DOI: https://doi.org/10.36910/6775-2524-0560-2024-55-12
УДК 004.056:004.725.5
Журавська Ірина Миколаївна, д.т.н., професор
https://orcid.org/0000-0002-8102-9854
Фісун Микола Тихонович, д.т.н., професор
https://orcid.org/0000-0003-1297-6230
Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна

РИЗИКИ ІНФОРМАЦІЙНИХ ВИТОКІВ З МОБІЛЬНИХ ПРИСТРОЇВ

Журавська І. М., Фісун М.Т. Ризики інформаційних витоків з мобільних пристроїв. У статті розглянуто загрози безпеці мобільних застосунків, уразливості мобільних операційних систем (ОС), канали витоку інформації, семантичну безпеку, безпеку, пов'язану з інфраструктурою, тощо. Зазначено, що порушення безпеки можна пом'якшити за допомогою покращення поведінки та ставлення до безпеки, а не лише за допомогою кращих технологій. Показано, що програми під керування як ОС Android, так і iOS за замовчуванням можуть отримувати доступ до датчиків, таких як акселерометр і гіроскоп, мікрофон і камера під час роботи у фоновому режимі без відома або згоди користувача. Проаналізовано ризики витоку інформації внаслідок надання прав системного доступу застосункам з root-правами, оновлення системи прошивками, що містять шкідливі програми або вразливості, які можуть бути використані зловмисниками. Проаналізовано методи перехоплення керуванням мобільними пристроями з використанням засобів пакету Smurf Suite, технологій фішингу та ін. Запропоновано практичні рекомендації щодо зменшення ризиків безпеки при використанні мобільних застосунків як для користувачів, так і для розробників. Наведено переваги використання, Apple Neural Engine і користувацьких моделей CreateML в мобільних пристроях з ОС iOS для обробки даних прямо на пристрої, щоб уникнути тривалих і потенційно ризикованих звертань до віддаленого сервера.
Ключові слова: загрози безпеці, виток інформації, мобільні пристрої, датчики, IoT-пристрої, конфіденційність, iOS, Android.

Zhuravska I., Fisun M. Risks of information leaks from mobile devices. The article covers mobile application security threats, mobile operating system (OS) vulnerabilities, information leakage channels, semantic security, infrastructure-related security, and more. It noted that security breaches can be mitigated through improved security behaviors and attitudes, not just better technology. By default, both Android and iOS apps have been shown to be able to access sensors such as accelerometer and gyroscope, microphone and camera while running in the background without the user's knowledge or consent. The risks of information leakage as a result of granting system access rights to applications with root rights, updating the system with firmware containing malicious programs or vulnerabilities that can be used by attackers have been analyzed. The methods of intercepting control of mobile devices using Smurf Suite tools, phishing technologies, etc. were analyzed. Practical recommendations for reducing security risks when using mobile applications are offered for both users and developers. Benefits of using Apple Neural Engine and custom CreateML models on iOS mobile devices to process data directly on the device to avoid lengthy and potentially risky calls to a remote server.
Keywords: security threats, leak of information, mobile devices, sensors, IoT devices, confidentiality, iOS, Android.

Постановка наукової проблеми. В сучасних умовах діджиталізації суспільства 78,3 % користувачів використовують свій телефон для банківських операцій, доступу до персональних даних (медичних та ін.), управління інвестиціями, торгівлі криптовалютами – по суті, для керування важливими даними та/або проведення конфіденційних транзакцій [1]. Але 44,5 % не використовують спеціальних програм або рішень для захисту власних мобільних пристроїв. В той же час, з поширенням інтелектуальних пристроїв Інтернету речей (IoT) на основі мобільних операційних систем (ОС), зростає кількість та функціонал шкідливих програм, націлених на пристрої IoT,

Зараз на ринку домінують дві ОС, а саме Android OS (74,69 % ринку) та iOS (22,34 % ринку). Відповідно, існує два окремих середовища розробки, включаючи мови програмування, SDK, API та різноманітні засоби створення компонентів, що відповідають двом ОС відповідно. Незважаючи на те, що розробники докладають величезних зусиль, щоб запобігти загрозам безпеці, реальність така, що жодне програмне забезпечення (ПЗ), у т. ч. ОС, не застраховано від злому, особливо під час цілеспрямованих атак [2]. Далі представлено більш детальне обговорення цих двох середовищ. Нещодавні дослідження показують, що порушення безпеки можна пом'якшити за допомогою покращення поведінки та ставлення до безпеки, а не лише за допомогою кращих технологій [3].

