

Розробка методів та  
програмних засобів для  
аналізу контентного  
введення інформації

Виконав  
студент групи 2ПІ-19м  
Харкевич К.А.  
Науковий керівник  
доц.,к.т.н Черноволик Г.О.

# Методи і задачі роботи

**Метою роботи** є підвищення рівня захисту інформації від некоректних дій персоналу на підприємствах за рахунок реалізації методів та програмних засобів аналізу контентного введення інформації.

Відповідно до поставленої мети в роботі вирішуються такі завдання:

- проведення аналізу існуючих методів аналізу контентного введення інформації для визначення їх продуктивності та надійності;
- розробка структури та алгоритмів програмного засобу;
- розробка інтерфейсу для аналізу контентного введення інформації;
- розробка методів прихованої та автоматизованої роботи програмного засобу;
- реалізація системних повідомлень зміни стану процесів аналізу;
- розробка панелі налаштувань програмного засобу.

**Об'єкт дослідження** – процес аналізу контентного введення інформації та його збереження.

**Предмет дослідження** – методи та засоби перехоплення та аналізу введеної інформації.

**Методи дослідження.** У процесі досліджень використовувались: прикладна теорія інформації; методи теорії алгоритмів для розробки алгоритмів і програмних модулів; методи процедурного програмування для розробки відповідних процедур програмного засобу; комп'ютерне моделювання для аналізу та перевірки отриманих теоретичних положень.



# Порівняння з аналогами



Параметри	Windows Spy Keylogger	Simple Logger	Klawik 1.3	Key Logger (розроблене ПЗ)
Встановлення налаштування додатку на автозапуск при завантаженні ОС	Так	Ні	Ні	Так
Аналіз інформації при копіюванні у буфер обміну	Ні	Ні	Ні	Так
Запис дати, часу та назви вікна в якому ведеться аналіз	Ні	Ні	Так	Так
Запуск додатку в прихованому режимі, в треї	Так	Ні	Так	Так
Аналіз (логування) української, англійської, російської розкладок клавіатури	Ні	Так	Ні	Так
Збереження налаштувань додатку у ini-файлі	Ні	Ні	Ні	Так

# Наукова новизна:

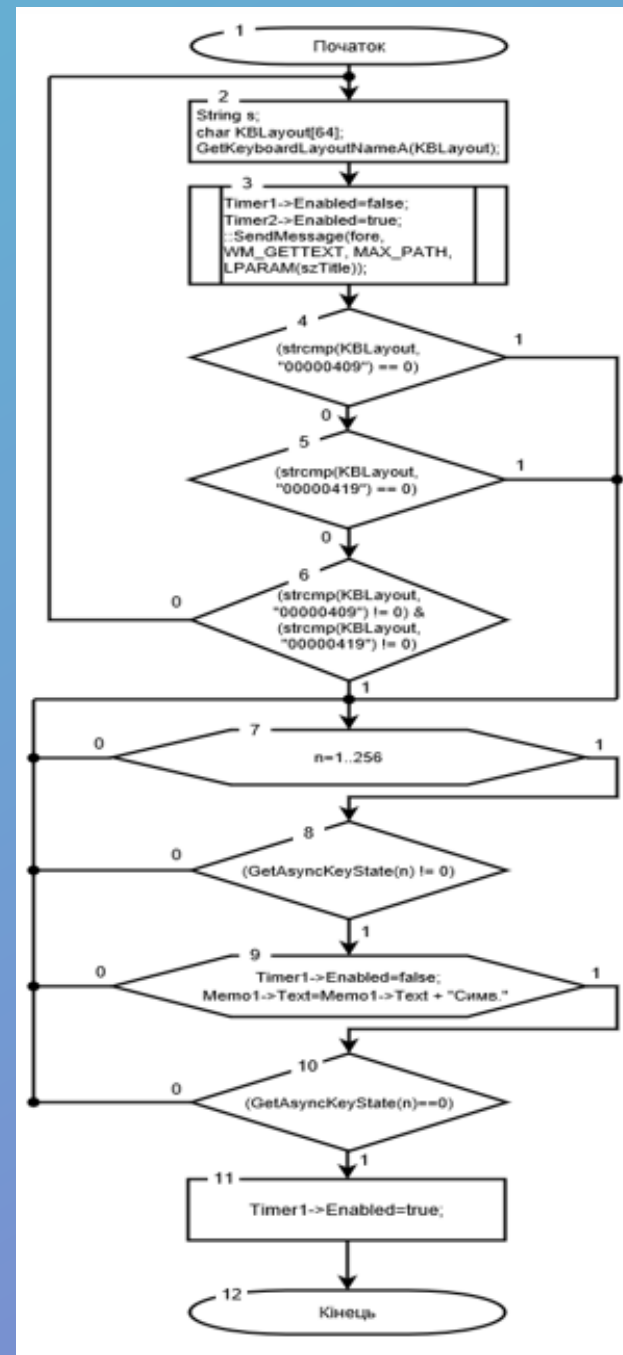
1) Подальшого розвитку отримав метод циклічного опитування стану клавіш клавіатури, відмінністю якого є реалізація функції опитування вмісту буферу обміну, що надає можливість додаткового контролю за інформацією якою оперує персонал.

2) Подальшого розвитку отримав метод зберігання та створення іні файлів для збереження налаштувань додатку, відмінністю якого є збереження вмісту логічних параметрів компонентів додатку у зашифрованому вигляді, без запису значень в реєстр операційної системи, що дає можливість перенесення додатку на інші пристрої зі збереженням параметрів у захищеному стані.



