

## **ПРИМЕНЕНИЕ МЕТОДОВ РАЗДЕЛЕНИЯ ДАННЫХ ДЛЯ УДАЛЕННОГО ХРАНЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ**

**Диденко Д. Э.**

**Научный руководитель – канд. техн. наук, доцент Канжелев Ю. А.**

Университет ИТМО

dimon.did.2014@gmail.com

### **Введение**

В условиях перехода к распределённым информационным системам удалённое хранение данных, предоставляемое услугами облачных провайдеров, стало распространённой практикой, позволяя организациям снизить затраты на поддержание собственной инфраструктуры. В то же время появляются угрозы, связанные с безопасным хранением информации в неконтролируемой среде [1]. Перед владельцами данных встаёт вопрос о целесообразности полного доверия их защиты облачному провайдеру. Современный подход основан на модели разделения ответственности: поставщик услуг обеспечивает защиту инфраструктуры, а клиент — безопасность своих данных, используя собственные или предоставляемые провайдером инструменты. Одним из перспективных направлений для разработки таких инструментов является применение методов разделения данных на стороне клиента перед их отправкой в удалённые хранилища [2]. Однако вопросы эффективного использования хранимых данных и внедрения существующих методов на практике остаются нерешёнными.

### **Основная часть**

В качестве решения поставленной проблемы в работе предлагается подход, основанный на алгоритмическом разделении данных перед их отправкой в облачную среду. В его основе лежит применение метода стирающего кодирования, при котором информация преобразуется в набор фрагментов. Распределяются эти фрагменты по нескольким независимым удалённым хранилищам, в том числе у разных облачных провайдеров. Это решает следующие вопросы безопасности: возможность восстановления информации при недоступности части хранилищ, отсутствие ценности для злоумышленника похищенных им данных из одного хранилища, а также снижение зависимости от единственного поставщика облачных услуг. Новизна подхода заключается в адаптации метода, традиционно используемого в распределённых системах хранения, для защиты данных в облаке. Реализованный в виде программного обеспечения на стороне клиента алгоритм не требует модификации инфраструктуры провайдеров и совместим со стандартной моделью объектного хранения. Это обеспечивает гибкость между уровнем безопасности, надёжностью и эксплуатационными затратами (объёмом хранилища, вычислительными ресурсами), адаптируя решение под конкретные требования и бюджетные ограничения организации.

### **Выводы**

Проведен сравнительный анализ методов разделения хранимых данных, разработан и реализован алгоритм преобразования информации перед ее отправкой в удалённое хранилище.

### Литература

1. Артемчук М.Д., Назаров Д.С. Исследование методов защиты информации в облачных хранилищах // Вестник науки. – 2024. – Т. 1, № 7 (76). – С. 481–486
2. Gao Z., Shi L., Reviriego P. Enhancing data protection with a distributed storage system based on the redundant residue number system // Wireless Networks. 2024. – Vol. 30, no. 6. – P. 1-12.