Аналіз досліджень. Проблеми з конфіденційністю та безпекою мобільних пристроїв активно вивчаються дослідниками [2; 3]. Але обмежена обчислювальна потужність та інтерфейс користувача мобільних пристроїв полегшують зловмисникам приховування своїх зловмисних дій. Основні теми, що обговорюються, включають загрози безпеці застосунків, уразливості мобільних

операційних систем (ОС), канали витоку інформації, семантичну безпеку, безпеку, пов'язану з інфраструктурою, тощо.

Захист мобільних застосунків від атак по побічним каналам можливий за допомогою вето на доступ до певних ресурсів [4], використання масштабованих систем виявлення зловмисного ПЗ мобільних ОС на основі аналізу шаблонів поведінки [5] та ін.

Сучасні смартфони зазвичай оснащені різними апаратними датчиками (наприклад, мікрофоном, GPS, датчиком освітлення, акселерометром тощо) для взаємодії з фізичним світом. Смартфони також мають доступ до особистої інформації користувача, такої як списки контактів, фотографії та паролі. Доступ сторонніх програм до цих датчиків/ресурсів та інформації користувача контролюється ОС за замовчуванням або під час встановлення програми, або під час її роботи.

Позитивним є те, що останні версії ОС забезпечують певний обмежений захист від цих атак із побічних каналів. Починаючи з Android 9.0, програми за замовчуванням більше не можуть отримувати доступ до датчиків, таких як акселерометр і гіроскоп, мікрофон і камера, під час роботи у фоновому режимі без запуску основної служби, видимої для користувачів як значок [6]. API AudioPlaybackCapture в Android 10, який дозволяє програмі записувати аудіо з іншої програми [7], також пропонує методи відмови, за допомогою яких програма може запобігти іншим програмам доступ до її аудіо. Як інший захист, Android надає доступ до камери та мікрофона лише одній програмі в кожен момент часу з певним обгрунтуванням включення, нп., мікрофона (табл. 1).

Таблиця 1. Обгрунтування включення мікрофона застосунком

Позитивне/ Негативне висловлювання	**Приклад анонсу функції (призначення)**	**Обгрунтування**
✓	Програма записує вночі, щоб виявити звуки хропіння.	Активне речення, яке чітко описує, як і чому програма збирає дані.
✗	Для кращої роботи потрібен доступ до мікрофона.	Пасивне речення, яке містить розпливчасте, невизначене обґрунтування.
✗	Увімкніть доступ до мікрофона.	Наказове речення, яке не дає жодного обґрунтування.

Однак, обмеження, заявлені застосунками у діалогових вікнах на використання камери/мікрофона, не заважає зловмисній програмі використовувати ці ресурси/датчики для атаки побічного каналу, якщо програмі-жертві не потрібен доступ до цих ресурсів.

Виділення раніше невирішених питань. Нещодавні зміни в контролі доступу в Android та iOS спрямовані на забезпечення більшого контролю над ресурсами: дозвіл на фонове використання для місцезнаходження в Android 10 [8], iOS 13 [9] і одноразовий дозвіл на місцезнаходження, камеру та мікрофон в Android 11 [10]. Але навіть із цими вдосконаленнями користувачі все ще можуть дозволити програмі завжди отримувати доступ до цих ресурсів (особливо для програм, які довго працюють і активно використовуються); тобто до видалення такі програми можуть використовувати надані дозволи.

Однак ресурси, які вважаються незначними або взагалі не становлять ризику для безпеки/конфіденційності, як-от акселерометр або гіроскоп, можуть використовуватися будь-якою програмою без відома або згоди користувача. Було продемонстровано багато атак з використанням цих так званих ненебезпечних або звичайних ресурсів [11; 12], а також ресурсів, які вимагають явної згоди користувача [13; 14]. Окрім компрометації PIN-кодів і паролів, атака [13] показує, що, здавалося б, безпечний акселерометр також можна використовувати для прослуховування динаміка телефону. Поточні моделі дозволів на основі схвалення користувача не можуть протистояти цим прихованим, але високоефективним атакам.

