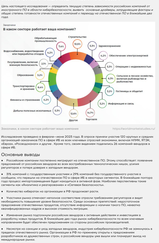
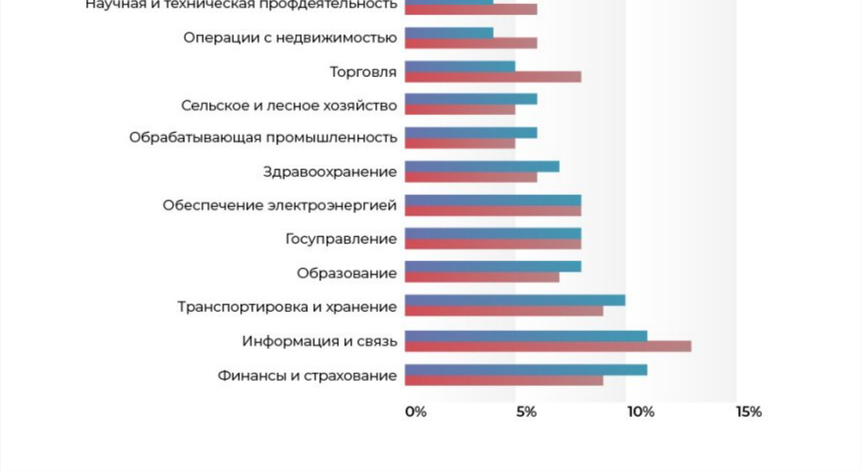
Реальность и перспективы российского рынка кибербезопасности 2023 — 2025

Российские сферы информационной безопасности развиваются в условиях вынужденной изоляции от наиболее популярных на мировом рынке решений, что стимулирует отечественных производителей к интенсивному росту. Российский рынок кибербезопасности демонстрирует уверенный рост, сопоставимый с мировыми показателями.

Цель настоящего исследования — выявить существующие тенденции развития российских компаний в сфере кибербезопасности, оценить их потенциал, а также определить ключевые факторы, влияющие на развитие отрасли.

Вопросы:
В каком сегменте работает ваша компания?

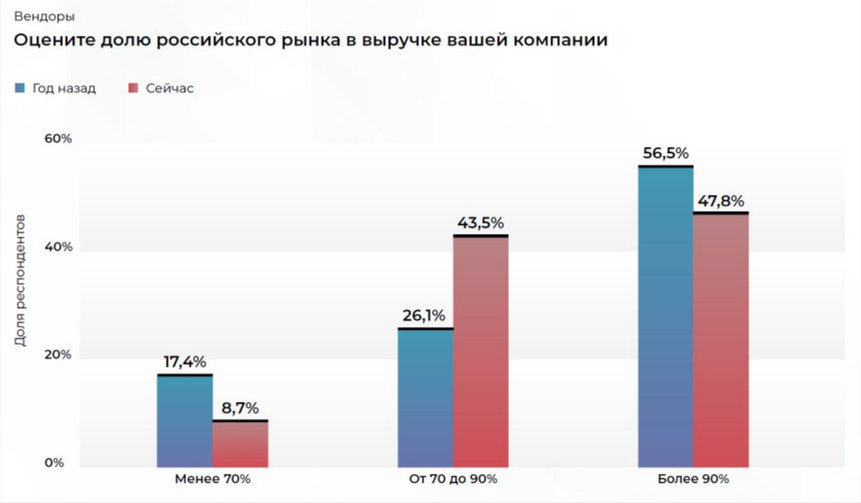

Разработчик прикладного ПО
Разработчик системного ПО
Разработчик аппаратного обеспечения
Системный интегратор
Сервисная компания
Консалтинговая компания
Аудиторская компания
Учебный центр
Дистрибьютор
Реализатор
Инфраструктурная компания
Научно-исследовательский институт
Другое
Сертификационный центр
Лаборатория
Инфраструктура связи
Телекоммуникационная компания
Интеграция
Аутсорсинг
Аутстаффинг
Хостинг
Облачные технологии
Информационные технологии
Информационная безопасность
Разработка ПО
Разработка аппаратного обеспечения
Разработка ПО и аппаратного обеспечения
Разработка ПО и информационная безопасность
Аппаратное обеспечение и информационная безопасность
Разработка ПО, аппаратное обеспечение и информационная безопасность
Разработка ПО, аппаратное обеспечение, информационная безопасность и телекоммуникации
Разработка ПО, аппаратное обеспечение и телекоммуникации
Разработка ПО и телекоммуникации
Аппаратное обеспечение и телекоммуникации
Информационная безопасность и телекоммуникации
Информационная безопасность и хостинг
Информационная безопасность и облачные технологии
Информационная безопасность и аутсорсинг
Информационная безопасность и аутстаффинг
Информационная безопасность и аудиторская компания
Информационная безопасность и консалтинговая компания
Информационная безопасность и сервисная компания
Информационная безопасность и системный интегратор
Информационная безопасность и учебный центр
Информационная безопасность и дистрибьютор
Информационная безопасность и реализатор
Информационная безопасность и инфраструктурная компания
Информационная безопасность и научно-исследовательский институт
Информационная безопасность и сертификационный центр
Информационная безопасность и лаборатория
Информационная безопасность и инфраструктура связи
Информационная безопасность и телекоммуникационная компания
Информационная безопасность и интеграция



