

Исследование

АНАЛИЗ ПРАКТИКИ ИСПОЛЬЗОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В РОССИЙСКИХ КОМПАНИЯХ



Инфосистемы Джет

JET
SECURITY
TEAM

ОГЛАВЛЕНИЕ

КЛЮЧЕВЫЕ ВЫВОДЫ	4
ПРОФИЛЬ ВЫБОРКИ	5
ИНСТРУМЕНТЫ VULNERABILITY MANAGEMENT	6
КРИТЕРИИ ВЫБОРА	7
СТЕПЕНЬ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛА VM-РЕШЕНИЙ	9

Управление уязвимостями обеспечивает фундамент киберустойчивости организации за счет целенаправленного сокращения потенциальной поверхности атаки. Незакрытые уязвимости становятся точкой входа для злоумышленников и причиной серьезных инцидентов. При этом среднее время возврата ИТ-систем в рабочее состояние после крупных атак составляет около двух недель, а полное время восстановления может занимать несколько месяцев¹.

Для качественного выстраивания процесса управления уязвимостями в компании принципиальное значение приобретает не только фактическое наличие решения Vulnerability management (далее — VM), но и эффективность и востребованность его функциональных возможностей, предлагаемых рынком. Мы решили выяснить, какие инструменты управления уязвимостями используют российские компании, какие характеристики решений для них критичны и насколько полно используется функциональность внедренных продуктов.

С 2025 по 2026 годы специалисты Лаборатории тестирования решений VM «Инфосистемы Джет» провели функциональное тестирование восьми решений по управлению уязвимостями, еще три решения находятся в процессе тестирования.

Методика тестирования включает в себя 102 критерия проверки. С методикой и результатами тестирования можно ознакомиться на сайте: <https://vm.jet.su/>

Мы рассмотрели пять основных типов используемых инструментов VM: коммерческое VM-решение, коммерческий сканер, VM как услуга, open-source-сканер и ПО для управления уязвимостями собственной разработки.

«Коммерческое VM-решение» и «коммерческий сканер» различаются уровнем зрелости: сканер обследует устройства и формирует отчет об уязвимостях на основе встроенного скоринга, тогда как VM-решение обладает полноценным функционалом управления активами, учитывает бизнес-контекст сканируемых устройств, дополнительно приоритезирует уязвимости на основе вендорской экспертизы и методик оценки критичности, автоматизирует отчетность и назначение ответственных за устранение уязвимостей специалистов, интегрируется с корпоративными системами заявок, предлагая ответственным специалистам инструкции по устранению.

Под **VM как услугой** в рамках исследования подразумевается два варианта: услуга, при которой VM располагается на мощностях сервис-провайдера и администрируется им, и услуга, при которой сервис-провайдер помогает с эксплуатацией и поддержкой решения, располагающегося в инфраструктуре заказчика.

¹ Согласно исследованию Jet CSIRT «Популярные тактики и техники нарушения киберустойчивости российских компаний»

КЛЮЧЕВЫЕ ВЫВОДЫ

52%

/01

опрошенных компаний используют полноценное коммерческое VM-решение

15%

/02

компаний выбирают одновременно два инструмента.

В 8 случаях из 10 имеет место связка коммерческого VM-решения и коммерческого сканера.

НАИБОЛЕЕ ПРИОРИТЕТНЫЕ ХАРАКТЕРИСТИКИ VM-РЕШЕНИЙ:

/03

- качество предоставляемых отчетов
- широкое покрытие базы уязвимостей
- качество детектирования
- собственная экспертиза вендора.

Практика приобретения отдельных VM-инструментов под конкретные задачи не получила широкого распространения, поэтому спрос сместился на продукты, готовые поддержать наиболее широкий функционал и наиболее полное покрытие базы уязвимостей.

ВЕНДОРЫ НАРАЩИВАЮТ ФУНКЦИИ БЫСТРЕЕ, ЧЕМ КОМПАНИИ УСПЕВАЮТ ИХ ОСВАИВАТЬ.

