УДК 004.75

Разработка прототипа эмулятора распределенной системы хранения данных для изучения угроз безопасности

Нестеренко Н.В.
Национальный исследовательский университет ИТМО, г. Санкт-Петербург

Научный руководитель преподаватель, Ищенко А.П.
Национальный исследовательский университет ИТМО, г. Санкт-Петербург

Введение. Облачные хранилища, в том числе распределенные системы, привлекают все больше внимания, и 60% корпоративных данных уже размещены в облаке. Это увеличивает риск атак, особенно учитывая, что 48% предприятий предпочитают облачные решения для секретных данных. Исследования от ermetic.com за 2019-2021 годы свидетельствуют о росте инцидентов утечек облачных данных с 79% до 98%. В данной работе рассматривается применение алгоритмов с целью усовершенствования безопасности распределенных систем хранения данных на примере эмулятора тестового стенда.

Основная часть. Цель данной работы – разработка прототипа эмулятора распределенной системы хранилища данных, для обеспечения безопасности которого применяются программные средства и алгоритмы, направленные на сохранность и конфиденциальность пользовательских данных.

В рамках проектирования тестового стенда были выделены следующие особенности системы:

- Система распределяется между несколькими вычислительными узлами, в том числе виртуальными машинами.
- Одна из машин является системой управления, взаимодействие пользователя с распределенной системой осуществляется посредством API системы управления.
- Машины связываются друг с другом по протоколу HTTP.
- В рамках тестового стенда, в виду ограниченных вычислительных ресурсов, было решено распределить систему хранения данных между 3 вычислительными узлами.
- Пользовательские данные хранятся в файловых системах вычислительных узлов.

При разработке современных распределенных систем хранения данных применяется множество различных программных подходов для обеспечения безопасности. При разработке тестового стенда было решено выбрать следующие из них:

- Разграничение доступа пользователей к файлам друг друга.
- Применение метода разделения пользовательских файлов на N частей с целью невозможности восстановления данных в случае захвата злоумышленником одного из вычислительных узлов.

- Применение методов БЧХ-кодирования для восстановления утерянных данных с целью обеспечения целостности информации.
- Применение технологии виртуализации данных RAID для восстановления данных в случае нарушения целостности данных на вычислительных узлах.

Выводы. В ходе проведения работы были разобраны современные тенденции к обеспечению безопасности распределенных систем хранения данных, а также разработаны алгоритмы, способные повысить их устойчивость к атакам злоумышленников.

Список использованных источников:

1. Проблемы облачной безопасности [электронный ресурс] // cyberleninka [официальный сайт] URL: https://cyberleninka.ru/article/n/problemy-oblachnoy-bezopasnosti

2. Tom Laszewski, Kamal Arora, Erik Farr, Piyum Zonooz «Cloud Native Architectures». 2021. 320 с.

3. Основные критерии RAID-массивов для обеспечения надёжного хранения информации [электронный ресурс] // cyberleninka [официальный сайт] URL: https://cyberleninka.ru/article/n/osnovnye-kriterii-raid-massivov-dlya-obespecheniya-nadyozhnogo-hraneniya-informatsii

4. Использование кодов Рида-Соломона для восстановления поврежденных файлов [электронный ресурс] // cyberleninka [официальный сайт] URL: https://cyberleninka.ru/article/n/ispolzovanie-kodov-rida-solomona-dlya-vosstanovleniya-povrezhdennyh-faylov

5. Особенности хранения данных в распределенных системах на примере службы каталогов [электронный ресурс] // cyberleninka [официальный сайт] URL: https://cyberleninka.ru/article/n/osobennosti-hraneniya-dannyh-v-raspredelennyh-sistemah-na-primere-sluzhby-katalogov