- резервні копії, застарілі файли, і на код стороні сервера;
- файли конфігурації та дамп бази даних файлів;
- спеціалізовані форуми;
- файли користувачів і паролів;
- клієнтський код;
- виявлення вразливостей;
- дослідження програмного забезпечення відомих вразливостей на основі виявлених технологій;
- перевірка URL та пасивне сканування через перехоплюючий проксі;
- інші документи, що представляють інтерес.

Одержано 30.10.2017

УДК 004.89

Олексій Феліксович ЛАНОВИЙ,
кандидат технічних наук, доцент, доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖІ DARKNET ДЛЯ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Серед основних тенденцій розвитку інформатизації суспільства, що стосується практично всіх сфер життєдіяльності слід відзначити стрімкий розвиток інформаційної мережі Інтернет. Розвиток інформаційних технологій сприяв виникненню нового виду злочинності – комп'ютерної, а перехід на цифрові технології, методи електронного управління технологічними процесами, конвергенція і глобалізація комп'ютерних мереж стали передумовою появи кіберзлочинності. Фахівці зазначають, що загроза поширення кіберзлочинності та кібертероризму за рівнем негативного впливу може бути порівняна з реальними бойовими діями. Водночас, розвиток інтернету призводить до виникнення низки проблем: соціальних, організаційних, юридичних тощо, але найгострішою є активне використання мережі злочинним світом. Міжнародним суспільством кіберзлочинність визнано загрозою не тільки національній безпеці окремих держав, а й людству та міжнародному порядку в цілому [1].

Тіньовий або глибинний Інтернет («Deep Web») – величезна частина Інтернету, яка знаходиться за межами стандартних методів пошуку. Значна частина тіньового Інтернету – це сай-

ти, які недоступні для пошуку за допомогою звичайних пошукових систем або захищені паролем. Частина глибинного Інтернету, відома також під назвою Даркнет («DarkNet»), доступна тільки за допомогою спеціальних програм, що відкривають доступ до напівлегальних і нелегальних товарів або послуг. Інтернет, і особливо Dark Web, зробили торгівлю людьми більш легкою для розповсюдження та приховування. Інтернет-реклама використовується, щоб заманити потенційних жертв торгівлі людьми, на закритих форумах обговорюють різні аспекти торгівлі людьми та послуги, що приховані в Dark Web [2]. Для більш ефективної боротьби з торгівлею людьми Агентство передових оборонних дослідницьких проектів (також відоме як DARPA), що входить до складу Міністерства оборони США, у 2014 році запустило програму Memex [3].

Законодавство України не забороняє використання програмного забезпечення і технічних засобів забезпечення зв'язку, що надають повну анонімність користувача для доступу в Даркнет, а також технічно не вирішено питання можливого блокування функціонування подібного роду програмних продуктів і технічних рішень. Тому суттєвими стають питання, пов’язані з можливістю одночасної ідентифікації осіб в мережах Інтернет та Даркнет.

В основу сучасної технології Data Mining (discovery-driven data mining) покладено концепцію шаблонів (патернів), що відображають фрагменти багатоаспектних взаємовідносин у даних. Ці шаблони містять закономірності, що властиві вибірках даних, які можуть бути виражені у зрозумілій формі. Пошук шаблонів в інформаційному просторі Даркнет у цьому випадку проводиться методами, що не обмежені рамками апріорних припущень про структуру вибірки.

Інформація, що знайдена в процесі використання методів Data Mining під час дослідження Даркнет, повинна описувати нові зв'язки між властивостями, передбачати значення одних ознак на основі інших тощо. Завдання, які вирішуються методами Data Mining, включають:

- класифікацію та віднесення об'єктів (спостережень, подій) до одного із заздалегідь визначених класів;
- прогнозування та встановлення залежності вихідних змінних від вхідних;
- кластеризацію – угруповання об'єктів (спостережень, подій) на основі даних або властивостей, що описують сутність цих об'єктів;

- асоціацію – виявлення асоціативних закономірностей;
- послідовні шаблони – встановлення закономірностей між пов'язаними в часі подіями, тобто виявлення залежності, згідно до якої якщо відбудеться подія X, то через заданий час відбудеться подія Y.

У зв'язку з неможливістю проведення контекстного пошуку та застосування методів Data Mining одночасно в мережах Інтернет та Даркнет, результати обробки інформації повинні зберігатися в окремих базах даних, які і будуть опрацьовуватись. З цією метою інформаційна система повинна:

- в режимі реального часу здійснювати збір та збереження інформації з тіньових форумів;
- визначати псевдоніми («ніки») зловмисників.

На підставі отриманих даних інформаційна система повинна надавати можливість проведення пошуку за патернами збережених об'єктів серед форумів мережі Даркнет та в соціальних мережах Інтернет з метою знаходження можливих збігів.

Список використаних джерел:

1. Lacey D., Salmon P. M. It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. *Engineering Psychology and Cognitive Ergonomics.* Vol. 9174 of Lecture Notes in Computer Science. 2015 PP. 117–128. URL: https://link.springer.com/chapter/10.1007/978-3-319-20373-7_12 (дата звернення: 22.10.2017).
2. Rathod Digvijaysinh. Darknet Forensics. *International Journal of Emerging Trends&Technology in Computer Science.* 2017. Vol. 6. Issue 4. PP. 77–79. URL: http://www.ijettcs.org/Volume6Issue4/ IJETTCS-2017-07-24-29.pdf (дата звернення: 22.10.2017).
3. Pellerin Cheryl DARPA Program Helps to Fight Human Trafficking URL: https://www.defense.gov/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ (дата звернення: 22.10.2017).

Одержано 27.10.2017