Утверждено

зав. кафедрой ПИ

\_\_\_\_\_\_\_\_\_Зори С.А.

«\_\_\_\_»\_\_\_\_\_\_\_\_ 2021 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на курсовой проект по дисциплине

«Безопасность программ и данных»

студенту группы ПИ-18б Моргунову Арсению Геннадьевичу

Тема: “Создание безопасного протокола обмена данными между клиентом и сервером для системы SILUR”

Вариант № 5

Задание:

Разработать клиентскую часть протокола безопасной аутентификации и передачи данных между клиентом и сервером.

1. Создание безопасного подключение для любых данных.

Генерация ключей при помощи алгоритма Деффи-Хеллмана.

Шифрование данных при помощи симметричного алгоритма AES.

2. Создание ассиметричного шифрования (RSA) при передачи данных повышенной важности (при генерации ключей для передачи данных).

3. Реализовать возможность сохранения сессии пользователем, чтобы при последующем подключении не запрашивать пароль пользователя заново.

Для восстановления сессии использовать цифровую подпись при помощи ассиметричного алгоритма RSA.

4. В базе данных хранить логины и соответствующие им токены пользователей.

5. Разработать команды управление между клиентом и сервером для предметной области системы SILUR.

Пример команд:

Получение списка подписок.

Создание подписки.

Просмотреть историю публикации (передача содержимого сообщений: подпись, текст, файлы и т.д.).

6. Тестирование протокола в реальных условиях.

7. Создание понятного пользовательского интерфейса.

График выполнения курсового проекта:

|  |  |
| --- | --- |
| Неделя | Работа |
| 1-2 | Выдача задания и изучение задания |
| 3 | Анализ требований к системе и способов их реализации |
| 4-5 | Проектирование |
| 6-7 | Организация процессов |
| 8 | Поддержка режимов работы, проектирование общей структуры |
| 9-13 | Разработка программ |
| 14 | Оформление пояснительной записки |
| 15-17 | Защита курсового проекта |

Дата выдачи задания 1.09.2021

Задание принял Моргунов А.Г.

Руководители проекта Чернышова А.В.

Ногтев Е.А.