DOI: 10.18372/2410-7840.25.17596
УДК 004.056.55

ПРАКТИЧНА ОЦІНКА РЕАЛІЗАЦІЇ РОЗПОДІЛЕНОГО КРИПТОАНАЛІЗУ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

Віталій Носов, Василь Лучик, Тетяна Колісник, Сергій Калякін, Віталій Світличний

Оперативні підрозділи відповідних спеціальних служб і органів державної влади при здійсненні своїх повноважень часто стикаються із задачею здійснення криптоаналізу отриманих зашифрованих даних. На практиці оперативне криптографічне розкриття таких даних зазвичай має дві суттєві обставини: відсутність спеціалізованих обчислювальних ресурсів та наявність лише обмеженої кількості персональних комп'ютерів з ОС Windows. Одним із актуальних способів підвищення ефективності криптоаналізу в таких умовах є реалізація паралельних розподілених клієнт-серверних обчислень на базі локальної мережі персональних комп'ютерів з ОС Windows, де сервер через деякий інтервал часу розподіляє виділені підмножини простору можливих ключів шифрування між агентами в локальній мережі, які в свою чергу передають задачу перебору ключів відповідній локальній програмі. Здійснений перший етап практичної оцінки застосунку Hashtopolis як інструмента розподіленого криптоаналізу в умовах обмежених ресурсів. Hashtopolis є працездатним у локальній мережі персональних Windows комп'ютерів і може бути використаний на практиці. Зростання швидкості паралельних обчислень не є прямо пропорційним кількості агентів, оскільки витрачається час на формування підмножин простору ключів, їхнього доставлення агентам та отриманням результатів перебору ключів. Практична оцінка Hashtopolis потребує подальшого дослідження зростання продуктивності його роботи у залежності від кількості агентів, інших типів геш-ів і типів криптоаналізу (за словником, комбінований) та контролю температури процесорів на агентських машинах. Ідентифікована задача оптимального вибору для агентів розміру підмножини простору можливих ключів в залежності від кількості агентів, їх поточної швидкості перебору, алгоритму геш-у і типу перебору.

***Ключові слова**: розподілений криптоаналіз, Hashtopolis, геш ключа, швидкість криптоаналізу, практична оцінка.*

ВСТУП

Широке використання криптографічних систем спеціальними службами іноземних держав, злочинними організаціями і окремими правопорушниками обумовлює постійну потребу у розвідувальних, контррозвідувальних і правоохоронних оперативних підрозділах відповідних органів державної влади при здійсненні своїх повноважень проводити криптоаналіз отриманих зашифрованих даних.

Проте на практиці оперативне криптографічне розкриття таких даних зазвичай має дві суттєві обставини: відсутність спеціалізованих обчислювальних ресурсів та наявність лише обмеженої кількості персональних комп'ютерів з ОС Windows. В таких умовах одним з актуальних способів підвищення ефективності криптоаналізу є реалізація паралельних розподілених клієнт-серверних обчислень на базі локальної мережі персональних комп'ютерів з ОС Windows, де сервер через деякий інтервал часу розподіляє виділені підмножини простору можливих ключів шифрування між агентами в локальній мережі, які в свою чергу передають задачу перебору ключів відповідній локальній програмі.

ОСНОВНА ЧАСТИНА

В [1] з точки зору оперативності і наявних обмежень застосовності для системи розподіленого криптоаналізу було сформульовані такі вимоги:

– максимальна універсальність до типів зашифрованих даних;

– відкриті вихідні коди і ліцензія вільного програмного забезпечення;

– функціонування на різних платформах;

– обчислення як на центральних, так і на графічних процесорах клієнтських персональних комп’ютерів;

– ОС Windows на клієнтських персональних комп’ютерах;

– необмежена кількість клієнтів.

Найбільш універсальним методом криптоаналізу різних типів зашифрованих даних є вилучення геш-у ключа шифрування із різних об’єктів зашифрованих даних (таких як *.pdf, *.7z, *.zip, *.rar, *.docx, і ін.) та обчислення геш-у від імовірних ключів для порівняння його із вилученим.

