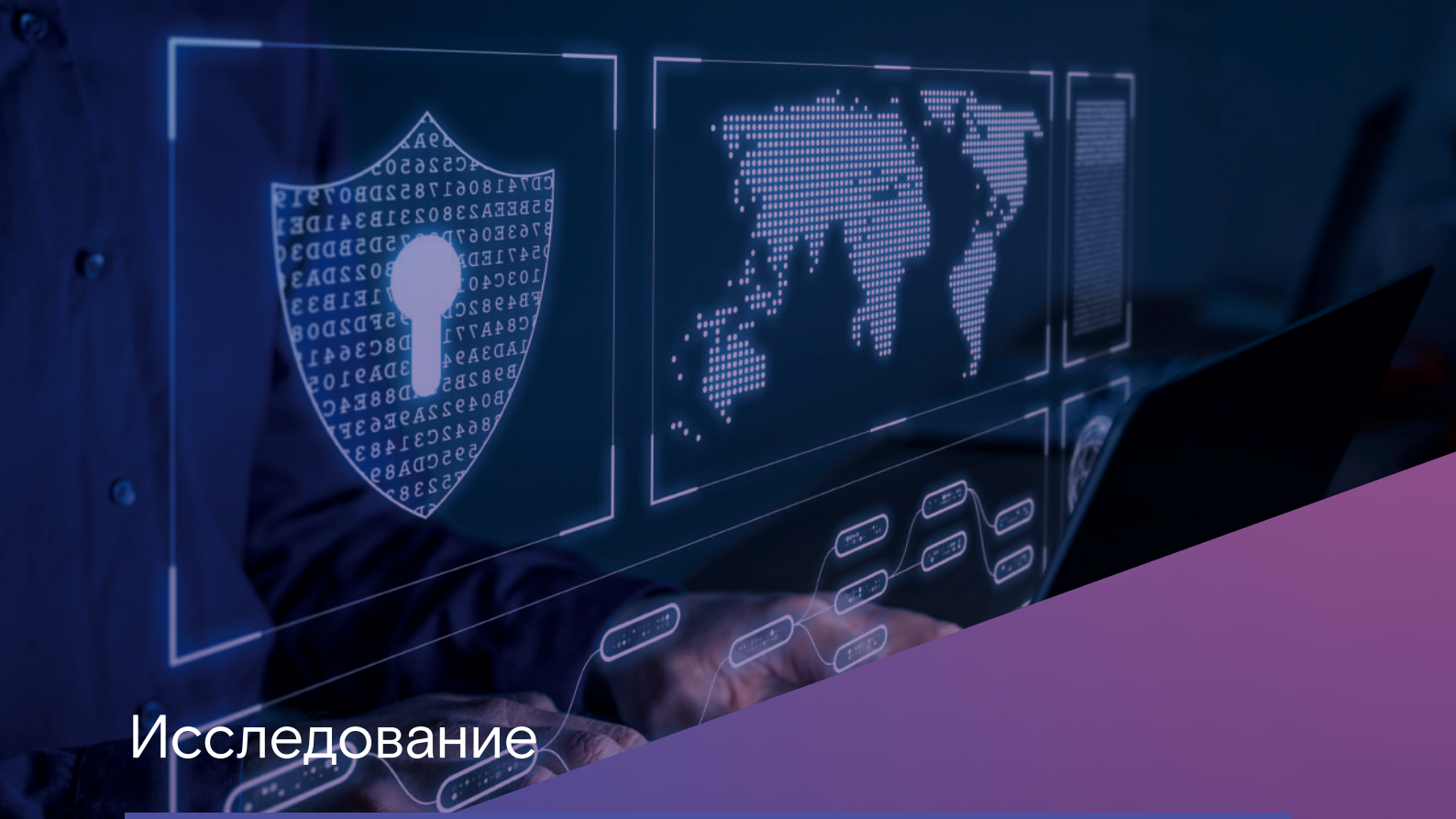


Исследование

«Удовлетворенность российскими технологиями кибербезопасности»

