивать, становится ли обеспечение киберустойчивости доступнее, как меняются отраслевые приоритеты и где сохраняется потребность в дополнительных мерах. Динамику итогового показателя необходимо анализировать вместе с изменениями его составляющих.

При интерпретации результатов следует учитывать ограничения методики:

1. Экспертное определение профиля защиты и ограниченная выборка рыночных оценок. Состав достаточного профиля защиты выбран экспертно для каждого типоразмера предприятия и отрасли. Расчётная стоимость усредняется с оценками производителей ИБ-решений, полученными через профильный опрос.
2. Перенос отраслевой структуры затрат на МСП. Коэффициенты затрат на ИТ и ИБ, полученные по данным Росстата для крупного и среднего бизнеса, применяются к типовым профилям МСП той же отрасли. Это допущение о сопоставимости структуры затрат предприятий разного размера требует дальнейшей проверки.
3. Условный характер отраслевой оценки связи с КИИ. Она основана на интерпретации законодательства и перечня типовых отраслевых объектов КИИ применительно к разделам и подразделам ОКВЭД. Такая оценка не устанавливает правовой статус конкретных организаций и их информационных систем. Для строительства связь с КИИ задана экспертно.

Благодарим Positive Technologies, «Лабораторию Касперского», VI.ZONE и ГК «Солар» за участие в подготовке исследования.

1. Ключевые выводы

Цифровизация бизнес-процессов усиливает зависимость малого и среднего бизнеса от информационных систем, облачных сервисов и онлайн-платежей. Как и у крупных компаний, сбои в их работе могут привести к нарушению деятельности и финансовым потерям. Высокие киберриски МСП подтверждаются российской и международной статистикой, а развитие генеративного искусственного интеллекта позволяет злоумышленникам проводить атаки быстрее и с меньшими трудозатратами.

За последний год 86% компаний сегмента малого и среднего бизнеса в мире сталкивались с киберинцидентами, а в России — 82%¹. При этом на Россию приходится 14–16% всех успешных атак в мире, а их число в 2026 году может вырасти ещё на 30–35% к уровню 2025 года². По данным CrowdStrike Global Threat Report 2026³, в 2025 году число наблюдаемых компанией атак со стороны злоумышленников, применяющих ИИ, выросло на 89% по сравнению с предыдущим годом. ИИ активно используется на разных этапах атаки: для поиска и сбора информации о целях, подготовки социальной инженерии, создания скриптов для кражи учётных данных и сокрытия следов.

При этом коммерческий рынок решений и услуг для обеспечения киберустойчивости ориентирован прежде всего на крупные организации. Для типового МСП комплексная защита и её постоянное поддержание могут оставаться слишком дорогими и сложными. Это проблема не только для малого предприятия: МСП входят в цепочки поставок крупного бизнеса как подрядчики, ИТ- и сервисные партнёры. Недостаточная защищённость таких МСП-контрагентов может стать причиной сбоев в работе крупных заказчиков или дать злоумышленникам доступ к их системам.

Российская и зарубежная практика поддержки киберустойчивости МСП различаются. В России, как и во многих других странах, обязательные требования к защите определяются прежде всего характером деятельности организации и обрабатываемых данных, а не размером бизнеса. В ряде зарубежных стран общие требования дополняются специальными программами поддержки, учитывающими ограниченные возможности МСП. Участие в них добровольное, а финансирование нередко берёт на себя государство. Такие программы включают:

- сертификацию и самодекларацию выполнения базовых мер киберустойчивости;
- адресные образовательные программы;
- методические материалы регуляторов, разработанные для МСП.

За рубежом это дает возможность профессиональным участникам рынка использовать подобные государственные программы, побуждая МСП внедрять меры защиты. Например, подтверждение выполнения мер через самодекларацию или сертификацию может быть условием киберстрахования. В России такие подходы к поддержке киберустойчивости МСП пока не получили сопоставимого развития.

Цифровая зависимость и экономический вклад МСП существенно различаются от отрасли к отрасли, а значит разной должна быть и адресность мер поддержки. Эффективное принятие решений о разработке тех или иных мер по усилению киберустойчивости МСП требует отраслевой приоритизации.

¹ Самые распространённые киберугрозы для МСП, «Лаборатория Касперского», 2026

² CODE RED 2026: Актуальные киберугрозы для российских организаций, Positive Technologies, 2026

³ Global Threat Report: The Evasive Adversary Wilds AI, CrowdStrike, 2026

В качестве такого инструмента приоритизации предлагается методика «отраслевого киберприоритета МСП». Она позволяет измерить, в каких отраслях сочетание потребности в киберустойчивости, её ограниченной доступности для МСП и экономической роли малого и среднего бизнеса требует первоочередного внимания. Для отслеживания динамики изменений рекомендуется проведение ежегодной оценки.

Предложенная методика отраслевой приоритизации вводит три показателя: отраслевую киберкритичность, доступность киберустойчивости для МСП и влияние МСП на отрасль, а также сводит их в единый отраслевой киберприоритет МСП. Такая оценка может быть полезна государству, поставщикам решений и услуг информационной безопасности, крупным заказчикам и отраслевым объединениям.

Для проверки методики был проведен пилотный расчет для пяти заведомо разноплановых отраслей:

- финансовому сектору — высокорегулируемому, с наибольшими затратами на ИТ и ИБ;
- энергетике — инфраструктурной отрасли в контуре регулирования КИИ с минимальной долей МСП;
- обрабатывающим производствам — отрасли с высокой киберкритичностью и значимым сегментом МСП;
- строительству — отрасли с максимальной ролью МСП, работающей в том числе подрядчиком на объектах КИИ;
- сельскому хозяйству — отрасли с низкой цифровизацией и высокой долей МСП.

