Розробка методу і засобів системи захисту даних з використанням технології динамічного завантаження коду в робочий процес

Автор:
ст. гр. 2ПІ-18м Андреєв А.О.

Науковий керівник:
к.т.н., доцент Войтко В.В.

Актуальність

Захист програмного продукту від несанкціонованого копіювання є актуальною задачею у зв'язку зі збереженням комерційних і авторських прав фірм і розробників:

- За висновками закордонних фахівців економічний збиток від "піратського" копіювання програмного забезпечення складає 53 млрд доларів станом на 2018 рік.
- На даний момент 41% програмного забезпечення є «піратським».
- Несанкціоноване розповсюдження ПЗ спричиняє банкротство та збитковість компаній-розробників, що, в свою чергу, загальмовує розвиток ІТ.

Мета, об’єкт та предмет дослідження

- **Мета** – підвищення захищеності програмних додатків від несанкціонованого копіювання шляхом розробки динамічно завантажуваної бібліотеки та модуля для управління процесом користувацького додатку, що підвищить захист програм від несанкціонованого доступу.
- **Об’єкт** – процес захисту від несанкціонованого доступу.
- **Предмет** – засоби захисту програмних додатків від несанкціонованого копіювання.

Задачі

- удосконалити метод динамічного завантаження програмного продукту або його частин та розробити модель і алгоритми системи захисту програмних додатків;
- розробити динамічно завантажувану бібліотеку, що буде завантажуватися у виконуваний процес та структуровано копіювати вхідну користувацьку бібліотеку;
- розробити модуль для завантаження користувацької бібліотеки з сервера;
- розробити модуль для управління процесом для користувацького додатку;
- провести тестування програмного продукту.

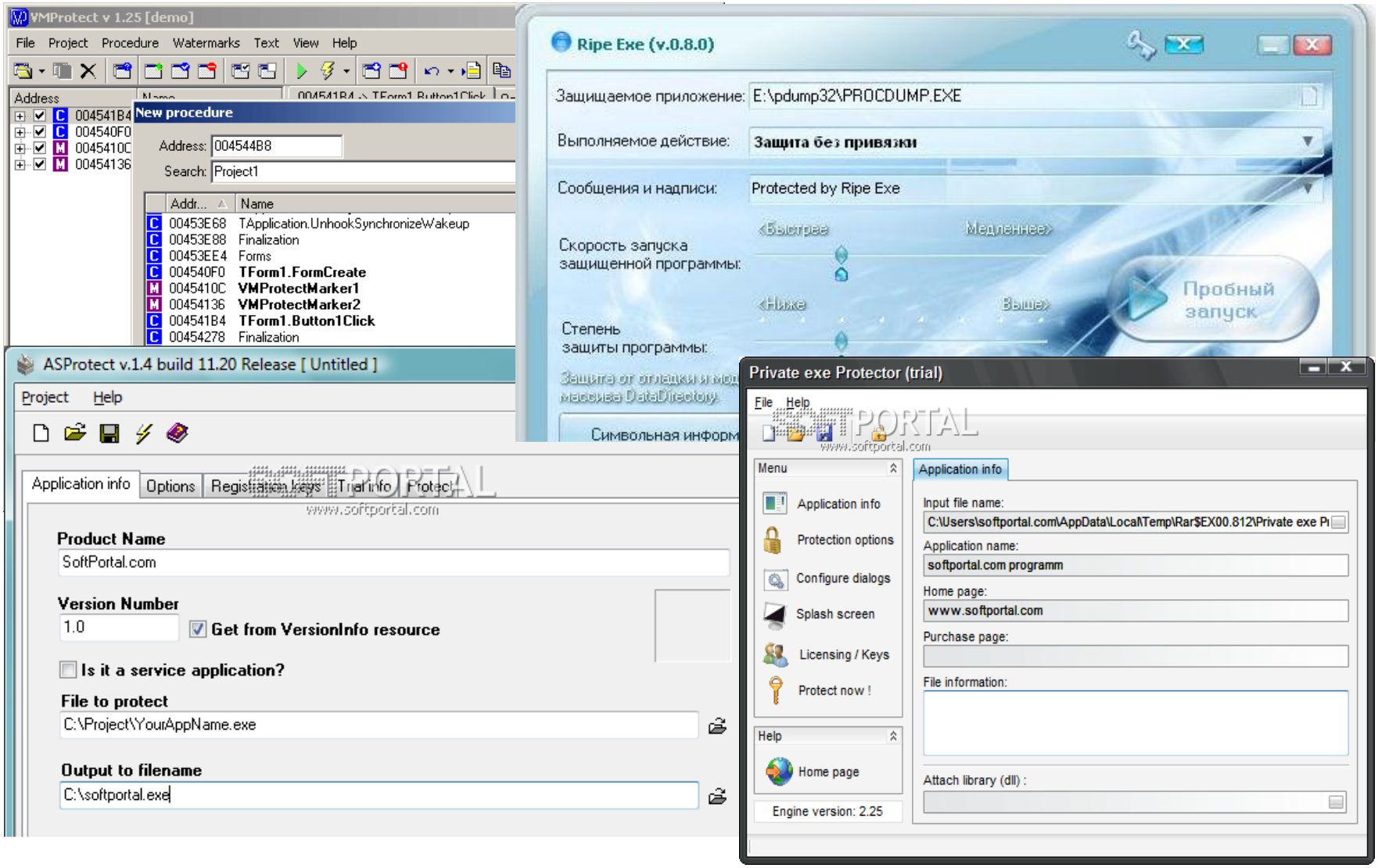
Наукова новизна та практичне значення

Наукова новизна одержаних результатів:

- Подальшого розвитку дістав метод динамічного завантаження програмного продукту або його частин, який, на відміну від існуючих, передбачає збереження виконуваного коду на сервері, а не на локальній машині користувача, та динамічне завантаження бібліотек у робочий процес, що забезпечує високий рівень захисту виконуваних файлів від несанкціонованого копіювання.
- Подальшого розвитку дістала модель системи захисту програмних продуктів від несанкціонованого доступу, яка, на відміну від існуючих, орієнтована на кодову ін’єкцію завантажуваних бібліотек у виконуваний процес, що дозволяє динамічно забезпечувати захист програм в робочому режимі.

