

Партнёры R-Vision рассказали, с какими запросами заказчики обращаются при выборе VM-решения, где возникают сложности и почему результат проекта зависит не только от набора функций.

Введение

Сравнение технических возможностей — обязательный этап выбора VM-решения. Оно помогает сформировать шорт-лист и понять, закрывает ли продукт базовые требования.

После технического сравнения заказчику важно понять, как решение покажет себя на пилоте, впишется ли в текущую архитектуру и кто будет сопровождать внедрение. Именно эти факторы помогают оценить не только возможности продукта, но и вероятность успешной реализации проекта.

Чтобы понять, какие факторы влияют на финальный выбор VM-продукта и успешность проекта, R-Vision провёл опрос партнёрского сообщества — компаний, участвующих во внедрении VM-решений у корпоративных заказчиков.



Методология

Опрос проводился среди партнёров R-Vision с 12 февраля по 9 апреля 2026 года. Данные собирались на партнёрской конференции, на вебинаре по R-Vision VM, на конференции R-EVolution 26, через e-mail-рассылку и индивидуальные обращения к партнёрам.

В нём приняли участие **43 респондента** — представители интеграторов и дистрибьюторов, работающих с VM-проектами у корпоративных заказчиков.

Респондентам предлагалось оценить запросы заказчиков, причины разочарований в VM-проектах и факторы финального выбора VM-решения по шкале от 1 до 10. Для анализа ответы были сгруппированы по уровню приоритета:

Высокий — 9–10

Средний — 7–8

Низкий — 1–6

Опрос отражает партнёрский взгляд на VM-проекты и не претендует на оценку всего рынка. Его задача — показать, как интеграторы и дистрибьюторы оценивают запросы заказчиков, причины сложностей в проектах и факторы, которые влияют на выбор VM-решения.

Ключевые выводы

Функциональность важна, но не закрывает всю оценку VM-решения. Список возможностей помогает сузить выбор, однако высокий приоритет этому фактору при финальном выборе VM-решения дали только треть респондентов.

Сканирование остается основной точкой входа в VM-проекты. Большинство заказчиков начинают с запроса на выявление уязвимостей. В свободных ответах респонденты отдельно отмечали важность точности сканирования: чем меньше ложных срабатываний, тем меньше времени команды тратят на ручную проверку.

Часть заказчиков уже на старте смотрит шире сканирования. Более половины респондентов отмечают интерес заказчиков к системам управления уязвимостями, а не только к сканерам.

Основные сложности проявляются после выбора решения. Чаще всего партнеры связывают разочарование в проектах со сложностью внедрения в процессы и нехваткой внутренних ресурсов.

Финальный выбор во многом зависит от команды реализации. Самым значимым для заказчиков фактором участники опроса назвали поддержку интегратора.

Пилот и архитектурная совместимость входят в число ключевых факторов выбора. Заказчикам важно проверить решение в своей инфраструктуре до покупки.



«Партнёры сопровождают VM-проекты на всех этапах — от выбора решения и пилота до внедрения, эксплуатации и работы с результатами. Благодаря этому они видят не только сильные стороны продукта, но и то, с какими сложностями сталкиваются заказчики в реальных проектах.

Результаты опроса подтверждают важную для нас логику: заказчики часто начинают с понятного запроса на сканирование уязвимостей, но дальше оценивают уже не только набор функций. Им важно понять, как решение покажет себя на пилоте, насколько точно выявляет уязвимости, как вписывается в архитектуру и помогает перейти от результатов сканирования к понятной работе по устранению.

Для R-Vision это принципиальный фокус развития VM-решения: качество сканирования, точность результатов и полноценные сценарии работы с уязвимостями должны усиливать друг друга.

VM-проект должен помогать командам не просто находить уязвимости, а быстрее понимать, что критично, кому это передать и как контролировать устранение без лишней ручной нагрузки».