Москва 2022
rt-solar.ru

Ростелеком
Солар

Содержание

О компании

«РТК-Солар» обеспечивает и гарантирует кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности. Компания предлагает сервисы первого и лидирующего в РФ коммерческого SOC — Solar JSOC, а также экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, IdM-систему Solar inRights, анализатор кода Solar appScreener, систему повышения эффективности труда Solar addVisor. Центр «Solar Интеграция» реализует масштабные проекты по созданию систем кибербезопасности, фокусируясь на защите территориально-распределенных объектов, центров обработки данных, а также объектов КИИ и АСУ ТП. Для повышения киберустойчивости всей России «РТК-Солар» развивает Национальный киберполигон, ключевым компонентом которого является платформа для практической отработки навыков защиты от киберугроз «Кибермир». Штат компании — 1600+ специалистов. Имеются представительства в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Деятельность компании лицензирована ФСБ России, ФСТЭК России и Министерством обороны России.

Направления услуг «Solar Интеграция»:

- Экспертный консалтинг и комплексный аудит
- Защита периметра и ИТ-инфраструктуры
- Защита бизнес-приложений и данных
- Защита конечных станций и пользователей
- Защита онлайн-систем и веб-сервисов
- Выявление и контроль уязвимостей
- Управление доступом
- Управление кибербезопасностью
- Кибербезопасность объектов КИИ и АСУ ТП
- Кибербезопасность ЦОД
- Обеспечение соответствия требованиям регуляторов
- Техническая поддержка и сопровождение 24/7

Введение

После ухода из России ряда иностранных производителей средств защиты российским компаниям пришлось изменить планы по развитию кибербезопасности, сместив фокус в сторону импортозамещения. По данным исследования, проведенного экспертами компании «РТК-Солар», к концу 2022 года почти половина (42%) российских организаций пришли к выводу, что им необходимо перестроить свою систему киберзащиты.

Среди основных причин, которые заставили компании пересмотреть подход к ИБ, — рост киберугроз, уход зарубежных вендоров из России, потребность в импортозамещении и новые регуляторные требования. Так, согласно указу Президента РФ № 166 от 30 марта, с 1 января 2025 года в стране будет запрещено использовать иностранное программное обеспечение на значимых объектах критической информационной инфраструктуры. В это же время начнет действовать запрет для стратегических и системообразующих организаций и госкомпаний на использование средств защиты из «недружественных» стран, введенный указом Президента РФ № 250 от 1 мая.

Данное исследование эксперты «Solar Интеграция» провели с целью определить критерии, наиболее важные для российских организаций при выборе отечественных средств защиты для внедрения в инфраструктуру, и оценить удовлетворенность специалистов и руководителей российскими технологиями кибербезопасности. Также в исследовании рассмотрены сложности, с которыми компании сталкиваются при внедрении отечественных средств защиты.

Методология

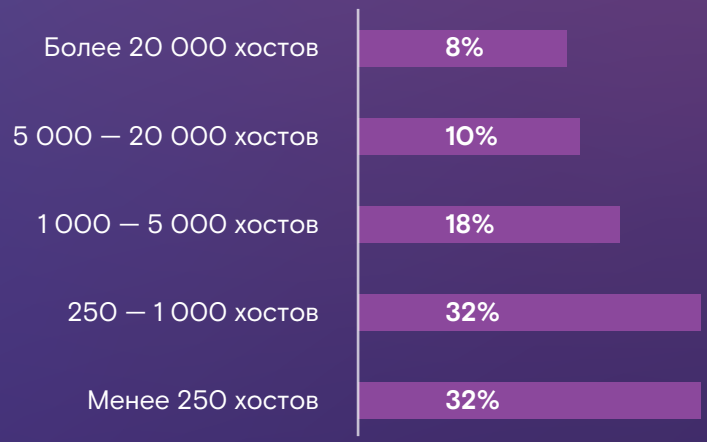
Отчет составлен на основе количественного онлайн-опроса, в котором приняли участие более 100 представителей различных российских организаций, отвечающих за выбор и внедрение продуктов кибербезопасности.