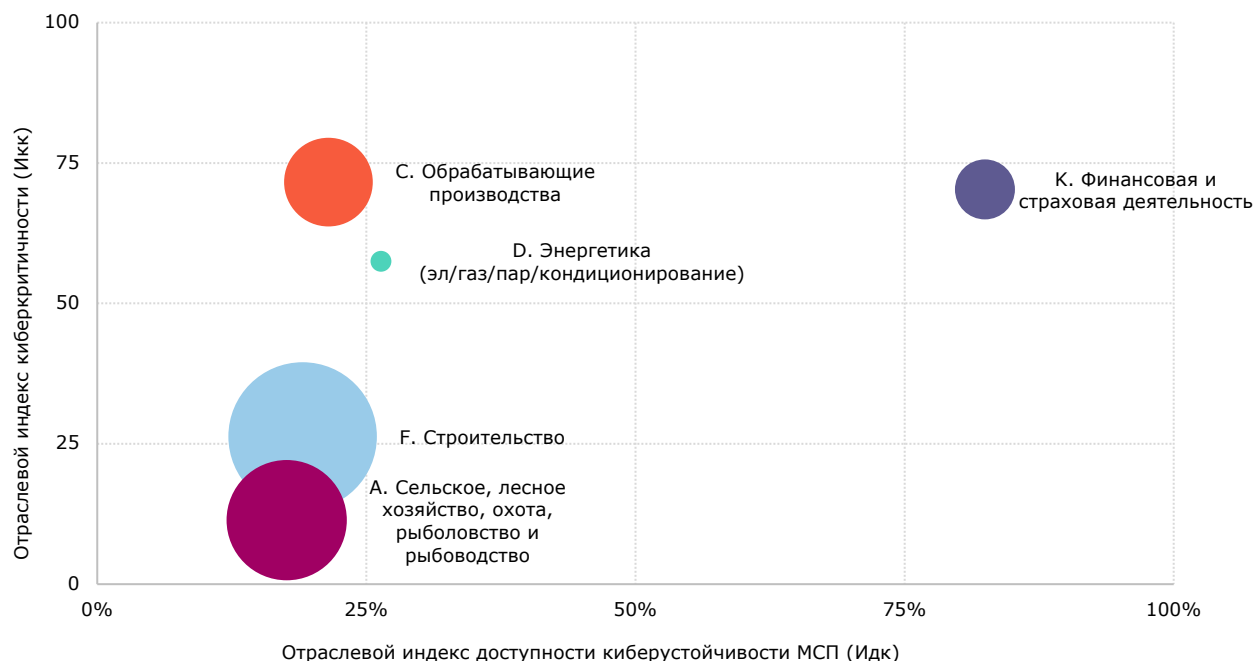
Такой набор позволяет проверить, дифференцирует ли методика отрасли с различной цифровой зависимостью, доступностью защиты и ролью МСП и согласуются ли её результаты с известными особенностями этих отраслей.

Согласно расчету, **наивысший киберприоритет МСП получают отрасли строительства и обрабатывающих производства** (51,8 и 50,8 из 100): в обеих отраслях низкая доступность киберустойчивости сочетается со значительным влиянием МСП — у строительства за счёт максимальной роли МСП, хотя малый строительный бизнес цифровизирован заметно ниже среднего по стране, у производства при высокой киберкритичности отрасли.

Сельское хозяйство занимает третье место (34,3).

Финансовый сектор и энергетика получают низкий итоговый приоритет, но по разным причинам: у финансового сектора — самая высокая среди пяти отраслей доступность киберустойчивости ($\approx 82,5$, близко к экономическому балансу) при относительно скромной роли МСП в отрасли, несмотря на высокую киберкритичность; у энергетики — минимальная роль МСП при высокой киберкритичности отрасли (основной риск сосредоточен у крупных инфраструктурных организаций вне периметра МСП и уже находящихся в контуре жесткого регулирования КИИ). Тем не менее, данный результат не является сигналом к отказу от поддержки МСП в этих отраслях — это только индикатор для соответствующей приоритизации усилий.

Сводная диаграмма отраслевых индексов киберприоритета МСП⁴:



В дальнейшем целесообразно расчёт киберприоритета МСП провести по всем разделам ОКВЭД и использовать как основу для адресных мер:

- определить отрасли, где поддержка киберустойчивости МСП даст наибольший эффект;
- проработать для них механизмы стимулирования — субсидирование доступа к управляемым ИБ-сервисам, добровольную сертификацию или самодекларацию базового уровня защиты;
- обеспечить доступ к образовательным программам.

Показатель доступности киберустойчивости показывает, насколько цена достаточной защиты расходится с возможностями типовых МСП в каждой отрасли. Для рынка информационной безопасности результаты указывают на МСП как на перспективный сегмент, которому нужны продукты и сервисы, рассчитанные на бюджет и компетенции малого бизнеса.

Важно отметить, что методика задумывалась прежде всего как инструмент для повторяемой оценки: регулярное обновление данных по единой методике позволит увидеть, сокращается ли разрыв доступности киберустойчивости со временем или нарастает в конкретных отраслях.

⁴ Объемный показатель – отраслевой индекс влияния МСП

2. Актуальность проблемы

Цифровая трансформация секторов экономики повышает производительность и конкурентоспособность бизнеса, одновременно усиливая его зависимость от информационных систем, облачных сервисов, онлайн-платежей и прочих цифровых каналов взаимодействия. Нарушение их работы может приводить к остановке бизнес-процессов, прямой потере выручки, дополнительным расходам и срыву контрактных обязательств.