Вищенаведеним вимогам відповідають такі локальні програмні інструменти перебору ключів, як Hashcat [2] і John the Ripper jumbo release (JtR) [3]. Для них розроблені взаємно сумісні скрипти вилучення ґешу ключа із великої кількості типів зашифрованих даних [4, 5]. В [1] зазначено, що інструментами розподіленого криптоаналізу, які сумісні з Hashcat або JtR і задовольняють встановленим вимогам, є: Hashtopolis [6], Fitcrack [7], Cracklord [80], GoCrack [9].

Загальною метою комплексного дослідження є практична оцінка ефективності зазначених застосунків розподіленого криптоаналізу, яка досягається через послідовну оцінку реалізації кожного застосунку, вибір критерію ефективності і їх взаємного порівняння за обраним критерієм.

Першим для оцінки було обрано застосунок Hashtopolis, який складається з двох частин: клієнтського агенту, що написаний на C# або Python та PHP/CSS серверу, який надає графічний інтерфейс управління адміністратора і керує з'єднанням із клієнтськими агентами. На стороні клієнта Hashtopolis-агент керує запуском із необхідними параметрами утиліти Hashcat, яка дає змогу реалізовувати атаки перебору ключів на більш ніж 200 алгоритмів ґешування.

Для реалізації атаки криптоаналізу попередньо з використанням скриптів [4, 5] видобувається ґеш ключа шифрування з блоку зашифрованих даних.

Практична оцінка реалізації застосунку Hashtopolis здійснювалась на базі локальної комп'ютерної мережі з 21 персонального комп'ютера, які мали такі основні параметри:

– операційна система: 64-bit Windows 7 Professional Service Pack 1;

– процесори: Intel® Core™ i5-4590 CPU @ 3.30 GHz 3.30 GHz;

– оперативна пам'ять: 4,00 ГБ.

Загальний порядок встановлення сервера та клієнта Hashtopolis зазначено в [6]. В експерименті у якості сервера через середовище віртуалізації Oracle VM VirtualBox була встановлена віртуальна машина з ОС Kali Linux Light 64 Bit, в якій спочатку були встановленні оновлення та гостьове доповнення:

```
# apt update && upgrade -y
# apt install virtualbox-guest-x11
```

Далі з відповідного репозиторію MySQL APT Repository був завантажений .deb пакунок і встановлено в систему MySQL сервер версії 5.6 з параметрами: Debian jessie (8); enable old packages:

```
# dpkg -i / PATH / mysql-apt-config _ 0.8.12-1_all.deb
# apt-get update
# apt install mysql-server
```

Далі було встановлений і запущений з необхідними модулями веб-сервер Apache 2 та веб-інтерфейс phpMyAdmin для адміністрування MySQL:

```
# apt install apache2
# apt install libapache2-mod-php php-mysql php php php-gd php-pear php-curl git curl
# service mysql start
# сервіс mysql status
# apt install phpmyadmin
```

Веб-інтерфейс phpMyAdmin встановлювався з параметрами: apache2; configure database for phpmyadmin with dbconfig-common - yes; setup password for administrator phpMyAdmin.

MySQL сервер налаштовувався через команду:

```
# mysql_secure_installation
```

Параметри: validate password plugin? – n; change the password for root? – n; remove anonymous user? – y; disallow root login remotely? – y; remove test database? – y; reload privilege tables now? – y.

Був запущений веб-сервер Apache 2 та встановлений автозапуск Apache 2, MySQL:

```
# service apache2 start
# service apache2 status
# update-rc.d apache2 enable
# update-rc.d mysql enable
```

Серверна частина Hashtopolis встановлювалась через команди:

```
# git clone https://github.com/s3inlc/hashtopolis.git
# cd hashtopolis/src
# mkdir /var/www/hashtopolis
# cp -r */var/www/hashtopolis
# chown -R www-data: www- data /var /www/ hashtopolis
```

Стартова сторінка Hashtopolis для веб-сервера була встановлена шляхом заміни рядка "DocumentRoot / var /www /html" на "Document Root /var / www/hashtopolis" у файлі конфігурації 000-default.conf:

```
# cd /etc/apache2/sites-enabled
# nano 000-default.conf
# service apache2 restart
```

Через веб інтерфейс phpMyAdmin: http://localhost/phpmyadmin, був створений обліковий запис користувача (рис. 1) і база даних hashtopolis (рис. 2) з максимальними привілеями.