Практична цінність отриманих результатів полягає у забезпеченні захищеності програмних рішень від несанкціонованого доступу до виконуваних файлів, а також їх копіювання.

Існуючі аналоги



Порівняння з аналогами

Загальне порівняння аналогів та додатку «DllLoadManager» наведено у таблиці

Критерій	VMProtect	Private exe Protector	ASProtect	Ripe Exe	DllLoadManager
Відсутність використання додаткових апаратних ресурсів	+	+	+	+	+
Відсутність необхідності використання віртуальної машини	+	-	+	+	+
Доступ до коду захищеної програми в будь якому вигляді	-	-	-	-	+
Можливість розширення	-	-	-	-	+
Небезпека при взломі програми-захисника	-	-	-	-	+
Відсутність необхідності додаткової обробки програмного продукту	-	-	-	-	+

Засоби розробки

Характеристики	Мова програмування		
	C++	C#	Java
Об'єктно-орієнтована	+	+	+
Створення багатовимірних масивів	+	+	-
Узагальнене програмування	+	+	+
Створення анонімних функцій	+	-	-
Створення динамічних масивів	+	+	+
Розробка програмного інтерфейсу	+	+	+

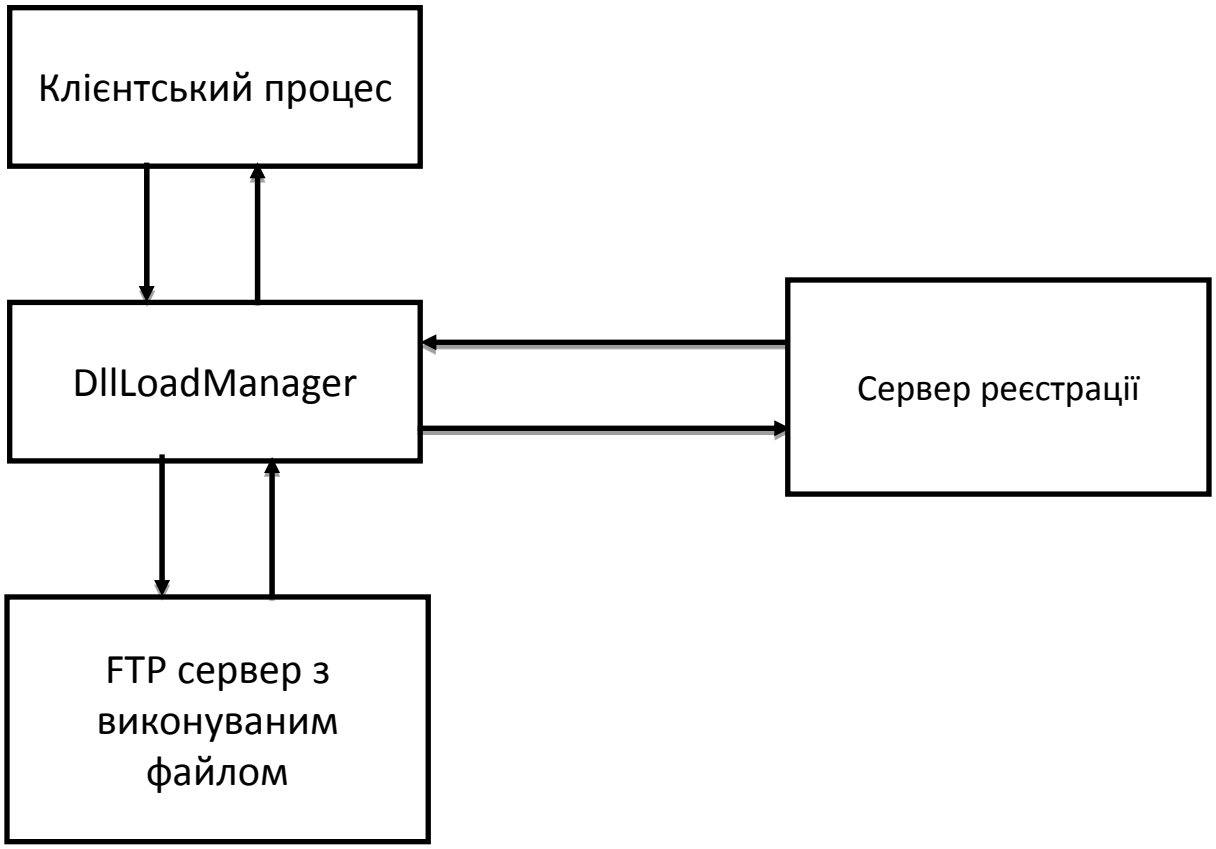
Функції	Середовище програмування		
	C++ Builder	Dev-C++	Microsoft Visual Studio
Підтримка MFC	-	-	+
Режим відлагодження	+/-	+/-	+
Кросплатформеність	-	-	+
Функція авто заповнення	+/-	-	+