Согласно данным ежегодного исследования Verizon DBIR 2026⁵, малые и средние организации составили около 96% жертв атак программ-вымогателей среди рассмотренных случаев, в которых был известен размер пострадавшей организации. При этом современные технологии генеративного искусственного интеллекта (GenAI, ИИ), активно применяемые злоумышленниками, позволяют проводить атаки намного быстрее и с меньшими трудозатратами. По данным CrowdStrike Global Threat Report 2026⁶, в 2025 году число наблюдаемых компанией атак со стороны злоумышленников, применяющих ИИ, выросло на 89% по сравнению с предыдущим годом. ИИ активно используется на разных этапах атаки: для поиска и сбора информации о целях, подготовки социальной инженерии, создания скриптов для кражи учётных данных и сокрытия следов. По наблюдениям CrowdStrike, среднее время от первоначального проникновения до начала перемещения злоумышленника внутри сети компании-жертвы в 2025 году составило всего 29 минут, а минимальное зафиксированное — 27 секунд. Согласно исследованию IDC & Sage 84% микро- и 65% малых предприятий не готовы к ИИ-угрозам или находятся на начальном этапе подготовки.⁷

По данным «Лаборатории Касперского»⁸ за последний год 86% компаний сегмента малого и среднего бизнеса в мире сталкивались с киберинцидентами, а в России — 82%. По частоте в мире лидирует фишинг (20% случаев), в России — массовые атаки вредоносным ПО (23%); на втором-третьем местах и в мире, и в России — эксплуатация уязвимостей ПО (17–18%) и получение удалённого доступа извне (16–18%). Отдельно стоит отметить новый быстро растущий вектор атак: с января по апрель 2026 года решения компании обнаружили более 33 тыс. атак на малый и средний бизнес по всему миру (включая Россию), где вредоносное ПО распространялось под видом популярных ИИ-сервисов (поддельные приложения ChatGPT, Claude, DeepSeek) — почти в 5 раз больше, чем за тот же период 2025 года.⁹

Positive Technologies отмечает¹⁰, что на Россию приходится 14–16% всех успешных атак в мире, а их число в 2026 году может вырасти ещё на 30–35% к уровню 2025 года. Рост атак, по оценке компании, затрагивает не только крупный бизнес, но и МСП — при этом малый и средний бизнес особенно уязвим из-за пробелов в защите в сочетании с высокой чувствительностью к репутационным потерям. Прогнозируется рост комбинированных последствий атак (одновременная утечка данных и остановка бизнес-процессов) и усиление атак на цепочки поставок.

По данным упомянутого ранее исследования Verizon, доля утечек, связанных с третьими сторонами и цепочкой поставок, выросла на 60% год к году и достигла 48% всех зафиксированных утечек (против 30% в отчёте за 2025 год и 15% годом ранее) — *«крупнейший разовый сдвиг за всю историю наблюдения»*, согласно авторам исследования. Европейское агентство по кибербезопасности также фиксирует¹¹ рост атак на подрядчиков и включает компрометацию цепочки поставок в число главных рисков для энергетики, транспорта, финансового сектора, госуправления и обрабатывающей промышленности. Один из самых известных примеров¹² такого сценария атаки — взлом сети розничных магазинов Target (США, 2013 год; NYSE: TGT, входит в индекс S&P 500, более 2000 магазинов по всей стране на 2026 год): злоумышленники не атаковали саму компанию напрямую, а провели фишинговую атаку на её подрядчика по обслуживанию систем отопления и

⁵ Data Breach Investigations Report, [Verizon](#), 2026

⁶ Global Threat Report: The Evasive Adversary Wields AI, [CrowdStrike](#), 2026

⁷ SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience, [IDC & Sage](#), 2026

⁸ Самые распространённые киберугрозы для МСП, [«Лаборатория Касперского»](#), 2026

⁹ Ландшафт угроз для малого и среднего бизнеса в 2026 году, [«Лаборатория Касперского»](#), 2026

¹⁰ CODE RED 2026: Актуальные киберугрозы для российских организаций, [Positive Technologies](#), 2026

¹¹ ENISA Threat Landscape, [ENISA](#), 2025

¹² Target HVAC Contractor Says It Was Breached By Hackers, [SecurityWeek](#), 2014

кондиционирования — небольшое предприятие Fazio Mechanical Services, имевшее удалённый доступ к сети Target. Через похищенные учётные данные подрядчика злоумышленники получили доступ уже во внутреннюю сеть Target, что в итоге привело к краже данных 40 млн банковских карт.

В России, согласно исследованию УЦБ SOC по данным первого полугодия 2026 года¹³, каждая третья успешная атака на компанию начиналась именно с проникновения через подрядную организацию. Похожую оценку дают¹⁴ и аналитики компании «Инфосистемы Джет». Центр исследования киберугроз «Солар» сообщал¹⁵, что к концу 2025 года 27% сложных атак на российские компании начинались через доверительные отношения — в 3,3 раза больше, чем в 2024 году.

Совокупность приведённых данных говорит о том, что недостаточная киберустойчивость МСП — это проблема не только для самого предприятия. Малые и средние предприятия выступают поставщиками, ИТ- и сервисными подрядчиками крупных компаний, участвуют в производственной кооперации, получают доступ к системам и данным заказчиков. Нарушение работы небольшого предприятия или компрометация его инфраструктуры способны затронуть других, в том числе крупных, участников цепочки поставок. Таким образом, обеспечение киберустойчивости МСП имеет сквозное значение для целых отраслей экономики государства.

Киберустойчивость — способность организации предупреждать киберинциденты, сохранять работоспособность критически важных бизнес-процессов в ходе сбоев и нарушений и своевременно восстанавливать нормальную работу, минимизируя операционный ущерб — является одним из условий устойчивого развития крупного, малого и среднего бизнеса.

Как и для крупных компаний, затраты МСП на обеспечение киберустойчивости включают непрерывную оценку рисков, приобретение и сопровождение средств защиты, организацию резервного копирования и восстановления, обучение сотрудников, привлечение специалистов или внешних исполнителей. При этом МСП острее сталкиваются с нехваткой финансовых средств, кадров и управленческих ресурсов для обеспечения киберустойчивости. Даже при наличии на рынке подходящих продуктов и услуг, в том числе отечественных, их совокупная стоимость и сложность использования могут оказаться несоразмерными возможностям малого предприятия. В таких условиях компании могут быть вынуждены сознательно принимать или заведомо игнорировать серьёзные киберриски, не располагая ресурсами для их снижения.