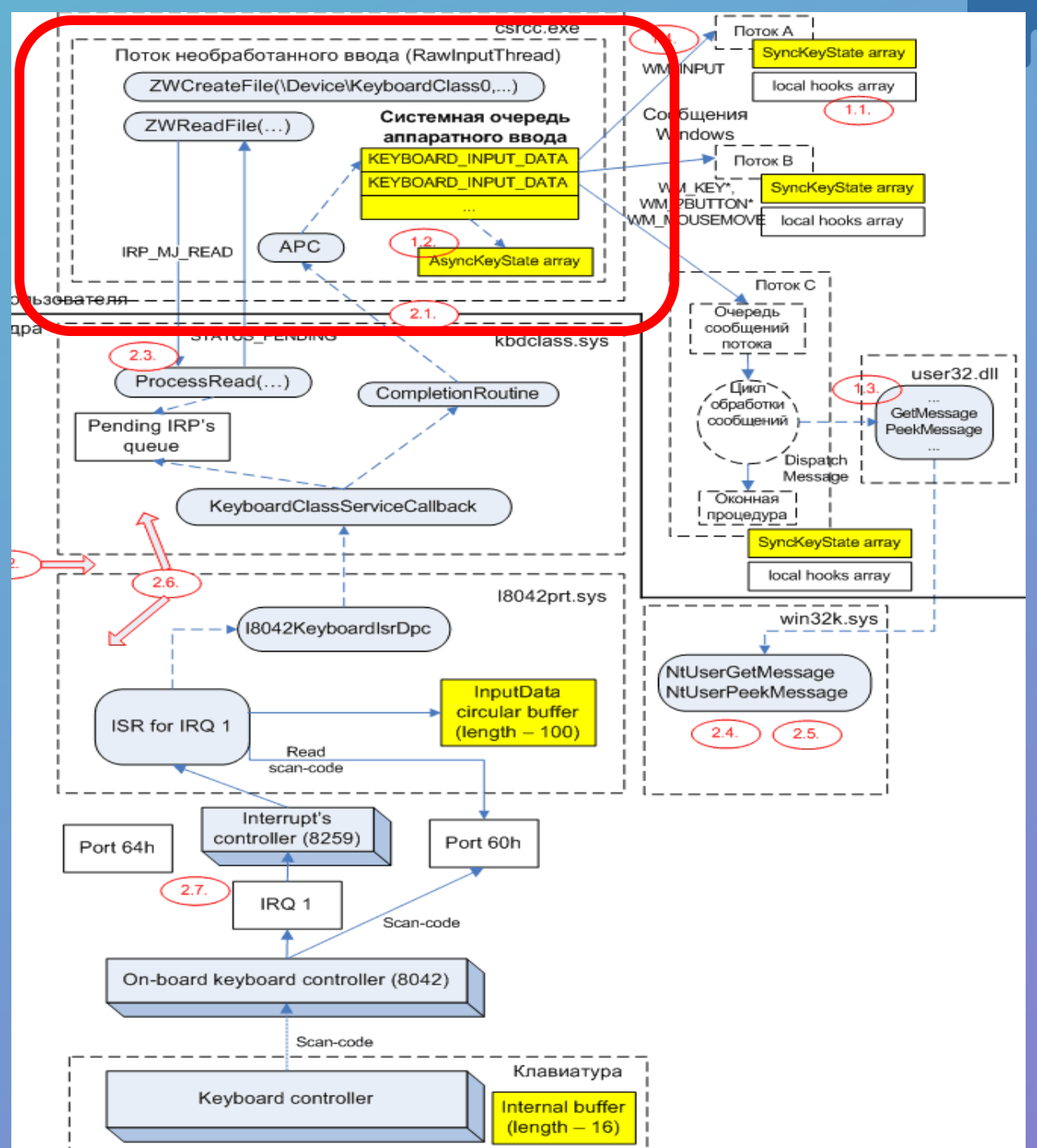
# Алгоритм методу циклічного опитування стану клавіатури з функцією опитування буферу обміну

## Схематичне зображення



# Загальна схема обробки клавіатурного введення в ОС Windows

У виділеній області продемонстровано де втручається метод циклічного опитування нашого додатку