Технології

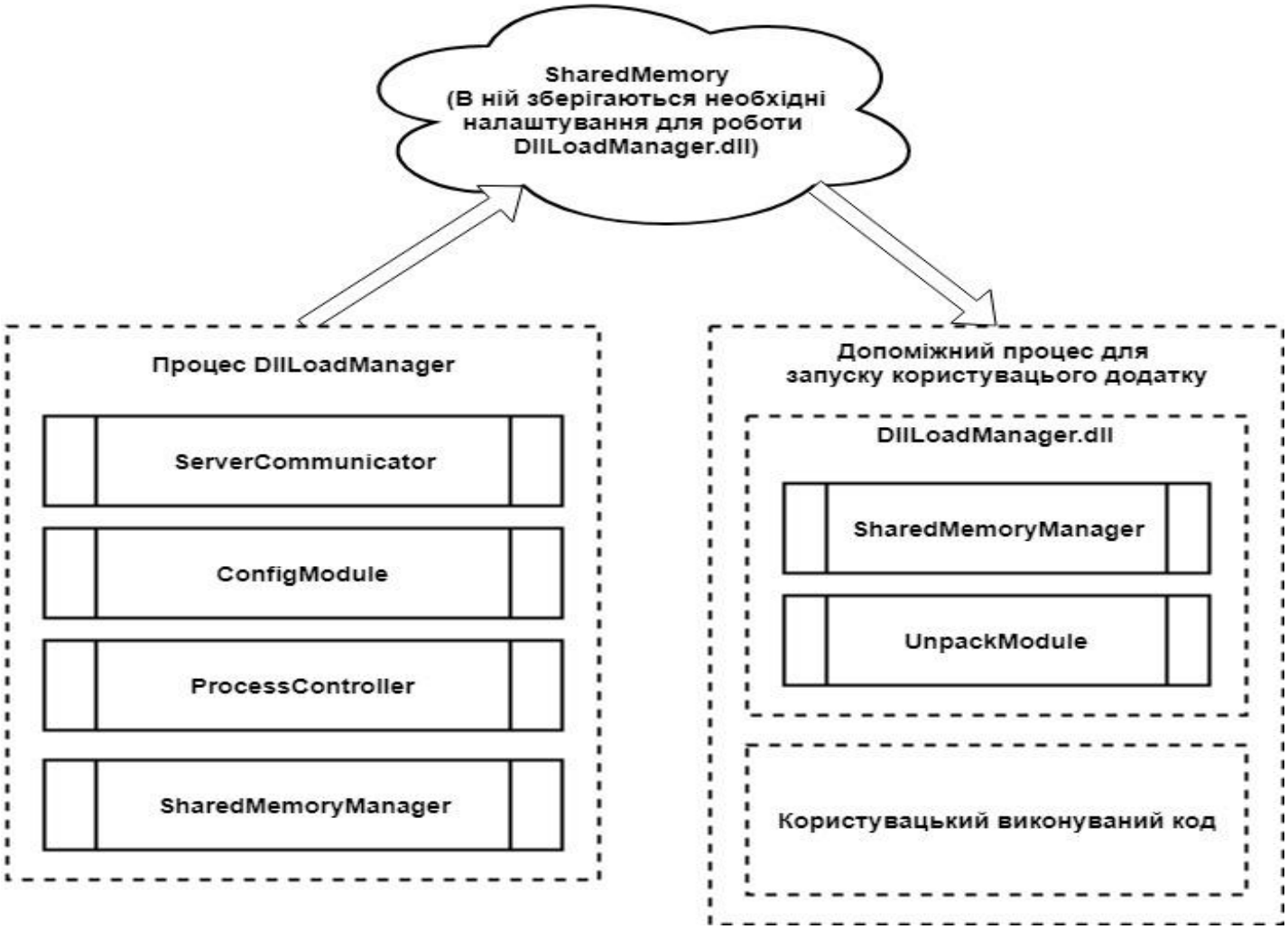
WIN32 API

curl://

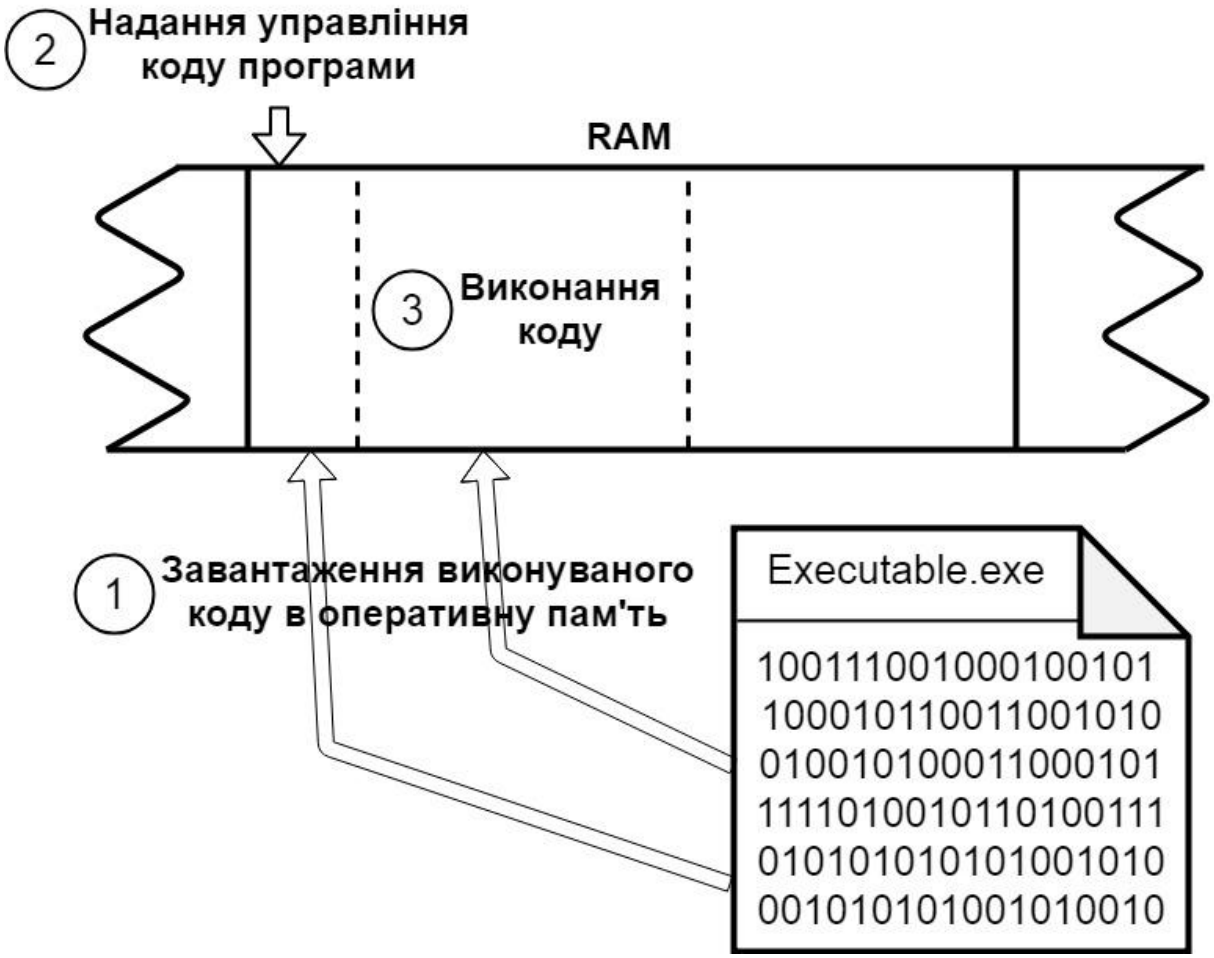
