УДК 343.98

**Сергій Павлович ЛАПТА,**
*кандидат юридичних наук, доцент,*
*доцент кафедри кримінально-правових дисциплін факультету № 6*
*Харківського національного університету внутрішніх справ;*
*ORCID: https://orcid.org/0000-0002-5401-5086*

# ЩОДО МОЖЛИВОСТЕЙ ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ ІГРОВИХ ПРИСТАВОК XBOX ONE ТА SONY PLAYSTATION4

Під час розслідування кіберзлочинів важливими джерелами доказів є різноманітні накопичувачі цифрової інформації. При проведенні обшуків у підозрюваних осіб слідчі вилучають системні блоки персональних комп'ютерів, ноутбуки, смартфони, зовнішні HDD та SSD накопичувачі цифрової інформації тощо. Однак, у пошуках більш надійних і менш підозрілих сховищ цифрової інформації, злочинці можуть використовувати у цій якості внутрішні носії ігрових приставок. Шкідливі програми, викрадені персональні дані, хакерські утиліти можуть розміщатися на ігрових платформах, які вже давно перестали бути пристроями виключно для розваг.

Останнім часом ігрові консолі за функціональністю значно наблизилися до персональних комп'ютерів, часто залишаючись в очах слідчих лише дорогою іграшкою, не вартою уваги. Найбільш популярними серед сучасних ігрових консолей можна назвати Xbox One від компанії Microsoft та Sony PlayStation 4 (PS4) від компанії Sony. Так, на кінець 2017 року у світі було продано більше 29 млн. консолей Xbox One і більше 73 млн. PS4 [1]. Окрім ігор, вони дозволяють користувачам прослуховувати музику, дивитись відео, зображення та використовувати USB-прилади. Обидві платформи обладнані 8-ядерними процесорами (Xbox One – 8-core x86 AMD CPU; PS4 – 8-core AMD "Jaguar" x86-64 CPU), 8GB оперативною пам'яттю (Xbox One – DDR3 RAM; PS4 – GDDR5 RAM), 500GB жорстким диском SATA, 802.11n WiFi та USB 3.0 [2, 3].

Вочевидь, присутні всі основні елементи, які входять до складу персонального комп'ютера, що дозволяє записувати, зберігати та зчитувати цифрову інформацію так саме, як і на персональному комп'ютері. Однак, як зазначають дослідники, боротьба виробників ігрових консолей з контрафактними комплектуючими, програмним забезпеченням та цифровою продукцією призвела до зміцнення внутрішніх систем захисту консолей, що у свою чергу суттєво ускладнило проведення їх експертного дослідження[4]. Так, якщо виявлення файлів, які просто зберігаються користувачем на жорсткому диску ігрової платформи можливе за допомогою стандартного інтерфейсу користувача, то, наприклад, відновлення видалених файлів

чи встановлення мережевої активності консолі вже становлять значну складність для експертів.

На жаль в Україні не проводилось наукових досліджень у даному напрямку, тому корисно буде ознайомитись із досвідом закордонних колег. Минулого року дослідники із Університету Зайїд[1], Дубаї (ОАЕ) провели дослідження ігрових консолей Xbox One та Sony PlayStation 4 за допомогою стандартних програмних інструментів, які використовуються для дослідження цифрової техніки.

Так, за допомогою FTK Imager[2] були створені образи дисків консолей, що досліджувались. X-Ways Forensics[3] використовувався для пошуку акаунтів користувачів і встановлення ігор, які запускались на консолях, за ключовими словами. Autopsy 3.1.3[4] застосовувалась для пошуку ключових слів. За її допомогою також були встановлені акаунти користувачів та ігри, які запускались на консолях. Крім того на обох платформах вдалося побачити внутрішню структуру файлової системи, однак розділи на PS4 виявились нечитабельними, у той час, як у Xbox One зміст розділів відкрився. FTK 5.5[5] розпізнав розділи файлової системи, однак не надав механізмів аналізу кожного з них. Багато файлів у Xbox One було виявлено зашифрованими, або представленими у невідомому бінарному форматі [5]. Стосовно PS4 було встановлене лише те, що її диск має 15 розділів і певний нерозподілений дисковий простір. У Xbox One було виявлено файлову систему у вигляді, подібному до файлової системи Windows, що зробило процес аналізу за допомогою стандартного експертного програмного забезпеченням більш простим, ніж у PS4.

Використання Magnet IEF Forensics[6] надало той же результат, що і FTK 5.5. Більше інформації вдалося отримати за допомогою метода Live Analysis[7]. Були встановлені профілі користувачів, відправлені та отримані повідомлення, повна історія активності користувача із зазначенням конкретного часу виконання тої чи іншої дії, IP-адреса, основний шлюз, адреси основного і додаткового DNS-серверів. У той же час, будучи досить ефективним для збору доказів, цей метод має і

[1] Zayed University.

[2] Програма для перегляду та клонування носіїв даних.

[3] Програмний комплекс для проведення комп'ютерних експертиз і дослідження носіїв інформації.

[4] Цифрова експертна платформа для дослідження комп’ютерної техніки.

[5] Forensic toolkit – експертне програмне забезпечення, призначене для отримання різноманітної інформації з жорстких дисків.

[6] Експернті програмні інструменти, призначені для отримання доказової інформації з цифрової техніки.

[7] «Живий аналіз» – метод пошуку і вилучення доказів у працюючій системі. Серед багатьох підходів до його здійснення для фізичних машин використовується стандартний інтерфейс користувача, імпортовані утиліти, модифікована система та додаткове обладнання.