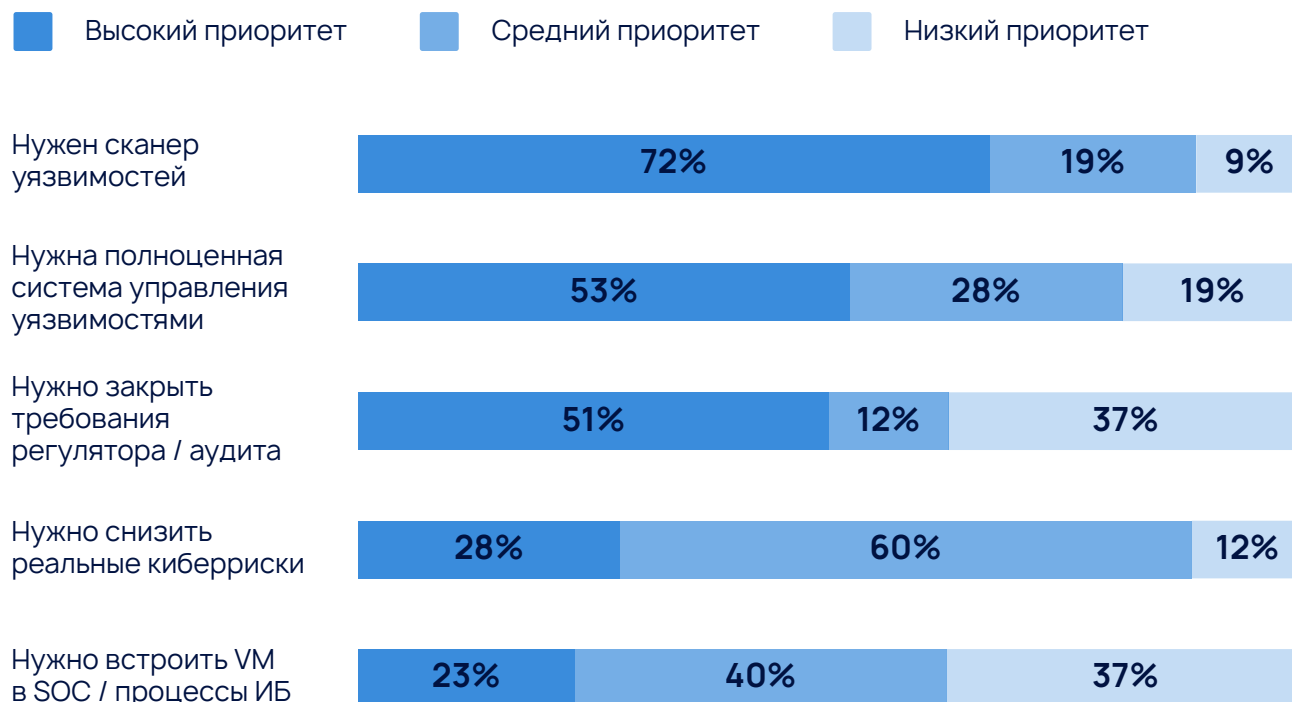


R-Vision

Ирина Карпушева,
менеджер по продуктовому
маркетингу компании R-Vision

С какими задачами заказчики приходят в VM

Чтобы понять, с чего для заказчиков начинается интерес к VM-решениям, мы спросили партнёров, с какими задачами к ним чаще всего обращаются:



По мнению респондентов, заказчики чаще всего приходят в VM с задачей сканирования уязвимостей — это остается базовой и понятной отправной точкой. При этом в комментариях партнёры уточняли: заказчикам важен не только сам факт обнаружения, но и качество результатов — чтобы данные сканирования требовали меньше ручной перепроверки и не перегружали команды ложными срабатываниями.

Это соотносится с [исследованием R-Vision](#), где 78% участников назвали качество сканирования одним из ключевых критериев выбора VM-систем.

При этом более половины респондентов отмечают, что заказчики всё чаще приходят с запросом уже не только на сканер, а на полноценную систему управления уязвимостями — с приоритизацией, контролем устранения и аналитикой.

Запрос на соответствие требованиям регуляторов и аудита также остается значимым, тогда как снижение реальных киберрисков и интеграция VM в SOC или процессы ИБ чаще воспринимаются как следующий этап развития зрелого подхода к управлению уязвимостями.

Почему выбор решения — только половина успеха

Респонденты связывают основные причины разочарования в VM-проектах не столько с самим продуктом, сколько с тем, насколько успешно проект удаётся реализовать после покупки.

По мнению партнёров, чаще всего проблемы возникают при интеграции решения в существующие процессы компании, а также при нехватке внутренних ресурсов и экспертизы со стороны заказчика.



В комментариях партнёры отдельно отмечали продуктовую составляющую этой проблемы: если решение не автоматизирует ключевые процессы «из коробки», дополнительная нагрузка ложится на интегратора и команду заказчика.

Например, для взаимодействия с ИТ важны готовые сценарии интеграции с Service Desk:

- постановка задач,
- отслеживание статусов,
- закрытие после устранения.