В число респондентов вошли коммерческие компании и организации государственного сектора, включая федеральные и региональные органы власти. В опросе принимали участие представители различных сегментов бизнеса: B2G, B2E, B2B, B2SMB.

География участников исследования охватила Москву и Санкт-Петербург, а также другие регионы страны. Опрос проводился в октябре-ноябре 2022 года. В ходе опроса респондентам предлагалось выбрать один или несколько из предложенных вариантов ответа.

География

Размер организации по количеству хостов



Должности респондентов

Ключевые цифры

52% **Каждая вторая организация** в России обращает внимание на наличие API при выборе отечественных средств защиты.

23% В то же время **почти каждый четвертый** респондент отмечает необходимость доработки решений именно в этой области.

45% Наиболее часто **сложности** на проектах по внедрению отечественных средств защиты **связаны с отсутствием** их **совместимости с последними версиями российских операционных систем и платформ виртуализации.**

36% **Опрошенных** заявляют о **проблемах производительности** решений.

Среди **наиболее распространенных российских средств защиты**, с которыми компании работали на практике, — **сканеры уязвимостей (47% респондентов), системы защиты веб-приложений (38%), системы управления событиями безопасности (35%), системы защиты от таргетированных атак (34%), системы контроля привилегированных пользователей (34%), системы защиты баз данных (33%) и межсетевые экраны следующего поколения (32%).**

Наиболее высоко компании оценивают отечественные **системы защиты конечных точек от сложных атак (EDR)**, удовлетворенность которыми отмечают **83% респондентов**, имеющих опыт работы с решениями этого класса. На **втором месте** находятся **системы защиты от таргетированных атак (82%)**, на **третьем — системы защиты баз данных (81%).**

Наименее высокую оценку получили российские **системы контроля привилегированных пользователей (PAM)**. Продуктами этого класса удовлетворены всего **58% опрошенных** из тех, кто работал с ними на практике. Одной из самых низких оказалась удовлетворенность российскими **сканерами уязвимостей**: об опыте использования этих продуктов компании заявляют наиболее часто, при этом такими решениями удовлетворены **61% респондентов**. Столько же опрошенных заявляют об удовлетворенности отечественными **межсетевыми экранами следующего поколения (NGFW).**

Результаты исследования

Какие факторы влияют на выбор российских средств защиты

В рамках исследования респондентам предлагалось назвать наиболее важные критерии выбора отечественных решений по кибербезопасности, помимо основной функциональности. При этом можно было выбрать несколько вариантов ответа.

Результаты распределились достаточно равномерно среди пяти критериев: почти половина опрошенных отметили в качестве наиболее важных факторов наличие гибких интерфейсов (API) для интеграции с другими решениями (52% опрошенных), поддержку отечественных операционных систем и платформ виртуализации (49%), наличие сертификата соответствия требованиям по безопасности информации (49%), соответствие заявленному уровню производительности (48%), а также реализацию отказоустойчивости на всех уровнях (46%). Менее важной в сравнении с остальными критериями оказалась возможность автоматизации развертывания решений на большом количестве хостов в среде Linux (35%), на этот критерий чаще обращают внимание крупные компании.

Что вы считаете наиболее важным при выборе российских средств защиты, помимо основной функциональности?

