Тенденції розвитку комп'ютерної форензики

Катерина Борисова

Харківський національний університет внутрішніх справ, м. Кам'янець-Подільський, Україна, ORCID: https://orcid.org/0009-0006-6015-1304, e-mail: kate.borisova0502@gmail.com

Віталій Світличний

Канд. техн. наук, доц., Харківський національний університет внутрішніх справ, м. Кам'янець-Подільський, Україна, ORCID: https://orcid.org/0000-0003-3381-3350, e-mail: vit.svet@ukr.net

Досліджено сучасний стан комп'ютерної форензики, окреслено основні напрями її розвитку. Розглянуто превентивні стратегії, спрямовані на запобігання кіберзагрозам. Зазначено важливу роль комп'ютерної форензики для підвищення загального рівня кібербезпеки.

Ключові слова: комп'ютерна форензика; кібербезпека; превентивні стратегії; методи розслідування.

Trends in Computer Forensics Development

Kateryna Borysova, Vitalii Svitlychnyi

The current state of computer forensics is investigated, the main directions of its development are outlined. Preventive strategies aimed at preventing cyber threats are considered. The important role of computer forensics in enhancing overall level of cybersecurity is emphasized.

Keywords: computer forensics; cybersecurity; preventive strategies; investigation methods.

Сучасне суспільство все частіше стикається з кіберзагрозами, що можуть призвести до серйозних наслідків для індивідів, компаній і держав. У сучасному цифровому світі злочини стають усе більш складними, підступними й досконалими, тому розвиток комп'ютерної форензики, яка виявляє, аналізує та розслідує кіберзлочини, стає критично важливим.

Термін *forensics* є похідним від *forensic science*, що дослівно означає «судова наука», яка спеціалізується на дослідженні доказів. У широкому сенсі форензика містить різноманітні галузі, включно з комп'ютерною криміналістикою [1].

Сучасна комп'ютерна форензика використовує провідні сучасні технології для збирання, аналізування й інтерпретування цифрових доказів. Методи роботи — відновлення видалених файлів, аналізування мережевого трафіку, розшифрування зашифрованих даних тощо. Особливу увагу приділено захисту приватності й відновленню інформації після кібератак.

Для повноцінного збирання й аналізування інформації використовують різні вузькоспеціалізовані утиліти. Можна виокремити такі групи програм та інструментів: мережевий аналіз, реал-тайм утиліти, робота з образами (створення, клонування), вилучення даних, артефакти інтернету, аналіз часових інтервалів, конвертори, робота з *RAM*, фреймворки, артефакти *Windows* (вилучення файлів, історій завантажень, *USB*-пристроїв), *HEX*-редактори, аналізування файлів, оброблення образів дисків тощо [1].

Тенденції розвитку комп'ютерної форензики містять широкий спектр напрямів, що відображають важливі зміни й удосконалення у цій галузі. Назвімо деякі з провідних тенденцій:

- зростання обсягів цифрових доказів;
- застосування штучного інтелекту та машинного навчання;
- зростання кіберзагроз;
- мобільність і хмарні технології;
- розвиток кібербезпеки;
- міжнародний спротив діяльності злочинців в інтернеті.

Ці тенденції свідчать про постійне еволюціонування комп'ютерної форензики та її важливість у сучасному цифровому світі.

Однією з провідних тенденцій розвитку комп'ютерної форензики є розвиток кібербезпеки, що передбачає спрямування особливої

уваги на превентивні стратегії із запобігання кіберзагрозам. Цю тенденцію відображено в таких аспектах: удосконалення заходів захисту (містить використання передових антивірусних програм, файрволів, систем виявлення вторгнень та інших засобів технічного захисту) та аудит безпеки (регулярні аудити дають змогу виявляти потенційні вразливості й ризики, якими можуть скористатися зловмисники). Слід також звертати увагу на такі аспекти, як навчання та постійне вдосконалення, адже швидкість розвитку технологій потребує постійного покращення стратегій і методів захисту, вивчення їхніх особливостей. Превентивні стратегії в кібербезпеці допомагають уникнути багатьох загроз і підвищують загальний рівень безпеки в інтернеті.

На наше переконання, у сучасному цифровому світі загрози кібербезпеці набувають усе більшою актуальності. Розвиток комп'ютерної форензики, яка спеціалізується на виявленні, аналізуванні та розслідуванні кіберзлочинів, відіграє критично важливу роль у боротьбі із цими загрозами. Використання провідних сучасних технологій (таких, як штучний інтелект і машинне навчання) дає змогу ефективно збирати й аналізувати цифрові докази. Превентивні стратегії в кібербезпеці, спрямовані на запобігання кіберзагрозам, допомагають уникнути багатьох потенційних негативних наслідків для індивідів, компаній і держав.

Отже, розвиток комп'ютерної форензики та застосування превентивних стратегій у кібербезпеці є ключовими напрямами із підвищення загального рівня безпеки в інтернеті.

Перелік джерел посилання

1. Cyber Witcher. Комп'ютерна криміналістика (форензика): добірка корисних посилань / HackYourMom. 09.05.2023. URL: https://hackyourmom.com/kibervijna/kompyuterna-kryminalistyka-forenzyka-dobirka-korysnyh-posylan/ (дата звернення: 20.03.2024).