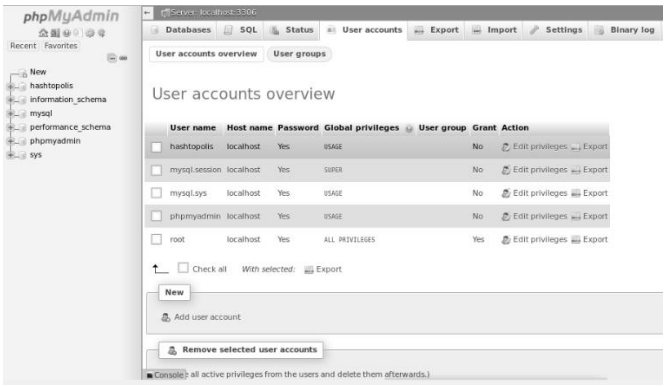

Рис. 1. Створення облікового запису користувача root

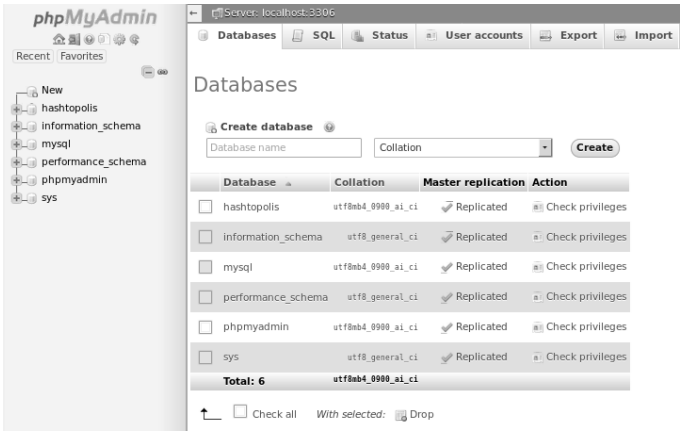

Рис. 2. Створення бази даних hashtopolis

Hashtopolis-сервер через веб інтерфейс http://localhost/ був встановлений наступними командами: “Install Hashtopolis / “, “Server hostname: localhost”, “Server port: 3306”, “MySQL user: hashtopolis”, “MySQL password: *****”, “Database name: hashtopolis”, “/ Continue / Create Admin User”, “Username: admin”, “Email Address: admin @ test.eu”, “Password: *****”, “/ create”. У результаті графічний інтерфейс керування Hashtopolis-сервером став доступним за посиланням http://localhost.

Далі на клієнтських Windows машинах були встановлений OpenCL драйвер версії 16.1.2_x64 для графічного процесору Intel GPU та середовище Python 3.7.2 з необхідними модулями:

> python -m pip install requests psutil wget

У серверній частині Hashtopolis через меню Agent/New Agent були створені облікові записи для 21 клієнта шляхом генерації ваучерів авторизації (рис. 3).

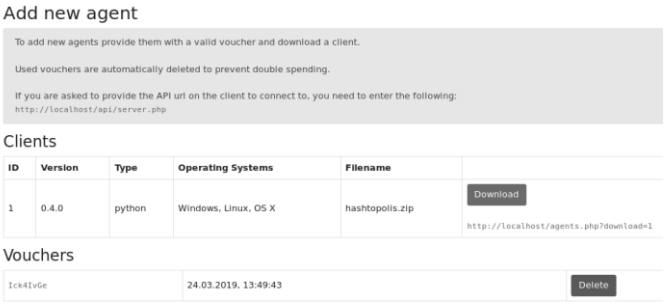

Рис. 3. Реєстрація на Hashtopolis-сервері агентів для клієнтських машин шляхом створення ваучерів

На клієнтських Windows машинах був створений каталог hashtopolis, завантажений із серверу агент hashtopolis.zip і зареєстрований через зарезервований ваучер клієнта:

> mkdir c:\hashtopolis && cd /D c:\hashtopolis

> python -m wget http: // 192. 168. 110. 141 / agents.php?download=1

> python hashtopolis.zip --url http: // 192.168. 110.141/api/server.php --voucher XXXXXX

У результаті на Hashtopolis-сервері у розділі Agents/Status відобразились статуси усіх агентів та температури процесорів клієнтських машин (рис. 4).

Рис. 4. Відображення статусу активності агентів та температури процесорів клієнтських машин

Далі у розділі Lists/New hashlist сервера для нового hashlist був вказаний тип алгоритму гешів MD5, завантажений тестовий текстовий файл геш-значень exampleMD5.hash, який містив 6494 гешів ключів з файлу example0.hash утиліти hashcat-5.1.0 (рис. 5).