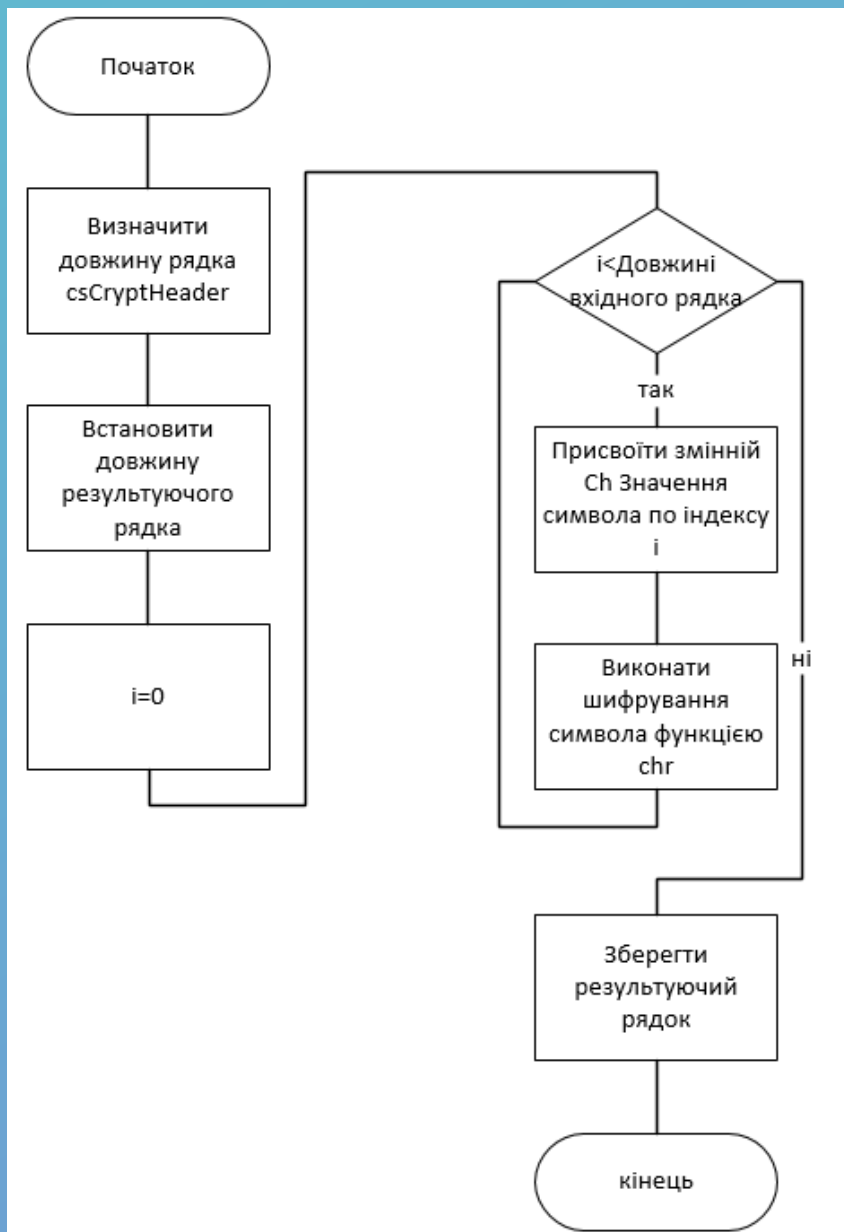




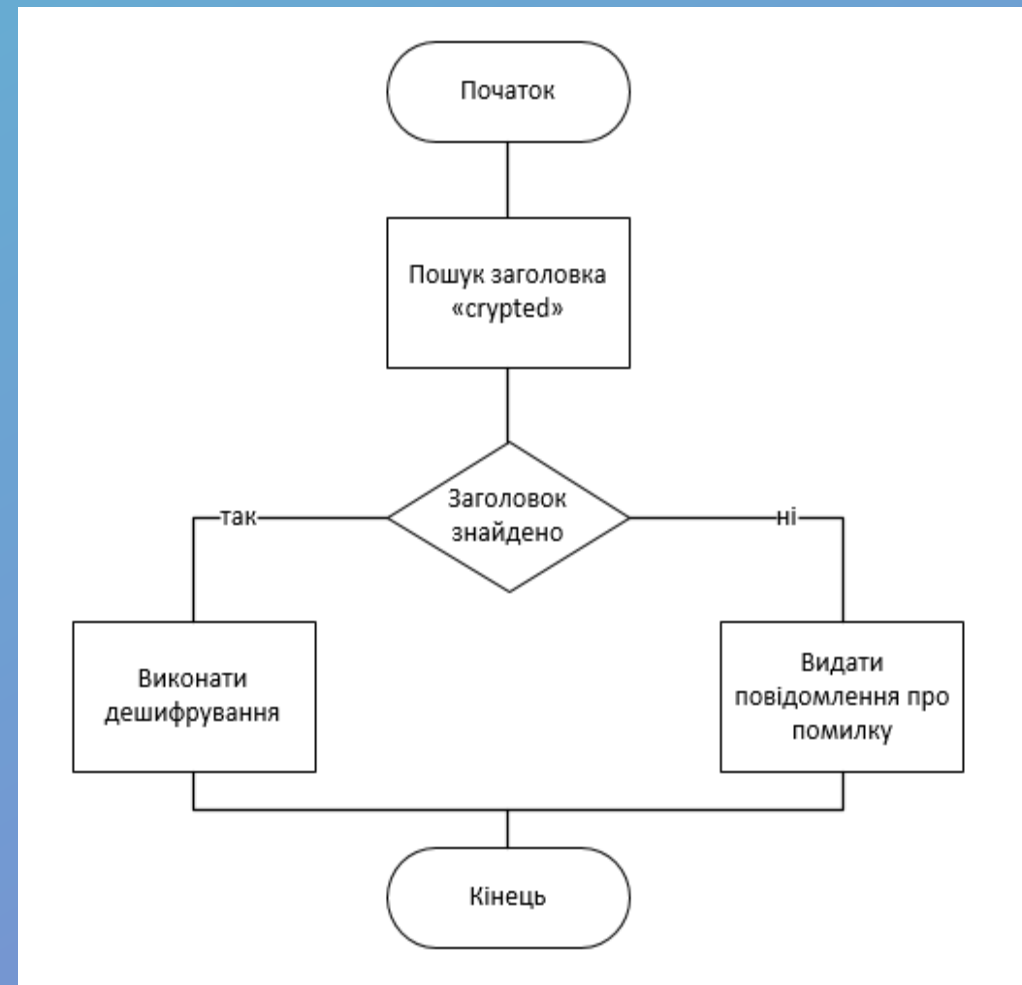
# Переваги вдосконаленого методу шифрованого збереження налаштувань в ini файл

- ✓ простота передачі файлу з налаштуваннями користувачам
- ✓ якщо розглядати доменну структуру з обмеженими правами користувачів, набагато зручніше використовувати ini файли
- ✓ швидкість читання вища ніж з реєстру
- ✓ не потрібно забруднювати реєстр
- ✓ захищеність від втручання до зміни налаштувань файлу