Модель системи захисту



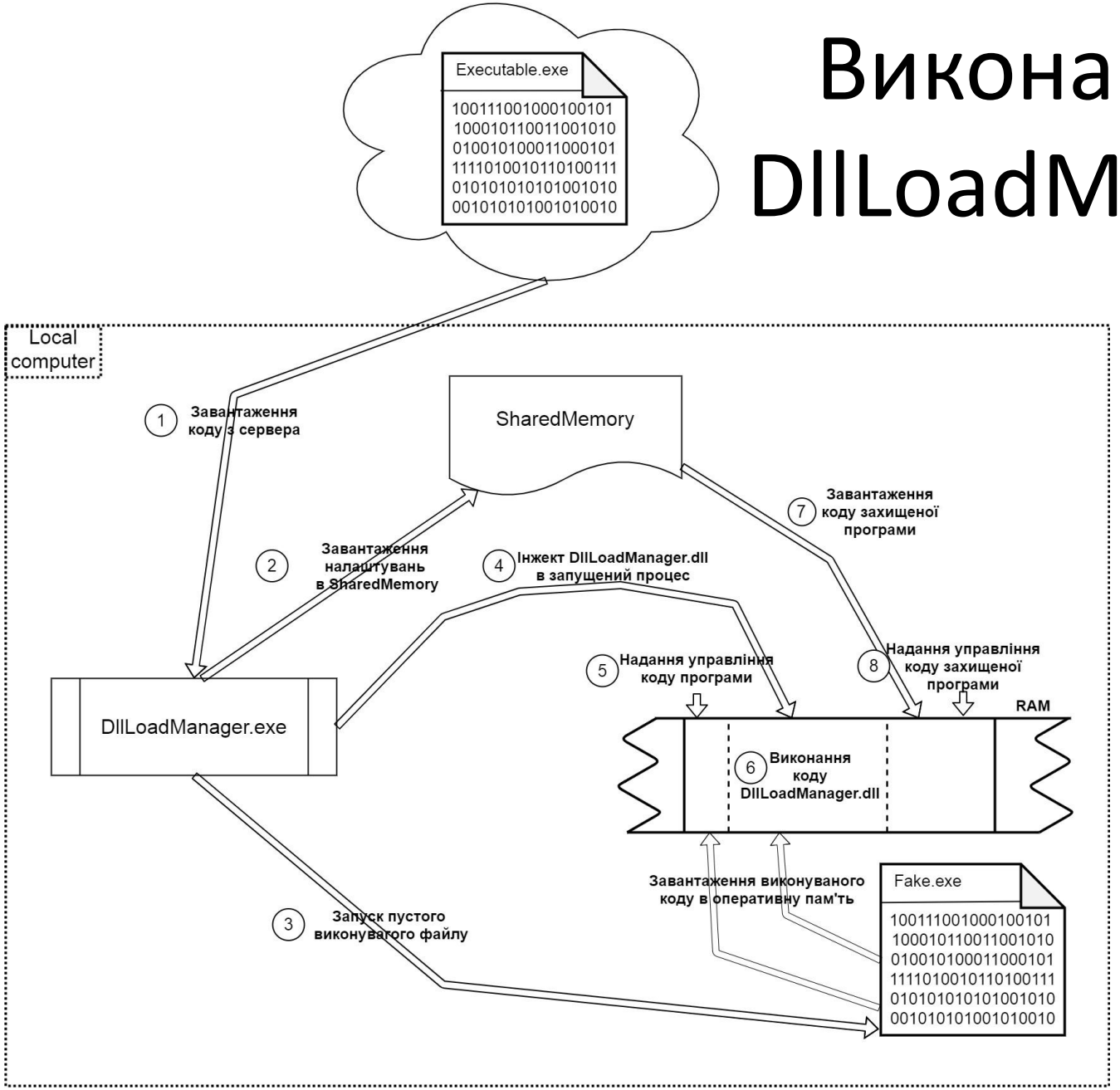
Модель взаємодії процесів DllLoadManager та користувацького додатку