С чем чаще всего связаны сложности при внедрении российских решений по кибербезопасности

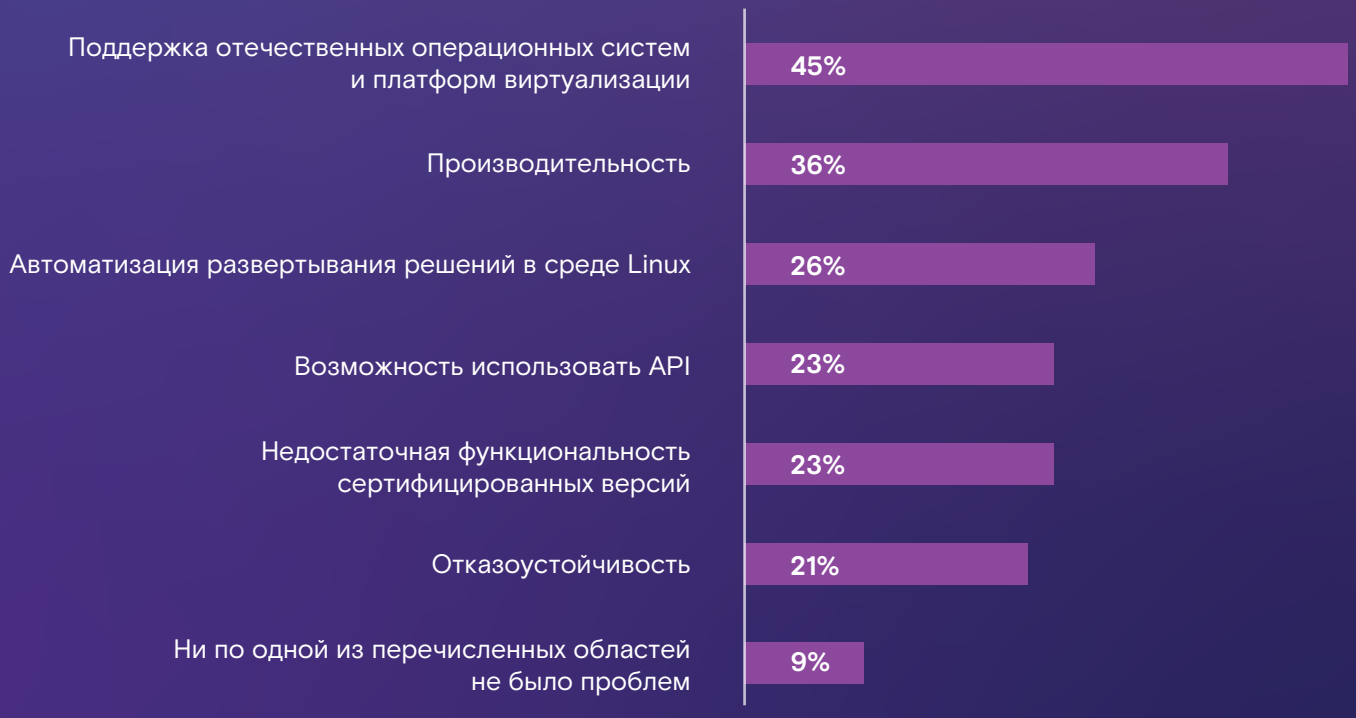
Также авторы исследования выяснили, с какими сложностями компании наиболее часто сталкиваются при реализации проектов по внедрению отечественных средств защиты. Отвечая на этот вопрос, респонденты могли выбрать несколько вариантов ответа.

Оказалось, что наиболее часто, в 45% случаев, сложности связаны с отсутствием совместимости российских продуктов по кибербезопасности с последними версиями отечественных операционных систем и платформ виртуализации.

На втором месте среди распространенных проблем — недостаточная производительность решений (36%). Как показали результаты опроса, проблемы производительности наиболее характерны для респондентов из крупных организаций.

Почти четверть опрошенных отметили сложности, связанные с отсутствием возможности автоматизации развертывания решений на большом количестве хостов в среде Linux (26%), отсутствием гибких интерфейсов для интеграции с другими решениями (23%) и ограниченной функциональностью сертифицированных версий (23%). Примерно каждый пятый респондент (21%) заявил о проблемах с отказоустойчивостью решения.