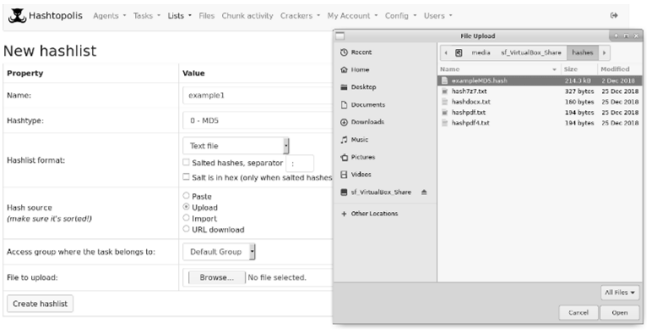

Рис. 5. Завантаження переліку
гешів для криптоаналізу

На сервері у розділі Task/New task було створено нове завдання для агентів з такими параметрами: “Attack command: -D 1 –a 3 #HL# ?a?a?a?a?a?a”, “Is CPU only task: Yes” (рис. 6), які задають для утиліти hashcat-5.1.0: використовувати центральний процесор, тип гешів - MD5, перебирати ключі завдовжки 6 символів з алфавіту:

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

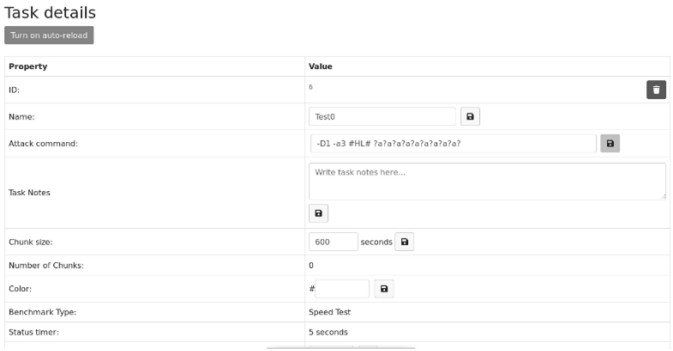

Рис. 6. Створення завдання для агентів

Далі у розділі Task/Show Task/Assigned agents через спадний список було призначено завдання агенту першої машини. Швидкість перебору гешів можливих ключів на одній машині становило близько 73 MH/s (рис. 7).

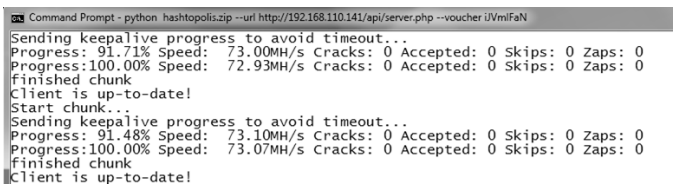

Рис. 7. Швидкість перебору гешів можливих ключів
на одній машині

Деталі виконання завдання агентом були відображені на сервері у вигляді графіка, де видні часові паузи в обчисленнях, що пов'язані з отриманням агентом нової підмножини (chunk) простору можливих ключів (рис. 8).

Рис. 8. Швидкість виконання завдання агентом

По мірі призначення завдання агентам підсумкова швидкість перебору ключів зростала (рис. 9) та стабілізувалась при включенні всіх агентів (рис. 10).

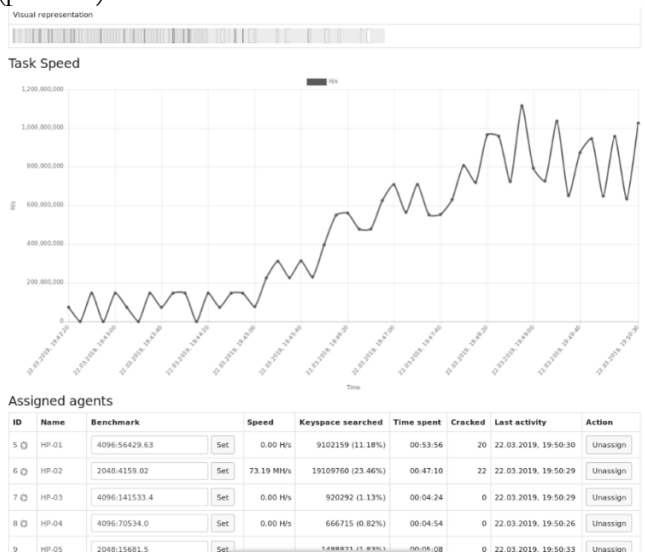

Рис. 9. Зростання підсумкової швидкості
перебору ключів при підключенні нових агентів

Усереднення за 380 секунд роботи підсумкової швидкості перебору ключів розподіленої системи з 21 агентом (табл. 1) дозволило отримати значення швидкості 895 MH/s.