Звичайне виконання програми



Виконання з DllLoadManager

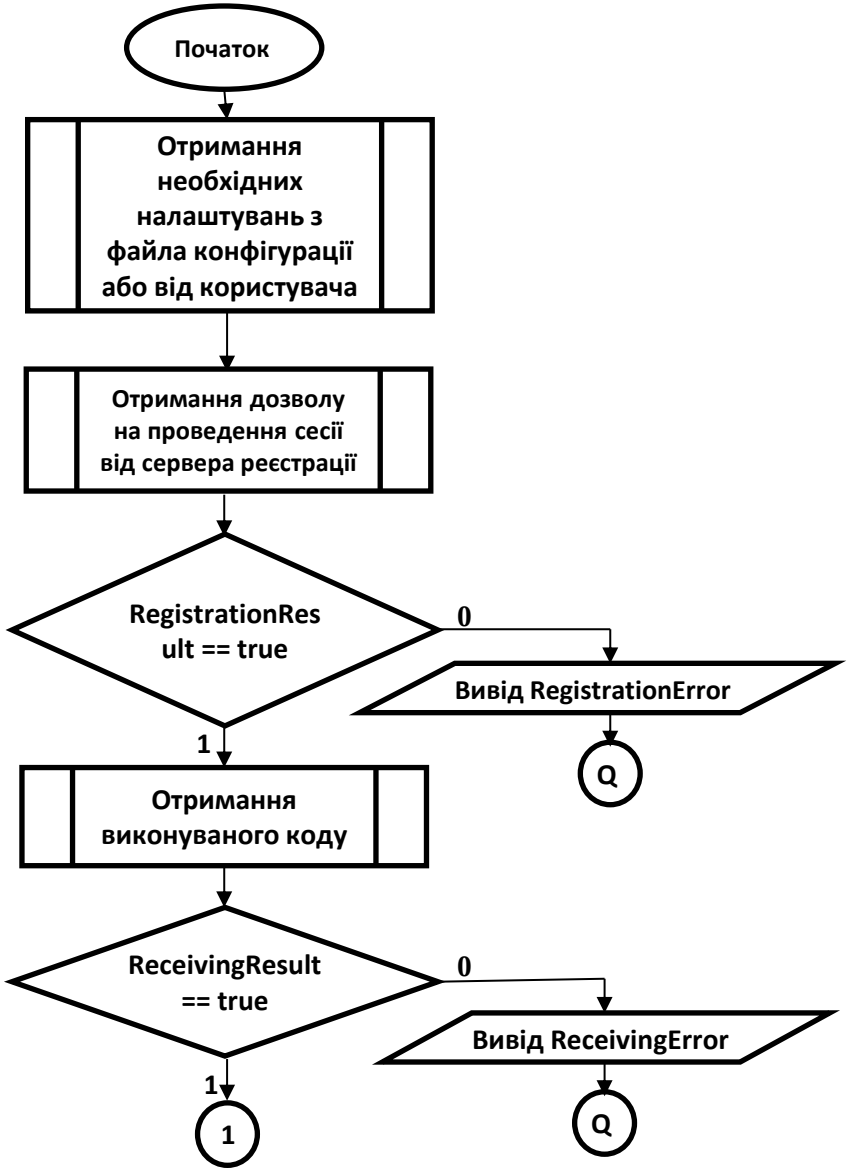


Рекомендації до використання

- Розміщення файлу виконуваного коду свого додатку на файловому сервері (FTP), заборонивши вільний доступ до нього та реалізувавши надання доступу за паролем.
- Запуск серверу реєстрації, що буде отримувати GET запити на отримання пароля для доступу до FTP сервера, перевіряючи дані користувача, що прийшли в запиті.
- Формування конфігураційного файлу, в якому потрібно прописати адреси серверів.
- Доставка користувачу-замовнику програмного забезпечення конфігураційного файлу та додатку DllLoadManager, а також порожнього виконуваного файлу, в який пізніше буде здійснено завантаження файлу.
- Реєстрація користувача-замовника ПЗ на сервері реєстрації.