Тому потрібні додаткові дослідження для зменшення ризиків безпеки як для користувачів, так і для розробників.

Формулювання мети і завдань дослідження. Метою статті є дослідження режимів роботи мобільних пристроїв для виконання ними необхідних функцій, не допускаючи витоку особистої інформації про пристрій або його користувача.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Конфіденційна інформація буде викрадена різними шляхами. Відмітимо основні з них:

- витоки інформації засобами операційної системи Андроїд;
- витоки інформації засобами фізичного доступу до телефону;
- витоки інформації засобами програмного забезпечення;
- витоки інформації шляхом фішингу та інших схожих методів.

Засобами ОС, здебільшого, дані можуть бути вкрадені, якщо не притримуватися оновлень системи, завантажувати і надавати права системного доступу застосункам з root-правами та перепрошивати систему, використовуючи чиїсь готові продукти (рис. 1).

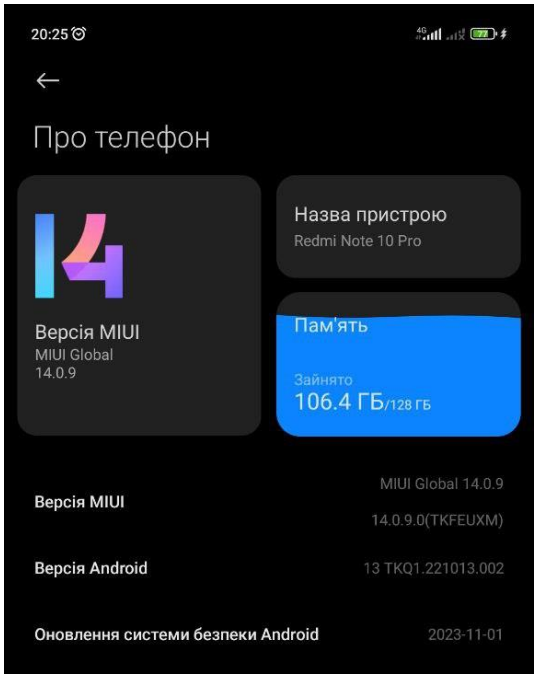

Рис. 1 – Відомості про телефон Xiaomi (версія телефона, ОС та вбудованого інтерфейсу)

Неактуальне ПЗ може бути однією з головних причин витоку інформації через операційну систему Android. Оновлення системи регулярно вирішує виявлені вразливості і запобігає можливим атакам.

Надання застосункам root-прав також може стати причиною витоку інформації, оскільки це дає їм розширений доступ до системи і даних користувача. Якщо застосунки з root-правами не контролюються або вони не мають достатнього рівня довіри, це може стати проблемою з безпекою.

Перепрошивка системи з використанням ненадійних або модифікованих прошивок також може призвести до витоку інформації, оскільки ці прошивки можуть містити шкідливі програми або вразливості, які можуть бути використані зловмисниками.

Витоки інформації засобами фізичного доступу до телефону можуть включати наступне:

Зловмисник, який має фізичний доступ до телефона, може отримати доступ до всієї збереженої інформації на пристрої, такої як фотографії, відео, повідомлення, контакти, електронні листи тощо. Зловмисник може встановити шпигунське ПЗ на телефон без відома користувача. Це ПЗ може стежити за активністю користувача, записувати клавіші, переглядати повідомлення та іншу конфіденційну інформацію.

Якщо телефон не захищений паролем або використовує прості паролі, зловмисник може отримати доступ до телефону і всіх збережених в ньому облікових записів, таких як соціальні мережі, електронна пошта, банківські акаунти тощо. Зловмисник може скопіювати SIM-карту і отримати доступ до всіх дзвінків і повідомлень, які надходять на номер телефону.

Якщо зловмисник отримав фізичний доступ до вашого телефону, він може спробувати використати методи атаки, такі як зламання пароля, використання експлойтів для отримання

доступу до системи або навіть фізичне пошкодження пристрою для отримання доступу до даних. Крім того, можуть бути використані методи перехоплення на кшталт «комплекту смурфів» (Smurf Suite) для Вкл./Викл. смартфона без відома Власника (Dreamy), відстеження Власника смартфона з більшою точністю за допомогою механізму геолокації (Tracker), управління мікрофоном смартфона для підслуховування того, що відбувається навколо смартфона (Curious) [15].

