Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: **«РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ПРОГРАМНИХ ДОДАТКІВ В ОС ANDROID»**

Виконав: студент групи KN1-M21
спеціальності 122 Комп’ютерні науки
**Продан Олександр Олександрович**

Керівник:
**Моцик Р.В.,**
кандидат педагогічних наук, доцент, доцент кафедри комп’ютерних наук

Рецензент:
**Сморжевський Ю.Л.,**
кандидат педагогічних наук, доцент, доцент кафедри математики

Кам’янець-Подільський – 2022

**ЗМІСТ**

# ВСТУП

У наш час мобільні пристрої дедалі більше стають характерною рисою і необхідним елементом як технологічного розвитку, так і життєзабезпечення. Поступово в умовах всеосяжної діджіталізації вони проникають у всі сфери життя людини. Завдяки мобільним пристроям здійснюється управління складними кіберфізичними системами, у тому числі через мережі Інтернету речей, стає доступним широкий спектр фінансових та соціальних послуг, організується обмін інформацією та моніторинг життєвоважливих функцій. Фактично, такого роду пристрої переходять із розряду іграшкових приладів у категорію критичних застосунків.

Питання забезпечення функціональної безпеки критичних застосунків достатньо глибоко висвітлено в наукових працях відомих закордонних та вітчизняних науковців, таких як A. Avizienis, G. Johnson, J.C. Laprie, B. Randell, Є. В. Брежнєв, О. М. Одарущенко, В. В. Скляр, В. С. Харченко. Виходячи із сформованої вказаними вченими загальної таксономії понять загальна проблема забезпечення функціональної безпеки належить до систем моніторингу та управління. На сучасному етапі функціональна безпека повинна спиратися на інформаційну безпеку та кібербезпеку, що доповнюють одна одну. У той час як мета інформаційної безпеки полягає в забезпеченні доступності, цілісності й конфіденційності даних системи, функціональна безпека забезпечує здатність системи виконувати передбачені функції при існуванні ризику виникнення небезпечних подій, в тому числі під впливом зовнішніх загроз.

Що стосується безпосередньо мобільних пристроїв, то тут особливо гостро питання функціональної безпеки постає перед найбільш поширеними реалізаціями на базі ОС Android, дослідженню функціональної безпеки яких присвячена значна кількість публікацій сучасних науковців та фахівців наукових лабораторій IT корпорацій: J. Warton, P. Roche, S. Felker, A. Саммерс, K. Gopal, A. Davies, M. Zhan, R. Mayer, A. Dao, D. Smith, T. Norby,

M. Alison, С. В. Зайцев, М. С. Дорош, І. В. Стеценко та ін. Отримані в межах даних досліджень результати вказують на те, що найбільший рівень загрози слід пов’язувати не з апаратними ресурсами та операційною системою (ОС), а саме з мобільними додатками, що містять у собі такі вразливості, як недосконалості у визначенні привілеїв користувачів, витік інформації, низький рівень захисту функціональних компонентів, уразливості міжкомпонентних комунікацій та інші. Більшість існуючих заходів безпеки, що надаються ОС Android, базуються на попереджувальних діях та системних обмеженнях для забезпечення безпеки платформи загалом.

Слід зазначити, що підходи на основі машинного навчання, статичного аналізу та штучних нейромережевих алгоритмів, що дозволяють визначити рівень загрози на основі базових параметрів програмного коду, наприклад, при аналізі викликів API (Application Programming Interface), також не забезпечують належний рівень функціональної безпеки. Враховуючи значну затримку у вирішенні питань безпеки та потенційний ризик втрати приватних даних або навіть порушення функціональної безпеки системи, існує потреба в додатковому блоці безпеки, який допоможе повідомити користувача про потенційно шкідливе програмне забезпечення під час виконання. Тому актуальним є наукове завдання із подальшого розвитку інформаційної технології забезпечення функціональної безпеки мобільних пристроїв за рахунок удосконалення існуючої моделі безпеки ОС Android шляхом впровадження методу динамічного виявлення потенційно небезпечних додатків з метою подальшого їх блокування для запобігання небажаних впливів.

*Об’єкт дослідження* система функціональної безпеки ОС Android та процес її функціонування в умовах зовнішніх загроз.

*Предмет дослідження* моделі та методи забезпечення функціональної безпеки на рівні операційної системи мобільних пристроїв.

*Мета* дипломної роботи полягає в покращенні функціональної безпеки мобільних пристроїв за рахунок удосконалення моделі безпеки ОС Android з можливістю врахування ризику використання шкідливих програмних додатків.