На коммерческом рынке производителями средств защиты представлены отдельные специализированные продукты для МСП – от антивирусного ПО до сетевых аппаратных решений, в том числе российского производства. Кроме того, растёт интерес интеграторов к малому бизнесу как аудитории управляемых, подписочных сервисов. Так, например, крупнейший российский провайдер управляемых услуг безопасности «Солар» ожидает¹⁶ более чем удвоения спроса МСП на ИБ-сервисы к 2030 году (до 35–37 млрд руб.). Открытым при этом остаётся вопрос комплексного покрытия решениями для киберустойчивости динамичной информационной инфраструктуры малых предприятий: полноценная защита обычно требует нескольких разных классов средств от разных вендоров, и ценовая доступность такого комплекса решений для типового МСП — открытый вопрос.

Высокие киберриски МСП подтверждаются как российской, так и международной статистикой и не ограничиваются самим предприятием: через цепочки поставок они затрагивают крупных заказчиков и отрасли в целом. Рынок предлагает отдельные продукты и сервисы для обеспечения киберустойчивости, но уверенных данных о том, что типовое малое предприятие в состоянии обеспечить себя защитой — нет.

¹³ Каждая третья атака на компании начинается с подрядчика, *CNews*, 2026

¹⁴ Ландшафт киберугроз - I полугодие 2026 года, *Инфосистемы Джет*, 2026

¹⁵ Миссия невыполнима, *Коммерсантъ*, 2026

¹⁶ Аналитика ГК «Солар», *Солар*, 2025

3. Меры поддержки киберустойчивости МСП

Рассмотрим общий подход к мерам государственного управления и поддержки обеспечения киберустойчивости МСП в РФ и других странах мира.

3.1. Международная практика

Обязательных государственных требований к МСП как классу с точки зрения киберустойчивости чаще всего не предъявляется. Вместо этого регуляторы и ведомства предлагают меры в виде:

- добровольной сертификации или самодекларации уровня защиты/киберустойчивости;
- образовательных программ для владельцев и управленческого состава малого бизнеса;
- методические рекомендации.

Несмотря на то, что такие требования не являются «де-юре» обязательными сами по себе, «де-факто» их используют для стимулирования повышения киберустойчивости МСП. Так, например, страховщики могут закреплять те или иные официальные рекомендации в качестве необходимых мер защиты в фактических требованиях к полисам киберстрахования. Приведем несколько примеров подобных мер и инструментов поддержки малого и среднего бизнеса.

В США агентство CISA предлагает разнообразные бесплатные ресурсы, ориентированные на безопасность МСП¹⁷, включая «Cyber Essentials Starter Kit»¹⁸ для руководителей малого бизнеса, а также бесплатные услуги Cyber Hygiene Services¹⁹ для ряда отраслей, включающие сканирование уязвимостей внешнего периметра. Кроме того, федеральное агентство по делам малого бизнеса США (SBA) ведёт раздел «Strengthen Your Cybersecurity»²⁰ — навигатор по уже существующим программам разных ведомств, включающим разнообразные инструменты, например, бесплатный конструктор политики ИБ (FCC Small Biz Cyber Planner), подходы к нетехнической самооценке (CISA Cyber Resilience Review), набор базовых рекомендаций или инструментов для управления рисками в цепочке поставок (ICT Supply Chain Risk Management Toolkit).

Европейское агентство ENISA публикует²¹ практическое руководство для малого бизнеса «12 шагов для защиты бизнеса», а федеральное управление по информационной безопасности Германии (BSI) предлагает образовательные материалы²² для МСП в сочетании с инструментами проверки, например, CyberRisikoCheck, когда внешний специалист проводит с представителями предприятия небольшое интервью и выдаёт структурированную оценку по стандарту DIN SPEC 27076.

В Великобритании доступна государственная сертификация Cyber Essentials (NCSC/IASME)²³, которая подтверждает наличие базовых технических контролей на предприятии. Согласно публичным данным²⁴, к марту 2026 было выдано более 215 000 сертификатов (49 248 — за предыдущие 12 месяцев). Интересно отметить, что по официальной информации компании с сертификатом Cyber Essentials на 92% реже сообщают о страховых случаях.

В Японии под эгидой министерства экономики торговли и промышленности и государственного агентства Innovation Platform Agency (IPA) с 2017 года действует²⁵ бесплатная схема самодекларации

¹⁷ Small and Medium-Sized Business Resources, [CISA](#), 2026

¹⁸ Cyber Essentials, [CISA](#), 2026

¹⁹ Cyber Hygiene Services, [CISA](#), 2026

²⁰ Strengthen your cybersecurity, [U.S. Small Business Administration](#), 2026

²¹ Cybersecurity guide for SMEs, [ENISA](#), 2021

²² Small and medium-sized enterprises, [BSI](#), 2026

²³ National Cyber Security Center, [gov.uk](#), 2025

²⁴ Cyber Essentials scheme: overview, [gov.uk](#), 2026

²⁵ Information security awareness promotion initiatives for SMEs, [IPA](#), 2026

SECURITY ACTION: компания публично обязуется следовать гайдлайнам ИБ для МСП и/или публикует базовую политику ИБ, проходя самопроверку по 25 пунктам соответствия.

В Австралии роль такого базового ориентира играет модель зрелости Essential Eight²⁶, на ней же строится и соответствующая образовательная программа для предприятий – Cyber Wardens²⁷. Программа нацелена на подготовку «кибер-хранителей» - обучению владельцев и сотрудников малого бизнеса²⁸, в том числе в контексте рисков, связанных с использованием ИИ. По состоянию на 2026 год программа имеет более 36 200 выпускников из свыше 22 600 компаний.

3.2. Российская практика

В России, также как и в других странах, нет отдельного федерального регулирования кибербезопасности, адресованного именно МСП как классу компаний. Требования, которые фактически затрагивают часть МСП (например, приказ ФСТЭК №117 от 11.04.2025²⁹), возникают косвенно: по типу обрабатываемых данных (например, персональные данные) или уровню доступа к системам (например, государственным информационным ресурсам); специальных требований именно для МСП как отдельного класса субъектов регуляторы не предъявляют. При этом внутриотраслевые стандарты могут формально учитывать размер организации. Так, например, ГОСТ Р 57580.1-2017, разработанный Центральным Банком России указывает, что определение необходимого уровня защиты («минимальный», «стандартный», «усиленный») учитывает в том числе отнесение финансовой организации к малым и микропредприятиям.

