УДК 004.62

Разработка хранилища с репликацией данных для системы управления криптографическими ключами

Айтуганов Д.А. (Университет ИТМО)**, Чебыкин И.Б. (**Университет ИТМО)
Научный руководитель – к.т.н., доцент Лукьянов Н.М.
(Университет ИТМО)

В данной работе проведены изучение и сравнительный анализ уже имеющихся сервисов совместного управления криптографическими ключами, а также способов реализации систем с резервными серверами. Описывается реализация собственного сервиса с репликацией хранилища данных.

Введение

В настоящее время большое количество коммерческих организаций шифруют свои данные в целях безопасности. Однако при шифровании, к примеру, на уровне баз данных или виртуальных машин возникает необходимость в отдельном сервисе, который бы осуществлял управление криптографическими ключами. В целях стандартизации работы таких сервисов группой OASIS был создан протокол совместного управления ключами или KMIP (Key Management Interoperability Protocol). Данный протокол определяет форматы сообщений для работы с ключами на сервере.

KMIP – это открытый протокол, который поддерживается многими крупными технологическими компаниями. В открытом доступе имеются уже готовые его реализации, такие как PyKMIP или HyTrust KMIP Server. Однако ни одна из них не является отказоустойчивой. В случае сбоя работы сервиса, использующая его коммерческая организация может временно потерять доступ к своим данным. В работе некоторых организаций такая ситуация является недопустимой.

Поэтому **актуальной задачей** является разработка сервиса с репликацией хранилищ данных, основные характеристики отказоустойчивости которого будут значительно выше, чем у находящихся в открытом доступе. Компании, которые будут использовать данный сервис, получат преимущество в качестве обслуживания клиентов перед своими конкурентами.

Основная часть

Таким образом, **цель** данной работы – повышение коэффициента готовности системы управления криптографическими ключами посредством добавления в систему резервных серверов. Для достижения данной цели были поставлены следующие задачи.

1. Выполнить сравнительный анализ существующих сервисов управления криптографическими ключами.
2. Выполнить сравнительный анализ видов реализации систем с резервными серверами.
3. Разработать сервис управления криптографическими ключами, на основе выбранной системы управления ключами и выбранного вида реализации систем с резервными серверами, обеспечивающего избыточность хранимых данных.

В ходе работы было выявлено, что наиболее подходящей реализацией системы управления криптографическими ключами является сервис PyKMIP. В качестве способа реализации систем с резервными серверами был выбран Активный-Активный.

Выводы

По завершении работы были достигнуты следующие результаты:

1. Составлена выборка имеющихся в открытом доступе реализаций протокола KMIP.
2. Выполнен сравнительный анализ имеющихся реализаций протокола на основании найденных теоретических сведений по данным системам.
3. Составлен перечень способов реализаций систем с резервными серверами.
4. Выполнен сравнительный анализ реализаций систем с резервными серверами на основании теоретических сведений.
5. Разработана система управления криптографическими ключами с репликацией хранилищ данных на базе сервиса PyKMIP.

Автор: _____

Научный руководитель: _____

Заведующий кафедрой: _____