УДК 343.9
DOI https://doi.org/10.32782/pyuv.v2.2024.20

О. П. Ващук
orcid.org/0000-0003-3161-2870
доктор юридичних наук,професор,
професор кафедри криміналістики,детективної та оперативно-розшукової діяльності
Національного університету «Одеська юридична академія»

МОДЕЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ ДЛЯ МОБІЛЬНИХ ДОДАТКІВ В ПРАВООХОРОННИХ ОРГАНАХ

Вступ. У епоху швидкого розвитку цифрових технологій, вчені постійно шукають шляхи до використання інновацій для підвищення ефективності роботи правоохоронних органів. Мобільні додатки, які нададуть слідчим доступ до необхідних інструментів та інформації безпосередньо на місці подій, стають невід'ємною вимогою сучасної правоохоронної практики. Водночас, з розвитком цих технологій зростає й кількість потенційних кіберзагроз та вразливостей, що можуть піддавати ризику конфіденційність та цілісність такої інформації.

Постановка завдання. У сучасному світі, де технології швидко розвиваються та займають все більше місце в кожній сфері людської діяльності, правоохоронні органи не можуть залишатися осторонь цих процесів. Використання мобільних додатків слідчими в поліції відкриває нові можливості для підвищення ефективності розслідувань, оперативності реагування та поліпшення взаємодії в команді. Однак, разом з новими можливостями з'являються й нові виклики, зокрема, пов'язані з безпекою даних.

Функціональні мобільні додатки в правоохоронних органах спрямовані на збирання, обробку та зберігання величезних обсягів конфіденційної інформації: від персональних даних громадян до деталей про хід розслідувань. Ризики, пов'язані з їх витоком або несанкціонованим доступом, мають серйозні наслідки, включаючи порушення прав людини, підрив довіри громадськості до правоохоронних органів та загрозу національній безпеці. Зовнішні загрози, такі як хакерські атаки, та внутрішні загрози, включно з можливістю зловживань з боку персоналу, потребують складної багаторівневої системи захисту. Враховуючи, що слідчі часто працюють в полі та будуть використовувати мобільні пристрої для доступу до даних в різних локаціях, особливої уваги заслуговує захист даних у транзиті та їх захист на самому пристрої.

Таким чином, актуальність впровадження мобільних додатків у роботу правоохоронних органів супроводжується критичною потребою ретельного моделювання загроз та оцінки ризиків, що забезпечить не тільки ефективність роботи слідчих, але й високий рівень захисту відомостей, що є запорукою правової безпеки та дотримання основоположних прав і свобод.

Метою є дослідження та аналіз потенційних загроз і вразливостей, які стосуються мобільних додатків для слідчих. В статті визначаються основні зовнішні та внутрішні ризики, асоційовані з такими додатками та надаються пропозиції до їх вирішення.

Аналіз останніх досліджень і публікацій. В цьому напрямку досліджуються новітні технології та інноваційні рішення для покращення ефективності розслідувань [1, 2, 3, 4, 5, 6]. Останні роботи зосереджуються на використанні штучного інтелекту для аналізу великих обсягів даних, розробці алгоритмів для автоматичного розпізнавання образів та текстів, а також на покращенні геолокаційних функцій [7, 8, 9]. Увага в цій області приділяється методам захисту даних, що збираються та обробляються, зокрема виділяються такі теми, як шифрування даних, захист передачі даних, аутентифікація користувачів та управління доступом [10, 11, 12, 13, 14]. Результати досліджень часто звертають увагу на вразливості технологій і пропонують рекомендації щодо їх усунення [15, 16, 17, 18, 19], акцентується на важливості дотримання правових та етичних норм при використанні нових технологій в правоохоронній сфері [20, 21, 22, 23, 24]. Обговорюються питання конфіденційності, зберігання персональних даних та їх використання [25, 26]. Аналізуються зміни в процедурах розслідування, взаємодії між слідчими та іншими відомствами, а також на загальну ефективність і швидкість виконання завдань [27, 28, 29]. Обговорюються технічні проблеми, з якими можуть зіштовхнутися розробники, включно з обмеженнями апаратного забезпечення, необхідністю інтеграції з існуючими системами та управлінням великими обсягами даних [30, 31, 32, 33].