# Процес шифрування



# Алгоритм дешифрування





# Використані технології при розробці ПЗ

## C++ Builder Seattle

Середовище  
розробки ПЗ

Переваги: зручне  
проекування інтерфейсу  
користувача за допомогою  
Windows Form

## Dr. Explain

Середовище  
розробки довідки

Переваги: велика кількість  
форматів  
для експорту

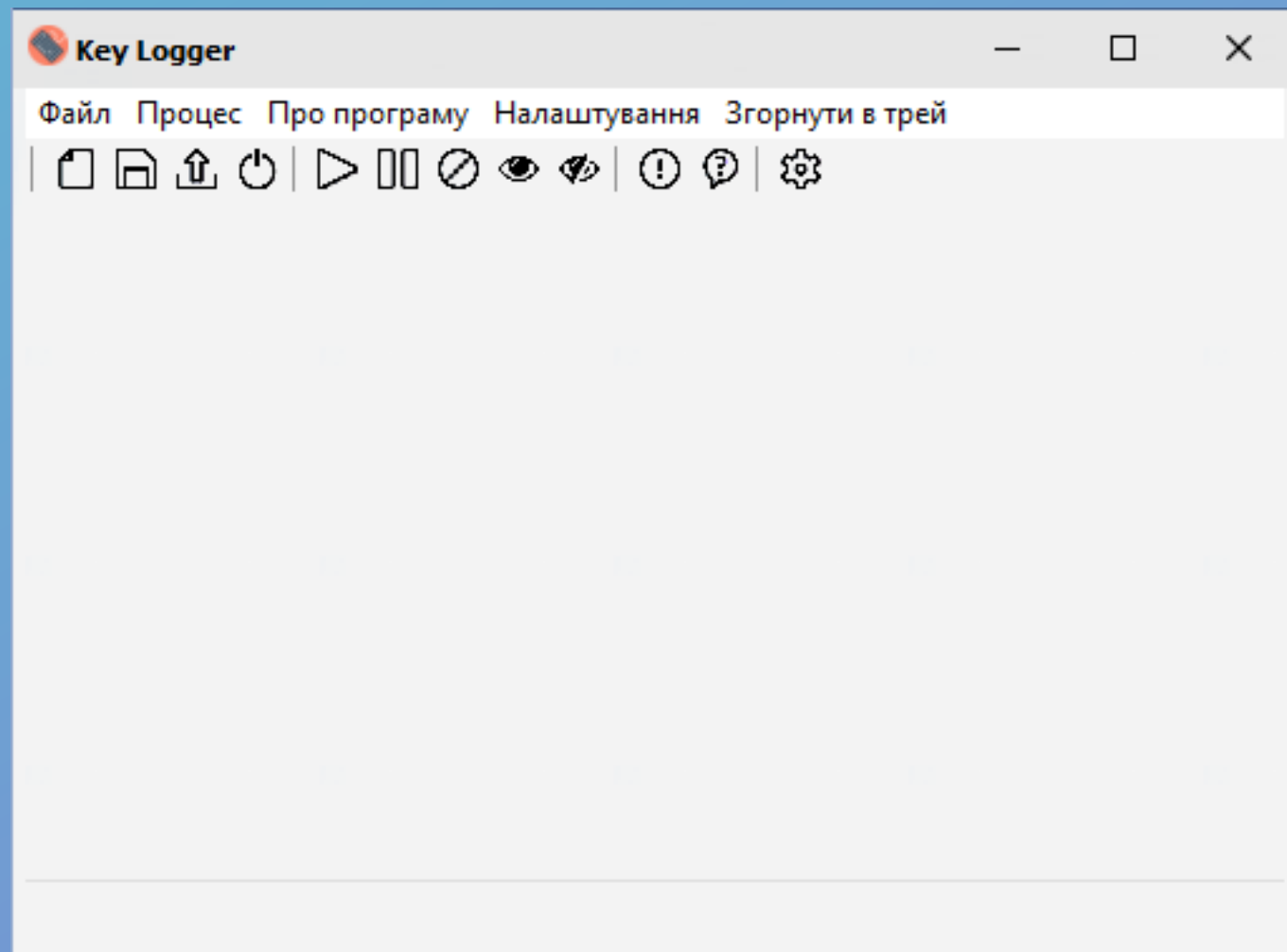
C + +

Мова програмування

Перевага: доступність  
процедурної  
парадигми програмування

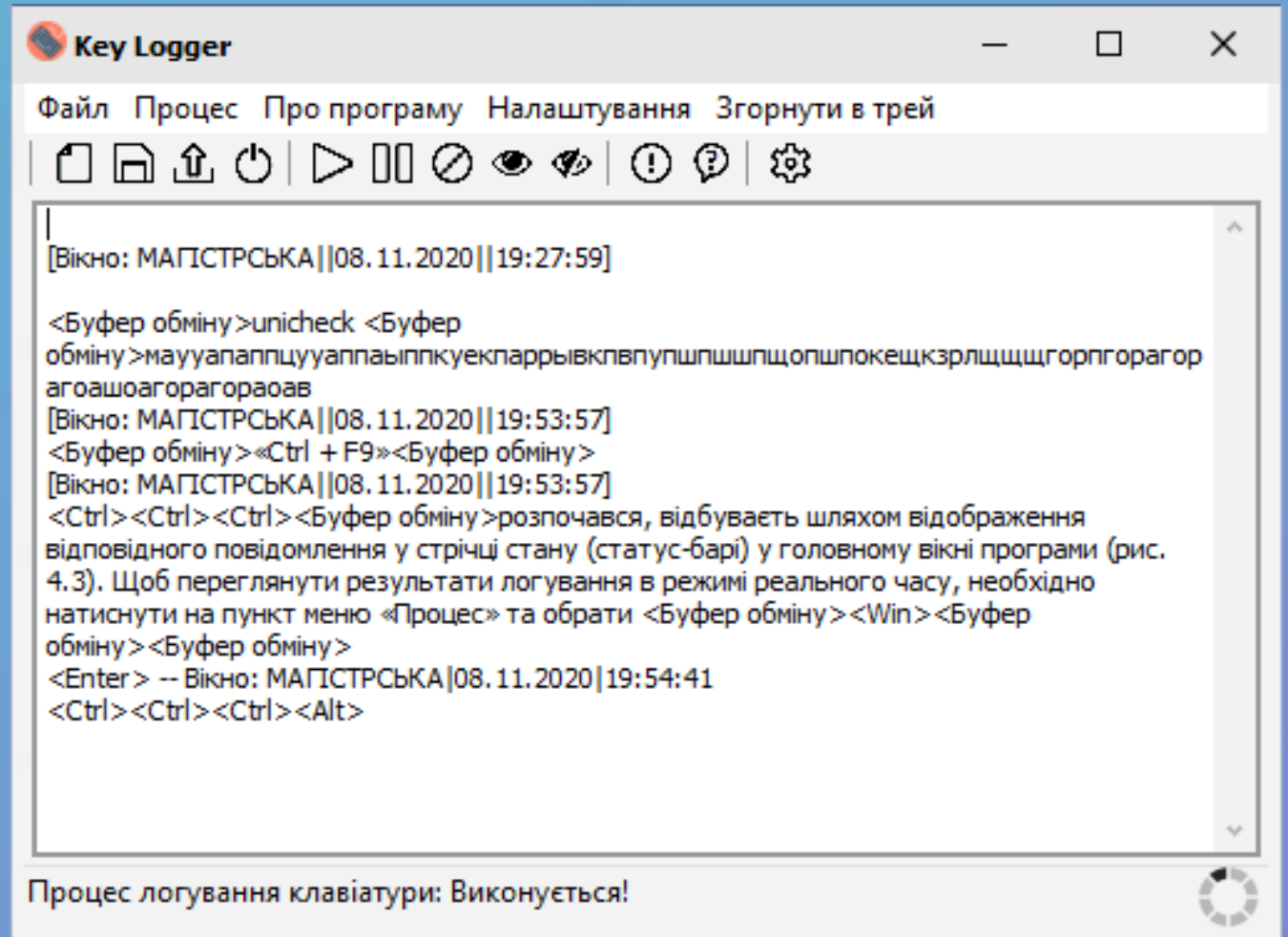
# Головна вікно додатку

01.



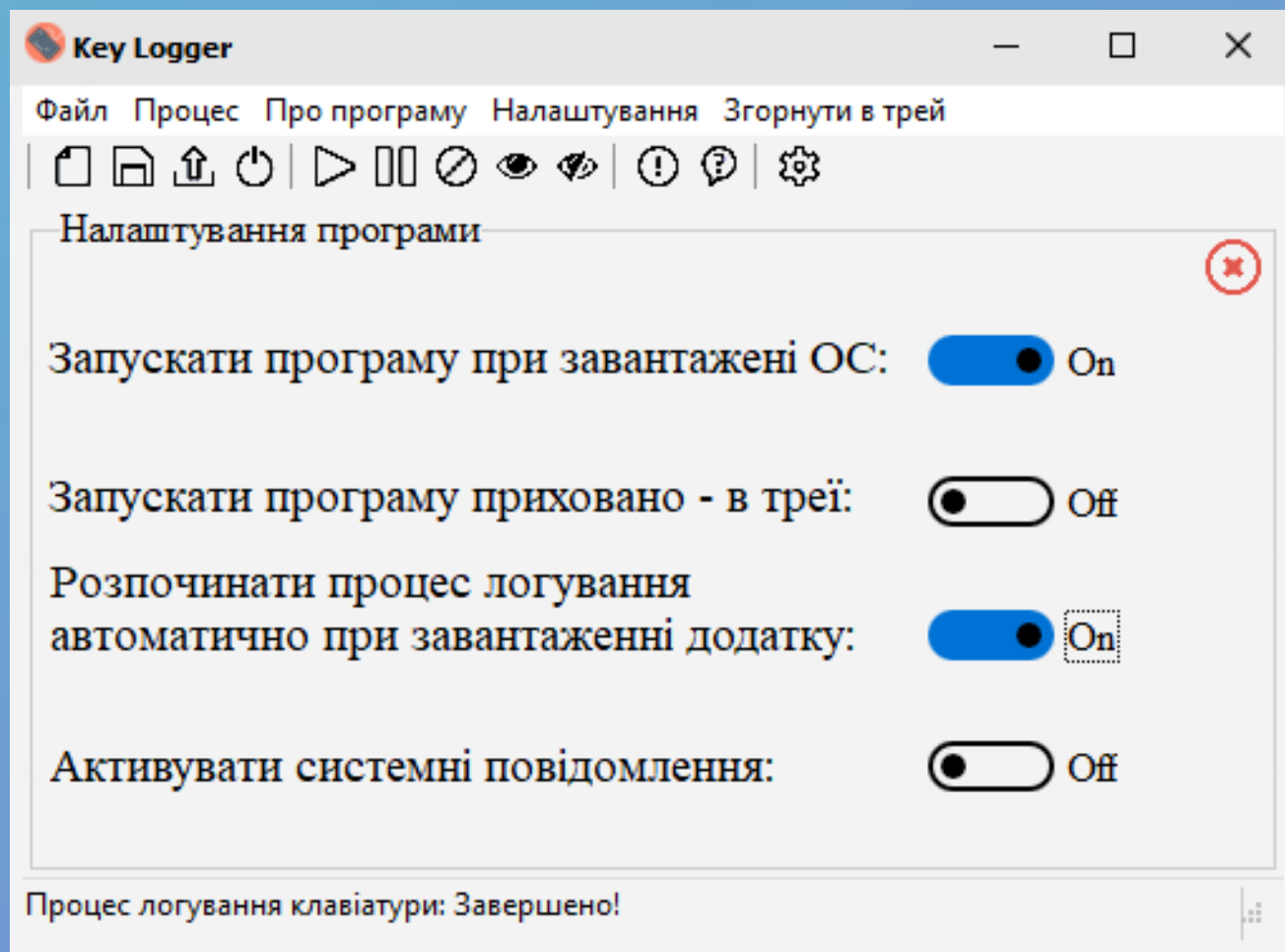
# Головне вікно додатку режимі виконання процесу логування із відображенням інформації