Для запобігання витокам інформації засобами фізичного доступу до телефону важливо встановлювати надійний пароль чи використовувати інші методи аутентифікації, такі як відбитки пальців або розпізнавання обличчя. Також рекомендується ніколи не залишати телефон без нагляду та використовувати функції шифрування даних, якщо вони доступні на пристрої.

Ні для кого не секрет, що компанії-велетні як Google чи Amazon збирають інформацію про користувачів своїх послуг, але роблять це «конфіденційно» для користувача, запевняючи того в цілісності даних, доступ до яких він сам надає [16]. Застосунки, такі як Instagram, TikTok та YouTube, пропонують рекомендації до відео на основі вподобань користувача, в незалежності від того, чи шукав він певну інформацію в застосунку, чи просто розмовляв з кимось, тримаючи телефон поряд.

Це відбувається через дозволи, які користувач сам надає компаніям, встановлюючи застосунки. При завантаженні на пристрій будь-якого застосунку він спитає у користувача надати йому доступ до певних функцій телефона користувача, тим самим відкриваючи можливість для застосунку на крадіжку інформації. Проте, з іншого боку, певні застосунки просто відмовляються виконувати свої функції без надання їм доступу. Саме через це треба уважно слідкувати, що і якому застосунку дозволяти зчитувати з свого телефона, але відмовлятися від усього теж не треба, адже на 100 % це не захистить користувача, а залишити без функціоналу застосунку може. В такому разу необхідно знайти пункт в налаштуваннях телефону «Захист конфіденційності», переглянути налаштування усіх пунктів і розібратися, які застосунки використовують певні доступи, котрі їм можна було б обмежити задля меншого витоку (рис. 2).

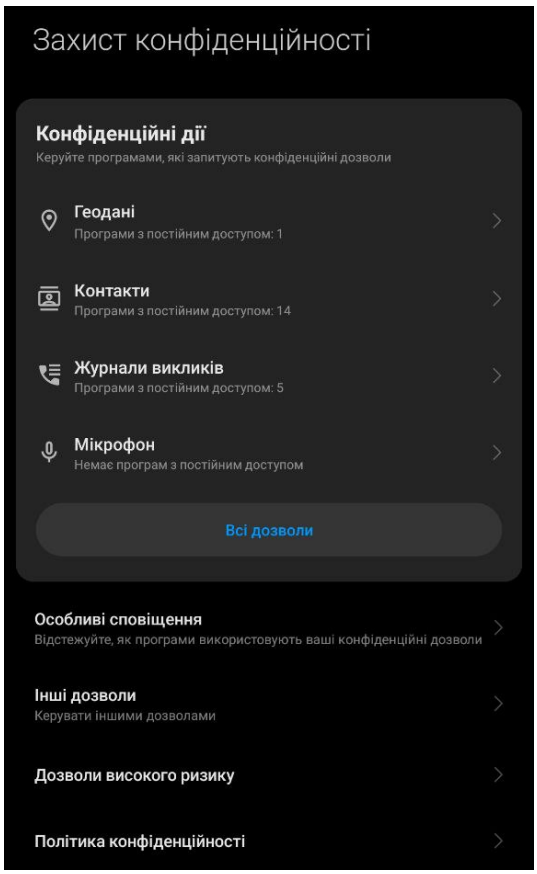

Рис. 2 – Налаштування «Захисту конфіденційності»

Як можна побачити на рис. 3, Instagram, Telegram, Viber та ще кілька застосунків мають доступ до списку контактів, а отже, користуючись цими застосунками, можливо бачити знайомих з

книги контактів одразу в них. Але тим самим власники цих застосунків вже можуть мати базу контактів власника у себе в офісі, а можливо навіть і в офісі у злодіїв, котрі скористалися нагодою вкрасти дані на етапі передачі з пристрою на сервер.