/04

41%

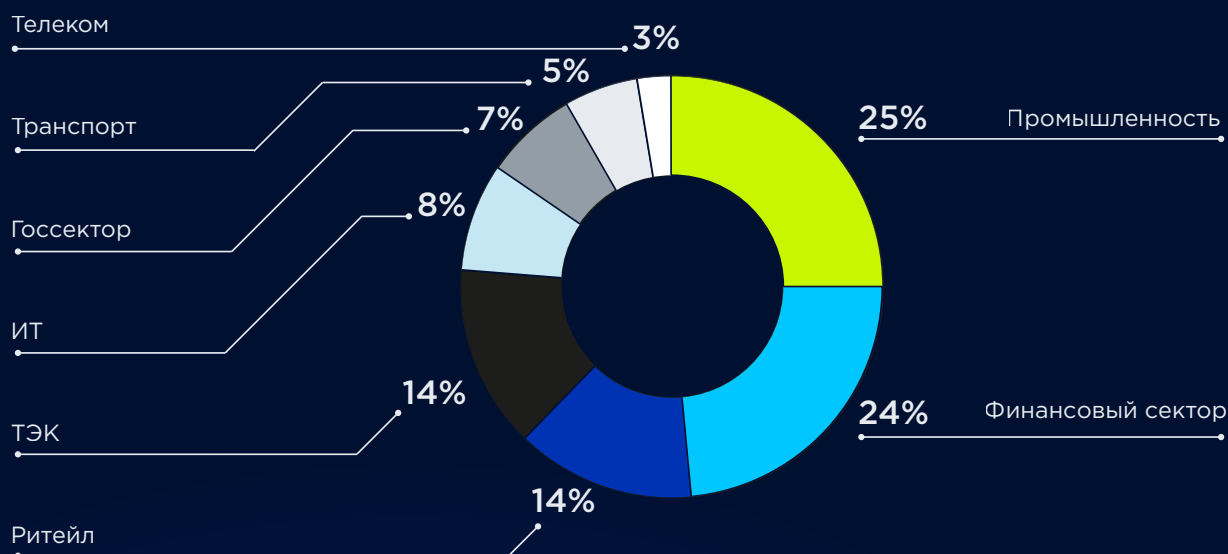
компаний используют не больше половины возможностей своего VM-решения.

Для компаний-пользователей это оборачивается перегруженным интерфейсом, при котором реально востребованными остаются два-три основных модуля.

ПРОФИЛЬ ВЫБОРКИ

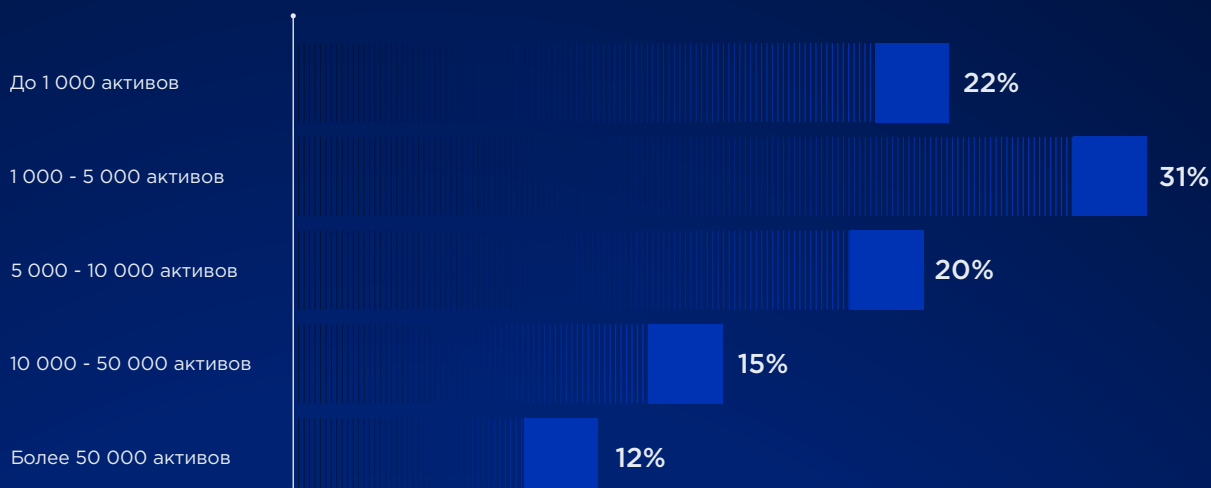
Основой для исследования стали результаты опроса компаний, который мы проводили в третьем квартале 2026 года среди специалистов и руководителей ИБ. Всего опросили более 100 компаний из 8 отраслей. Большую часть выборки составили компании из отрасли промышленности, финансового сектора, ритейла и ТЭК.