Результати дослідження. Захист інформації в мобільних додатках для слідчих, є критично важливим, оскільки загрози можуть прийти з багатьох джерел. Загрози можна класифікувати на зовнішні та внутрішні, кожна з яких має

свої специфічні ризики та потребує особливих заходів захисту.

Зовнішні загрози становлять атаки, які ініціюються ззовні правоохоронного органу або системи, є різноманітними і включають:

– хакерські атаки (хакерські атаки стають все більш витонченими і складними, з використанням таких методів, як масштабовані DDoS атаки, експлуатація день-нуль вразливостей і застосування шкідливого програмного забезпечення. Ці атаки часто спрямовані на отримання доступу до конфіденційної інформації, включаючи особисті дані, інформацію про розслідування та внутрішні комунікації);

– фішинг (фішингові атаки часто використовують інженерію соціальних мереж для обману жертв, щоб ті розкрили паролі, банківські дані або іншу важливу інформацію. Зловмисники часто вдаються до маскування під легітимні джерела, такі як технічна підтримка або відділ кадрів, щоб здаватися переконливими);

– спам-атаки (спам може бути використаний для поширення шкідливого програмного забезпечення через вкладені файли або посилання, які ведуть на інфіковані веб-сайти. Велика кількість спаму перевантажує системи, що знижує ефективність робочих процесів та відволікає від завдань).

Внутрішні загрози виникають внаслідок дій або недбалості користувачів всередині правоохоронного органу, що включає:

– несанкціонований доступ. Недостатньо складні паролі легко можуть бути зламані за допомогою брутфорс атак та внутрішнє зловживання (працівники з доступом можуть використовувати свої повноваження для особистої вигоди або вигоди для третіх осіб та працівників, які не мають необхідних дозволів, отримують доступ до конфіденційної інформації, що може призвести до її неправомірного використання або розголошення);

– помилки програмного забезпечення: баги (недоліки в програмуванні відкривають вразливості, які зловмисники використовують для доступу до систем або їх злому); оновлення (відсутність своєчасних оновлень залишає систему вразливою перед відомими загрозами); витік інформації (недбалість (випадкове розкриття інформації через втрату пристроїв або небезпечне зберігання даних) або зловмисне розголошення (свідомий витік конфіденційної інформації, який може бути спричинений особистими мотивами або зовнішнім впливом).

У контексті кібербезпеки мобільних додатків для використання правоохоронними органами, існують ключові технічні вразливості, що можуть піддавати системи ризикам. Розуміння цих слабких місць є важливим для вжиття ефективних заходів забезпечення безпеки:

– детальний аналіз технічних вразливостей. Недостатність шифрування. Проблема: дані, що передаються між мобільним додатком та сервером, а також дані, що зберігаються на мобільному пристрої, можуть бути не захищені достатньо, що робить їх вразливими до перехоплення або несанкціонованого доступу. Рішення: шифрування даних у транзиті (використання сучасних протоколів шифрування, таких як TLS 1.3 (Transport Layer Security), який забезпечує захист даних під час передачі, за допомогою нового шифрування каналу зв'язку); шифрування даних на пристрої (застосування алгоритмів шифрування, таких як AES-256 (Advanced Encryption Standard), для забезпечення безпеки даних, збережених на мобільному пристрої, навіть у випадку фізичного доступу до пристрою);

– вразливості в API (Application Programming Interface), що використовуються мобільними додатками для зв'язку з серверами, можуть містити вразливості, що дозволять зловмисникам виконувати несанкціоновані дії або отримувати доступ до конфіденційної інформації. Рішення: захист API (використання технік безпеки на стороні сервера, таких як OAuth для управління доступом, HTTPS для шифрування даних та використання межових маркерів безпеки (security tokens) для забезпечення автентичності запитів); регулярне аудитування і тестування (проведення пентестів і аудитів безпеки API для виявлення та усунення потенційних вразливостей);