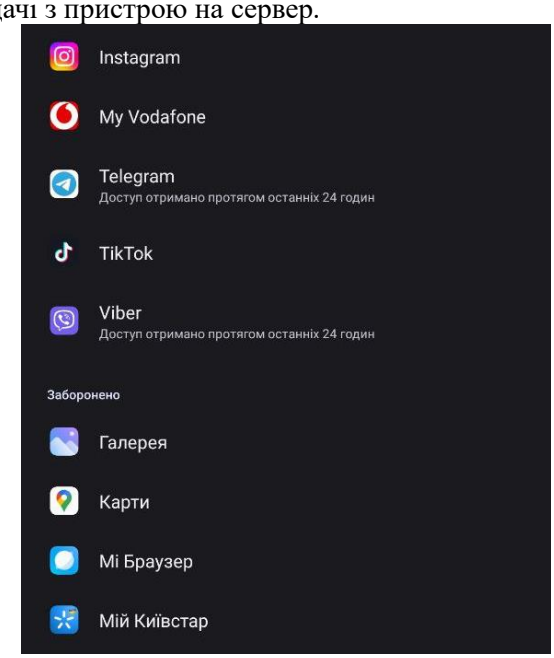

Рис. 3. Доступ до розділу «Контакти» на телефоні

Ну і останнє, але не найменше, – це витоки інформації шляхом фішингу. Все більше і більше людей стає популярними в наш час, і вони хочуть заохотити свою авдиторію роблячи розіграші і тому подібні конкурси. Тут на арену виступають «рибаки», котрі під прикриваючись вашим улюбленим блогером виманюють з вас данні карток, паролі і т. д. Ця схема працює не тільки в даному кейсі, а і під прикриттям банків, колекторів, розробників й т. ін.

Занотуймо основні способи:

Зловмисники можуть відправляти електронні листи, що виглядають як повідомлення від відомих компаній чи сервісів. У таких повідомленнях можуть міститися посилання на фальшиві веб-сайти, які виглядають як офіційні, але насправді призначені для крадіжки особистої інформації, такої як паролі або дані банківських карток.

Зловмисники також можуть використовувати соціальні мережі для поширення фішингових повідомлень, спробуючи отримати особисту інформацію від користувачів через маніпуляцію або використання підступних методів.

Зловмисники можуть відправляти фішингові SMS з повідомленнями про виграші, акції або інші привабливі пропозиції. Ці повідомлення можуть містити посилання на фальшиві веб-сайти або номери телефонів, що намагаються витягнути особисту інформацію від отримувачів.

Деякі шахраї можуть створювати фішингові застосунки або ігри, що виглядають як популярні або цікаві програми, але насправді призначені для збору особистої інформації з пристрою користувача.

Шахраї також можуть використовувати соціальну інженерію, щоб отримати особисту інформацію користувача, наприклад, видаючи себе під представників банків, компаній або інших організацій та запитуючи конфіденційні дані.

Висновки та перспективи подальшого дослідження. В результаті роботи було оглянуто ризики витоку інформації через мобільні платформи, представлено декілька прикладів різних видів витоку, розглянуто, чому і які дії можуть стати ключовими у втраті особистих даних через телефон, та розглянуто методи протидії певним з цих методів. Запропоновано практичні рекомендації щодо зменшення ризиків безпеки при використанні мобільних застосунків як для користувачів, так і для розробників, а саме:

а) обробляти дані на пристрої, де це можливо. В iOS, наприклад, можливо скористатися перевагами Apple Neural Engine і користувацьких моделей CreateML для обробки даних прямо на пристрої, щоб уникнути тривалих і потенційно ризикованих звертань до віддаленого сервера;

б) використовувати визначені системою засоби захисту конфіденційності та дотримуватися передових методів безпеки. Наприклад, в iOS 15 і новіших версіях можна покластися на CloudKit, щоб забезпечити шифрування та керування ключами для додаткових типів даних, як-от рядків, чисел і дат;

в) використовувати резервне копіювання важливих даних як на самому телефоні або інших зовнішніх носіях (нп., за допомогою iTunes для iPhone або Samsung Smart Switch для Samsung Galaxy), так і в хмарному сховищі, як-от Google Drive, iCloud, OneDrive і Dropbox;

г) запитувати дозвіл до:

– особистих даних, включаючи інформацію про місцезнаходження, стан здоров'я, фінанси, контакти та іншу особисту інформацію;

– контенту, створеного користувачами, як-от електронні листи, повідомлення, дані календаря, контакти, інформація про ігри, діяльність Apple Music, дані HomeKit, аудіо-, відео- та фотовміст;

– захищених ресурсів, як-от периферійні пристрої Bluetooth, функції домашньої автоматизації (IoT- пристрої та компоненти «розумного будинку»), з'єднання Wi-Fi та локальні мережі;

– такі можливостей пристрою, як камера, мікрофон тощо;

д) запитувати лише ті дані, які дійсно потрібні для роботи певного застосунку. Якщо запитувати більше даних, ніж потребує функція, користувачам буде важко довіряти такому застосунку.

