УДК 004

ОТЕЧЕСТВЕННАЯ СИСТЕМА РЕЗЕРВНОГО КОПИРОВАНИЯ «КИБЕР БЭКАП»: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИНТЕГРАЦИИ В КОРПОРАТИВНУЮ ИТ-СРЕДУ

Токтаров Т.М.

Магистрант,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Белаш В.Ю.

к.п.н., доцент,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Аннотация: В статье рассматриваются вопросы импортозамещения систем резервного копирования в корпоративном секторе Российской Федерации. Анализируются риски эксплуатации зарубежных решений, в условиях санкционных ограничений и отсутствия официальной технической поддержки. Представлен обзор функциональных возможностей отечественной платформы «Кибер Бэкап», включая поддержку российских операционных систем, платформ виртуализации. Описана гибридная модель миграции, позволяющая минимизировать риски при переходе на отечественное решение. Сформулированы рекомендации по интеграции «Кибер Бэкап» в корпоративную ИТ-среду на основе анализа успешных практик внедрения.

Ключевые слова: резервное копирование, импортозамещение, Кибер Бэкап, системы защиты данных, корпоративная ИТ-инфраструктура, российское программное обеспечение, миграция данных, технологический суверенитет.

"CYBER BACKUP" DOMESTIC BACKUP SYSTEM: FEATURES AND INTEGRATION PROSPECTS IN CORPORATE IT ENVIRONMENT

Toktarov T.M.
master's student,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia
Belash V.Yu.
Ph.D., Associate Professor,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Abstract: The article examines the issues of import substitution of backup systems in the corporate sector of the Russian Federation. It analyzes the risks of using foreign solutions under sanctions restrictions and the lack of official technical support. An overview of the functional capabilities of the domestic platform "Cyber Backup" is presented, including support for Russian operating systems and virtualization platforms. A hybrid migration model is described as minimizing risks during the transition to a domestic solution. Recommendations are formulated for integrating "Cyber Backup" into a corporate IT environment based on the analysis of successful implementation practices.

Keywords: backup, import substitution, Cyber Backup, data protection systems, corporate IT infrastructure, Russian software, data migration, technological sovereignty.

В условиях современных геополитических событий и последовательной реализации курса на обеспечение технологического суверенитета Российской Федерации вопросы импортозамещения критической ИТ-инфраструктуры выходят на первое место. Системы резервного копирования данных (СРК)

относятся к категории критически важного программного обеспечения, поскольку именно от их надежности и бесперебойной работы зависит возможность восстановления бизнес-процессов после аппаратных сбоев, программных ошибок или целенаправленных кибератак [3].

Согласно исследованию Центра экспертизы К2Тех, проведенному в марте 2026 года, 70% крупных российских компаний продолжают использовать западные системы резервного копирования, при этом безусловным лидером остается Veeam, развернутый примерно у трети респондентов (рисунок 1). При этом компании все больше сталкиваются с растущими сложностями при обслуживании этих решений собственными силами. Отсутствует официальная техническая поддержка со стороны вендора. Теперь невозможно получить актуальные обновления и исправления безопасности. Возросли риски, связанные с возможной блокировкой или ограничением функциональности ПО [5].