Досягнення поставленої мети передбачає вирішення таких *завдань*:

- визначення потенційних загроз функціонуванню мобільних пристроїв.
- аналіз існуючої системи безпеки ОС Android щодо загроз безпечній роботі програмних додатків.
- розробка програмних засобів реалізації запропонованих методів забезпечення функціональної безпеки.
- оцінка ефективності розроблених моделей, методів та інформаційної технології шляхом проведення експериментів із реальними пристроями та додатками.

*Методи дослідження.* При розв'язанні поставлених завдань були використані: методи системного аналізу та методи теорії множин при аналізі системи безпеки ОС Android та розробці моделі прав доступу, методи біоінформатики у процесі розробці методу динамічного виявлення потенційно небезпечних додатків, теорії ймовірностей та математичної статистики для планування та статистичного аналізу результатів експериментів із реальними додатками, об'єктно--орієнтованого аналізу та графічні нотації UML — при проєктуванні та розробці програмних засобів, які реалізують запропоновану інформаційну технологію забезпечення функціональної безпеки мобільних пристроїв.

*Структура та обсяг дипломної роботи*. Дипломна робота складається зі вступу, двох розділів, висновків, списку використаних джерел та додатків. Повний обсяг дипломної роботи становить 68 сторінок, у тому числі: 67 сторінок основного тексту, 26 рисунків, 2 таблиць, список використаних джерел із 22 найменувань та 1 додатку.

# ВИСНОВКИ

У дипломній роботі сформульовано та вирішене актуальне завдання з подальшого розвитку інформаційної технології забезпечення функціональної безпеки мобільних пристроїв за рахунок удосконалення існуючої системи безпеки ОС Android шляхом впровадження методу динамічного виявлення потенційно небезпечних додатків.

Для досягнення поставленої мети, яка полягає в підвищенні ефективності системи функціональної безпеки мобільних пристроїв за рахунок удосконалення моделі безпеки ОС Android з можливістю врахування ризику використання шкідливих програмних додатків, були отримані такі результати:

1. Визначено поняття функціональної безпеки щодо програмних додатків апаратно-програмної платформи Android. Показано, що аналіз ефективності функціональної безпеки має проводитись на рівні категорій показників, через визначення набору властивостей програмного коду додатку, які характеризують процес його функціонування, а також встановлення рівня шкідливості додатка.

2. Проведено аналіз існуючих систем забезпечення функціональної безпеки мобільних додатків ОС Android як комплексу систем моніторингу та управління. Розглянуто схему роботи мобільного пристрою з погляду забезпечення функціональної безпеки.

3. Виділено основні типи загроз, пов’язаних із використанням програмних додатків, такі як наявність зловмисного програмного коду, наявність вразливостей у програмних застосунках, перехоплення зловмисниками конфіденційних даних, некоректний опис програмного застосунку.

4. Запропоновано класифікацію типів шкідливих додатків, яка, на відміну від існуючих, базується на групуванні API функцій додатків та дає можливість оцінити їх за ступенем потенційних впливів при прийнятті

рішень на використання додатків за запропонованими атрибутами вектора атаки.

5. Описана система прав доступу при взаємодії ОС Android із програмними додатками, яка встановлює відношення між групами дозволів, дозволами та функціями API та дає можливість ввести кодування функцій для їх ідентифікації.

6. Визначено базову модель псевдосимволу СФЛД, яка складається з етапів послідовного знаходження збігів та індексації групи привілеїв, самого привілею та відповідної API функції. Псевдосимволи, створені на основі цієї моделі, дозволяють унікально ідентифікувати API-функції, що використовує програмний додаток, та прискорити пошук збігів СФЛД.

7. Розглянуто метод динамічного аналізу програмних додатків, що базується на побудові сигнатури функціонального ланцюжка додатка API функції та порівняння його з шаблонною СФЛД. Визначено основні етапи процесу аналізу додатків ОС Android та розроблено відповідний математичний апарат на основі відомих алгоритмів вирівнювання послідовностей з біоінформатики. Проведено аналіз ефективності роботи запропонованого методу на основі статистичних даних та зразків зловмисного програмного коду з Android Malgenome Project.

8. Проведено аналіз сучасного програмного забезпечення функціонального трасування API викликів для операційної системи Android. Запропонована функціональна схема перехоплення та декорування API викликів за допомогою розроблених скриптів для Frida Framework.

