УДК 004.056.3

СИСТЕМА КРИТЕРИЕВ И ПРОЦЕДУРА ОЦЕНКИ ПРИМЕНИМОСТИ РЕШЕНИЙ РЕЗЕРВНОГО КОПИРОВАНИЯ В ИНФРАСТРУКТУРАХ ОГРАНИЧЕННОГО ДОСТУПА

Бесчастнов А.А. (Научно-технологический университет «Сириус»)
Научный руководитель – кандидат экономических наук Е. В. Нехорошков
(Научно-технологический университет «Сириус»)

Введение. Обеспечение доступности и восстановимости информации является важным аспектом информационной безопасности современных информационных систем, поскольку значительная доля инцидентов, включая атаки типа ransomware, сопровождается нарушением доступности сервисов и утратой данных [1-2]. В инфраструктурах, функционирующих в условиях ограниченного доступа и изоляции, применение облачных моделей резервного копирования, как правило, невозможно, а процессы резервного копирования и восстановления реализуются внутри доверенного периметра организации в соответствии с требованиями стандартов информационной безопасности и управления непрерывностью деятельности [3-4]. В связи с этим возникает необходимость формализованного подхода к оценке применимости решений резервного копирования с учетом эксплуатационных ограничений и требований информационной безопасности.

Основная часть. В работе предложена система критериев и процедура оценки применимости решений резервного копирования в инфраструктурах ограниченного доступа, разработанная с учетом особенностей эксплуатации и сложности процессов восстановления в современных ИТ-инфраструктурах [5]. В рамках исследования рассматриваются инфраструктуры, для которых характерны изоляция, ограниченный доступ и невозможность использования внешних облачных сервисов резервного копирования.

Система критериев сформирована с учетом требований стандартов ISO/IEC 27001 [3] и ISO 22301 [4] и практических ограничений эксплуатации и включает четыре группы показателей:

1) критерии средовой применимости, отражающие возможность автономной эксплуатации решений, использование локальных хранилищ и наличие механизмов контроля и разграничения доступа;
2) критерии управляемости конфигураций, характеризующие воспроизводимость настроек резервного копирования и степень зависимости их корректности от ручных операций;
3) критерии обеспечения восстановимости, включающие соответствие заданным показателям RTO и RPO, а также наличие механизмов проверки корректности резервных копий и тестирования восстановления;
4) критерии архитектурной применимости, отражающие возможность использования решений в динамически изменяемых средах и их интеграции с оркестраторными платформами.

Процедура оценки основана на последовательном применении сформированной системы критериев и включает предварительный отбор решений по обязательным условиям эксплуатации в инфраструктурах ограниченного доступа и последующую многофакторную оценку по оставшимся критериям с целью сравнительного анализа и ранжирования решений резервного копирования

Выводы. Разработана система критериев и процедура оценки применимости решений резервного копирования в инфраструктурах ограниченного доступа, позволяющая учитывать эксплуатационные ограничения и требования информационной безопасности и применимая при выборе и обосновании решений резервного копирования в изолированных on-premise инфраструктурах.

Список использованных источников:

1. ENISA Threat Landscape 2025. – European Union Agency for Cybersecurity. ENISA Threat Landscape 2025 / European Union Agency for Cybersecurity. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата обращения: 24.01.2026).
2. State of Backup and Recovery Report 2025. – Unitrends. The State of Backup and Recovery Report 2025. – URL: https://www.unitrends.com/media/downloads/resources/The-State-of-Backup-and-Recovery-Report-2025.pdf (дата обращения: 29.01.2026).
3. ISO/IEC 27001:2022. Information security management systems – Requirements. – International Organization for Standardization. ISO/IEC 27001:2022. – URL: https://www.iso.org/standard/27001.html (дата обращения: 01.02.2026).
4. ISO 22301:2019. Security and resilience – Business continuity management systems — Requirements. – International Organization for Standardization. ISO 22301:2019. – URL: https://www.iso.org/standard/75106.html (дата обращения: 04.02.2026).
5. Obermeier S., Jösler T., Renggli S., Unternährer M., Hämmerli B. Automating Recovery in Mixed Operation Technology/IT Critical Infrastructures // IEEE Security & Privacy. 2023. Vol. 21, pp. 43-54. DOI: 10.1109/MSEC.2023.3264595.