**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ**

**ВИКОНАВЧОГО ОРГАНУ КИЇВСЬКОЇ МІСЬКОЇ РАДИ**

**(КИЇВСЬКОЇ МІСЬКОЇ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ)**

**КИЇВСЬКЕ ТЕРИТОРІАЛЬНЕ ВІДДІЛЕННЯ**

**МАЛОЇ АКАДЕМІЇ НАУК УКРАЇНИ**

|  |
| --- |
| **Відділення:** Комп’ютерні науки  **Секція:** Технології програмування  **Базова дисципліна**: Математика |

**Створення компілятора мови програмування Alan та програмного середовища розробки**

**РОБОТУ ВИКОНАВ:**

кандидат у члени МАН

**Краснянський Тимур Максимович**,

учень 11 класу

Києво-Печерського ліцею №171 «Лідер» м.Києва

**Науковий керівник:**

Свідерський Кирило Сергійович,

учитель Києво-Печерського

ліцею №171 «Лідер» м.Києва,

провідний фахівець навчальної мережі GoITeens

**Педагогічний керівник**:

Богомолова Наталія Іванівна,

учитель Києво-Печерського

ліцею №171 «Лідер» м.Києва,

Заслужений учитель України

**Київ 2019 р.**

**Створення компілятора мови програмування Alan та програмного середовища розробки**

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 4](#_Toc26182565)

[ВСТУП 5](#_Toc26182566)

[**Основна частина** 8](#_Toc26182567)

[1.1. \* 8](#_Toc26182568)

1.2. \* ……………………………………………………………………..10

[2.1. \* 12](#_Toc26182569)

[2.1.1. \*\*\*\* 13](#_Toc26182570)

[2.1.2. \* 17](#_Toc26182571)

[Висновки 23](#_Toc26182572)

[**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** 24](#_Toc26182573)

[ДОДАТОК А 26](#_Toc26182574)

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ПЗ – програмне забезпечення

CPU – Central processing unit

OS – Operating system

API – Application programming interface

## ВСТУП

Науковий прогрес, станом на 2020 рік, робить нові виклики. Сучасні проблеми цифровізації людської діяльності потребують сучасних рішень. Все більш розповсюджена модель віддаленої праці над великими спільними проектами. На момент проведення дослідження у світі створено сотні різних рішень для спільної роботи в проектах, але вони мають або велику вартість або концептуальні недоліки. Автор поставив за мету створити зручний, інтуїтивно зрозумілий, ефективний засіб для створення програмного забезпечення. Завдання передбачає, і розробку самої мови програмування, і технічну реалізацію. Дослідження на практичні розробки базуються на сучасних парадігмах програмування, що робить проект «Alan» *актуальним* та *важливим*.

Мета роботи: провести дослідження та аналіз програмних засобів, створити власну мову та систему програмування.

Об’єкт дослідження: системи програмування.

Предмет дослідження: створення власної мови програмування, системи програмування.

Задачі дослідження:

1. Навчальна: дослідити існуючі методи та технології програмування.
2. Комерційна: створити умовно-безоплатний, зручний, ефективний продукт.

Наукова новизна:

**Основна частина**

## Висновки

Засоби захисту від атак нульового дня зараз дуже актуальні. Вони є найбільш інтелектуальними і високотехнологічними, вирішуючи при цьому найбільш складну проблему захисту від невідомих шкідливих кодів. Емуляція використання файлів у віртуальному середовищі для визначення його потенційної небезпеки – в пісочниці – є одним з механізмів захисту від атак нульового дня.

Отриманий шкідливий файл вже не можна виявити за допомогою стандартних методів захисту, адже сигнатур цього шкідливого програмного забезпечення в базах ІБ-компаній ще немає.

Емуляція – один з найефективніших способів захисту від невідомих загроз. Вона являє собою відкриття (або запуск) підозрілого файлу в ізольованому середовищі і спостереження за його поведінкою. З точки зору архітектури емуляція можлива як на рівні периметра (шлюзу безпеки), так і на рівні робочої станції.

За межами периметра організації також потрібен захист від невідомих загроз, так як робоча станція – останній рубіж оборони корпоративних даних. Антивірусна пісочниця – це рішення для захисту кінцевих пристроїв, яке дозволяє запобігти загрозам і атакам, пов’язаними з підключенням до зовнішнього Wi-Fi, з шифрованим трафіком, підключенням до ПК зовнішніх носіїв і горизонтальним поширенням атаки в мережі.

Проаналізовано ринок мережевих та антивірусних пісочниць, з яких були обрані оптимальні рішення, які задовільнять потребам захисту у корпоративній мережі, а саме:

- Check Point SandBlast Zero-Day Protection;

- ESET Dynamic Threat Defense.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Advanced Persistent Threat (APT). Таргетированные или целевые кибератаки «Развитая устойчивая угроза» : [Електронний ресурс]. – Режим доступу: [http://www.tadviser.ru/index.php/Статья:APT\_-\_Таргетированные\_или\_целевые\_атаки](http://www.tadviser.ru/index.php/Статья:APT_-_Таргетированные_или_целевые_атаки%20)
2. Иван Бойцов. Обзор рынка защиты от целевых атак. : [Електронний ресурс]. – Режим доступу: <https://www.anti-malware.ru/analytics/Market_Analysis/protection-market-against-targeted-attacks-review>
3. Венеамин Левцов, Николай Демидов. Что же представляет из себя таргетированная атака? : [Електронний ресурс]. – Режим доступу: <http://lib.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-2>
4. Актуальные киберугрозы. I квартал 2019 года: [Електронний ресурс]. – Режим доступу: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q1.pdf>
5. Кибербезопасность АСУ ТП: вести с передовой : [Електронний ресурс]. – Режим доступу: <https://appau.org.ua/info/kyberbezopasnost-asu/>
6. Lam L., Chiueh T. Automatic extraction of accurate application-specific sandboxing policy / L. Lam, T. Chiueh // Lecture Notes in Computer Science. – B.: Springer Berlin, 2004. – Vol.3224. – P.1-20
7. Jeremy D'Hoinne , Lawrence Orans. Market Guide for Network Sandboxing. Gartner. – 2015 : [Електронний ресурс]. – Режим доступу: <https://www.gartner.com/en/documents/2995621>.
8. E. Cooke, F. Jahanian, and D. McPherson, “The zombie roundup: Unsterstanding, detecting, and disrupting botnets,” in Proceedings of the first Workshop of Steps to Reducing Unwanted Traffic on the Internet (SRUTI), July 2017.
9. The Problem with Traditional Sandboxing : [Електронний ресурс]. – Режим доступу до ресурсу: <https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/>.
10. Luis J. G. Malware Detection System by Payload Analysis of Network Traffic [Електронний ресурс] / Javier Garcia Luis // IEEE. – 2015. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7069114/metrics#metrics.