Существующие меры господдержки цифровизации в РФ не имеют в данный момент акцента, связанного с киберустойчивостью МСП: нацпроект «Экономика данных и цифровая трансформация государства»³⁰ включает федеральный проект «Инфраструктура кибербезопасности», но он ориентирован на защиту государственных информационных систем и противодействие мошенничеству в отношении граждан.

Отсутствию единого режима регулирования киберустойчивости, распространяющегося на все МСП исключительно по факту их принадлежности к этому сегменту — общая мировая практика. Российская специфика заключается в том, что за рубежом этот пробел системно закрывается добровольной сертификацией и другими элементами активно продвигаемой (и нередко финансируемой государством) инфраструктуры поддержки МСП, а сам рынок дополнительно подталкивает к внедрению базовых мер, в том числе через страхование. В России сопоставимой по охвату инфраструктуры пока нет: программы поддержки цифровизации не выделяют киберустойчивость МСП отдельно. Действующие зарубежные механизмы — добровольная самодекларация базового уровня защиты, адресные образовательные программы — могут служить ориентиром при выборе мер в российских условиях.

²⁶ Essential Eight explained, ACSC, 2023

²⁷ Cyber Wardens, The Council of Small Business Organisations Australia, 2026

²⁸ Cyber security and digital support services for small businesses, gov.au, 2024

²⁹ Приказ ФСТЭК 117, ФСТЭК, 2025

³⁰ Национальный проект «Экономика данных и цифровая трансформация государства», Минцифры РФ, 2025

4. Методология оценки киберприоритета

Из обзора мер поддержки может показаться, что для России достаточно перенести зарубежный опыт: запустить добровольную сертификацию базового уровня защиты, образовательные программы и методические рекомендации для МСП. Однако рассмотренные зарубежные механизмы в основном универсальны: они адресованы малому бизнесу в целом, не учитывают отраслевую специфику и не отвечают на вопрос, в каких отраслях поддержка даст наибольший эффект сейчас. При ограниченных ресурсах государства и рынка этот вопрос становится первостепенным.

От отрасли к отрасли могут существенно различаться цифровая зависимость МСП, их экономический вклад, роль в цепочках поставок и (экономическая) доступность защиты для них, а вместе с этим и возможные последствия киберинцидентов, структура затрат на ИТ и информационную безопасность. Кроме того, по отраслевому принципу во многом организованы и те, кто способен влиять на ситуацию: отраслевые регуляторы и объединения, крупные заказчики, выстраивающие работу со своими поставщиками, производители средств защиты, предлагающие отраслевые решения.

Исходя из этого, исследование предлагает инструмент отраслевой приоритизации. Он позволяет измерить, в каких отраслях сочетание потребности в киберустойчивости, её ограниченной доступности для МСП и экономической роли малого и среднего бизнеса требует первоочередного внимания, и проследить, как эта картина меняется со временем. Такая оценка может быть полезна государству, поставщикам решений и услуг информационной безопасности, крупным заказчикам и отраслевым объединениям: методика приоритизации даёт возможность направлять усилия по поддержке МСП туда, где они сейчас нужнее всего, и точно развивать методические и сертификационные инструменты.

Каждая отрасль оценивается по трём показателям по шкале 0–100:

1. **Отраслевой индекс киберкритичности (Икк)** – отражает совокупную значимость потенциальных нарушений киберустойчивости на предприятиях отрасли, учитывающую долю отрасли в ВДС, занятости, инвестициях и налогах, глубину цифровизации и принадлежность субъектов отрасли к критической информационной инфраструктуре.
2. **Отраслевой индекс доступности киберустойчивости МСП (Идк)** – отражает экономический баланс — долю стоимости эффективного набора средств защиты, которую типовое предприятие отрасли может себе позволить покрыть располагаемым бюджетом. Стоимость рассчитывается для типовых профилей предприятий (см. ниже) по открытым ценам российских поставщиков и усредняется с экспертными оценками поставщиков СЗИ, располагаемый бюджет МСП — вычисляется по отраслевым долям затрат на ИБ к выручке.
3. **Отраслевой индекс влияния МСП (Ивл)** – отражает долю малого и среднего бизнеса в ВДС, занятости, инвестициях и налогах отрасли с поправкой на то, насколько МСП отрасли используют цифровые технологии: МСП, мало зависящие от цифровых систем, при той же экономической роли вносят меньший вклад в совокупный киберриск.

Итоговый **Отраслевой индекс киберприоритета МСП** представляет собой интегральное значение параметров киберкритичности, доступности киберустойчивости и влияния МСП на отрасль: он высок только когда отрасль критична, защита для предприятий отрасли (МСП) экономически недоступна и МСП играют в ней заметную роль одновременно. Так методика отвечает на вопрос, в каких отраслях недостаточная доступность киберустойчивости для МСП способна стать фактором риска как для самой отрасли, так и для связанных с ней цепочек кооперации.

Оценка строится на типовых профилях предприятий согласно Федерального закона от 24.07.2007 № 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации».

Табл. 1. Базовые профили МСП

	Микропредприятие	Малое предприятие	Среднее предприятие
Величина дохода	До 120 млн руб.	До 800 млн руб.	До 2 млрд руб.
Среднесписочная численность работников	До 15 человек	До 100 человек	До 250 человек

Внутри каждой категории выделяются по три типоразмера, всего девять профилей: от микропредприятия с 5 работниками и выручкой 30 млн руб. до среднего предприятия с 250 работниками и выручкой 2 млрд руб. Для каждого профиля определяются количество защищаемых объектов (рабочих мест, серверов, площадок) и эффективный набор средств защиты.