Сферы деятельности опрошенных компаний



Помимо отраслевой принадлежности, фиксировали размер ИТ-инфраструктуры опрашиваемых компаний: количество активных устройств в сетевом контуре. 78% участников исследования составляют организации крупного корпоративного сегмента, управляющих инфраструктурой от 1 000 активных устройств. При подобном масштабе инфраструктуры респонденты обладают сформированными требованиями к VM-решениям.

Размеры инфраструктуры опрошенных компаний

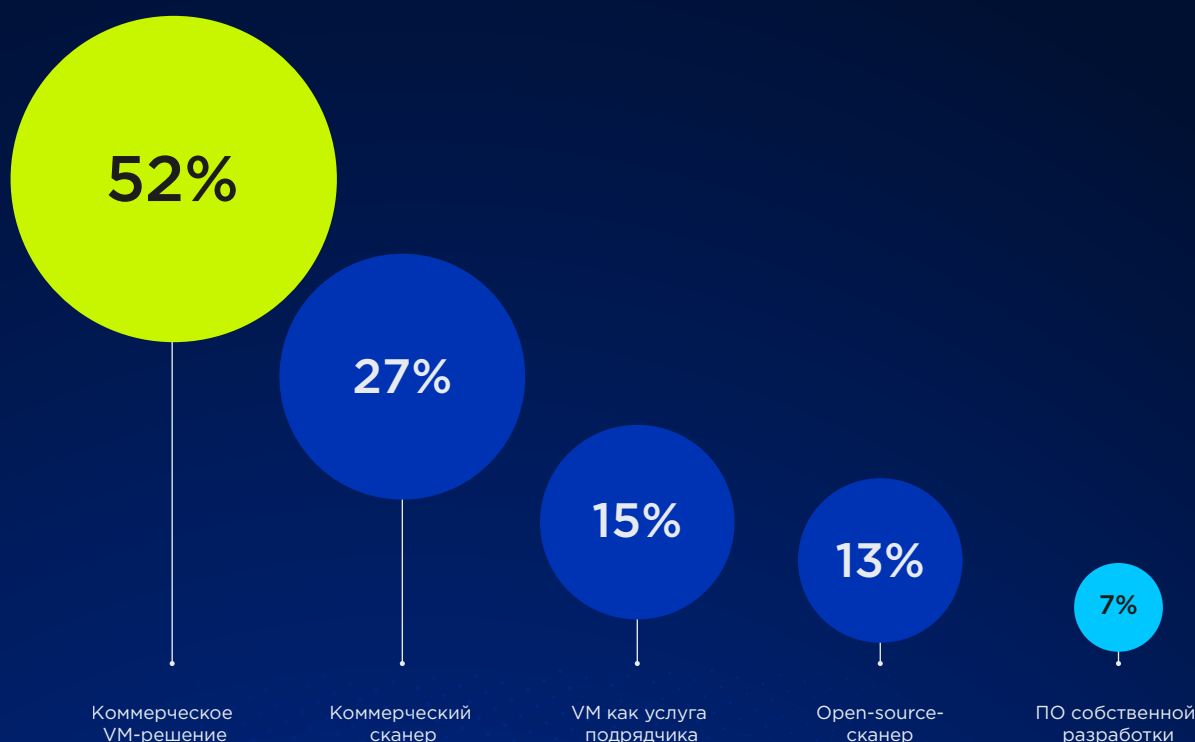


ИНСТРУМЕНТЫ VULNERABILITY MANAGEMENT

Полноценное коммерческое VM-решение использует каждый второй респондент (52%). 15% компаний используют одновременно два инструмента, причем в 8 случаях из 10 используется связка коммерческого VM-решения и коммерческого сканера. 13% респондентов используют open-source-сканер уязвимостей, половина из них — это компании с размером инфраструктуры до 1 000 активов. VM собственной разработки встречается в компаниях, имеющих свыше 5 000 активов, и зачастую также используется в связке с уже имеющимся коммерческим VM-решением. Компании со средним (от 1 000 до 10 000) и большим количеством активов (от 10 000 до 50 000) наиболее часто используют VM как услугу от подрядной организации.