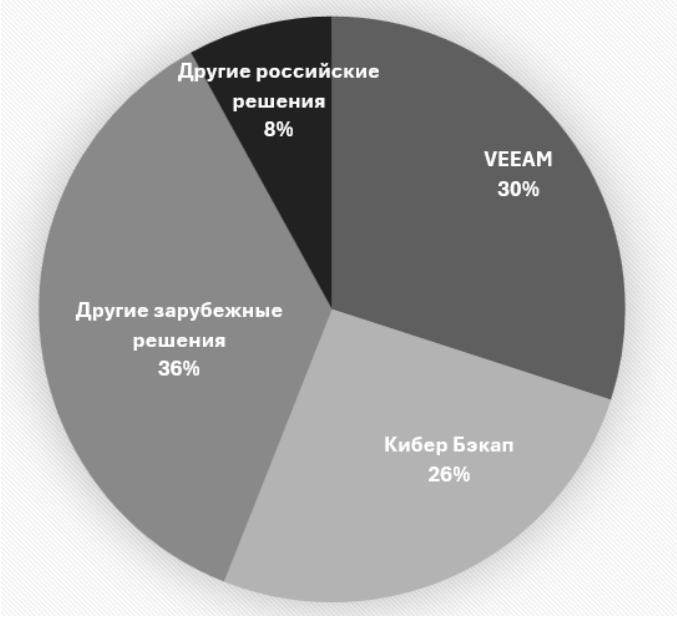

Рисунок 1 Доля рынка систем резервного копирования в корпоративной среде[1]

На фоне остановки развития западных продуктов и ухода иностранных вендоров с российского рынка наблюдается активный рост отечественных

[1] Составлено авторами

разработок в сфере защиты данных. Платформа «Кибер Бэкап» компании «Киберпротект» демонстрирует устойчивую динамику развития и занимает, по данным различных аналитических агентств, долю до 26% на российском рынке СРК, что делает ее вторым по совокупному проникновению решением после Veeam [6].

Целью настоящей статьи является анализ функциональных возможностей отечественной системы резервного копирования «Кибер Бэкап», оценка ее готовности к замещению зарубежных аналогов, а также разработка рекомендаций по интеграции данной платформы в корпоративную ИТ-среду с учетом современных требований информационной безопасности и регуляторных ограничений.

Эксплуатация систем резервного копирования иностранного производства в текущих условиях сопряжена с рядом критических рисков, таких как:

– юридический риск, отсутствие возможности заключения новых лицензионных соглашений и получения официальных обновлений программного продукта;

– риск информационной безопасности связан с отсутствием своевременного закрытия уязвимостей, выявляемых ФСТЭК России. Так, в 2025 году были обнаружены критические уязвимости в Veeam Backup&Replication с уровнем опасности 9.9 из 10, позволяющие удаленное выполнение кода на сервере резервного копирования. Отсутствие официального патча делает такие системы крайне уязвимыми;

– технический риск заключается в невозможности обеспечения совместимости с российскими операционными системами такими как Astra Linux, Альт Linux, РЕД ОС, платформами виртуализации zVirt, Альт Виртуализация;

– регуляторный риск связан с потенциальным несоответствием требованиям импортозамещения для государственных заказчиков и организаций критической информационной инфраструктуры (КИИ).

Таким образом, появилась объективная необходимость перехода на отечественную систему резервного копирования, способную обеспечить полную функциональную замену зарубежных решений при соблюдении всех требований российского законодательства.

Система резервного копирования «Кибер Бэкап» представляет собой комплексное решение, предназначенное для защиты ИТ-инфраструктуры. Ключевым преимуществом платформы является высокая масштабируемость: начиная с версии 18.0, одна инсталляция сервера управления поддерживает до 20 000 виртуальных машин и до 60 000 почтовых ящиков, что превосходит аналогичные показатели Veeam B&R (поддержка до 10 000 ВМ).

Архитектура системы включает следующие основные компоненты: сервер управления, обеспечивающий координацию всех операций резервного копирования и восстановления, агенты резервного копирования для защищаемых систем, поддерживаются ОС Windows, Linux, узлы хранения файлов, поддерживающие различные типы хранилищ такие как SMB/CIFS, NFS, iSCSI и S3, прокси-серверы для оптимизации передачи данных. Такая модульная архитектура позволяет распределить нагрузку и обеспечить высокую отказоустойчивость.

В области технологий защиты данных «Кибер Бэкап» реализует многоуровневую систему безопасности. В последней версии программы присутствует активная защита от шифровальщиков на базе машинного обучения, которая отслеживает операции с файловой системой и распознает характерные паттерны атак. Система обеспечивает блокировку подозрительных процессов, разрыв соединений и автоматическое восстановление поврежденных файлов. А шифрование данных на стороне

клиента гарантирует конфиденциальность информации при передаче и хранении данных между сервером и клиентом.