# 02.



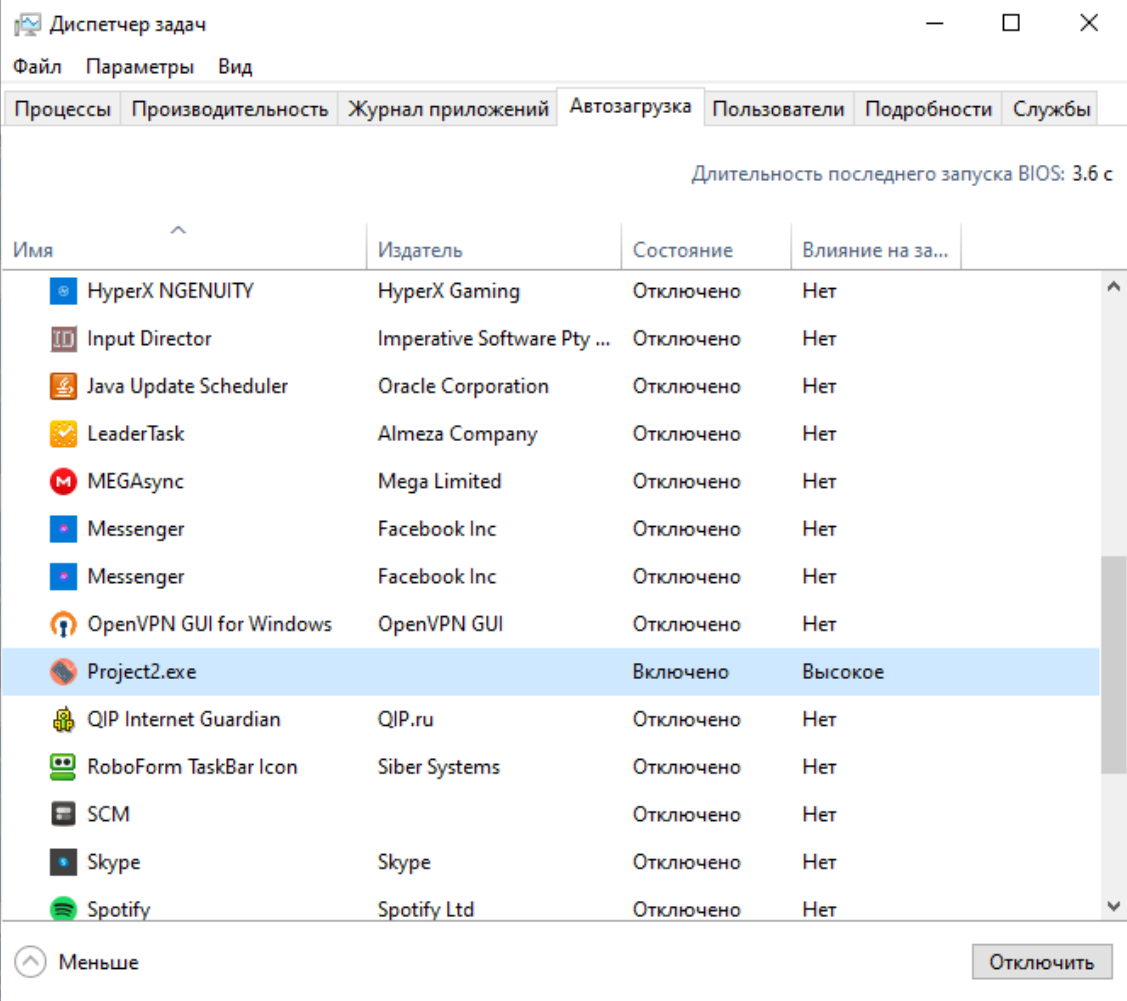
# Панель налаштування додатку

# 03



# Відображення процесу додатку в вікні автозавантаження ОС

3.1



Диспетчер задач

Файл Параметры Вид

Процессы Производительность Журнал приложений Автозагрузка Пользователи Подробности Службы