Если есть только формальный API, эти сценарии приходится выстраивать на проекте, что увеличивает нагрузку на интегратора и команду заказчика.

Следующий значимый фактор — разрыв между ожиданиями и реальными возможностями проекта (высокий приоритет ему поставили 53% респондентов) .

Партнёры отмечали, что на практике VM может требовать больше времени, ресурсов и изменений в процессах, чем заказчик закладывает на старте.

В свободных ответах респонденты также упоминали скорость реакции вендора. Если доработки функциональности или корректировка логики детекта затягиваются, заказчик быстрее теряет ощущение практической ценности продукта в проекте.

Масштабируемость решения и выбор продукта без предварительной практической проверки участники опроса оценили как менее критичные причины по сравнению со сложностями внедрения, нехваткой ресурсов и общей готовностью компании к запуску проекта.

Это не снижает роли пилота при выборе: он помогает проверить решение до покупки, но не заменяет готовность заказчика к внедрению и работе с результатами.

От чего зависит финальный выбор VM-решения

Техническое сравнение помогает определить подходящие VM-решения, но финальный выбор обычно зависит не только от продукта, но и от условий его внедрения. По мнению участников опроса, решающими чаще всего становятся факторы, которые помогают снизить риски проекта: поддержка интегратора, результаты пилота и архитектурная совместимость.



Самый высокий приоритет получила поддержка интегратора

77%

Для партнёрского опроса этот результат ожидаем, но важен как индикатор более широкой логики выбора: на заключительном этапе заказчики оценивают не только VM-систему, но и реализуемость будущего проекта. Им важно понимать, кто поможет провести пилот, учесть ограничения инфраструктуры, встроить решение в процессы и довести внедрение до результата.

При этом качество поддержки зависит не только от экспертизы интегратора, но и от взаимодействия с вендором: обучения команды, сопровождения пилота, доступности консультаций и скорости реакции на вопросы внедрения. Для заказчика такая связка снижает неопределённость и делает проект более управляемым.

Высокую значимость также получили результаты пилота:

53%

И архитектурная совместимость:

51%

Эти факторы позволяют проверить решение в инфраструктуре заказчика и понять, насколько оно впишется в текущую архитектуру и процессы.

Функциональности высокий приоритет дали:

37%

респондентов

Средний приоритет дали:

63%

респондентов

Функциональность остается важной частью оценки, но не всегда становится решающим аргументом на финальном этапе. Это означает, что список возможностей помогает попасть в число рассматриваемых решений, но сам по себе не гарантирует победу в финальном выборе.

Цена, репутация вендора и соответствие регуляторным требованиям также значимы, но, по мнению партнеров, уступают по приоритетности более прикладным критериям: результатам пилота, поддержке интегратора и архитектурной совместимости.

Это можно объяснить тем, что интеграторы чаще видят ту часть проекта, где формальные критерии уже пройдены, а ключевым становится вопрос реализации - пилота, совместимости, настройки и внедрения.





«Как сервис-провайдер мы оцениваем VM-решение не только по набору функций, но и по тому, насколько удобно с ним работать аналитикам и клиентам сервиса. Качество выявления уязвимостей остается базовым критерием: от точности определения уязвимостей, полноты базы и качества результатов зависит доверие к системе и сервису. Но если инструмент сложен в эксплуатации, это влияет на стоимость предложения, сроки внедрения и трудозатраты на сопровождение. Это актуально не только для MSSP, но и для локальных внедрений у заказчиков.

Поэтому при выборе решения важен пилот с поддержкой партнёра. Он помогает проверить не только выявление уязвимостей, но и практические сценарии: настройку профилей и задач сканирования, построение отчётов и дашбордов, интерпретацию результатов и приоритизацию не только по метрикам и скорингам, но и с учётом инфраструктуры заказчика. В итоге заказчик видит, как результаты сканирования будут превращаться в понятные действия по устранению уязвимостей»



Роман Долгий,

руководитель направления специальных сервисов Solar JSOC ГК «Солар»



«Широкий функционал сегодня есть у большинства VM-решений. Ключевое отличие зрелого продукта – не количество «фич», а точность детекта и экспертиза вендора. База должна оперативно отражать реальные атаки, минимизируя ложные срабатывания и пропуски.

Успех проекта зависит не от «мощности» инструмента, а от выстроенных вокруг него процессов. Даже самое продвинутое решение бесполезно без отлаженного цикла VM: инвентаризация, выявление, приоритизация, устранение и контроль. Только описав эти шаги, закрепив ответственных и установив SLA, можно реально снизить риски.