суттєвий недолік – будь-яка дія, яку виконує експерт викликає незворотну зміну досліджуваного стану системи [6]. У деяких країнах такі модифіковані, змінені докази є недопустимими, у інших (зокрема, у ОАЕ) – такі докази вважаються допустимим в суді, навіть за наявності змін, якщо вони є мінімальними, добре документованими та повторюваними [5].

Загалом, закордонні експерти сходяться на наступних складнощах дослідження вказаних ігрових консолей:

– неадекватні завданням, що виникають, знання про роботу і функціональність ігрових консолей;

– відсутність добре навчених експертів із цифрового дослідження ігрових консолей та виявлення і вилучення доказів з них;

– відсутність спеціалізованих інструментів для експертного дослідження ігрових консолей;

– обмежена документація та інформація про архітектуру ігрових консолей [5];

– наявність запатентованих файлових систем, де дані зберігаються у форматі, що не підтримується існуючими засобами експертного аналізу (PS4) [7];

– можливість зберігати дані користувача в інших місцях, окрім локальних жорстких дисків, таких, як хмарні сервіси (PlayStation Network, Xbox Live).

Підводячи підсумки, слід зазначити, що в Україні проблема з підготовкою експертів до досліджень таких об’єктів та розробка спеціалізованих експертних приладів і програмного забезпечення стоїть не менш гостро. Слідчі, під час розслідувань кіберзлочинів, проводячи обшуки за місцем мешкання підозрюваних часто не звертають уваги на ігрові консолі, як можливі сховища кримінальної інформації. Тому необхідно більш активно залучати передовий іноземний досвід у даній сфері і більш тісно співпрацювати з іноземними колегами, як у галузі розслідувань, так і у галузі проведення експертних та наукових досліджень.

**Список бібліографічних посилань**

1. Owen S. Good PS4 is outselling Xbox One 2-to-1, if you do the math. URL: https://www.polygon.com/2018/5/9/17336138/ps4-xbox-one-sales-chart-figures-numbers (дата звернення: 08.10.2018).

2. Sebastian Antony. Xbox One: Hardware and software specs detailed and analyzed. URL: http://www.extremetech.com/gaming/156467-xbox-one-hardware-and-software-specs-detailed-and-analyzed (дата звернення: 08.10.2018).

3. PlayStation 4 Teardown URL: https://www.ifixit.com/Teardown/PlayStation +4+Teardown/19493 (дата звернення: 08.10.2018).

4. Jason Moore, Ibrahim Baggili, Andrew Marrington, Armindo Rodrigues. Preliminary forensic analysis of the Xbox One. URL: https://www.sciencedirect.com/science/article/pii/S1742287614000577?via %3Dihub (дата звернення: 09.10.2018).

5. Salam Khanji, Farkhund Iqbal, Raja Jabir, Andrew Marrington. Forensic analysis of Xbox one and Playstation 4 gaming consoles. URL: https://www.researchgate.net/publication/312560894_Forensic_analysis_of_xbox_one_and_playstation_4_gaming_consoles (дата звернення: 09.10.2018).

6. Sasa Mrdovic, Alvin Huseinovic, Ernedin Zajko. Combining Static and Live Digital Forensic Analysis in Virtual Environment. URL: http://people.etf.unsa.ba/~smrdovic/publications/ICAT2009-Mrdovic_Huseinovic_Zajko.pdf (дата звернення: 10.10.2018).

7. Matthew Davies, Huw Read, Konstantinos Xynos, Iain Sutherland. Forensic analysis of a Sony PlayStation 4: A first look. URL: https://www.researchgate.net/publication/273261827_Forensic_analysis_of_a_Sony_PlayStation_4_A_first_look (дата звернення:11.10.2018).

*Одержано 22.10.2018*

УДК 004.492.3

**Богдан Володимирович ЛИТВИНЕНКО,**
*студент Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»*
**Михайло Віталійович ЦУРАНОВ,**
*старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»*

## МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ ЯК ЗАСІБ ВИЯВЛЕННЯ КІБЕРЗЛОЧИНЦІВ

Останнім часом масштабні кіберзлочини на території України стали досить частим явищем. Як повідомив начальник кіберполіції Сергій Демедюк в інтерв'ю виданню «Економічна правда» в січні 2018 року, в Україні кількість виявлених злочинів у сфері кібербезпеки збільшується в середньому на 2,5 тисячі щорічно[1], що свідчить не тільки про зростання їх кількості, але й про збільшення ефективності роботи підрозділів кіберполіції з фіксації злочинів. Об'єктами зловмисників все частіше стають державні установи, акаунти держслужбовців у різних соціальних мережах.

До найбільших кібератак за останні 5 років можна віднести:

1) грудень 2015 року – кібератака віруса BlackEnergy на «Укренерго», в результаті чого в Прикарпатті, Київській та Чернівецькій областях без електроенергії залишились близько 220 тис. споживачів[2]. В результаті розслідування було виявлено, що атака почалась ще у травні 2014 року з розсилки на поштові скриньки робітників електронного листа, який містив файл з троянською програмою, що збирала інформацію про систему та відправляла її зловмисникам. З червня 2014 по жовтень 2015 року продовжились розсилки і 23 грудня 2015 року зловмисниками була проведена скоординована кібератака на інфраструктуру українських обленерго. Після внесення змін до режиму роботи розподільчих станцій програма