Слід підкреслити, що будь-яке програмне забезпечення для мобільних платформ повинно мати документацію або навіть коротку анотацію, якій чітко описано, як програма використовує можливості, дані або ресурси, які запитує. Крім того, підтвердженням, що програма безпечна для використання, може бути підписання програми дійсним ідентифікатором розробника.

Список бібліографічного опису

1. Truță F. Top reasons why consumers shun mobile security apps. Publ. April 16, 2024. URL: https://www.bitdefender.co.uk/blog/hotforsecurity/top-reasons-why-consumers-shun-mobile-security-apps/ (Last accessed: 03.05.2024).
2. Kadir A. F. A., Lashkari A. H., Firoozjaei M. D. Mobile application security. *In book: Understanding Cybersecurity on Smartphones.* Jan. 2024. P. 89–101. DOI: 10.1007/978-3-031-48865-8_6.
3. Balapour A., Nikkhah H. R., Sabherwal R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management.* 2020. Vol. 52, No. 102063. DOI: 10.1016/j.ijinfomgt.2019.102063.
4. Osman T., Mannan M., Youssef A., Hengartner U., Youssef A. Securing applications against side-channel attacks through resource access veto. *Digital Threats: Research and Practice.* Dec. 2020. Vol. 1, No. 4. Article 22. 29 p. DOI: 10.1145/3416124.
5. Lei T., Qin Z., Zhibo W., Li Q., Dengpan Ye. EveDroid: Event-aware Android malware detection against model degrading for IoT devices. *IEEE Internet of Things Journal.* Aug. 2019. Vol. 6(4). P. 6668–6680. DOI: 10.1109/JIOT.2019.2909745.
6. Behavior changes: all apps. Android 9 (API level 28). Publ. Mar. 01, 2024. URL: https://developer.android.com/about/versions/pie/android-9.0-changes-all (Last accessed: 03.05.2024).
7. Turner D. Capturing Audio in Android Q. Publ. July 03, 2019. URL: https://android-developers.googleblog.com/2019/07/capturing-audio-in-android-q.html (Last accessed: 03.05.2024).
8. Privacy changes in Android 10. Publ. Apr. 30, 2024. URL: https://developer.android.com/about/versions/10/privacy/changes#app-access-device-location (Last accessed: 03.05.2024).
9. About privacy and Location Services in iOS, iPadOS, and watchOS. Publ. Mar. 27, 2024. URL: https://support.apple.com/en-us/102515 (Last accessed: 03.05.2024).
10. Privacy in Android 11. URL: https://developer.android.com/about/versions/11/privacy (Last accessed: 03.05.2024).
11. Spreitzer R., Moonsamy V., Korak T., Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Commun. Surveys Tutor.* 2018. Vol. 20, Is. 1. P. 465–488.
12. Xu F., Diao W., Li Z., Chen J., Zhang K.. BadBluetooth: Breaking Android security mechanisms via malicious Bluetooth peripherals. *Proc. of the Network and Distributed System Security Symposium (NDSS'19)*, San Diego, CA, USA, 24–27 Feb. 2019. DOI: 10.14722/ndss.2019.23482.
13. Ba Z., Zheng T., Zhang X., Qin Z., Li B., Liu X., Ren K. Learning-based practical smartphone eavesdropping with built-in accelerometer. *Proc. of the Network and Distributed System Security Symposium (NDSS'20)*, San Diego, CA, USA, 23–26 Feb. 2020. DOI: 10.14722/ndss.2020.240762020.
14. Simon L., Anderson R. PIN Skimmer: Inferring PINs through the camera and microphone. *Proc. of the 3rd ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM'13).* 08 Nov. 2013. P. 67–78. DOI: 10.1145/2516760.2516770.