Выберите области, в которых у вас возникали сложности при внедрении российских средств защиты с начала 2022 года



Уровень удовлетворенности российскими технологиями кибербезопасности

В рамках исследования эксперты «Solar Интеграция» предложили респондентам выбрать классы российских средств защиты, с которыми они работали на практике, и оценить уровень удовлетворенности этими технологиями.

В выборку вошли технологии, которые сейчас наиболее активно рассматриваются в рамках решения задач импортозамещения. В ходе опроса респондентам не предлагалось оценить системы защиты от утечек данных (DLP), средства антивирусной защиты и платформы оркестрации, автоматизации и реагирования на киберинциденты (SOAR), поскольку большинство компаний уже использует российские решения в этой области в силу их зрелости и преимуществ по сравнению с западными.

Как показали данные опроса, наиболее часто российские организации заявляют об опыте эксплуатации и внедрения отечественных сканеров уязвимости (47% опрошенных). Достаточно равномерно результаты распределились между шестью классами решений: от 30 до 40% респондентов отметили наличие опыта использования российских систем защиты веб-приложений (38%), систем управления событиями безопасности (35%), систем защиты от таргетированных атак (34%), систем контроля привилегированных пользователей (34%), систем защиты баз данных (33%), межсетевых экранов следующего поколения (32%). Менее часто респонденты заявляли об опыте работы с системами защиты конечных точек от сложных атак (24%) и системами защиты мобильных устройств (16%).

С какими российскими ИБ-решениями компании чаще сталкиваются в работе

Более половины опрошенных из тех, кто имеет опыт работы с российскими средствами защиты, заявляют об удовлетворенности отечественными технологиями кибербезопасности. Респонденты поставили оценку в 4 и 5 баллов по пятибалльной шкале по всем рассмотренным классам систем. При этом продукты нескольких классов заметно выделяются на фоне остальных. Лучше всего по итогам опроса себя показали отечественные решения для защиты конечных точек от сложных атак (EDR), системы для защиты от таргетированных атак (Anti-APT), а также системы защиты баз данных (DAM) — удовлетворенность российскими продуктами этих классов отмечают свыше 80% опрошенных, работавших с ними на практике.

Наименее высокую оценку среди рассмотренных решений получили системы контроля привилегированных пользователей (PAM) — ими удовлетворены всего 58% респондентов, имеющих опыт эксплуатации и внедрения таких продуктов. Примечательно, что одной из самых низких оказалась удовлетворенность российскими сканерами уязвимостей: об опыте их использования компании заявляли наиболее часто, при этом ими удовлетворены только 61% опрошенных из тех, кто использовал их на практике. Столько же респондентов заявляют об удовлетворенности отечественными межсетевыми экранами следующего поколения.

Рейтинг удовлетворенности российскими технологиями кибербезопасности

Направления для развития российских технологий кибербезопасности

Кроме того, в рамках исследования эксперты «Solar Интеграция» выяснили основные причины, по которым респонденты не удовлетворены каждым из рассматриваемых классов российских средств защиты.

Сканеры уязвимостей

- Создают высокую нагрузку на сеть
- Отсутствие гибких интерфейсов для интеграции (API)

Системы защиты мобильных устройств (MDM)

- Ограниченность возможностей политик контроля
- Отсутствие гибких интерфейсов для интеграции (API)

Системы защиты веб-приложений (WAF)

- Отсутствует поддержка отечественных стандартов безопасности ГОСТ и сертификация в качестве СКЗИ
- Ограниченность функциональности

Системы управления событиями безопасности (SIEM)

- Сложность разработки собственных правил нормализации
- Небольшое количество поставляемых в составе наборов конфигурации

Средства защиты от таргетированных атак (Anti-APT)

- Сложность эксплуатации

Системы контроля привилегированных пользователей (PAM)