Интерес к переходу на отечественное ПО по секторам экономики https://worldmarketstudies.ru/

Планы развития российских вендоров

Хотя российский рынок для отечественных вендоров продолжает играть главную роль, опрос указывает на то, что они увеличивают свое присутствие в других странах. Больше половины вендоров (57%) ответили, что год назад на долю российского рынка приходилось более 90% их выручки, но сейчас таких вендоров, которые практически исключительно сконцентрированы на России, на 10 процентных пунктов меньше. Стоит отметить, что доля компаний, у которых доля иностранной выручки больше 30%, уменьшилась с 17% до 9%.
Можно предположить, что параллельно идут два процесса: увеличение доли в странах ближнего зарубежья и сокращение присутствия на рынках государств, которые ввели санкции против РФ.



Доля российского рынка в выручке компаний https://worldmarketstudies.ru/

Это говорит о том что все больше российских вендоров всерьез рассматривает для себя международную экспансию, в первую очередь в дружественные страны.

С учетом обратного тренда российские заказчики готовы рассматривать не только отечественное ПО, но и продукцию из дружественных государств. Несмотря на санкции и уход западных вендоров, рынок кибербезопасности РФ не оказался в изоляции. Это позволит не только достичь технологического суверенитета, но и поддерживать конкурентоспособность отечественных продуктов на высоком уровне.

Итоги

- По мнению двух третей опрошенных заказчиков доля отечественного ПО в сфере ИБ в их компаниях составит, как минимум, 80% через 2 года. При этом 17% респондентов-вендоров считает, что российские игроки полностью вытеснят с рынка зарубежных. Но на данный момент говорить о самодостаточности рынка рано, так как уровень отечественного ПО остается ниже отметки 80%, которая самими участниками рынка обозначена как критически важная.
- 90% компаний, штат которых превышает 10 тыс. человек, либо уже перешли, либо планируют переход на отечественное ПО с сфере ИБ в следующие 12 месяцев. В компаниях с числом сотрудников от 1 до 10 тыс. перешли только 27%. 45% организаций со штатом от 500 до 1 тыс. человек планируют переходить в ближайший год. Таким образом можно сделать вывод о том, что крупные компании, располагающие большими бюджетами, более оперативно адаптируются к новым условиям.
- На фоне ухода западных вендоров долю на рынке ИБ могут получить не только российские игроки, но и компании из дружественных государств. В частности, более 30% заказчиков готовы переходить на китайские решения. Таким образом на российском рынке на горизонте ближайших двух лет на смену конкуренции между российскими и западными вендорами придет конкуренция между отечественными разработчиками и вендорами из дружественных стран. За это время необходимо насытить рынок российскими решениями в критически важных сегментах. Если это удастся сделать, суверенитет в сфере кибербезопасности не будет вновь утрачен.
- Российские вендоры, которым зарубежные рынки приносили существенную долю выручки, пересмотрели свою стратегию и сосредоточились на продвижении в России. В то же время компании, которые были сфокусированы исключительно на отечественном рынке, начали открывать для себя рынки дружественных стран.
- 76% опрошенных заказчиков отметили рост числа киберугроз за последний год. При этом две трети компаний уверены, что способны эффективно противостоять угрозам. Однако лишь 28% привлекали для проверки сторонних экспертов. Таким образом восприятие уровня защищенности у топ-менеджмента компаний может быть искажено.
- Отечественные вендоры продуктов ИБ в целом положительно смотрят на эффективность принимаемых правительством мер для повышения кибербезопасности. 43% вендоров-респондентов оценивают эффективность на 8 баллов по 10-бальной шкале или выше.
- По мнению вендоров, в данный момент отрасль не проходит тест на соответствие указам регуляторов на «отлично». Лишь 9% вендоров оценили готовность сектора к реализации указов на 9-10 баллов из 10 возможных. Основной причиной, которая препятствует реализации указов, является низкий уровень подготовки ИБ-специалистов в компаниях.
- Над разработкой ПО, которое должно закрыть образовавшиеся ниши, трудятся в 74% компаний-вендоров. Две трети вендоров планируют выпустить такие продукты в течение ближайших 12 месяцев.
- Заказчики планируют в первую очередь переходить на отечественные решения в области ИБ в сферах аналитики и реагирования, а также сетевой безопасности. На эти две сферы пришлась почти половина ответов. Этот результат подтверждается ответами со стороны вендоров.
- Если говорить о причинах, которые приводят к замедлению темпов импортозамещения в сфере ИБ, то в первую очередь можно назвать трудовые затраты и организационные усилия, которые необходимы для перехода. Выгода от импортозамещения для некоторых респондентов меньше, чем усилия, затраченные на смену продукта. Следующее по частоте упоминания возражение — новые продукты будет невозможно интегрировать в уже сложившуюся систему кибербезопасности. На эти два возражения приходится около 80% указываемых респондентами причин задержки перехода на отечественное ПО. Высокая стоимость перехода останавливает около 16% опрошенных.
- Только 5% респондентов беспокоит отсутствие российских аналогов, что говорит о том, что уже сейчас отечественные разработчики предлагают аналогичные продукты во всех сферах ИБ.