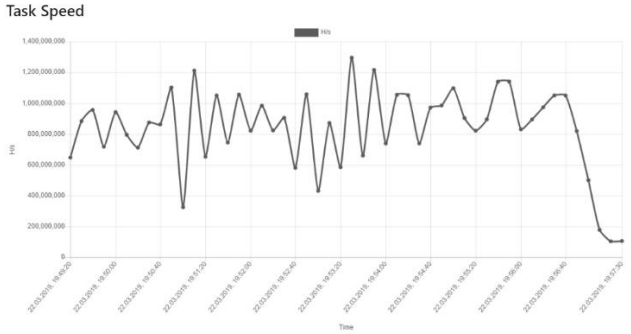

Рис. 10. Стабілізація підсумкової швидкості перебору ключів

ВИСНОВКИ

Застосунок Hashtopolis є працездатним у локальній мережі персональних Windows комп'ютерів і може бути використаний на практиці.

Зростання швидкості паралельних обчислень не є прямо пропорційним кількості агентів, що відповідає очікуванням, оскільки витрачається час на формування підмножин простору ключів, їхнього доставлення агентам та отриманням результатів перебору ключів.

Таблиця 1

Зафіксовані підсумкові швидкості перебору ключів на протязі 380 секунд з інтервалом 10 с

Time	19:49:20	19:49:30	19:49:40	19:49:50	19:50:00	19:50:10	19:50:20	19:50:30
Speed, MH/s	647	884	957	718	942	795	712	875
Time	19:50:40	19:50:50	19:51:00	19:51:10	19:51:20	19:51:30	19:51:40	19:51:50
Speed, MH/s	862	1102	325	1211	653	1050	745	1056
Time	19:52:00	19:52:10	19:52:20	19:52:30	19:52:40	19:52:50	19:53:00	19:53:10
Speed, MH/s	821	984	824	905	580	1058	431	872
Time	19:53:20	19:53:30	19:53:40	19:53:50	19:54:00	19:54:10	19:54:20	19:54:30
Speed, MH/s	584	1295	660	1216	739	1055	1052	739
Time	19:54:40	19:54:50	19:55:00	19:55:10	19:55:20	19:55:30	19:55:40	19:55:50
Speed, MH/s	971	985	1097	903	821	895	1140	1141
Time	19:56:00	19:56:10	19:56:20	19:56:30	19:56:40	19:56:50	19:57:00	-
Speed, MH/s	830	895	973	1050	1050	819	500	-

Практична оцінка Hashtopolis потребує подальшого дослідження зростання продуктивності його роботи у залежності від кількості агентів, інших типів ґешів і типів криптоаналізу (за словником, комбінований) та контролю температури процесорів на агентських машинах.

Необхідне вирішення задачі оптимального вибору для агентів розміру підмножини простору можливих ключів (chunk) в залежності від кількості агентів, їх поточної швидкості перебору, алгоритму ґешу і типу перебору.

ЛІТЕРАТУРА

[1] Носов В.В. Розподілений криптоаналіз при обмежених ресурсах для потреб правоохоронних органів // Протидія кіберзлочинності та торгівлі людьми: зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків нац. ун-т втур. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2020, С. 117-119.

[2] Hashcat advanced password recovery [Електронний ресурс]. URL: https://hashcat.net/ (дата звернення: 18.04.2023).

[3] John the Ripper password cracker [Електронний ресурс]. URL: https: // www. openwall.com/john/ (дата звернення: 18.04.2023).

[4] Hashstack-server-plugin-hashcat. Scrapers at master. Stricture/hashstack-server-plugin-hashcat. GitHub [Електронний ресурс]. URL: https://github. com / stricture / hashstack - server-plugin-hashcat/ tree/master/scrapers (дата звернення: 18.04.2023).