– проблеми з аутентифікацією та контролем доступу (слабкі аутентифікаційні механізми та політики контролю доступу дозволяють неавторизованим особам отримувати доступ до чутливих даних або системних ресурсів). Рішення: багатофакторна аутентифікація (MFA) (впровадження MFA для всіх користувачів системи, що значно знижує ризик несанкціонованого доступу); мінімізація привілеїв (застосування принципу найменшого привілею, згідно з яким користувачам надаються лише ті права доступу, які строго необхідні для виконання їхніх завдань);

– проблеми з програмним забезпеченням (баги в програмному забезпеченні створюють потенційні вразливості, які зловмисники використовують для атак на систему). Рішення: регулярне оновлення програмного забезпечення (своєчасне впровадження патчів безпеки та оновлень для виправлення відомих вразливостей); розробка за принципами безпеки (впровадження практик безпечного кодування та тестування програмного забезпечення на ранніх етапах розробки для мінімізації наявності багів і помилок).

Моделювання атак є критичним компонентом стратегії безпеки будь-яких мобільних додатків, що допомагає ідентифікувати та усувати потен-

ційні вразливості до того, як зловмисники зможуть їх використати. Ключові етапи, що входять до процесу моделювання атак такі:

1. Визначення об'єктів атаки (першим кроком є визначення активів, які є потенційними цілями для атак. Це можуть бути дані користувачів, конфіденційна інформація про розслідування, логін-дані слідчих та інша чутлива інформація, що зберігається або передається через мобільний додаток).

2. Розробка сценаріїв атак (на основі визначених активів розробляються детальні сценарії потенційних атак. Кожен сценарій моделює конкретний тип загрози або атаку, які включає:

– SQL ін'єкції (атаки, які використовують вразливості в базах даних для введення шкідливого коду або вилучення даних);

– перехоплення даних (сценарії, де дані перехоплюються під час їх передачі через незахищені мережі);

– атаки, в яких перехоплюється та змінюється комунікація між двома користувачами без їхнього відома;

– фішинг (методи, які використовують соціальну інженерію для отримання конфіденційної інформації від користувачів) [34, 35, 36, 37].

3. Тестування системи на вразливість (кожен сценарій атаки використовується для проведення тестів на проникнення, які дозволяють перевірити реакцію мобільного додатка на спробу атаки, що допомагає виявити слабкі місця в захисті та ефективності наявних заходів безпеки. Тестування включає:

– автоматичні та ручні тести (використання автоматизованих інструментів та ручних методик для виявлення вразливостей);

– симуляція атак (виконання контрольованих атак згідно з розробленими сценаріями для перевірки реакції системи);

– оцінка реакції системи (аналіз часу реакції на атаку, ефективності захисних механізмів та здатності системи відновлювати нормальну роботу після атак).

4. Вдосконалення захисних стратегій (на основі результатів тестування розробляються рекомендації щодо покращення системи безпеки мобільного додатка, що включає за необхідності, технічні вдосконалення, зміни в програмному забезпеченні, а також навчання персоналу з питань кібербезпеки).

Моделювання атак та тестування вразливостей мобільних додатків є необхідними для забезпечення їхньої безпеки в умовах постійно зростаючих кіберзагроз, зокрема в контексті правоохоронної діяльності, де захист інформації має вирішальне значення.

Аналіз відмовостійкості системи має на меті визначити, наскільки добре мобільні додатки та їх інфраструктура можуть витримувати і відновлюватися після різних видів кібератак або технічних збоїв. Основна мета полягає в тому, щоб забезпечити неперервність служби навіть під час серйозних інцидентів. Детальний опис ключових елементів цього процесу полягає у такому:

1. Сценарії симуляції відмов (розробка сценаріїв, які симулюють різні види відмов, включаючи):

1.1. Фізичні збої обладнання (тестування на відмову критичних компонентів, таких як сервери та мережеве обладнання);

1.2. Відмови програмного забезпечення (симуляція збоїв у програмному забезпеченні, які викликані помилками коду або несумісностями);

1.3. Атаки на мережеву інфраструктуру (включають симуляції DDoS атак, які намагаються перевантажити систему та змусити її зупинитися).