15. UK spies can hack smartphones: Snowden. Publ. Oct. 05, 2015. URL: https://phys.org/news/2015-10-uk-spies-hack-smartphones-snowden.html (Last accessed: 03.05.2024).
16. Відсота Д. Як глобальні медіа та IT-платформи збирають персональні дані користувачів. Опубл. 16 лютого, 2021. URL: https://biz.nv.ua/ukr/experts/osobisti-dani-ta-socmerezhi-facebook-mesendzheri-ostanni-novini-50142213.html (дата звернення: 03.05.2024).

References

1. Truță F. Top reasons why consumers shun mobile security apps. Publ. April 16, 2024. URL: https://www.bitdefender.co.uk/blog/hotforsecurity/top-reasons-why-consumers-shun-mobile-security-apps/ (Last accessed: 03.05.2024).
2. Kadir A. F. A., Lashkari A. H., Firoozjaei M. D. Mobile application security. *In book: Understanding Cybersecurity on Smartphones.* Jan. 2024. P. 89–101. DOI: 10.1007/978-3-031-48865-8_6.
3. Balapour A., Nikkhah H. R., Sabherwal R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management.* 2020. Vol. 52, No. 102063. DOI: 10.1016/j.ijinfomgt.2019.102063.
4. Osman T., Mannan M., Youssef A., Hengartner U., Youssef A. Securing applications against side-channel attacks through resource access veto. *Digital Threats: Research and Practice.* Dec. 2020. Vol. 1, No. 4. Article 22. 29 p. DOI: 10.1145/3416124.
5. Lei T., Qin Z., Zhibo W., Li Q., Dengpan Ye. EveDroid: Event-aware Android malware detection against model degrading for IoT devices. *IEEE Internet of Things Journal.* Aug. 2019. Vol. 6(4). P. 6668–6680. DOI: 10.1109/JIOT.2019.2909745.
6. Behavior changes: all apps. Android 9 (API level 28). Publ. Mar. 01, 2024. URL: https://developer.android.com/about/versions/pie/android-9.0-changes-all (Last accessed: 03.05.2024).
7. Turner D. Capturing Audio in Android Q. Publ. July 03, 2019. URL: https://android-developers.googleblog.com/2019/07/capturing-audio-in-android-q.html (Last accesse: 03.05.2024).
8. Privacy changes in Android 10. Publ. Apr. 30, 2024. URL: https://developer.android.com/about/versions/10/privacy/changes#app-access-device-location (Last accessed: 03.05.2024).
9. About privacy and Location Services in iOS, iPadOS, and watchOS. Publ. Mar. 27, 2024. URL: https://support.apple.com/en-us/102515 (Last accessed: 03.05.2024).
10. Privacy in Android 11. URL: https://developer.android.com/about/versions/11/privacy (Last accesse: 03.05.2024).
11. Spreitzer R., Moonsamy V., Korak T., Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Commun. Surveys Tutor.* 2018. Vol. 20, Is. 1. P. 465–488.
12. Xu F., Diao W., Li Z., Chen J., Zhang K.. BadBluetooth: Breaking Android security mechanisms via malicious Bluetooth peripherals. *Proc. of the Network and Distributed System Security Symposium (NDSS'19)*, San Diego, CA, USA, 24–27 Feb. 2019. DOI: 10.14722/ndss.2019.23482.
13. Ba Z., Zheng T., Zhang X., Qin Z., Li B., Liu X., Ren K. Learning-based practical smartphone eavesdropping with built-in accelerometer. *Proc. of the Network and Distributed System Security Symposium (NDSS'20)*, San Diego, CA, USA, 23–26 Feb. 2020. DOI: 10.14722/ndss.2020.240762020.
14. Simon L., Anderson R. PIN Skimmer: Inferring PINs through the camera and microphone. *Proc. of the 3rd ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM'13).* 08 Nov. 2013. P. 67–78. DOI: 10.1145/2516760.2516770.
15. UK spies can hack smartphones: Snowden. Publ. Oct. 05, 2015. URL: https://phys.org/news/2015-10-uk-spies-hack-smartphones-snowden.html (Last accessed: 03.05.2024).
16. Vidsota D. How global media and IT platforms collect users' personal data. Publ. Feb. 16, 2021. URL: https://biz.nv.ua/ukr/experts/osobisti-dani-ta-socmerezhi-facebook-mesendzheri-ostanni-novini-50142213.html (Last accessed: 03.05.2024).