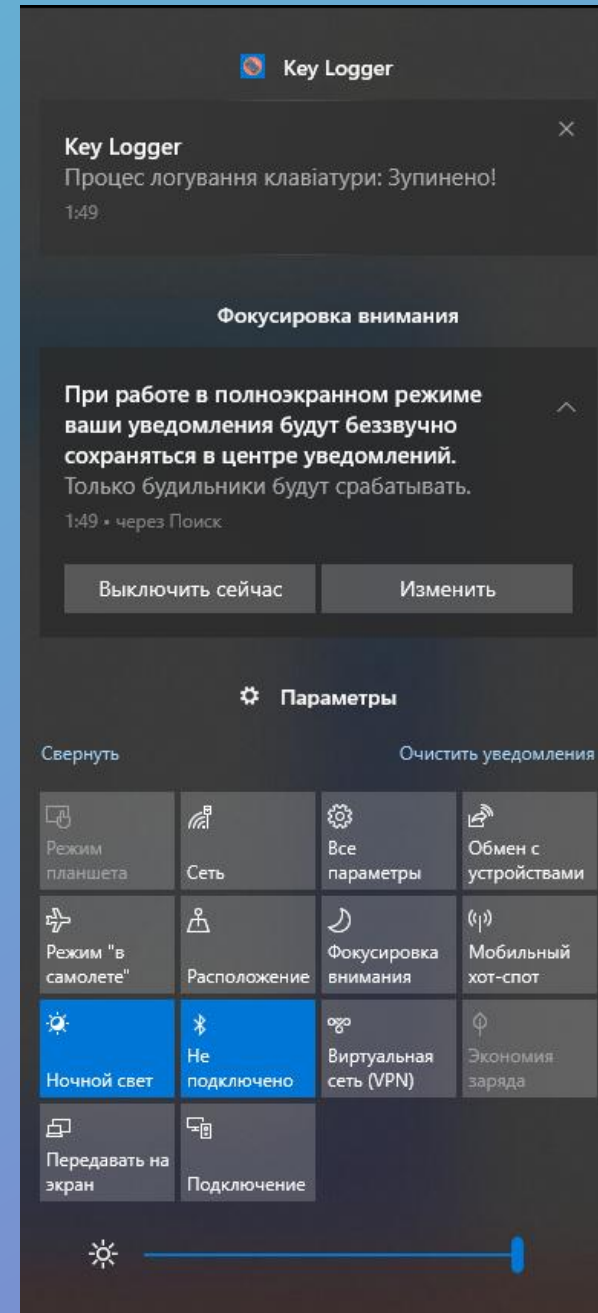
Длительность последнего запуска BIOS: 3.6 с

Имя	Издатель	Состояние	Влияние на за...
HyperX NGENUITY	HyperX Gaming	Отключено	Нет
Input Director	Imperative Software Pty ...	Отключено	Нет
Java Update Scheduler	Oracle Corporation	Отключено	Нет
LeaderTask	Almeza Company	Отключено	Нет
MEGAsync	Mega Limited	Отключено	Нет
Messenger	Facebook Inc	Отключено	Нет
Messenger	Facebook Inc	Отключено	Нет
OpenVPN GUI for Windows	OpenVPN GUI	Отключено	Нет
<b>Project2.exe</b>		<b>Включено</b>	<b>Высокое</b>
QIP Internet Guardian	QIP.ru	Отключено	Нет
RoboForm TaskBar Icon	Siber Systems	Отключено	Нет
SCM		Отключено	Нет
Skype	Skype	Отключено	Нет
Spotify	Spotify Ltd	Отключено	Нет

Меньше Отключить

# Вигляд системного повідомлення при активованому налаштуванню

3.2





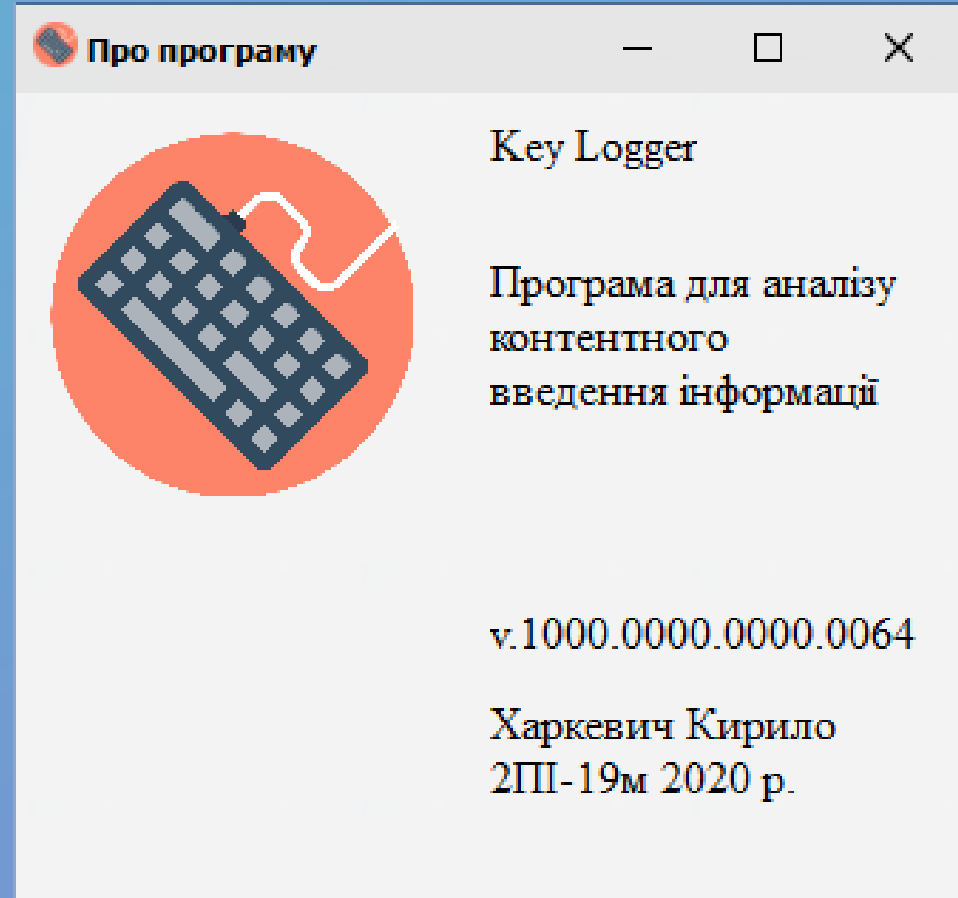
# Прихована робота додатку (відображення в треї)