Расчёт опирается на следующие данные:

- Федеральный закон № 187-ФЗ и распоряжение Правительства РФ № 360-р о перечне типовых отраслевых объектов КИИ;
- статистика Росстата и ЕМИСС, в том числе данные форм федерального статистического наблюдения: №3-информ «Сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг» по предприятиям крупного, среднего и малого бизнеса; форма МП (микро) «Сведения об основных показателях деятельности микропредприятия»; форма ПМ «Сведения об основных показателях деятельности малого предприятия»; форма П-4 «Сведения о численности и заработной плате работников»; форма П-2 «Сведения об инвестициях в нефинансовые активы»;
- данные ФНС России: Единого реестра субъектов МСП, ЕГРЮЛ; сведения об уплаченных организациями налогах и данные о начислениях и поступлениях налогов, сборов и страховых взносов в бюджетную систему Российской Федерации по основным видам экономической деятельности (1-НОМ);
- открытые прайс-листы российских производителей средств защиты и поставщиков ИБ-сервисов для МСП;
- оценки стоимости защиты, полученные от производителей ИБ-решений через профильный опрос.

4.1. Отраслевой индекс киберкритичности

Отраслевой индекс киберкритичности (Икк, 0–100) оценивает потенциальный масштаб последствий киберинцидентов для отрасли в целом. Показатель не связан напрямую с МСП и опирается на данные обо всех обследуемых организациях отрасли. Он рассчитывается на базе трёх блоков:

- **социально-экономическая значимость** — доля отрасли в валовой добавленной стоимости (данные Росстата), численности занятых (Росстат, формы МП (микро), ПМ, П-4), инвестициях в основной капитал (Росстат) и налоговых поступлениях (данные ФНС России) за 2025 год;
- **цифровая зависимость** — число персональных компьютеров на 100 работников, доля организаций, использующих прикладное программное обеспечение, и широта цифровизации, то есть доля организаций, использующих облачные сервисы, интернет вещей, центры

обработки данных, технологии больших данных, электронный документооборот, обмен данными с внешними системами и использование веб-ресурсов (Росстат, форма №3-информ);

- **принадлежность организаций отрасли к критической информационной инфраструктуре (КИИ)** — оценка по соответствию отрасли сферам деятельности субъектов КИИ (187-ФЗ, ст. 2 п. 8) с учётом детализации перечня типовых отраслевых объектов КИИ в распоряжении Правительства РФ от 26.02.2026 №360-р.

4.2. Отраслевой индекс доступности киберустойчивости МСП

Отраслевой индекс доступности киберустойчивости (Идк, 0–100) оценивает, насколько типовые МСП отрасли экономически способны обеспечить эффективный уровень собственной киберустойчивости. Для каждого из девяти профилей предприятий в отрасли рассчитываются:

- **эффективный профиль защиты** — набор средств, объем которых задается экспертно, в соответствии с типоразмером предприятия и отрасли: базовая или расширенная защита конечных точек, уровень межсетевого экранирования, защита почты, облачных ресурсов, использование сервисов управляемого обнаружения и реагирования на инциденты и прочее;
- **стоимость эффективного профиля защиты** — ожидаемые затраты предприятия, которые рассчитываются по единым для всех отраслей ценам (открытые прайс-листы российских производителей и облачных сервисов, для части позиций — экспертная калибровка); расчётные затраты усредняются с предоставленными оценками поставщиков решений (опрос);
- **располагаемый бюджет на ИБ** — среднестатистические затраты организации соответствующего типоразмера, которые оцениваются на основании заданной выручки типового предприятия и доле затрат на ИБ в соответствующей отрасли (Росстат, форма №3-информ);
- **коэффициент покрытия затрат** — располагаемый бюджет на ИБ, делённый на фактическую стоимость профиля защиты.

Отраслевой **Идк** вычисляется как среднее арифметическое коэффициента покрытия затрат по девяти профилям отрасли, в процентах.

4.3. Отраслевой индекс влияния МСП

Отраслевой индекс влияния МСП (Ивл, 0–100) показывает, насколько значим сегмент МСП внутри отрасли. Он складывается из экономической роли МСП в отрасли и поправки на уровень их цифровизации.

Экономическая роль МСП в отрасли оценивается по четырём компонентам:

- **доля МСП в ВДС отрасли** — расчетная оценка на основе доли МСП в выручке отрасли, скорректированная с учетом общероссийской доли МСП в ВДС ввиду отсутствия официальных данных Росстата о ВДС МСП в отраслевом разрезе;
- **доля МСП в занятости отрасли** — среднесписочная численность работников (без внешних совместителей) МСП отрасли, делённая на среднесписочную численность работников по полному кругу организаций той же отрасли;
- **доля МСП в инвестициях в основной капитал отрасли** — отношение объема инвестиций в основной капитал по полному кругу организаций, за вычетом крупных предприятий, к общему объему инвестиций;

- **доля МСП в налоговых поступлениях отрасли** — отношение объема налогов, уплаченных организациями — субъектами МСП соответствующей отрасли, идентифицированными по данным Единого реестра МСП, к общему объему налоговых поступлений по виду экономической деятельности по данным ФНС России (по форме 1-НОМ).

Четыре компонента сводятся в **отраслевой индекс влияния МСП**. Однако экономическая роль сама по себе не говорит о том, насколько МСП отрасли подвержены киберугрозам. Поэтому показатель корректируется коэффициентом цифровизации МСП, рассчитываемым по данным формы №3-информ по малым предприятиям за 2025 год о доле организаций, использующих шесть категорий цифровых технологий, общих для всех отраслей: веб-ресурсы или соцсети, финансовые платформы, искусственный интеллект, облачные сервисы, технологии больших данных и центры обработки данных. Категории, отражающие специфику отдельных отраслей (маркетплейсы, промышленные роботы, интернет вещей), не используются.

4.4. Итоговый показатель — Отраслевой индекс киберприоритета МСП

Все три рассчитанных ранее показателя сводятся в интегральный отраслевой индекс киберприоритета МСП:

$$П_{мсп} = \sqrt[3]{((И_{кк}/100) \times (1 - И_{дк}/100) \times (И_{вл}/100)) \times 100}$$

Показатель рассчитывается как среднее геометрическое для учета мультипликативных эффектов, т.к. приоритет должен быть высоким, только если все три фактора неблагоприятны одновременно: отрасль критична, защита для её МСП недоступна и МСП играют в ней заметную роль.

