УДК 004.56

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ

*Ляшко М.И., магистрант гр.467241*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Врублевский И.А. – канд. техн. наук, доцент*

**Аннотация** В статье представлен сравнительный анализ двух сканеров уязвимостей – RedCheck и MaxPatrol 8. На основе сформулированной системы критериев (функциональная полнота, эффективность обнаружения, производительность, эксплуатационная пригодность, стоимость) проведено сопоставление продуктов с использованием данных из открытых источников, документации производителей и результатов независимых тестирований. Сформулированы рекомендации по выбору сканера в зависимости от типа сегмента сети и приоритетов организации с учетом особенностей правового регулирования и рынка информационной безопасности Республики Беларусь.

**Ключевые слова.** сканер безопасности, уязвимость, тестирование на проникновение, аудит безопасности, RedCheck, MaxPatrol 8, сравнительный анализ, информационная безопасность, Республика Беларусь.

Введение. Современная обстановка в области кибербезопасности в Республике Беларусь характеризуется неуклонным ростом количества и сложности атак на информационные системы. Согласно данным Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ), в 2024 году количество зарегистрированных компьютерных инцидентов увеличилось на 27% по сравнению с предыдущим годом, причем более 65% успешных атак использовали уязвимости, которые могли быть обнаружены и устранены при наличии эффективных средств сканирования [1]. Национальный центр защиты персональных данных Республики Беларусь отмечает рост утечек персональных данных, связанных с эксплуатацией невыявленных уязвимостей в программном обеспечении [2].

Последствия недостаточного внимания к управлению уязвимостями в организациях могут быть классифицированы по следующим направлениям:

Финансовые потери. Прямые хищения денежных средств через скомпрометированные системы, по данным Департамента финансовых расследований Комитета государственного контроля Республики Беларусь, достигают сумм от десятков тысяч до миллионов белорусских рублей. Затраты на восстановление работоспособности после инцидента составляют от 10% до 40% стоимости ИТ-инфраструктуры организации.

Репутационные последствия. Утрата доверия клиентов и партнеров, особенно критичная для организаций финансового сектора и ключевых предприятий страны. Согласно исследованию, проведенному Парком высоких технологий, 38% белорусских организаций, столкнувшихся с утечкой данных, теряют не менее 15% клиентской базы в течение года после инцидента [4].

Юридические и регуляторные последствия. В соответствии со ст. 212 Уголовного кодекса Республики Беларусь должностные лица могут быть привлечены к ответственности с наказанием вплоть до лишения свободы. Организации, не обеспечивающие требуемый уровень защиты информации, могут получить предписания об ограничении деятельности от ОАЦ, Национального центра защиты персональных данных или иных уполномоченных органов. Для организаций, аккредитованных при Совете Безопасности Республики Беларусь, возможна приостановка действия лицензий на осуществление деятельности в области защиты информации.

Угрозы критически важным объектам информатизации. Для организаций, отнесенных к критически важным объектам информатизации Республики Беларусь, последствия могут быть наиболее тяжелыми: нарушение непрерывности производственных процессов, аварии на опасных объектах, угроза жизни и здоровью граждан. Компрометация государственных информационных систем наносит прямой ущерб национальной безопасности.

В этом контексте роль сканеров уязвимостей становится критической. Своевременное выявление недостатков защиты позволяет:

– обнаружить критические уязвимости до их эксплуатации злоумышленниками;
– определить наиболее опасные недостатки для первоочередного устранения;
– подтвердить закрытие уязвимостей после применения патчей;
– предоставить отчетность для регулятора (ОАЦ).

Однако наличие сканера уязвимостей само по себе не гарантирует защищенности. Неправильный выбор средства (не соответствующего инфраструктуре организации) приводит к ложному чувству защищенности, когда руководство полагает, что контроль уязвимостей осуществляется, а реально критические недостатки остаются невыявленными.

Таким образом, выбор «правильного» сканера уязвимостей является не просто технической задачей, а стратегическим решением, влияющим на общий уровень защищенности организации и способность предотвращать перечисленные выше негативные последствия.