3.3



# Допоміжне вікно додатку «Про програму»

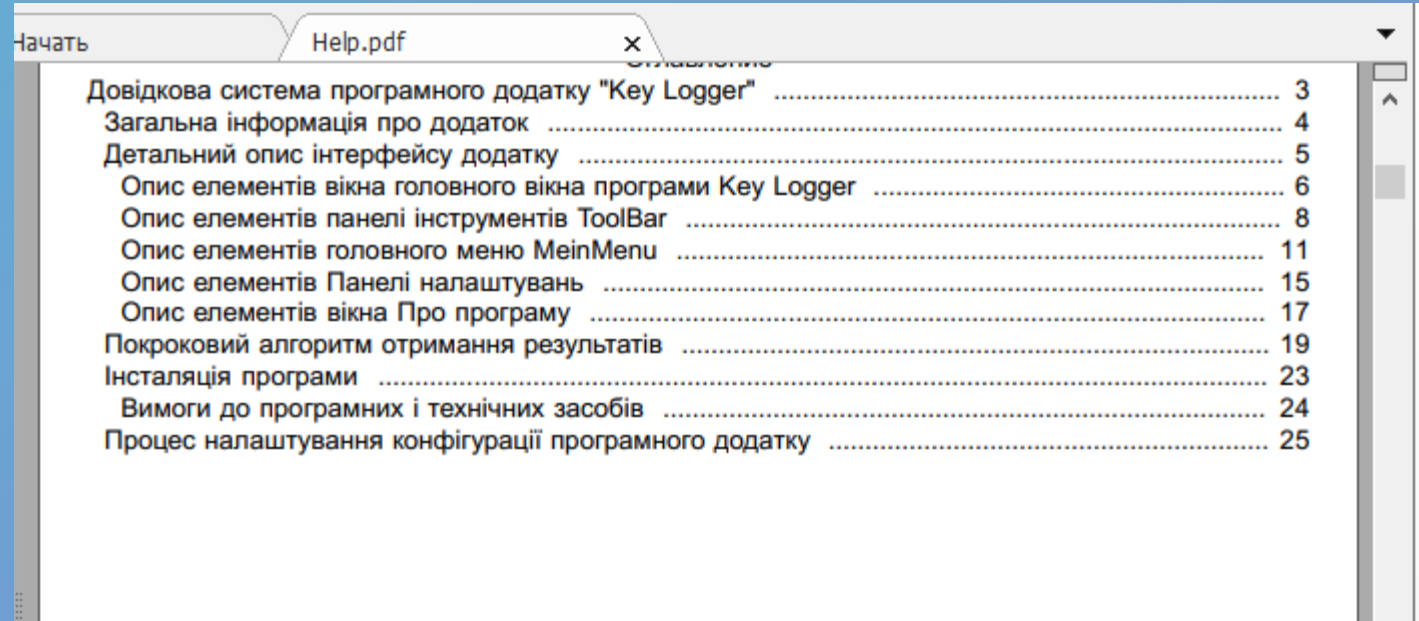
04.





# Відображення довідкової системи додатку

05.



The screenshot shows a help document viewer with a single tab titled 'Help.pdf'. The document content is a table of contents for the 'Key Logger' software. The table lists various sections and their corresponding page numbers.

Довідкова система програмного додатку "Key Logger" .....	3
Загальна інформація про додаток .....	4
Детальний опис інтерфейсу додатку .....	5
Опис елементів вікна головного вікна програми Key Logger .....	6
Опис елементів панелі інструментів ToolBar .....	8
Опис елементів головного меню MeinMenu .....	11
Опис елементів Панелі налаштувань .....	15
Опис елементів вікна Про програму .....	17
Покроковий алгоритм отримання результатів .....	19
Інсталяція програми .....	23
Вимоги до програмних і технічних засобів .....	24
Процес налаштування конфігурації програмного додатку .....	25

# Акт впровадження ТОВ НВЦ «ОЛАНД»



**ТОВ НВЦ «ОЛАНД»**



ЄГРПОУ 32931701  
ІПН 329317006243  
Бердичів, 13300, Україна,  
вул. Данилівська 4,  
Тел.: (04143) 4-15-17

Вих. №67/20  
«12» листопада 2020 р.

**Завідувач кафедри ПЗ ВНТУ  
Романюк О. Н.**

В результаті виконання магістрської кваліфікаційної роботи студентом ВНТУ групи ЗПІ-19м Харкевичем К.А. було розроблено програмний додаток для аналізу контентного введення інформації, який успішно впроваджений на підприємстві ТОВ НВЦ «Оланд».

В результаті чого було автоматизовано контроль за комерційною таємницею інформації на підприємстві. Даний програмний додаток забезпечив швидкий збір та аналіз інформації якою оперує персонал підприємства при використанні робочих комп'ютерів, та дав змогу адміністратору переглядати чи не було витоку даної інформації за межі підприємства.


З повагою,  
Директор ТОВ НВЦ «Оланд»

  
  
Гришук О.О.



## **Апробація матеріалів магістерської кваліфікаційної роботи.**

Основні положення магістерської кваліфікаційної роботи доповідалися та обговорювалися на міжнародній науково-практичній конференції «Інформаційні технології і автоматизація – 2020» (Одеса, 2020). Також основні результати досліджень було опубліковано у матеріалах конференції.



ДЯКУЮ  
ЗА  
УВАГУ!