Приобретение различных инструментов VM под разные задачи не имеет широкого распространения, что приводит к запросу о максимально широкой функциональности единого продукта и наиболее полной базы уязвимостей.

Используемые инструменты VM (вопрос допускал несколько вариантов ответа)



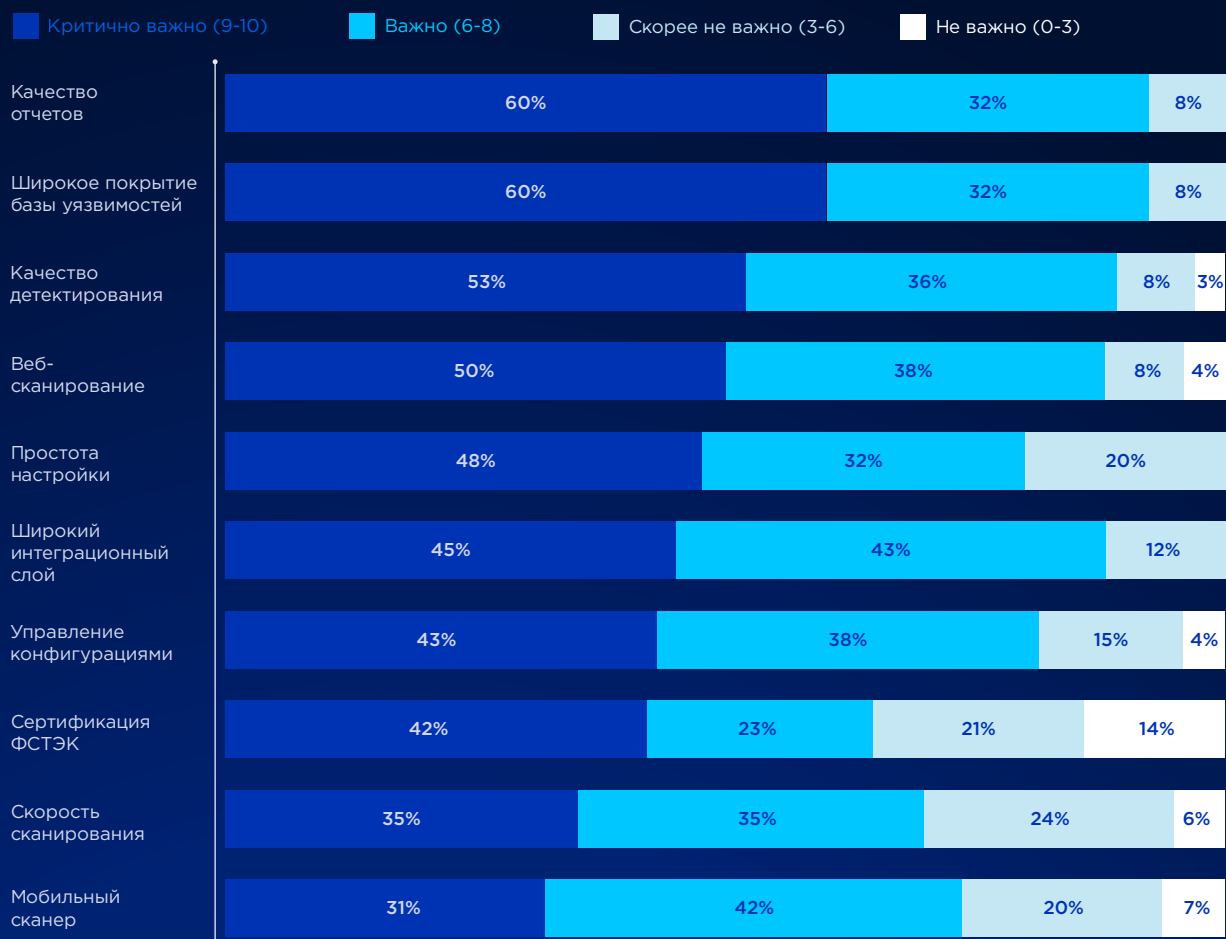
КРИТЕРИИ ВЫБОРА

В рамках исследования респондентам предлагалось оценить важность характеристик VM-решений по шкале от 0 до 10. Наиболее приоритетными характеристиками для VM-решений стали:

- качество предоставляемых отчетов (наличие у решения интуитивно понятных и полезных отчетов по умолчанию, а также возможность настраивать кастомные отчеты внутри системы);
- широкое покрытие базы уязвимостей (для ОС, сетевого оборудования, стороннего ПО и другого);
- качество детектирования (полнота и актуальность базы уязвимостей сканера — покрытие международных баз (CVE, NVD, БДУ ФСТЭК России и других), а также собственная экспертиза вендора (исследования и лучшие практики).

Менее приоритетные характеристики по мнению респондентов — это скорость сканирования, наличие у решения портативного модуля для сканирования (мобильного сканера) и сертификации ФСТЭК России, ценность которых варьируется в зависимости от специфики деятельности и ИТ-инфраструктуры компании.

Приоритизация характеристик VM-решений



Качество отчетов, формируемых VM, вышло на первое место по востребованности. Несмотря на длящуюся уже несколько лет всеобщую тенденцию ухода от рутинных действий в пользу автоматизации процессов ИБ, такая консервативная задача как формирование отчетов все еще является ключевым и самым востребованным функционалом у пользователей. Стремление к инновационным подходам опережает устоявшиеся процессы компаний: VM-решения постоянно развиваются, а механика работы с уязвимостями внутри организаций не всегда успевает за ними. В таких условиях краеугольным камнем процесса остается понятный всем «отчет об уязвимостях».

Широкое покрытие базы уязвимостей неслучайно разделяет первое место с качеством предоставляемых отчетов. Значимость полноты охвата (ПО, операционных систем, сетевого оборудования, СУБД и прочего) возрастает с каждым годом: продолжается импортозамещение, инфраструктуры растут, парки оборудования расширяются, а отдельные филиалы / дочерние компании формируют собственные сегменты со своей обособленной инфраструктурой. При этом под контролем VM должно оставаться все.

Однако, **широкий интеграционный слой** является третьим функционалом по востребованности, по сумме ответов со значением «Критично важно» и «Важно», и первым, если смотреть только по отметке «Важно». Потребность в интеграциях со смежными системами растет и уже входит в число ключевых требований к системе управления уязвимостями, что можно считать признаком растущей зрелости VM как процесса. Интеграционный слой позволяет VM-решениям существовать в ИБ-контексте организации взамен обособленного выполнения узконаправленных задач. Если рассматривать конкретнее — интеграции решают две задачи:

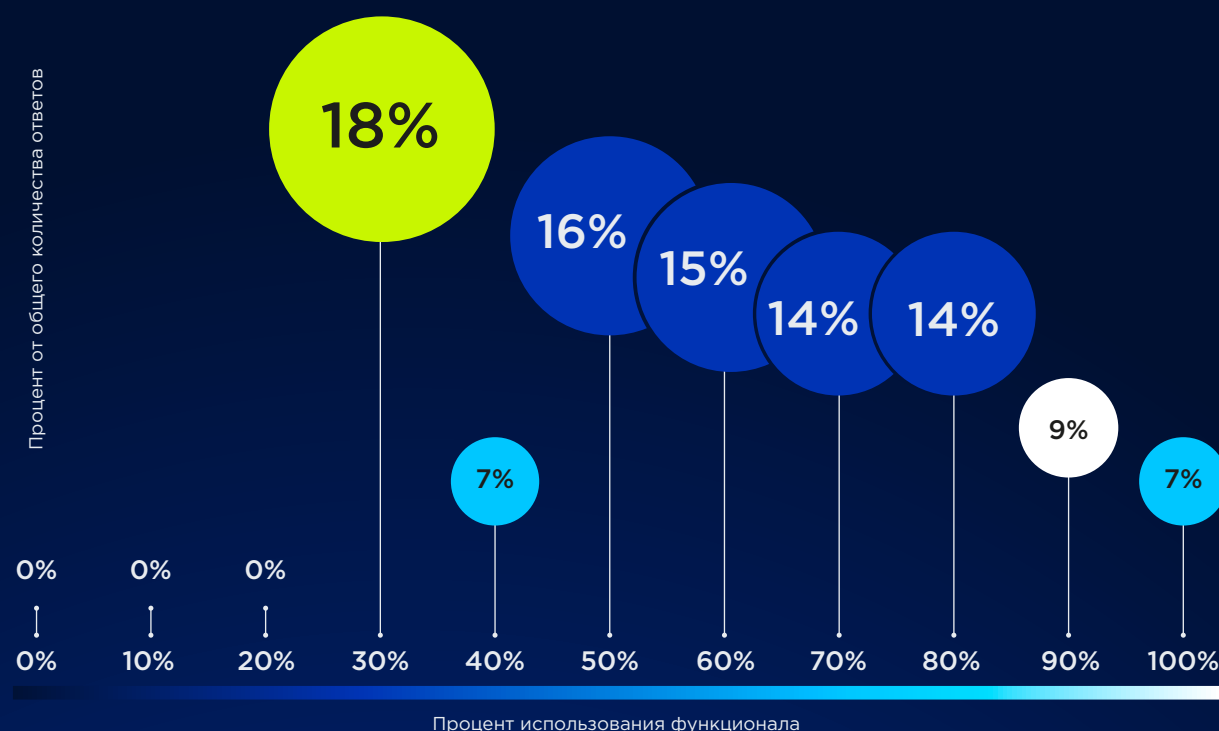
- автоматизация (постановка задач в Service Desk / ITSM / тикет-системы ускоряет устранение уязвимостей);
- обогащение данных об инфраструктуре — источниками сведений об активах выступают системы классов антивирусной защиты, EDR, SIEM, CMDB, и каждая добавляет свой уникальный контекст. Антивирусная защита детектирует запуск эксплойта (что позволяет пересмотреть приоритизацию уязвимостей с аналогичным эксплойтом внутри этой же инфраструктуры), SIEM сообщает об инцидентах со схожим уязвимым ПО на смежных хостах, а CMDB способна предоставить информацию об активах в бизнес-контексте, который демонстрирует приоритизацию активов на уровне управления организацией.

СТЕПЕНЬ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛА VM-РЕШЕНИЙ

В рамках исследования респондентам также было предложено оценить объем функций VM-решений, которые фактически используются компаниями. 41% компаний используют не более половины возможностей, предоставляемых решением.

На графике отражен процент ответов респондентов по субъективной доле используемого ими функционала VM-решений.

Востребованность функциональных возможностей VM-решений



Вендоры ведут напряженную гонку функциональности: новые модули выпускаются для того, чтобы удержаться в конкурентной среде, однако новые возможности зачастую не находят широкого практического применения. Из-за этого компании-пользователи в реальности используют лишь два-три основных модуля, не желая разбираться в перегруженном интерфейсе. Наиболее эффективной в таком случае является обратная стратегия: не наращивать число функций, а развивать сильные стороны продукта и повышать зрелость базовой функциональности.

”

Рынок Vulnerability Management в 2026 году заметно растёт: появляются гибридные и облачные модели, все больше нужны мониторинг внешней поверхности атаки и контроль конфигураций. Цифры говорят сами за себя: в прошлом году около 65% инцидентов начиналось с эксплуатации уязвимостей, у каждой четвертой уязвимости уже есть публичный эксплойт, а времени между ее публикацией и атакой с ее использованием становится все меньше. Успевать патчить в таком темпе становится все сложнее, а в крупных инфраструктурах — практически невозможно.

Поэтому фокус рынка смещается с отдельных уязвимостей на уровень защищенности в целом. Он складывается из грамотного управления активами, контроля ключевых недостатков в инфраструктуре и проверки возможности реальной эксплуатации уязвимостей



Виктор Кирпаль,

руководитель направления Vulnerability
Management, «Инфосистемы Джет»



security@jet.su
jetcsirt.su