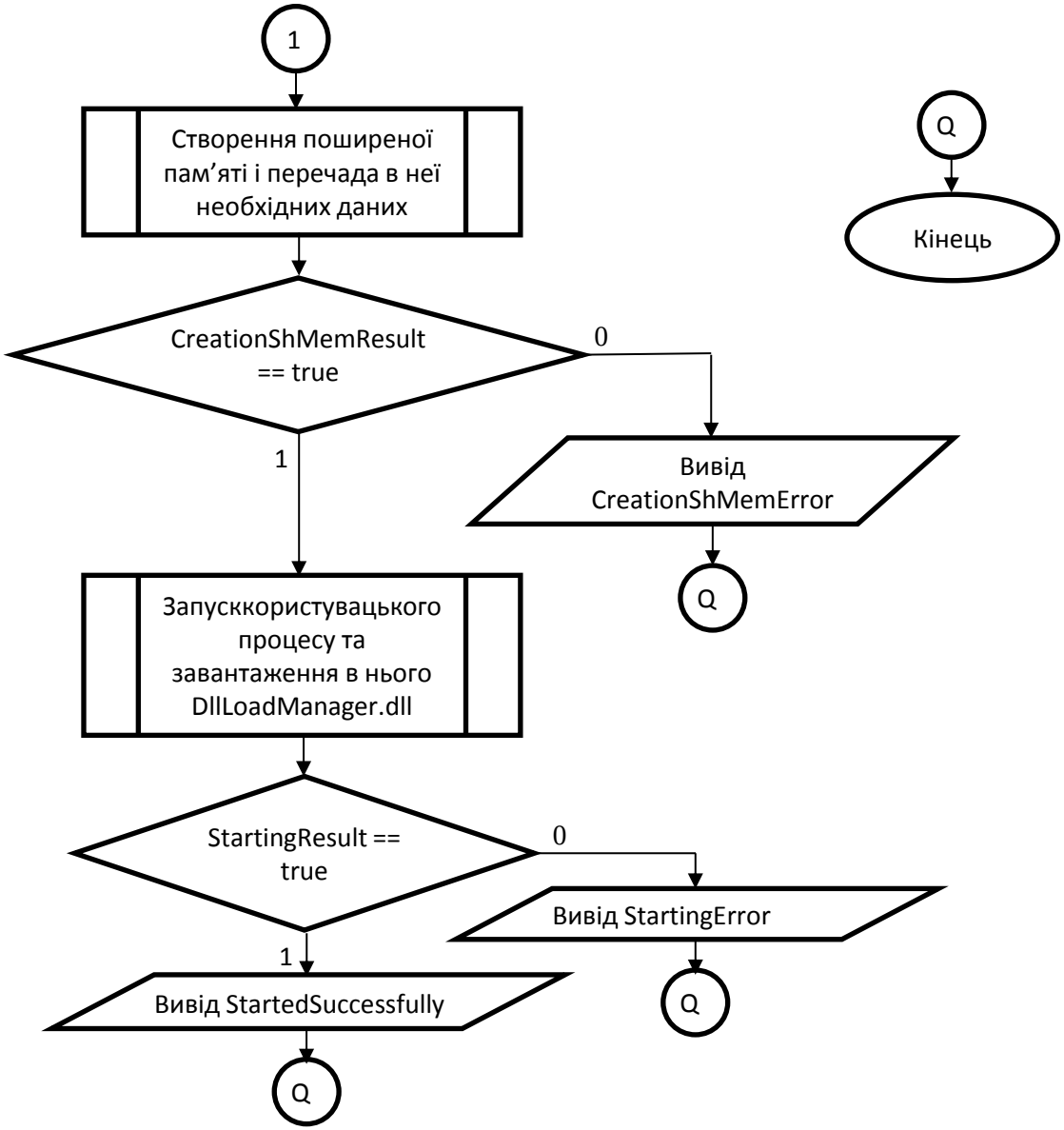
Розробка алгоритмів

Загальний алгоритм роботи додатку



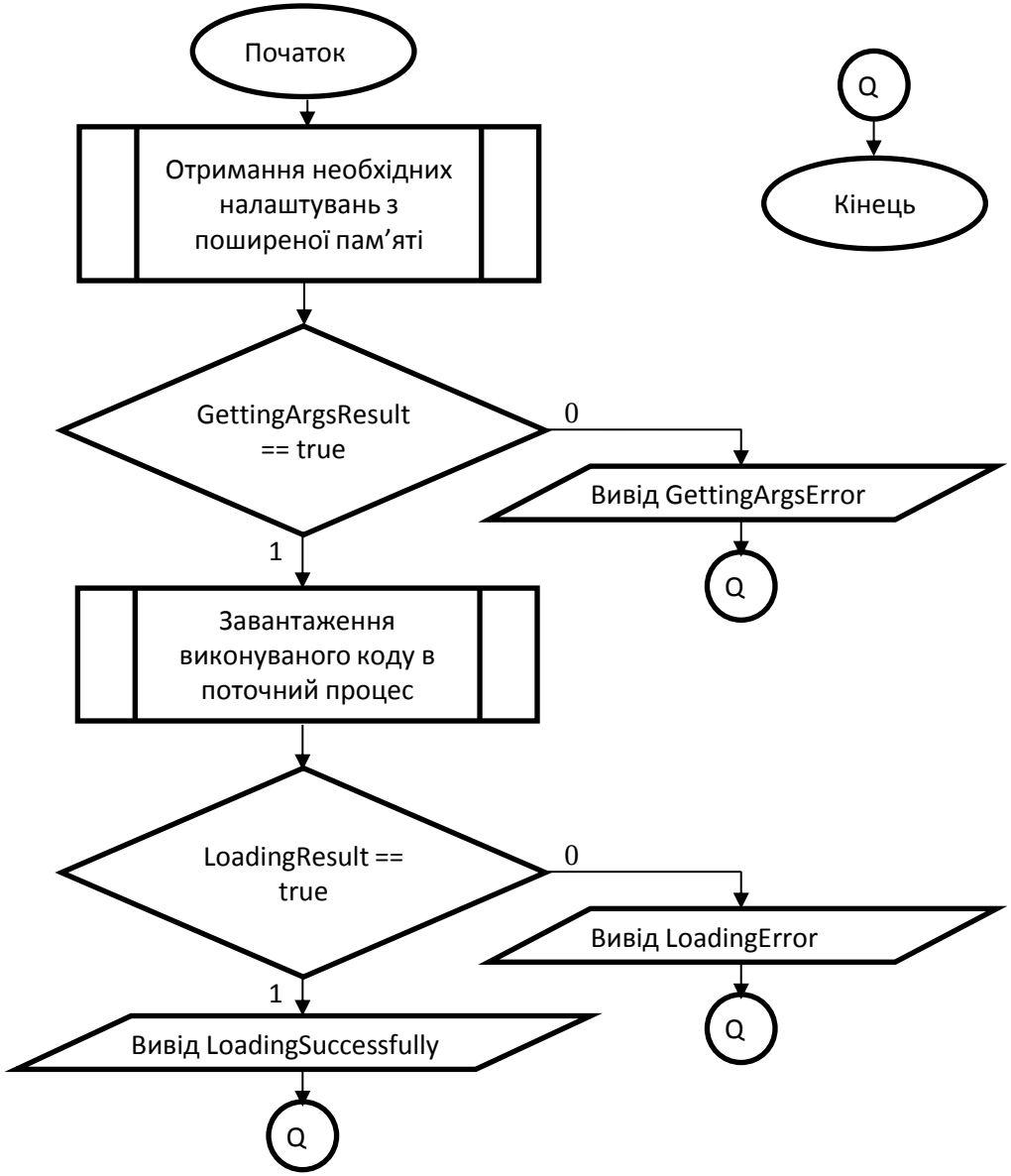
Розробка алгоритмів

Продовження загального алгоритму роботи додатку



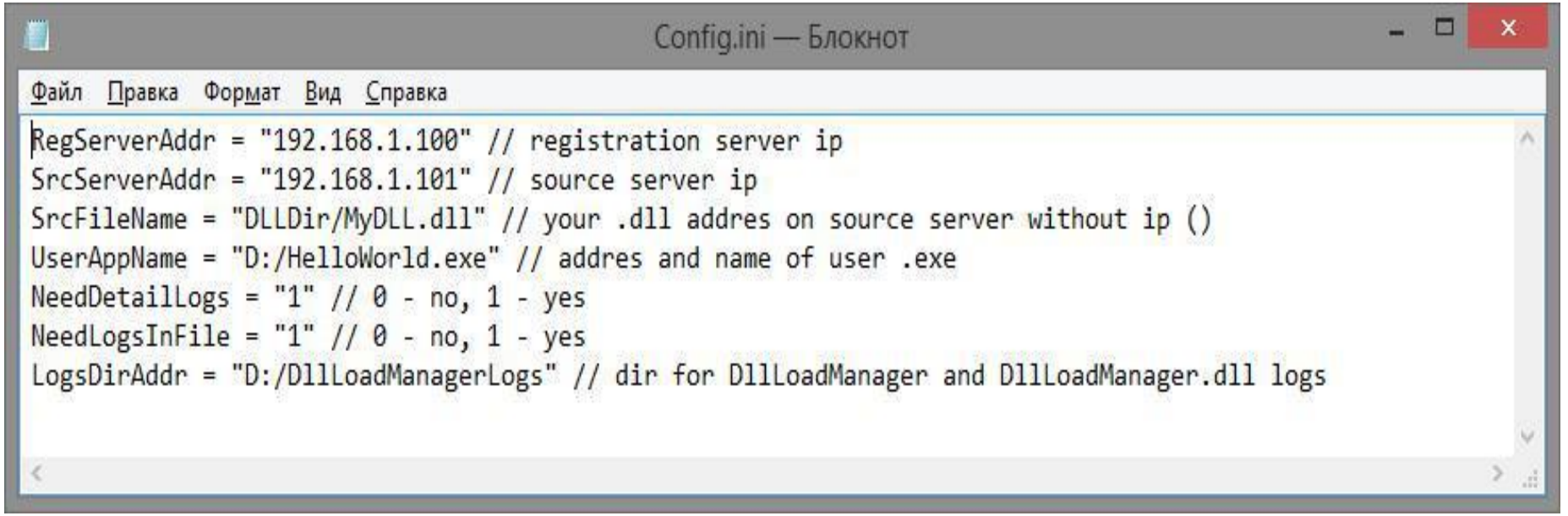
Розробка алгоритмів

Загальний алгоритм роботи бібліотеки

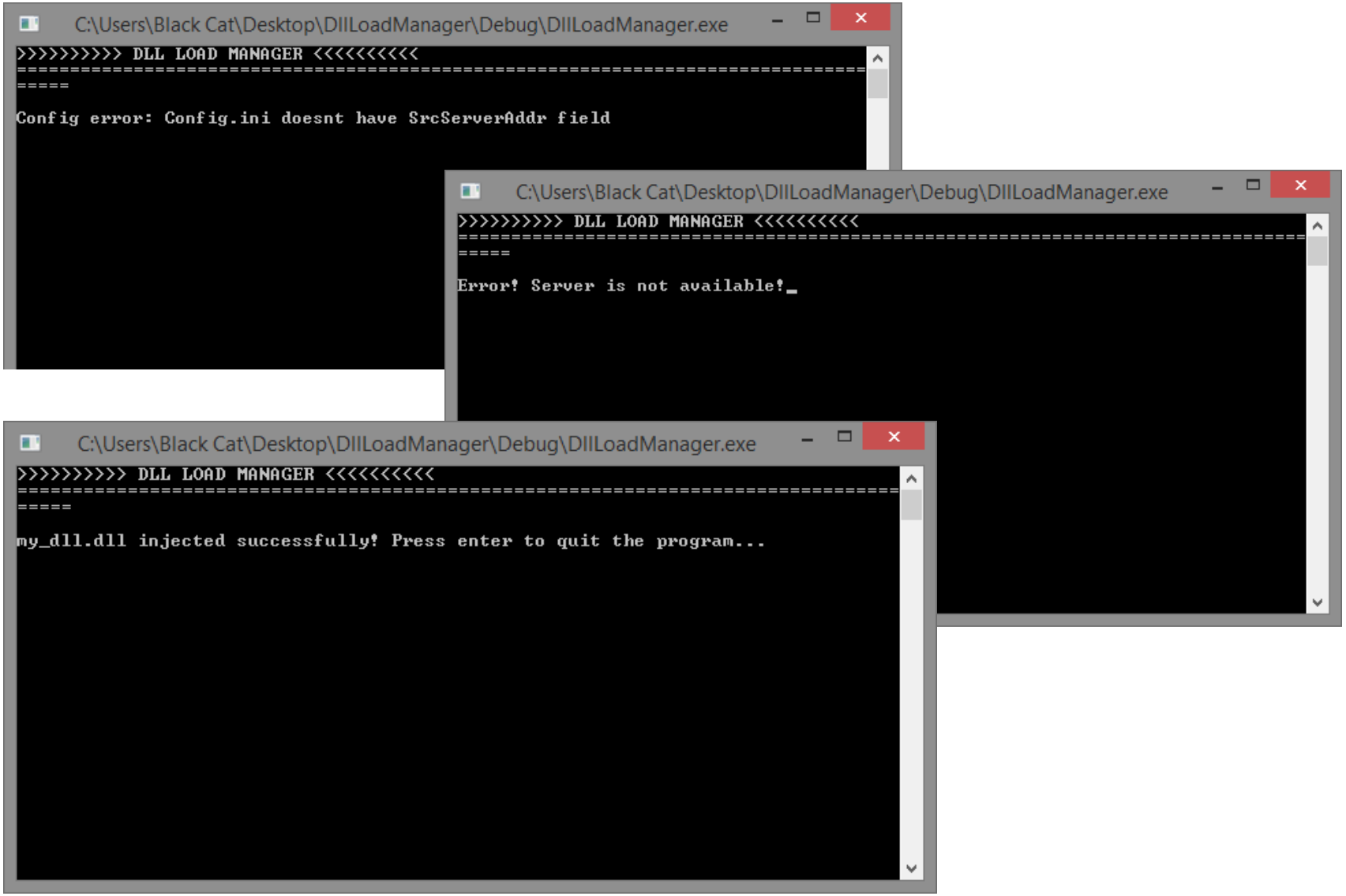


Файл конфігурації

Налаштування роботи програмного додатку здійснюється за допомогою файлу конфігурації. Цей фай має вигляд:



Тестування програми



Висновки

- удосконалено метод динамічного завантаження програмного продукту або його частин, який передбачає збереження виконуваного коду на сервері, а не на локальній машині користувача, та динамічне завантаження бібліотек у робочий процес, що забезпечує високий рівень захисту виконуваних файлів від несанкціонованого копіювання;
- розроблено динамічно завантажувану бібліотеку, що буде завантажуватись в виконуваний процес та структуровано копіювати вхідну користувацьку бібліотеку;
- розроблено модуль для завантаження користувацької бібліотеки з сервера;
- розроблено модуль для управління процесом для користувацького додатку;