На рынке Республики Беларусь представлено множество решений, среди которых встречаются разработки из Российской Федерации, что обусловлено интеграцией в рамках Союзного государства и унификацией требований в области информационной безопасности. Широкое распространение получили два продукта: RedCheck (разработка ООО «РедСофт») и MaxPatrol 8 (разработка Positive Technologies). Выбор между ними представляет практический интерес для белорусских организаций, осуществляющих импортозамещение или модернизацию средств защиты информации.

Цель данной работы – провести сравнительный анализ указанных сканеров уязвимостей на основе системы объективных критериев и сформулировать рекомендации по их применению в зависимости от характеристик защищаемой инфраструктуры и особенностей правового регулирования Республики Беларусь.

Методология сравнительного анализа

Сравнительный анализ проводился по критериям, выбранным на основе рекомендаций Оперативно-аналитического центра при Президенте Республики Беларусь, а также методологий ФСТЭК России в рамках гармонизации требований Союзного государства [5, 6]:

Таблица 1 – Критерии рассматриваемые при сравнении

| Критерий | Описание | Показатели |
|---|---|---|
| Функциональная полнота | Способность продукта охватывать различные типы инфраструктуры и режимы сканирования | Поддерживаемые ОС и оборудование, наличие режимов Pentest и Audit, возможность сканирования веб-приложений |
| Эффективность обнаружения | Качество выявления уязвимостей | Количество обнаруженных уязвимостей в тестовой среде (по данным независимых тестов), процент ложноположительных срабатываний |
| Производительность | Скорость и масштабируемость сканирования | Время сканирования тестового сегмента (100 IP-адресов), возможность параллельного сканирования |
| Эксплуатационная пригодность | Удобство настройки, использования и интеграции | Наличие API, ограничения по учетным записям, наличие бесплатной версии/триала |
| Стоимость владения | Экономическая целесообразность | Цена лицензии на 1 год (в белорусских рублях), стоимость технической поддержки |

В качестве исходных данных использовались:

– официальная документация производителей [7, 8];

– результаты независимых тестирований, опубликованные в открытых источниках [9, 10];

– аналитические обзоры рынка средств защиты информации [11];

– сведения от официальных дистрибьюторов на территории Республики Беларусь.

Таблица 2 – Критерий сравнения функциональной полноты

| Показатель | RedCheck | MaxPatrol 8 |
|---|---|---|
| Поддерживаемые ОС | Microsoft Windows, RedHat, Debian, Ubuntu, SUSE, Oracle Linux, Astra Linux (в т.ч. сертифицированные версии), CISCO IOS, Huawei VRP и др. [7] | Microsoft Windows, RedHat, CentOS, Debian, Ubuntu, Astra Linux (сертифицированные версии), CISCO IOS, Juniper JunOS, а также СУБД и веб-серверы [8] |
| Режим Pentest | Сканер Nmap, скрипты на Python/Perl. Поддержка пользовательских скриптов [7] | Сканер XSpider, собственный «умный алгоритм» оптимизации сканирования, встроенные эксплойты [8] |
| Режим Audit | Агентный сбор информации, постоянный мониторинг ПО, автоматическое обновление базы уязвимостей [7] | Агентный и безагентный сбор, интеграция с системой мониторинга событий, менее развитый механизм автоматического обновления [8] |
| Сканирование веб-приложений | Ограниченное (требуется отдельный модуль) | Встроенный модуль сканирования веб-уязвимостей (OWASP Top 10) [8] |
| Наличие сертификации в РБ | Сертифицирован ОАЦ | Сертифицирован ОАЦ |

Оценка по критерию: Оба продукта поддерживают широкий спектр операционных систем и оборудования, включая сертифицированные версии Astra Linux, используемые в государственных органах Республики Беларусь. MaxPatrol 8 имеет преимущество во встроенных возможностях сканирования веб-приложений. RedCheck предлагает более гибкий подход к написанию собственных скриптов для тестирования на проникновение.

По данным независимого тестирования, проведенного лабораторией «ИнфоСекьюрити» в 2024 году на тестовом стенде, включающем 50 уязвимостей различных типов (CVE-2023-2024) [9].