Следует обратить внимание, что в формулу входит не доступность защиты, а её дефицит ($1 - И_{дк}/100$). Поэтому нулевая доступность, когда бюджет совсем не покрывает защиту, даёт максимальный вклад в приоритет, а доступность, близкая к 100% (рынок в балансе), сводит приоритет к нулю.

4.5. Интерпретация показателей

Интерпретация отраслевого индекса доступности киберустойчивости (ось X):

- Очень высокий: 75–100 (рынок в балансе, МСП отрасли в состоянии обеспечить собственную киберустойчивость)
- Высокий: 50–74 (допустимый дисбаланс в ряде категорий МСП в отрасли)
- Средний: 25–49 (серьезный дисбаланс рынка, реализация рекомендуемого уровня киберустойчивости затруднена для значительной части МСП)
- Низкий: 0–24 (реализация необходимого уровня киберустойчивости экономически недоступна для основной части типовых профилей МСП)

Интерпретация отраслевого индекса киберкритичности (ось Y):

- Очень высокий: 75–100 (отрасль значима для экономики, полностью зависит от цифровых технологий и платформ и входит в сферу КИИ; киберинцидент может затронуть смежные отрасли и экономику в целом)
- Высокий: 50–74 (заметный экономический вклад отрасли сочетается с высокой цифровизацией или связью с КИИ; есть возможность «аналогового» управления в случае сбоя, но это стоит «дорого»)

- Средний: 25–49 (последствия киберинцидента ощутимы, но ограничены: цифровая трансформация отрасли частичная, экономический вклад или связь с КИИ умеренные; есть возможность «аналогового» управления в случае сбоя)
- Низкий: 0–24 (слабая зависимость от цифровых технологий, небольшой экономический вклад, отрасль вне сферы КИИ; последствия киберинцидентов в основном локальны)

Интерпретация отраслевого индикатора влияния МСП (объемный показатель): показывает относительную значимость МСП в отрасли, с учетом отраслевого ВДС, занятости населения, налоговых и инвестиционных показателей, а также уровня цифровизации самих МСП.

Границы диапазонов заданы экспертно и носят предварительный характер: возможно их уточнение по мере накопления данных, в частности, после расчёта по всем разделам ОКВЭД.

Методика опирается на воспроизводимые официальные источники (Росстат, ЕМИСС, ФНС, ЕГРЮЛ, законодательство о КИИ) там, где это возможно, и явно отделяет экспертные допущения от измеренных величин. Экспертными остаются состав профиля защиты, оценка связи строительства с КИИ — именно их в первую очередь стоит уточнять в следующих версиях расчёта. Остальные данные обновляются из официальных источников, поэтому результат можно регулярно пересчитывать, в том числе с учётом новых ответов производителей ИБ-решений на профильный опросник, без пересмотра самой методики.

5. Результаты пилотного расчёта

Главная задача пилотного расчёта — проверить, как методика работает на отраслях с заведомо разными условиями. Выбранные отрасли различаются регулированием, затратами на ИТ и ИБ, связью с КИИ, уровнем цифровизации и ролью МСП, поэтому по ним видно, различает ли методика такие отрасли и согласуются ли её результаты с их известными особенностями. Результаты пилота иллюстрируют работу методики и не являются отраслевым рейтингом.

Пилотный расчёт также формирует исходную базу для дальнейшего мониторинга. Регулярное, например ежегодное, повторение исследования при сопоставимых исходных данных и правилах расчёта позволит отслеживать изменение доступности киберустойчивости и отраслевых приоритетов. При этом динамику сводного показателя необходимо рассматривать вместе с изменениями его отдельных составляющих. Разовое значение мало говорит об абсолютном уровне риска, но фиксирует исходную точку и позволяет обращать внимание на приоритетные отрасли заблаговременно, а не по факту состоявшихся масштабных инцидентов.

Пилотный расчёт проведён для пяти разделов ОКВЭД:

- К. Финансовая и страховая деятельность;
- D. Обеспечение электрической энергией, газом и паром; кондиционирование воздуха;
- C. Обрабатывающие производства;
- F. Строительство;
- A. Сельское, лесное хозяйство, охота, рыболовство и рыбоводство.

