УДК 351.74

ІНШЕКОВА Юлія Юріївна,
старший викладач кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0009-0000-1202-2651

ІНТЕРНЕТ РЕЧЕЙ (IoT) У КРИМІНАЛІСТИЦІ ТА ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Із розвитком технологій Інтернету речей (IoT) з'являються нові можливості та виклики у криміналістиці та правоохоронній діяльності. Інтернет речей - концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку [1]. За даними аналітичної компанії Gartner, кількість підключених до інтернету пристроїв перевищить 25 мільярдів до 2025 року [2]. Інтернет речей включає в себе різні пристрої, об'єднані в мережу для збору та обміну даними. Це створює нові можливості для збирання доказів, але також породжує нові вразливості та правові питання. Мета цієї роботи – дослідити виклики та можливості використання IoT у криміналістиці, аналізуючи нормативно-правову базу та практичні аспекти застосування технологій.

Застосування IoT у криміналістиці вимагає дотримання міжнародних і національних нормативно-правових актів. Наприклад, Загальний регламент захисту даних (GDPR) в ЄС регулює обробку персональних даних і встановлює суворі вимоги до захисту інформації [3]. Будапештська конвенція про кіберзлочинність надає правові рамки для боротьби з кіберзлочинами, включаючи ті, що пов'язані з IoT [4]. Крім того, законодавство багатьох країн передбачає специфічні положення щодо збору та зберігання цифрових доказів, що є критично важливими у розслідуванні злочинів з використанням IoT-технологій.

IoT-пристрої часто стають мішенями для кіберзлочинців через їхню вразливість. Ненадійна безпека цих пристроїв може призвести до зламу та несанкціонованого доступу до конфіденційних даних. Використання застарілого програмного забезпечення та недостатній захист мережевих підключень – основні фактори ризику для IoT-пристроїв. Криміналісти можуть використовувати дані з IoT-пристроїв як цифрові докази у розслідуваннях, що підвищує необхідність у належному збиранні та зберіганні таких даних. Наприклад, смарт-камери

можуть надавати відеодокази, а розумні термостати – дані про присутність людей у приміщенні [5]. Водночас, аналіз таких даних потребує спеціалізованих знань та інструментів.

Однією з основних проблем є вразливість IoT-пристроїв, що можуть бути використані зловмисниками для отримання несанкціонованого доступу до даних. Для підвищення безпеки IoT-пристроїв необхідно використовувати надійні системи безпеки, включаючи шифрування даних, автентифікацію користувачів та регулярне оновлення програмного забезпечення. Зокрема, шифрування даних зменшить ризик перехоплення інформації під час передачі, а автентифікація користувачів дозволить уникнути несанкціонованого доступу [6].

Навчання правоохоронців є критично важливим для ефективного використання IoT у криміналістиці. Регулярні тренінги допоможуть правоохоронцям освоїти нові технології та методи аналізу даних з IoT-пристроїв. Також важливо забезпечити співпрацю з виробниками IoT-пристроїв, які можуть надати додаткову інформацію про технічні характеристики та вразливості своїх продуктів. Це дозволить правоохоронцям більш ефективно використовувати IoT-дані у своїх розслідуваннях.

Правове регулювання використання IoT-даних у криміналістиці має бути чітким і зрозумілим. Розробка нових законодавчих актів, що враховують специфіку IoT-технологій, забезпечить законність та етичність їх використання у розслідуваннях. Це включає регулювання збору, зберігання та використання даних, а також захист прав громадян на конфіденційність.

Інтернет речей (IoT) відкриває нові горизонти у криміналістиці та правоохоронній діяльності, надаючи можливості для ефективнішого збору та аналізу даних. Проте, для успішної інтеграції IoT у ці сфери, необхідно вирішити низку викликів, пов'язаних з безпекою, правовим регулюванням та навчанням правоохоронців. Тільки таким чином можна досягти максимальної ефективності та безпеки у використанні цих технологій для боротьби зі злочинністю.

Список бібліографічних посилань

1. Wikipedia. Інтернет речей. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9 (дата звернення: 20.06.2024).

2. Gartner. Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. Gartner, 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

3. European Union. General Data Protection Regulation (GDPR). EU, 2016. URL: https://gdpr.eu/.

4. Council of Europe. Budapest Convention on Cybercrime. Council of Europe, 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

5. Kumar, P., & Patel, A. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 2014, 90(11), 20-26. URL: https://ijcaonline.org/archives/volume90/number11/15873-4531.

6. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011. URL: https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-12-374268-1.