1. Чорний Р. В., Горбовцова І. В., Сердюк Н. М. Кіберфізичні системи у сучасному світі. *Комп'ютерні інтелектуальні системи та мережі:* мат. XIII Всеукр. наук.-практ. WEB-конф. аспірантів, студентів та молодих вчених (24-26 березня 2020 р.). Кривий Ріг: Криворізький національний університет, 2020. С. 214-216.

2. Невлюдов І. Ш., Євсєєв В. В., Андрусевич А. О., Максимова С. С. Моделі та методи кіберфізичних виробничих систем в концепції Industry 4.0 : монографія. Харків, 2023. 321 с.

3. Фурсов І., Шматко О. Питання визначення порушень безпеки кіберфізичних систем. *Молодий вчений*. 2020. № 9 (85). С. 109-114.

4. Дудикевич В., Микитин Г., Галунець М., Кутень, Р. Кіберфізична система «Розумний дім»: структура–загрози–безпека. URL: sci.ldubgd.edu.ua.

5. Биков М. М., Грищук Т. В., Ковалюк О. О., Ковтун В. В., Юхимчук М. С. Модель експлуатації кіберфізичної системи в умовах впливу негативних зовнішніх факторів. *Вісник Вінницького політехнічного інституту.* 2023. № 6. С. 30-38.

6. Kozhedub Y., Kramska Y., Hyrda V. Analysis of the human factor influence on the cyber-physical system. *Collection «Information Technology and Security».* 2020. № 8(1). Pp. 102–115. URL : https: //doi.org/10.20535/2411-1031.2020.8.1.21 8013.

ЛУНГОЛ Ольга,
кандидат педагогічних наук, доцент,
доцент кафедри оперативно-розшукової
діяльності та інформаційної безпеки
факультету підготовки фахівців
для підрозділів кримінальної поліції
Донецького державного
університету внутрішніх справ
(м. Кропивницький, Україна)
ПОЗІГУН Богдан,

рядовий поліції, курсант факультету
підготовки фахівців для підрозділів
кримінальної поліції Донецького
державного університету внутрішніх справ
(м. Кропивницький, Україна)

МЕТОДИ ЗАХИСТУ ЦИФРОВОГО ВІДБИТКУ ПРИСТРОЮ В ОНЛАЙН-СЕРЕДОВИЩІ

Цифровий відбиток пристрою – це унікальний ідентифікатор, який створюється під час використання гаджету в інтернеті або в інших електронних системах. Цей ідентифікатор складається з унікальних параметрів, таких як IP-адреса, MAC-адреса, серійний номер пристрою, відомості про виробника та модель пристрою, а також інші технічні характеристики, такі як тип та версія операційної системи, браузера та інших програм. Унікальний ідентифікатор може бути використаний для ідентифікації та відслідковування пристрою в мережі. Відбиток пристрою дозволяє визначати, які пристрої підключені до мережі, відстежувати їх активність та взаємодію з іншими пристроями й ресурсами в мережі.

Цифровий відбиток пристрою дозволяє вебсайтам, рекламним компаніям та іншим зацікавленим організаціям відстежувати користувачів через пристрої та вивчати їхню активність в інтернеті. Цифрові відбитки пристроїв також є об’єктом зацікавленості для кіберзлочинців, які можуть використовувати унікальні іден-

тифікатори для збору інформації або атак на пристрої користувачів.

З моменту появи цифрового відбитку пристрою зросла увага до захисту приватності користувачів. Багато вебсайтів і компаній вживають заходів для обмеження збору і використання даних пристроїв без відповідного дозволу користувача. Захист особистого цифрового відбитку пристрою в онлайн-середовищі є надзвичайно важливим для збереження приватності та безпеки користувачів в інтернеті. Існують різні методи, які можна використовувати для захисту особистого цифрового відбитку пристрою. Використання VPN дозволяє шифрувати трафік між пристроєм користувача та інтернетом, що робить його складнішим для перехоплення та відстеження з боку третіх сторін. Проксі-сервери можуть приховати IP-адресу користувача та забезпечити додатковий шар анонімності при використанні інтернету. Важливо використовувати захищені мережі Wi-Fi з паролем, щоб уникнути можливості несанкціонованого доступу до пристрою через незахищені мережі. Регулярне оновлення операційних систем та програмного забезпечення на пристрої допоможе у виправленні виявлених вразливостей та забезпечить додаткову безпеку. Важливо використовувати складні паролі або біометричні методи аутентифікації, такі як відбиток пальця або розпізнавання обличчя, для захисту доступу до пристрою та облікових записів. Вимкнення непотріб-

них служб та функцій пристрою допоможе уникнути можливих атак та збільшить загальну безпеку.

Існують браузерні розширення, які дозволяють приховати або змінити цифровий відбиток пристрою. Деякі з них можуть змінювати ідентифікатори, такі як user-agent string, який браузер надсилає на вебсайти, інші можуть блокувати відслідковування вебаналітикою або захищати приватні дані. Однак варто зауважити, що використання таких розширень може мати вплив на функціональність деяких вебсайтів, оскільки можуть вимагати певних параметрів від пристрою для коректної роботи.

Навіть коли значна кількість гаджетів використовує ту саму операційну систему, кожен з них має унікальну комбінацію програмного забезпечення, обладнання, браузера, плагінів, мови, часового поясу й персональних налаштувань. Використання різних браузерів може призвести до неузгодженості в процесі збору інформації для ідентифікації користувача, але сучасні методи кросбраузерного зняття цифрових відбитків використовують для уникнення таких обмежень [4].

Отже, цифровий відбиток пристрою відіграє важливу роль у відстеженні та ідентифікації пристроїв у мережі, але водночас потребує виваженого підходу до захисту приватності та безпеки користувачів.

Список використаних джерел:

7. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права.* 2022. № 1. С. 176-180.

8. Струков В. М., Гуділін В. В. Технологія отримання цифрового відбитку пристрою як спосіб ідентифікації особи в мережі Інтернет. *Застосування інформаційних технологій у діяльності правоохоронних органів:* зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.). Харків : ХНУВС, 2020. С. 123-125.

9. Шабельник С. П. Вдосконалення способів фільтрації небезпечного трафіку на основі реєстру цифрових відбитків пристроїв : магістерська робота. Інститут електроенергетики. Дніпро, 2022. 101 с.

10. Цифровий відбиток пристрою: наскільки ви вразливі? Безпека. Конфіденційність. *Binance Academy*. Опубліковано 26.08.2019, оновлено 11.12.2023. URL: https://academy. binance.com/uk/articles/device-fingerprinting-how-exposed-are-you.

ЛЯЛЮК Галина,
доктор педагогічних наук,
доцент кафедри теоретичної психології
Інституту управління психології та безпеки
Львівського державного
університету внутрішніх справ
(м. Львів, Україна)

ОСОБИСТІСНА РЕСУРСНІСТЬ ПРАЦІВНИКА МВС ЯК ФАКТОР ПОДОЛАННЯ НАПРУЖЕНИХ СИТУАЦІЙ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ

Різке зростання навантаження у професійній діяльності фахівців МВС в умовах воєнного стану висуває