2. Тестування відновлення після відмов. Оцінка того, наскільки швидко та ефективно система відновлює свої операції після несподіваних збоїв або атак:

2.1. Відновлення даних (тестування процедур відновлення даних з резервних копій для переконання в тому, що критична інформація не втрачена);

2.2. Перемикання на резервні системи (перевірка механізмів автоматичного перемикання на резервне обладнання або сервери в іншому місцерозташуванні);

2.3. Оцінка резервування інфраструктури (оцінка та підготовка резервної інфраструктури для забезпечення роботи додатків у випадку збою основної системи).

3. Географічне розподілення (розміщення серверів у різних локаціях для зниження ризиків, пов'язаних з природними катастрофами або регіональними перебоями).

4. Обробка навантаження (використання балансувальників навантаження та інших технологій для розподілу трафіку та запитів, забезпечуючи стабільність і доступність сервісів).

5. Навчання персоналу та регулярні тренування (навчання з процедур відновлення (регулярне проведення тренінгів для технічних команд з питань ефективного і швидкого реагування на інциденти); симуляції інцидентів (проведення планових симуляцій інцидентів для перевірки готовності команд та оптимізації процесів реагування).

Аналіз відмовостійкості є невід'ємною частиною стратегії кіберзахисту, яка допомагає не лише ідентифікувати потенційні ризики та вразливості, а й забезпечує готовність системи до їх ефективного усунення. Це забезпечує неперервність діяльності та захист критично важливих

даних, що має життєво важливе значення для правоохоронних органів.

Висновки. В даній статті було досліджено моделювання загроз та оцінку ризиків для мобільних додатків, які можуть використовуватися в правоохоронних органах, де завдяки швидкому розвитку технологій, правоохоронні органи вже зовсім скоро почнуть інтегрувати мобільні додатки в свою роботу, що з одного боку підвищить ефективність та оперативність їхніх дій, але з іншого – породить значні виклики пов'язані з безпекою даних.

Основним внеском статті є аналіз потенційних зовнішніх та внутрішніх загроз, які впливають на безпеку мобільних додатків. Зовнішні загрози включають хакерські атаки, фішинг, та спам-атаки, які намагаються викрасти або пошкодити цінну інформацію. Внутрішні загрози включають несанкціонований доступ, помилки в програмному забезпеченні та потенційний витік інформації через недбалість або зловмисні дії працівників.

В статті також розглядається важливість технічних заходів безпеки, таких як шифрування даних у транзиті та на пристроях, захист API, а також ретельні методи аутентифікації та контролю доступу. Такі заходи критично важливі для забезпечення цілісності та конфіденційності персональних даних та інформації про розслідування.

Додатково, в статті було визначено потребу в ретельному моделюванні загроз та аналізі відмовостійкості, що дозволяє правоохоронним органам ефективно реагувати на інциденти та забезпечувати безперервність своєї роботи. Аналіз показав, що регулярне тестування та симуляції відмов не тільки виявляють вразливі місця, але й сприяють оптимізації відповідей на інциденти.

Враховуючи обговорені аспекти, підкреслено, що впровадження мобільних додатків у правоохоронну діяльність має супроводжуватися комплексним підходом до безпеки, що включає ретельне планування, постійний моніторинг та швидке реагування на потенційні загрози. Такий підхід забезпечить не тільки ефективність роботи слідчих, але й високий рівень захисту інформації, що є запорукою правової безпеки та дотримання прав і свобод громадян.

Література

1. Благута Р. І. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Благута Р. І., Мовчан А. В. Львів: ЛьвДУВС. 2020. 256 с.

2. Журавель В. А., Шепітько В. Ю. Розвиток криміналістики та судової експертизи в Україні: наближення до єдиного європейського простору. Правова наука України: сучасний стан, виклики та перспективи розвитку. Монографія. Харків. 2021. С. 651–669.

3. Шепітько В. Ю. Інновації в криміналістиці як віддзеркалення розвитку науки. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матер. міжнар. круглого столу (Харків, 12 грудня 2019 р.). Харків: Право. 2019. С. 147–150.

4. Дуфенюк О. М., Марко О. І. Інноваційні технології 3D-сканування в криміналістичній діяльності. *Порівняльно-аналітичне право.* 2018. № 1. С. 313–315.

5. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія. Кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Х.: ВА «Апостіль». 2017. 260 с.

