інформації збереженої на облаштуванні користувача у вигляді соокіев-файлів, інших тимчасових файлів; відбитку файлової системи пристрою.

Під відбитком файлової системи розуміється інформація про структуру файлової системи, а не отримання математичної свертки даних у файловій системі. Особлива увага приділяється файлам старше за місяць, в яких не відбувалося змін за цей час. Вони мають достатню стабільність, щоб на деякий час стати ідентифікуючою ознакою. Для створення відбитку файлової системи пропонується використовувати інформацію про їх ім'я, місце розташування, розмір, дату створення і дату редагування.

Інформація про користувача складається з: днів тижня, часу доби використання, тривалості активності програмного забезпечення; друкарських помилках, що повторюються, словах паразитах, помилках при наборі тексту; подіях миші або клавіатури.

Кінцевою метою дослідження завдання ідентифікації людини і пристрою є побудова розпізнавана, здатного із задовільною точністю робити ідентифікацію. Особливість цього пристрою полягає в непостійному наборі вхідних значень, що повинне відбиватися на його внутрішній структурі.

УДК 343.9 + 51-77

ОКСАНА ПЕТРІВНА МЕЛАЩЕНКО
старший викладач кафедри інформаційних технологій факультету №4 Харківського національного університету внутрішніх справ
КСЕНІЯ ВОЛОДИМИРІВНА ЮРТАЄВА
кандидат юрідичниїх наук, доцент кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

КОРЕЛЯЦІЙНА ЗАЛЕЖНІСТЬ ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА ТА РІВНЯ КІБЕРЗЛОЧИННОСТІ

Впровадження електронно-обчислювальної техніки в управлінські процеси та інші сфери життя суспільства сприяло не лише стрімкому розвитку наукової думки та успішному вирішенню багатьох технічних і соціальних проблем, але й призвело до появи нових видів злочинів, зокрема, незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, розкрадання, присвоєння, вимагання комп'ютерної інформації, вчинення агресивних злочинів з використанням комп'ютерних технологій тощо. У науці сукупність суспільно небезпечних посягань з використанням комп'ютерної техніки отримало назву кіберзлочинність.

На міжнародному рівні кіберзлочини були криміналізовані у 2001 році Конвенцією РЄ про кіберзлочинність. На національному рівні поняття кіберзлочину отримало закріплення лише нещодавно 5 жовтня 2017 р. у ст. 1 закону України «Про основні засади забезпечення кібербезпеки України» [1].

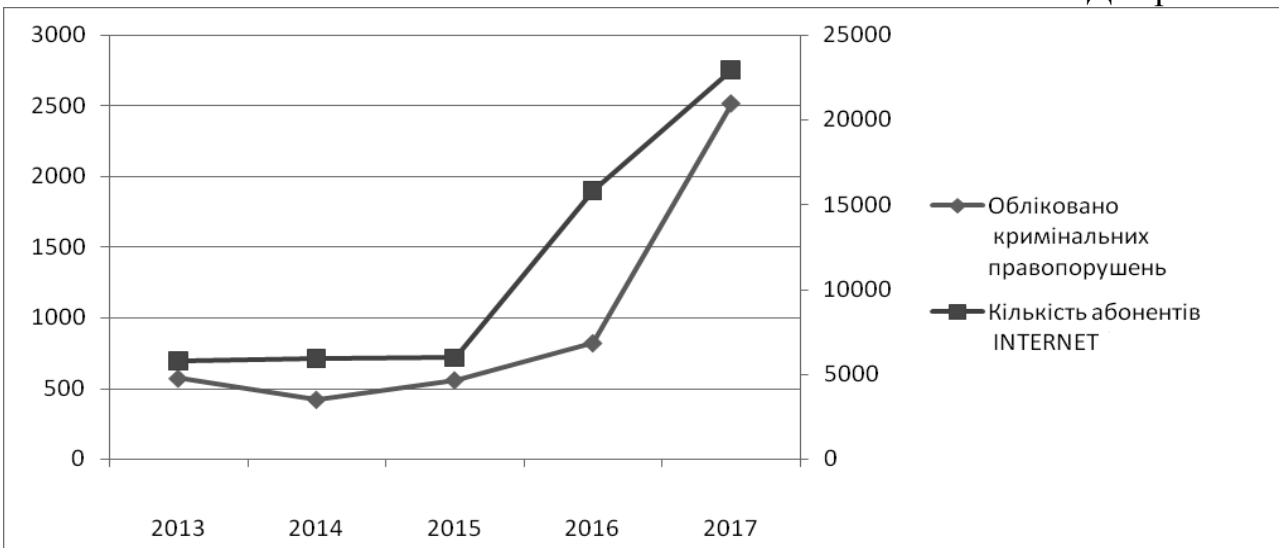
Дослідники зазначають, що одною з потужних детермінантів комп'ютерних злочинів є постійне збільшення кількості пристроїв, які використовують комп'ютерні технології, та їх широке використання в різних сферах суспільного життя. Згідно прогнозу експертів Управління ООН по наркотикам і злочинності у 2020 році кількість пристроїв буде у шість разів перевищувати чисельність населення. За такої ситуації важко уявити комп'ютерний злочин, а можливо, навіть будь-який злочин, який не супроводжувався б електронними доказами, пов'язаними з підключенням до мережі Інтернет [2, p. X].