[5] John/run at bleeding-jumbo. Openwall/john. GitHub [Електронний ресурс]. URL: https://github. com/ openwall / john / tree / bleeding-jumbo/ run (дата звернення: 18.04.2023).

[6] GitHub - hashtopolis/server: Hashtopolis - A Hashcat wrapper for distributed hashcracking [Електронний ресурс]. URL: https://github.com/s3inlc /hashtopolis (дата звернення: 18.04.2023).

[7] GitHub - nesfit/fitcrack: A hashcat-based distributed password cracking system [Електронний

ресурс]. URL: https://github.com/nesfit/fitcrack (дата звернення: 18.04.2023).
[8] GitHub - jmmcatee/cracklord: Queue and resource system for cracking passwords [Електронний ресурс]. URL: https: // github. com/jmmcatee/cracklord (дата звернення: 18.04.2023).
[9] GitHub - mandiant/gocrack: GoCrack is a management frontend for password cracking tools written in Go [Електронний ресурс]. URL: https: // github.com/fireeye/gocrack (дата звернення: 18.04. 2023).

A PRACTICAL EVALUATION OF THE IMPLEMENTATION OF DISTRIBUTED CRYPTOANALYSIS IN THE CONDITIONS OF LIMITED RESOURCES

The operational units of relevant special services and public authorities frequently encounter the task of cryptanalysis encrypted data during the execution of their duties. In practical terms, the operational disclosure of such data through cryptographic means typically faces two significant challenges: limited specialized computing resources and the availability of only a restricted number of personal computers operating on the Windows operating system. To enhance the efficiency of cryptanalysis under such circumstances, one of the most pertinent approaches is the implementation of parallel distributed client-server computing within a local network of Windows PCs. In this setup, the server assigns specific subsets of the potential encryption key space to agents within the local network at regular intervals. Subsequently, these agents delegate the task of key searching to their corresponding local programs. The initial phase of practical evaluation has been conducted to assess the Hashtopolis application's viability as a tool for distributed cryptanalysis under resource-constrained conditions. Hashtopolis demonstrates operability within a local network of Windows PCs and holds practical utility. However, the increase in parallel computing speed is not directly proportional to the number of agents involved, as additional time is required for the subset formation, distribution to agents, and retrieval of key search results. Further investigation is necessary to evaluate Hashtopolis effectively, taking into account the performance growth in relation to the number of agents, different types of hashes, various forms of cryptanalysis (dictionary-based, combined), and monitoring the temperature of processors on agent machines. Additionally, determining the optimal selection of subset size within the potential key space for agents, based on factors such as the number of agents, their current search speed, the hash algorithm employed, and the type of search, poses a distinct challenge.

Keywords: distributed cryptanalysis, Hashtopolis, hash, cryptanalysis speed, practical assessment.

Носов Віталій Вікторович, кандидат технічних наук, доцент, професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ.

Vitalii Nosov, Candidate of Technical Sciences, Associate, Professor of the Department of Combating Cybercrime of the Kharkiv National University of Internal Affairs.
E-mail: vitnos@ukr.net.
Orcid ID: 0000-0002-7848-6448.

Лучик Василь Єфрімович, доктор економічних наук, професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ.

Vasil Luchik, Doctor of Economic Sciences, Professor of the Department of Combating Cybercrime of the Kharkiv National University of Internal Affairs.
E-mail: luchik-vasil@ukr.net.
Orcid ID: 0000-0002-1997-0272.

Колісник Тетяна Петрівна, кандидат педагогічних наук, доцент, доцент кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ.

Tetiana Kolisnyk, Candidate of Pedagogical Sciences, Associate, Associate of the Department of Combating Cybercrime of the Kharkiv National University of Internal Affairs.
E-mail: ktp201505@gmail.com.
Orcid ID: 0000-0002-7442-8136.

Калякін Сергій Володимирович, викладач кафедри протидій кіберзлочинності Харківського національного університету внутрішніх справ.

Serhii Kaliakin, Lecturer of the Department of Combating Cybercrime of the Kharkiv National University of Internal Affairs.
E-mail: svkalyakin@ukr.net.
Orcid ID: 0000-0002-7848-6448.

Світличний Віталій Анатолійович, кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ.

Vitalii Svitlychnyi, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Combating Cybercrime of the Kharkiv National University of Internal Affairs.
E-mail: vit.svet@ukr.net.
Orcid ID: 0000-0003-3381-3350.