6. Інформаційне забезпечення юридичної діяльності: підручник. Кол. авт.; за заг. ред. В. Б. Вишні. Дніпро: ДДУВС. 2019. 228 с.

7. Климчук М. П., Кунтій А. І. Виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Вип. 3 (9). С. 111–118.

8. Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. *Криміналістика і судова експертиза.* 2015. Вип. 60. С. 117–125.

9. Поляк Ю. П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його результатів під час досудового розслідування: дисертація на здобуття ступеня доктора філософії (081 – Право). Львів: Львівський державний університет внутрішніх справ. 2022. 230 с.

10. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2013. № 5. С. 256–260.

11. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2022. № 3 (99). С. 283–294.

12. Думчиков М. О. Процеси діджиталізації і криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза.* 2020. Вип. 65. С. 100–108.

13. Konovalova V. O., Shevchuk V. M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. Advanced discoveries of modern science: experience, approaches and innovations: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific Conference, January 20, 2023. pp. 73–77.

14. Shevchuk V. M. Criminalistic didactics in modern conditions of war and digital technologies. Scientific Collection «InterConf+», 29(139) : with the Proceedingsof the 4thInternational Scientific and Practical Conference «Scientific Goals and Purposes in XXI Century» (January 19-20, 2023; Seattle, USA). 2023. pp. 121–140.

15. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник. К.: Кондор. 2004. 384 с.

16. Кормич Б. А. Інформаційне право: підручник. Х.: БУРУН і К. 2011. 334 с.

17. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Х.: Право. 2022. 408 с.

18. Павлова Т. О. Діджиталізація кримінального процесу: в Україні планують перевести провадження в електронний формат. URL: https://uazmi.org/news/post/bReTCc20Q04a1jCN6zj9y2.

19. Столітній А. Концепція електронного кримінального провадження в Україні. *Вісник Національної академії прокуратури України.* 2018. № 4(56). С. 24–35.

20. Літкевич Д. О. Теоретико-правові основи використання досягнень науково-технічного прогресу у кримінальній процесуальній формі: дис. ... канд. юрид. наук: 12.00.09. Х., 2020. 266 с.

21. Тетерятник Г. К. Кримінальне провадження в умовах надзвичайних правових режимів: теоретико-методологічні та праксеологічні основи: монографія. Одеса: Видавничий дім «Гельветика». 2021. 500 с.

22. Гуртієва Л. М. Етичний аспект кримінально-процесуальних відносин слідчого; Етичні основи діяльності слідчого : дис. ... канд. юрид. наук. Одеса. 2008. 201 с.

23. Гіренко С. П. Змістовний компонент формування конфліктологічної культури майбутніх слідчих ОВС у фаховій підготовці. *Вісник Національного університету оборони України*. 2013. Вип. 6 (37). С. 42–47.

24. Баулін О. В. Процесуальна самостійність і незалежність слідчого та їх правові гарантії. Монографія. О. В. Баулін, Н. С. Карпов. К.: Національна академія внутрішніх справ України. 2001. 232 с.

25. Карпушин С. Ю. Проведення слідчих (розшукових) дій: дис. ... канд. юрид. наук: 12.00.09. К. 2016. 210 с.

26. Чигрина Л. Г. Перспективи запровадження міжнародного досвіду електронного кримінального провадження в Україні. *Прикарпатський юридичний вісник.* Випуск. 2(23). 2018. С. 72–76.

27. Когутич І. І. Про окремі виклики криміналістики та шляхи її усталення. *Криміналістика і судова експертиза.* 2020. Вип. 65. С. 5–19.

28. Гловюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу IX-1 Кримінального процесуального кодексу України (станом на 03.05.2022 р.). Видання 2. Дніпро-Львів-Одеса-Харків. 2022. 58 с.

29. Гресь Ю. О. Формування технологічного підходу у криміналістичній тактиці: дис. ... канд. юрид. наук: 12.00.09. Одеса. 2017. 255 с.

30. Говоруха В. І., Степанов В. А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право.* 2020. № 3 (34). С. 69–74.

31. Голубєв В. О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів. Під ред. О. П. Снігерьова. Запоріжжя: ВЦ «Павел». 1998. 144 с.