9. Розроблено програмний комплекс, який працює у хмарному середовищі та забезпечує перевірку програмних додатків, що використовуються мобільними пристроями, на предмет їх збігу зі шкідливими додатками за послідовністю викликів API функцій з одночасним інформуванням користувача про можливі наслідки використання шкідливого програмного забезпечення з визначенням потенційного ризику.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mobile Statistics Report, 2019-2023 – Executive Summary.

https://www.radicati.com/wp/wpcontent/uploads/2019/01/Mobile_Statistics_Report,_2019-2023_Executive_Summary.pdf

2. Oberlo. (n.d.). *How many people have smartphones in 2021?* https://www.oberlo.com/statistics/how-many-people-have-smartphones.

3. Кабінет Міністрів України (2018). *Про схвалення розвитку цифрової економіки та суспільства України*. https://zakon.rada.gov.ua/laws/show/67-2018%D1%80#Text.

4. *Державні послуги онлайн*. https://diia.gov.ua/

5. Toninelli, D., Revilla, M. (2016). Smartphones vs PCs: Does the Device Affect the Web Survey Experience and the Measurement Error for Sensitive Topics?
A Replication of the Mavletova & Couper's 2013 Experiment. *Survey Research Methods, 10*(2), 153-169.

6. Basant, A., & Mittal, N. (2012). Hybrid approach for detection of anomaly network traffic using data mining techniques. *Proc. Technol.*, 6, 996-1003.

7. Dusan, S., Vlajic, N., & An, A. (2012). Detection of malicious and nonmalicious website visitors using unsupervised neural network learning. *Applied Soft Comput.*, 13: 698-708.

8. Ghazali, K.W.M., & Hassan, R. (2011). Flooding distributed denial of service attacks-a review. *J. Comput. Sci.*, 7, 1218-1223.

9. Mahmoudi, C. (2017). Cloud and Mobile Cloud Architecture, Security and Safety. In *Handbook of System Safety and Security* (pp. 199-223).

10. Roche, E., Hochleitner, M., & Summers, A. (2017). Introduction to functional safety assessments of safety controls, alarms, and interlocks: How efficient are your functional safety projects? *Process Safety Progress*, 36(4), 392-398.

11. В.С. Харченко, В.В. Скляр, Е.В. Брежнев. *Безопасность информационно-управляющих систем и инфраструктур*. Palmarium Academic
Publishing, 2013. 528 с.

12. Pandita R, Xiao X, Yang W, Enck W, Xie T (2013) WHYPER: towards automating risk assessment of mobile applications. *Proceedings of the 22nd USENIX conference onsecurity*. https://www.usenix.org/system/files/conference/
usenixsecurity13/sec13paper_pandita.pdf.

13. Hoque, N., Monowar, H., Bhuyan, M.H., Baishya, R.C., Bhattacharyyaa, D.K., & Kalitab J.K. (2014). Network attacks: Taxonomy, tools and systems.

14. Allen, G. (2015). Android Security and Permissions. Beginning Android.

15. Android Security Internals. (2015). *Network Security*, 2015(6), 4.

16. *Oracle Mobile Security. A Technical Overview*. (May 2015). Oracle white paper. https://www.oracle.com/technetwork/middleware/id-mgmt/overview/omsstechnical-wp-2104766.pdf.

17. Gentile, M., Summers, A.E. (2006). Random, systematic, and common cause failure: How do you manage them? *Process Safety Progress, 25*(4), 331-338.

18. Zhang, M., & Yin, H. (2016). Automatic Generation of Security-Centric Descriptions for Android Apps. *SpringerBriefs in Computer Science Android Application Security* (pp. 77-98).

19. ДСТУ EN 61508-1:2019 (2019). *Функційна безпечність електричних,* електронних, *програмованих систем*. http://online.budstandart.com/ua/ catalog/doc-page.html?id_doc=84383.

20. Clarke, S. ExVeritas Limited. *An Introduction to Functional Safety and Safety Integrity Levels.*

https://www.exveritas.com/wpcontent/uploads/2013/01/anintroductiontosafetyintegritylevels.pdf.

21. Kumar, P.A.R., & Selvakumar, S. (2012). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. *Comput. Commun*., 36, 303-319.

22. Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., & K. Rieck (2014). Drebin: Effective and explainable detection of android malware in your pocket. *Proc. of Annual Symposium on Network and Distributed System Security(NDSS)*. *The Internet Society*. https://www.ndss-symposium.org/wp-content/uploads/2017/09/11_3_1.pdf.