- проведено тестування програмного продукту.

Апробація результатів роботи

- на міжвузівському студентському вебінарі «Інноваційні та інформаційні технології в бізнесі та освіті». – Вінниця: ВТЕІ КНТЕУ. – 21 жовтня 2015 р.
- на науково-практичній Інтернет-конференції «Електронні інформаційні ресурси: створення, використання, доступ – 2015». – Вінниця: ВНТУ, 2015 р.;
- на міжнародній науково-практичній Інтернет-конференції «Електронні інформаційні ресурси: створення, використання, доступ – 2018». – Вінниця: ВНТУ, січень 2018 р.

Результати роботи впроваджено

- на ТОВ «Он-лайн».

Публікації

- Войтко В.В. Система захисту програмних додатків з використанням динамічного завантаження виконуваного коду в робочий процес / В.В. Войтко, С.В. Бевз, С.М. Бурбело, А.О. Андреєв // Електронні інформаційні ресурси: створення, використання, доступ // Збірник наукових праць міжнародної науково-практичної Інтернет-конференції. – Вінниця: ВНТУ, січень-2018. – С.248-253.
- Войтко В.В. Розробка та провадження на ринок програмного додатку з вивчення хімії / В.В. Войтко, А.О. Андреєв, О.В. Дажура, С.В. Козловський, В.В.Туйчев // Інноваційні та інформаційні технології в бізнесі та освіті // Матеріали міжвузівського студентського вебінару / відп. ред. Л.Б. Ліщинська. – Вінниця: ВТЕІ КНТЕУ. – 21 жовтня 2015р. – С. 6-7.
- Войтко В.В. Автоматизація процесів формування новин у різних соціальних мережах / В.В. Войтко, С.В. Бевз, А.О. Андреєв, О.В. Дажура, В.В.Туйчев, О.В. Дикий // Електронні інформаційні ресурси: створення, використання, доступ // Збірник наукових праць міжнародної науково-практичної Інтернет-конференції. – Вінниця: ВНТУ, 2015. – С. 91-92
- Войтко В.В. Комп’ютерна програма «Програмний продукт для автоматизації роботи з різними соціальними мережами» / В.В. Войтко, А.О.Андреєв, О.В. Дикий, О.В. Дажура, В.В. Туйчев // Свідоцтво про реєстрацію авторського права на твір № 64732 від 01.04.2016.

Нагороди

Результати роботи були подані на Всеукраїнський та Міжнародний студентські конкурси, де отримано призові місця:

- диплом переможця ІІ ступеня у Всеукраїнському конкурсі студентських наукових робіт з напрямку «Інформатика і кібернетика»
- диплом за зайняте ІІ місце у Фіналі Міжнародної студентської олімпіади з інформаційних технологій IT-UNIVERSE в конкурсі «Кращий диплом з кібербезпеки».

Дякую за увагу!