32. Тіщенко В. В. Криміналістичне розпізнавання в розслідуванні злочинів. 2020/5/15. Одеса: Гельветика.

33. Шепітько В. Ю., Шепітько М. В. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право. 2021. 508 с.

34. What is a cyber attack? URL: https://www.techtarget.com/searchsecurity/definition/cyber-attack.

35. Denial-of-Service (DoS) Attack: Examples and Common Targets. URL: https://www.investopedia.com/terms/d/denial-service-attack-dos.asp.

36. Cyber Crime – Identity Theft. URL: https://www.geeksforgeeks.org/cyber-crime-identity-theft/

37. Man in the Middle (MITM) Attacks. URL: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks

Анотація

Ващук О. П. **Моделювання загроз та оцінка ризиків для мобільних додатків в правоохоронних органах.** – Стаття.

Стаття присвячена моделюванню загроз та оцінці ризиків для мобільних додатків у правоохоронних органах, висвітлюючи актуальність і необхідність інтеграції мобільних технологій в повсякденну діяльність правоохоронних органів. Зростання залежності від цифрових технологій вимагає від правоохоронців адаптації до сучасних цифрових інструментів, які можуть значно підвищити ефективність і швидкість розслідувань, а також покращити координацію і комунікацію в межах команд. Однак, разом з перевагами, які надають мобільні додатки, з'являється і велика кількість ризиків, пов'язаних із захистом конфіденційної інформації.

Стаття акцентує увагу на потенційних зовнішніх і внутрішніх загрозах, які можуть компрометувати безпеку збереження та передачі даних. Зокрема, аналізується, як хакерські атаки, фішинг, спам та інші кіберзагрози можуть нанести шкоду системам зберігання даних. Також обговорюються вразливості, що виникають внаслідок можливих зловживань з боку працівників або недбалості, які можуть призвести до несанкціонованого доступу або витоку даних.

Пропонується комплексний підхід до оцінки ризиків, який включає моделювання потенційних атак та тестування систем на вразливість. Увага приділяється методам шифрування даних, захисту передачі даних, а також розробці ефективних стратегій аутентифікації та контролю доступу, що спрямовані на мінімізацію можливості неавторизованого доступу та забезпечення цілісності інформації.

Результати дослідження підкреслюють необхідність регулярного оновлення заходів безпеки та проведення аудитів, щоб відповідати зростаючим загрозам в цифровому середовищі. В статті закликається до більшої уваги до цих питань, щоб забезпечити не тільки ефективність, але й законність роботи правоохоронних органів в контексті використання мобільних додатків.

Ключові слова: моделювання загроз, оцінка ризиків, мобільний додаток, слідчий, правоохоронний орган, криміналістика, кримінальний процес.

Summary

Vashchuk O. P. **Treat modelling and risk assessment for law enforcement mobile applications.** – Article.

The article is devoted to threat modelling and risk assessment for mobile applications in law enforcement agencies, highlighting the relevance and necessity of integrating mobile technologies into the day-to-day activities of law enforcement agencies. The growing dependence on digital technologies requires law enforcement officers to adapt to modern digital tools that can significantly increase the efficiency and speed of investigations, as well as improve coordination and communication within teams. However, along with the benefits that mobile applications provide, there are also a large number of risks associated with the protection of confidential information.

The article focuses on potential external and internal threats that can compromise the security of data storage and transmission. In particular, it analyses how hacker attacks, phishing, spam and other cyber threats can harm data storage systems. Vulnerabilities resulting from

possible abuse or negligence by personnel that could lead to unauthorized access or data leakage are also discussed.

A comprehensive approach to risk assessment is proposed, which includes modelling potential attacks and testing systems for vulnerability. Attention is paid to methods of data encryption, protection of data transmission, as well as the development of effective authentication and access control strategies aimed at minimizing the possibility of unauthorized access and ensuring the integrity of information.

The research findings highlight the need for regular security updates and audits to meet the growing threats in the digital environment. The article calls for greater attention to these issues in order to ensure not only the effectiveness, but also the legality of the work of law enforcement agencies in the context of the use of mobile applications.

Key words: threat modelling, risk assessment, mobile application, investigator, law enforcement agency, criminalistics, criminal process.