Рис. 1. Сводная диаграмма отраслевых индексов киберприоритета МСП

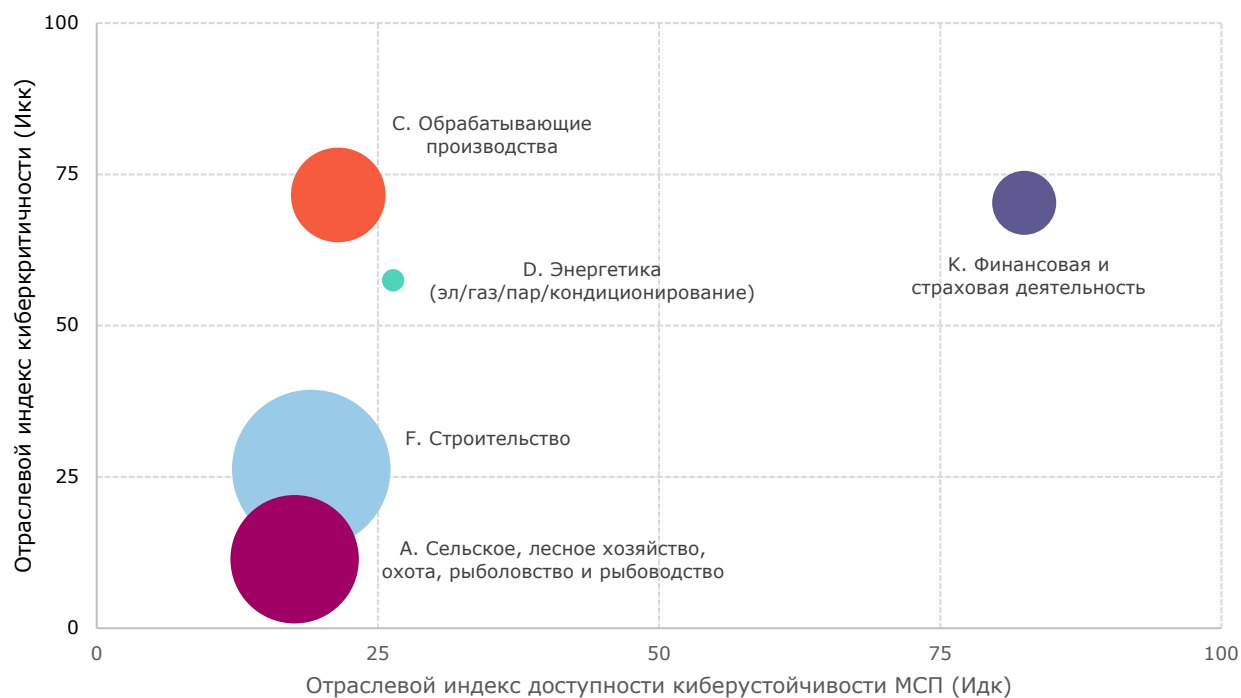


Табл. 2. Результаты пилотного расчета

	Отрасль	Отраслевой индекс кибер-критичности	Отраслевой индекс доступности кибер-устойчивости МСП	Отраслевой индекс влияния МСП	Индекс кибер-приоритета МСП
1	Г. Строительство	26,3	19,1	65,5	51,8
2	С. Обрабатывающие производства	71,6	21,5	23,3	50,8
3	А. Сельское хозяйство	11,4	17,6	42,9	34,3
4	К. Финансы	70,3	82,5	10,7	23,6
5	Д. Энергетика	57,5	26,4	1,3	17,6

Актуальный расчёт показывает существенную неоднородность положения МСП в разных отраслях. Наиболее высокий отраслевой киберприоритет получают строительство и обрабатывающие производства — 51,8 и 50,8 из 100, разница между ними несущественна. В обеих отраслях низкая доступность киберустойчивости (19,1 и 21,5) сочетается со значительным влиянием МСП, но за счёт разных факторов. У строительства максимальная среди пяти отраслей экономическая роль МСП, которая даже с поправкой на невысокую цифровизацию малого строительного бизнеса даёт наибольшее влияние МСП (Ивл = 65,5), но киберкритичность отрасли невысока (Икк = 26,3). У обрабатывающих производств высокая киберкритичность отрасли (Икк = 71,6) при умеренном влиянии МСП (Ивл = 23,3).

Сельское хозяйство занимает третье место (34,3): доступность киберустойчивости там самая низкая (17,6), роль МСП высокая, но низкая киберкритичность отрасли (11,4) снижает итоговый приоритет. Финансовый сектор занимает четвёртое место (23,6): при высокой киберкритичности (70,3) у него самая высокая среди пяти отраслей доступность киберустойчивости (82,5) и скромное влияние МСП (Ивл = 10,7). Энергетика, несмотря на умеренно высокую киберкритичность (57,5) и низкую доступность (26,4), получает самый низкий итоговый приоритет (17,6) из-за минимальной роли МСП в отрасли (Ивл = 1,3): основной риск в отрасли сосредоточен у крупных инфраструктурных организаций, которые уже находятся в контуре регулирования КИИ. Низкий итоговый приоритет финансового сектора и энергетики не означает, что МСП этих отраслей не нуждаются в поддержке: показатель указывает лишь на приоритетность приложения усилий.

Полученное ранжирование в целом согласуется с независимыми наблюдениями о структуре отраслей и рынка: строительство и обрабатывающие производства — отрасли с традиционно высокой долей МСП и низким приоритетом инвестиций в ИТ/ИБ; финансовый сектор — отрасль с исторически наибольшими относительными затратами на ИТ и ИБ среди рассматриваемых, что закономерно даёт высокую доступность защиты. Разрыв между строительством и обрабатывающими производствами (51,8 против 50,8) несущественен и чувствителен к методическим решениям — в частности, к экспертной оценке КИИ-блока для строительства.

Пилотный расчёт показывает, что методика различает отрасли с разными условиями и даёт результаты, согласующиеся с их известными особенностями. Доступность киберустойчивости для МСП существенно различается по отраслям: финансовый сектор близок к экономическому балансу (82,5), тогда как в остальных четырёх отраслях доступность не превышает 27. Строительство и обрабатывающие производства сочетают низкую доступность со значительным влиянием МСП и получают наибольший приоритет, сельское хозяйство занимает третье место, финансовый сектор и энергетика получают заметно более низкий приоритет. Результаты следует анализировать с учётом принятых ограничений.

Следующим шагом целесообразно уточнить методику, сокращая долю экспертных оценок, и распространить расчёт на все разделы ОКВЭД. Полный отраслевой рейтинг позволит определить отрасли, где поддержка киберустойчивости МСП даст наибольший эффект, и проработать для них механизмы стимулирования: субсидирование доступа к управляемым ИБ-сервисам, добровольную сертификацию или самодекларацию базового уровня защиты по аналогии с зарубежными примерами. Для коммерческого рынка информационной безопасности результаты указывают на МСП как на перспективный сегмент, которому нужны продукты и сервисы, рассчитанные на бюджет и компетенции малого бизнеса. Отраслевые объединения могут использовать оценку как измеримый аргумент в диалоге с регуляторами и рынком ИБ, а крупные заказчики — при работе над повышением киберустойчивости своих поставщиков.



Авторы



Екатерина Кваша

Заместитель генерального директора ЦСР



Никита Иванов

Директор центра региональной политики ЦСР



Выражаем благодарность **Роману Краснову**,
основателю Фонда Цифровых Исследований "КиберПрогноз"
за участие в подготовке данного материала

© 2026 Фонд «Центр стратегических разработок» (ЦСР).
Все права защищены. При использовании информации
из документа ссылка на ЦСР обязательна.

Москва, 125009, Газетный пер., 3–5 стр. 1, 3 этаж
Тел.: +7 (495) 725-78-06
Факс: +7 (495) 725-78-14
E-mail: info@csr.ru

csr.ru