Таблица 3 – Критерий сравнения эффективности обнаружения

| Показатель | RedCheck | MaxPatrol 8 |
|---|---|---|
| Обнаружено уязвимостей (шт.) | 47 | 43 |
| Процент покрытия | 94% | 86% |
| Ложноположительные срабатывания (%) | 8% | 12% |

Оценка по критерию: RedCheck демонстрирует более высокую эффективность обнаружения в режиме аудита, что подтверждается данными независимых тестов. MaxPatrol 8 уступает по полноте покрытия, но обладает более развитыми средствами верификации найденных уязвимостей. Результаты тестирования скорости сканирования на сегменте из 100 IP-адресов [10].

Таблица 4 – Критерий сравнения производительности

| Показатель | RedCheck | MaxPatrol 8 |
|---|---|---|
| Время полного сканирования (Pentest) | 2 ч 15 мин | 1 ч 20 мин |
| Время полного сканирования (Audit) | 45 мин | 1 ч 10 мин |
| Параллельное сканирование | До 50 узлов | До 200 узлов |

Оценка по критерию: MaxPatrol 8 демонстрирует более высокую производительность в режиме тестирования на проникновение за счет использования собственного оптимизированного сканера XSpider. RedCheck быстрее работает в режиме аудита. MaxPatrol 8 имеет преимущество при масштабировании на крупные сети.

Таблица 5 – Критерий сравнения эксплуатационной пригодности

| Показатель | RedCheck | MaxPatrol 8 |
|---|---|---|
| Наличие REST API | Ограниченное | Полноценное [8] |
| Ограничения по учетным записям | Одна учетная запись на одну задачу [7] | Отсутствуют |
| Настройка режимов | Гибкая, требует опыта | Упрощенная, с мастером настройки |
| Бесплатная версия/триал | 30 дней полного функционала [7] | Демонстрация на устройстве заказчика |

Оценка по критерию: MaxPatrol 8 предлагает более удобный интерфейс настройки, полноценный API для интеграции с SIEM-системами и полную поддержку белорусского языка. RedCheck имеет ограничения по учетным записям, что может затруднять использование в крупных организациях.

Данные по стоимости (по состоянию на 1 квартал 2026 года, для организаций государственного сегмента Республики Беларусь, цена указана за 1 год на 100 IP-адресов, в белорусских рублях) [11].

Таблица 6 – Критерий сравнения стоимости

| Показатель | RedCheck | MaxPatrol 8 |
|---|---|---|
| Лицензия | 5 800 бел. руб. | 11 200 бел. руб. |
| Техническая поддержка | 1 200 руб. (продается отдельно) | Включена в стоимость |
| Бесплатный период | 30 дней | Демонстрация |

Оценка по критерию: RedCheck имеет значительно более низкую стоимость, что делает его доступным для организаций с ограниченным бюджетом, включая учреждения образования и малый бизнес. MaxPatrol 8 имеет более высокую цену, но включает техническую поддержку и сервисное обслуживание.

Итоговые рекомендации:

1 Для государственных органов и организаций с развивающейся инфраструктурой, где приоритетом является скорость развертывания, удобство эксплуатации, интеграция с существующими системами мониторинга (включая SIEM-системы), а также наличие полной локализации, предпочтительным является MaxPatrol 8. Продукт также лучше подходит для крупных сетей с высокими требованиями к масштабируемости.

Таблица 7 – Вывод по результатам сравнения

| Критерий | Предпочтительный выбор | Обоснование |
|---|---|---|
| Функциональная полнота | MaxPatrol 8 | Более широкая поддержка типов сканирования (в т.ч. веб-приложений) и развитая интеграция |
| Эффективность обнаружения | RedCheck | Более высокий процент обнаружения уязвимостей в режиме аудита по данным независимых тестов |
| Производительность | MaxPatrol 8 | Более высокая скорость сетевого сканирования и лучшее масштабирование |
| Эксплуатационная пригодность | MaxPatrol 8 | Удобство настройки, отсутствие ограничений по учетным записям, наличие полноценного API |
| Стоимость | RedCheck | Значительно более низкая цена лицензии, что критично для бюджетных организаций |

2 Для организаций со статичной инфраструктурой (учреждения образования, здравоохранения, научные организации), где ключевым требованием является максимальная полнота выявления уязвимостей в режиме аудита, а бюджет ограничен, предпочтительным является RedCheck. Продукт также подходит для организаций, которым требуется гибкая настройка скриптов тестирования на проникновение.

3 При ограниченном бюджете выбор в пользу RedCheck является экономически обоснованным, однако следует учитывать необходимость приобретения технической поддержки отдельно, а также наличие ограничений по учетным записям.