С учетом современных практик импортозамещения, наиболее эффективной является гибридная модель перехода, при которой зарубежное решение сохраняется на наиболее критичных контурах, а отечественное развертывается параллельно для защиты остальных систем. Такая модель позволяет минимизировать риски, обеспечить непрерывность бизнес-процессов.

Процесс миграции можно разбить на следующие этапы (таблица 1).

Таблица 1. Этапы процесса миграции[2]

Этап	Название этапа	Длительность (недели)	Ключевые задачи
1	Анализ и планирование	2-3	На этом этапе планируется провести инвентаризацию всех защищаемых объектов, оценка объемов данных, формирование плана миграции, отметить наиболее критичные объекты, которые будут мигрированы в последнюю очередь
2	Развертывание инфраструктуры «Кибер Бэкап»	1-2	Установка серверов управления на базе отечественных операционных системах Astra Linux или РЕД ОС, развертывание узлов хранения с использованием существующей СХД, настройка сетевого взаимодействия, интеграция с платформами виртуализации.
3	Настройка политик резервного копирования	1	Создание планов резервного копирования для виртуальных машин, настройка резервного копирования СУБД, внедрение политик хранения с использованием дедупликации данных.
4	Тестирование и верификация	1-2	Проведение тестовых запусков, верификация целостности резервных копий, тестирование восстановления на тестовом стенде.
5	Миграция и перевод в промышленную эксплуатацию	4-6	Поэтапное переключение заданий резервного копирования на «Кибер Бэкап», настройка мониторинга, обучение персонала, вывод иностранной системы из эксплуатации.

[2] Составлено авторами

После полного перехода на «Кибер Бэкап» рекомендуется обеспечить сохранность существующих ранее созданных резервных копий в течение 1 года.

Проведенный анализ позволяет сформулировать следующие выводы. Отечественная система резервного копирования «Кибер Бэкап» обеспечивает полный спектр функций, необходимых для замещения зарубежных аналогов. Решение поддерживает широкий спектр российских операционных систем, платформ виртуализации и приложений, что позволяет создавать полностью импортонезависимые ИТ-инфраструктуры. Встроенные механизмы защиты от шифровальщиков на базе машинного обучения обеспечивают надежную защиту резервных копий.

Предприятиям, планирующим переход на отечественные системы резервного копирования, рекомендуется применять гибридную модель миграции, начинать переход с наименее критичных систем для накопления опыта эксплуатации и использовать возможности для интеграции с существующими системами мониторинга и управления.

Библиографический список:

1. Иванько, А.Ф. Портал государственных услуг: насколько эффективна помощь гражданскому обществу? / А.Ф. Иванько, М.А. Иванько, В.А. Сорокина // Инновационная наука. – 2017. – №1-2. – С. 73-77.

2. Лебедева, О.А. Состояние и перспективы развития рынка информационных технологий в России / О.А. Лебедева, Т.Н. Макарова, Ю.П. Соболева, Е.В. Дроганцева // Таврический научный обозреватель. – 2015. – №2-1. – С. 33-37.

3. Плотников, А.И. Государственная поддержка IT-сферы в условиях санкций: современные вызовы и перспективы развития / А.И. Плотников // Вопросы экономики. –2023. – №4. – С. 56–62.

4. Технология разработки программного обеспечения: конспект лекции / сост. И.И. Савенко; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2014. – 67 с.

5. 70% компаний сохраняют зависимость от западных систем резервного копирования [Электронный ресурс] GlobalCIO. – 2026. – 19 марта. – URL: https://globalcio.ru/news/57712/ (дата обращения: 29.03.2026)

6. CNewsMarket: Рейтинг BaaS-платформ 2025 [Электронный ресурс] CNews.ru. – 2025. – 15 октября. – URL: https://www.cnews.ru/reviews/oblachnye_servisy_rezervnogo_kopirovaniya (дата обращения: 30.03.2026)

7. Киберпротект Кибер Бэкап: документация [Электронный ресурс] Киберпротект. – 2025. – URL: https://docs.cyberprotect.ru/ru-RU/CyberBackup/ (дата обращения: 30.03.2026)