Защита приложения от несанкционированного запуска и копирования

Описание программы

2017

Оглавление

[1. Общие сведения о программе 3](#_Toc485033043)

[2. Функциональное назначение 3](#_Toc485033044)

[3. Описание логической структуры программы 3](#_Toc485033045)

[4. Используемые технические средства 4](#_Toc485033046)

[5. Вызов и загрузка 4](#_Toc485033047)

[6. Входные данные 4](#_Toc485033048)

[7. Выходные данные 4](#_Toc485033049)

# Общие сведения о программе

Программное обеспечение «Защита приложения от несанкционированного запуска и копирования» состоит из двух программ «Прикладная программа» и «Сервер аутентификации». В прикладную программу встроена двухуровневая система защиты. Первый уровень — это проверка лицензии с помощью сервера аутентификации. Второй уровень – проверка наличия электронного ключа. Модуль Программное обеспечение написано на C++, для его работы необходимо сетевое подключение.

1. Функциональное назначение

Программное обеспечение предназначено для защиты целевого приложений от несанкционированного запуска и копирования.

Основные функции прикладной программы:

* Запуск целевой программы
* Запрос лицензионного ключа пользователя
* Проверка лицензионного ключа пользователя
* Сохранение и дальнейшее использование корректного лицензионного ключа
* Проверка подключенного электронного ключа.

Основные функции сервера аутентификации:

* Единовременная обработка множества клиентов
* Окно управления сервером
* Хранение лицензионных ключей и соответствующих им параметров оборудования.
* Ответ на запрос о достоверности лицензионного ключа

Разработанная программа предназначена для использования в операционных системах семейства Windows.

# Описание логической структуры программы

Структурно программное обеспечение разделено на две функциональные подсистемы, отвечающие за обеспечение определенных функций изделия.

* 1. **Прикладная программа**

Прикладная программа состоит из четырех подсистем.

**Подсистема Net**

Позволяет взаимодействовать с сервером.

Файл NetClient.h – отвечает за взаимодействие клиентской программы с сервером аутентификации. Предоставляет возможность отправки на сервер данных о системе и лицензионный ключ. В ответ, предоставляет информацию о активационном ключе. При неверных входных данных, возвращает код ошибки.

**Подсистема Program**

Позволяет запускать целевую программу.

Файл MyProgram.h – целевая программа, для которой организованна вся система защиты. Ее запуск осуществляется только при подтверждении корректности лицензионного ключа. Точка запуска программа MyProgram.run(). В данной место может быть подставлена любая другая программа.

**Подсистема Repository**

Позволяет хранить данные.

Файл MemberRepository.h – интерфейс для хранения данных.

Файл LocalRepository.h – реализация интерфейса MemberRepository, позволяющая хранить данные в текстовом файле в json формате.

**Подсистема Protetion**

Осуществляет проверку наличия лицензии для запуска целевой программы.

Файл Protect.h – предоставляет интерфейс для проверки лицензии программы с помощью сервера аутентификации и проверки наличия электронного ключа.

Файл sha256.h – необходим для проверки корректности активационного ключа.

* 1. **Сервер аутентификации**

Сервер состоит их трех подсистем

**Подсистема Commander**

Файл Commander.h позволяет выполнять команды администратора сервера.

**Подсистема LicenseCheck**

Файл LicenseChecker.h – позволяет проверить параметры полученный от клиента. Возвращает код ошибки при неудаче или активационный ключ при успехе.

Файл DataAccessObject.h – позволяет обращаться к базе данных

Файл sha256 – позволяет генерировать активационный ключ.

**Подсистема TSPServer**

Файл TSPServer.h – позволяет обрабатывать всех клиентов, подключающихся к серверу.

# Используемые технические средства

Для работы данной системы необходим персональный компьютер с операционной системой семейства Windows. При использовании выделенного сервера, также необходимо интернет подключение. Электронным ключом является USB Flash накопитель.

# Вызов и загрузка

Для использования данной программы необходимо установить все файлы программы в соответствии с документом «Руководство системного администратора» и запустить сначала программу сервер, а затем прикладную программу.

# Входные данные

Входными данными для прикладной программы является ключ лицензии.

Входными данными для сервера аутентификации являются команды администратора сервера, а также данные от клиентов: лицензионный ключ и данные о системе.

# Выходные данные

Выходными данными для прикладной программы является запущенное целевое приложение, или сообщение об ошибке от одного из модулей защиты.

Выходными данными для сервера аутентификации является активационный ключ или код ошибки, передаваемые клиенту.