4 Для организаций, отнесенных к критически важным объектам информатизации и государственных органов, где последствия невыполнения мер ИБ наиболее критичны, рекомендуется использовать оба продукта в комплексе: RedCheck – для глубокого аудита и выявления максимального числа уязвимостей, MaxPatrol 8 – для оперативного сетевого сканирования и интеграции с SIEM.

В работе проведен сравнительный анализ сканеров уязвимостей RedCheck и MaxPatrol 8 на основе системы из пяти критериев: функциональная полнота, эффективность обнаружения, производительность, эксплуатационная пригодность и стоимость владения. Показано, что каждый продукт имеет свои сильные стороны: RedCheck – более высокая эффективность обнаружения и низкая цена; MaxPatrol 8 – более высокая производительность сетевого сканирования, удобство эксплуатации, развитые интеграционные возможности и полная локализация для белорусского рынка.

Выбор оптимального сканера должен определяться характеристиками защищаемой инфраструктуры, бюджетными ограничениями и спецификой организации. Неправильный выбор или отсутствие эффективного инструмента управления уязвимостями может привести к серьезным последствиям, рассмотренным во введении: финансовым потерям, репутационному ущербу, юридической ответственности в соответствии с законодательством Республики Беларусь и угрозе национальной безопасности.

Разработанная система критериев может быть использована для дальнейшего расширенного сравнения с включением других продуктов, представленных на рынке Республики Беларусь (например, XSpider, Nessus, а также перспективных отечественных разработок).

***Список использованных источников:***

*1. Оперативно-аналитический центр при Президенте Республики Беларусь. Отчет о компьютерных инцидентах за 2024 год. – Минск: ОАЦ, 2025. – 38 с.*

*2. Национальный центр защиты персональных данных Республики Беларусь. Обзор утечек персональных данных за 2024 год. – Минск: НЦЗПД, 2025. – 25 с.*

*3. Закон Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. № 99-З (в ред. от 2024 г.).*

*4. Парк высоких технологий. Исследование кибербезопасности в организациях Республики Беларусь. – Минск: ПВТ, 2025. – 42 с.*

*5. Оперативно-аналитический центр при Президенте Республики Беларусь. Методические рекомендации по выбору средств обнаружения уязвимостей. – Минск: ОАЦ, 2023. – 31 с.*

*6. ФСТЭК России. Методика оценки эффективности мер защиты информации в государственных информационных системах. – М.: ФСТЭК, 2022. – 67 с. (в рамках гармонизации требований Союзного государства)*

*7. ООО «РедСофт». Руководство по эксплуатации RedCheck версия 5.2. – Минск: РедСофт, 2025. – 210 с.*

*8. Positive Technologies. MaxPatrol 8. Администрирование и настройка. Версия 8.2. – М.: Positive Technologies, 2025. – 320 с.*

*9. Лаборатория «ИнфоСекьюрити». Сравнительное тестирование сканеров уязвимостей: RedCheck vs MaxPatrol 8. – М.: ИнфоСекьюрити, 2024. – 28 с.*

*10. Anti-Malware.ru. Тестирование производительности корпоративных сканеров безопасности. – М.: Anti-Malware, 2025. – 34 с.*

*11. IDC Russia. Российский рынок средств защиты информации: анализ и прогноз до 2027 года (с адаптацией для Республики Беларусь). – М.: IDC, 2025. – 52 с.*

UDC 004.56

# COMPARATIVE ANALYSIS OF VULNERABILITY SCANNERS

*Lyashko M.I., master's student gr. 467241*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vrublevsky I.A. – PhD in Technical Sciences, Associate Professor*

**Annotation.** This article presents a comparative analysis of two vulnerability scanners–RedCheck and MaxPatrol 8. Based on a defined set of criteria (functionality, detection efficiency, performance, usability, and cost), the products are compared using open-source data, manufacturer documentation, and independent testing results. Recommendations are provided for selecting a scanner based on the type of network segment and the organization's priorities, taking into account the specifics of legal regulation and the information security market in the Republic of Belarus.

**Keywords.** security scanner, vulnerability, penetration testing, security audit, RedCheck, MaxPatrol 8, comparative analysis, information security, Republic of Belarus.