Как итог, зрелую систему управления уязвимостями можно построить даже на базе классического сканера при наличии компетенций. Дорогой, но неинтегрированный в ежедневную работу «комбайн» — это пустая трата бюджета».



Виктор Кирпаль,

руководитель направления VM,
«Инфосистемы Джет»



«Vulnerability Management — процесс, имеющий четкие границы, а также понятный и измеримый результат. Коробочный продукт в данном случае должен вписываться не только в функциональные требования, но и в принятый в компании темп работы.

Один из ключевых критериев при выборе VM-решения — его способность органично встроиться в работу ИБ-подразделения и не создавать дополнительной нагрузки на поддержку. Однако соответствие этому требованию, как правило, можно установить только на пилоте или в результате боевого внедрения продукта.

На этом этапе чаще всего проявляется и разница в ожиданиях участников проекта. Подходы к оценке и интерпретации результатов внедрения Vulnerability Management вызывают разногласия среди участников рынка. Это не только постоянный выбор между доступностью и безопасностью, но и поиск баланса между ИТ и ИБ, их целевыми показателями. Из-за разницы критериев требования к продукту в части оценки степени серьезности (severity scoring) и механизмов интерпретации достаточно значительные. Как итог, многие заказчики ждут от VM-платформы не только операционной работы с уязвимостями, но и аналитики на уровне поверхности атаки.

В этой логике интегратор становится ключевой фигурой, которая транслирует лучшие практики работы с Vulnerability Management как с полноценным инструментом управления уязвимостями. Такой подход выходит далеко за рамки использования ПО как встроенного сканера и инструмента для подготовки отчетов руководству.

Для успешной реализации партнерского проекта требуется серьезное включение разработчика. Важно, чтобы вендор не только обучал и обеспечивал поддержку в рамках конкретного процесса или доработки продукта, но и давал возможность реализовывать пользовательские сценарии как единую неразрывную операцию. Ключевыми критериями успеха в данном случае являются готовность продукта к эксплуатации, а также его возможности по внедрению, миграции, масштабированию и интеграции с существующими процессами кибербезопасности».



 **Бастион**

Артём Береговой,
технический директор компании «Бастион»

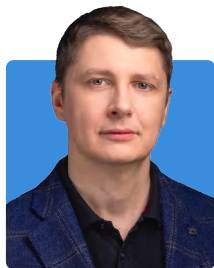




«Для эффективной работы VM-решения необходима правильная техническая интеграция, чтобы оно могло агрегировать данные об уязвимостях из разных источников (сканеры, EASM, ручной ввод) и приземлять их на карту активов. Кроме того, решение должно помогать в приоритизации уязвимостей, оценке их влияния на бизнес-процесс и отслеживании их жизненного цикла вплоть до подтверждения устранения.

При этом простое внедрение VM не решает задачу автоматически. На бумаге кажется, что после установки всё должно идти по простой схеме: нашёл уязвимость — передал ИТ — ИТ её закрыли — проконтролировал. На практике всё куда сложнее. Далеко не всегда понятно, реально ли и где используется найденный уязвимый компонент, кто за него ответственен, не навредят ли изменения в нём рабочим процессам. И таких клубков надо распутать десятки. Управление уязвимостями — это в первую очередь процесс, эффективность которого зависит от слаженной работы специалистов ИТ и ИБ разных уровней, разработчиков, а также подрядчиков, которые внедряют и обслуживают систему.

Поэтому как интегратор, мы видим свою миссию не просто во внедрении и правильной настройке VM-решения, но и в налаживании взаимодействия между подразделениями, обучении и экспертном сопровождении проекта. ИТ и ИБ должны находиться в едином информационном поле и четко понимать свои зоны ответственности, чтобы устранение уязвимостей было оперативным, но не нарушало работу системы и бизнес-процессов»



K2 кибер
безопасность

Аскар Добряков,

ведущий эксперт направления защиты данных
и приложений в K2 Кибербезопасность

R-Vision — разработчик систем цифровизации и кибербезопасности. С 2011 года компания создаёт технологии, которые помогают организациям эффективно противостоять киберугрозам, поддерживать надёжность ИТ-инфраструктуры и обеспечивать цифровую трансформацию.

Технологии R-Vision используются в крупнейших банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

sales@rvision.ru
+7 (499) 322 80 40

t.me/rvision_pro
vk.ru/rvision_ru