- Ограниченность функциональности
- Ограниченный состав контролируемых протоколов

Системы защиты баз данных (DAM)

- Ограниченный набор поддерживаемых баз данных
- Ограниченность функциональности

Межсетевые экраны следующего поколения (NGFW)

- Ограниченность функциональности
- Ограниченность возможностей диагностики

Системы защиты конечных точек от сложных атак (EDR)

- Создают высокую нагрузку на АРМ
- Ограниченность функциональности

Класс решений

Причины неудовлетворенности

Выводы

Как показали результаты исследования, каждая вторая компания при выборе средств защиты обращает внимание на наличие API для взаимодействия с другими решениями. При этом почти каждый четвертый респондент отмечает необходимость доработки российских средств защиты именно в этой области. Наличие API в продуктах сейчас особенно важно на проектах миграции, поскольку позволяет автоматизировать задачи по переносу конфигураций, правил и политик на новое решение и, как следствие, сэкономить время специалистов.

Среди проблем, с которыми компании сталкиваются на проектах, первое место занимает отсутствие совместимости внедряемых отечественных продуктов по кибербезопасности с последними версиями российских операционных систем и платформ виртуализации. Причина этих проблем кроется в высокой динамике развития российского ИТ-ландшафта, которая также обусловлена задачами импортозамещения. Российские организации активно выбирают отечественные аналоги, что заставляет производителей операционных систем и платформ виртуализации дорабатывать функциональность под их требования. Этот процесс уже стартовал, и можно прогнозировать, что в долгосрочной перспективе он будет только набирать обороты. В этих условиях совместимость отечественных средств защиты с ИТ-окружением становится одним из приоритетных факторов, влияющих на выбор продуктов кибербезопасности.

Как видно из результатов исследования, на сегодняшний день в ТОП-3 решений в рейтинге удовлетворенности российскими технологиями кибербезопасности входят продукты для защиты конечных точек от сложных атак (EDR), системы для защиты от таргетированных атак (Anti-APT), а также специализированные системы для защиты баз данных (DAM). В случае с EDR-системами, которые сейчас находятся на первой строчке рейтинга, пользователи ожидают от производителей снижения нагрузки на рабочие станции и расширения функциональности по аналогии с иностранными продуктами. При оценке систем Anti-APT компании отметили, что требуются доработки, связанные с упрощением эксплуатации продукта. Ожидаемые пользователями векторы развития решений класса DAM, которые также получили высокую оценку, — расширение набора поддерживаемых баз данных и увеличение функциональности по аналогии с зарубежными продуктами. Расширение функциональности компании ожидают от многих классов решений, очевидно, что это общая точка роста для российских средств защиты.

Выводы

Примечательно, что системы контроля привилегированных пользователей (PAM), межсетевые экраны (NGFW) и сканеры уязвимостей оцениваются на самом низком уровне среди рассмотренных классов решений. Это связано с тем, что компании активно использовали иностранные аналоги в этой части и привыкли к более широкой функциональности и более удобным интерфейсам управления. Поэтому респонденты возлагают на российских производителей наиболее высокие ожидания в отношении развития и увеличения зрелости данных решений.

Несмотря на отмечаемые сложности, российские технологии кибербезопасности уже сейчас оцениваются довольно высоко по всем рассмотренным классам систем. И как показывает практика, многие российские вендоры готовы обучать специалистов, отвечающих за внедрение, активно помогать с возникающими проблемами и в ряде случаев гибко дорабатывать продукты. Всё это говорит о высоком потенциале российских технологий кибербезопасности и позволяет дать позитивную оценку перспективам импортозамещения в среднесрочной перспективе.

Ростелеком
Солар

Email:

integration@rt-solar.ru
pr@rt-solar.ru

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы
+7 (499) 755-02-20 – техническая поддержка

Адрес:

г. Москва, Никитский пер., д. 7, стр. 1