Порівняльний аналіз облікованих кримінальних правопорушень за даними Генеральної прокуратури України [3] та кількості користувачів мережні Інтернет в Україні за даними Державної служби статистики України [4] засвідчує пряму залежність цих показників (див. Таблиця 1 і Діаграма 1).

Таблиця 1

Період	2013	2014	2015	2016	2017
Обліковано кримінальних правопорушень	568	418	556	818	2514
Кількість абонентів мережі Інтернет	5759,9	5910,8	5951,6	15834,9	22957,5

Діаграма 1



Таким чином можна зробити висновок, що рівень кіберзлочинності буде продовжувати зростати паралельно з рівнем інформатизації суспільства.

Важливою складовою поліпшення протидії кіберзлочинності є поєднання правових методів і методів точних наук під час виявлення та

розслідування кіберзлочинів. Так, зокрема, В. І. Трапезніков наголошує на важливості застосування методу статистичної класифікації кіберзлочинів для організації збору статичних даних про кіберзлочини в рамках інформаційно-аналітичної роботи правоохоронних органів [5, с. 367]. В. В. Мурадов визначає необхідність вдосконалення технічних і правових засад використання електронних доказів в кримінально-процесуальному доказуванні [6]. Передовою у цьому зв'язку є ініціатива MULTI-FORESEE в рамках Європейської співпраці в науці і технологіях (COST), яка вже сьогодні об'єднує зусилля дослідників різних країн світу з метою використання сучасних методів комп'ютерного моделювання, оптики, спектроскопії, хімії, фізики для передачі не лише електронних доказів, а й відбитків пальців, біоречовин, фарби, волокон тощо [7].

Підсумовуючи, зазначимо, що необхідна активізація використання передових цифрових технологій і методів точних наук у протидії кіберзлочинності.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 р. 2163-VIII. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.12.2018).
2. Всестороннее исследование проблем киберпреступности, февраль 2013 года. Управление ООН по наркотикам и преступности. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата звернення: 01.12.2018).
3. Статистична інформація Генеральної прокуратури України за 1913-2018 рр. URL: https://www.gp.gov.ua/ua/statinfo.html (дата звернення: 01.12.2018).
4. Державної служби статистики України URL: http://www.ukrstat.gov.ua.
5. Трапезников В. И. Характеристика и значение международной статистики киберпреступности / В. И. Трапезников // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4, № 4. – С. 363-369.
6. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльно-аналітичне право. 2013. № 3-2. С. 313-315.
7. Action CA16101 COST Homepage link. URL: https://multiforesee.com/ (дата звернення: 01.12.2018).