УДК 004.491

Кива В. Ю.;
Дрозд Ю. С.

Науковий центр дистанційного навчання Національного університет оборони України імені Івана Черняховського, Київ

# Аналіз існуючих методів кібернетичної розвідки інформаційно-телекомунікаційних мереж

**Резюме.** У статті розглянуто питання важливості забезпечення національної безпеки держави у кібернетичному просторі. Обґрунтовано актуальність та необхідність проведення розвідувальних заходів у кібернетичному просторі противника. Визначено етапи, складові та методи кібернетичної розвідки у кібернетичному просторі, а також критичні дані, які необхідно добути у ході проведення розвідувальних заходів для забезпечення командування інформацією про противника.

**Ключові слова:** національна безпека, кібернетичний простір, кібернетична розвідка, кібернетичний вплив, несанкціонований доступ, дослідження противника, засоби розвідки, інформаційно-телекомунікаційні мережі.

**Постановка проблеми.** Вивчення противника з метою виявлення його можливостей і намірів є однією з найстаріших форм інформаційної діяльності. З вдосконаленням формування інформаційного суспільства характер цієї діяльності істотно змінився. З одного боку, з'явилися нові засоби добування та обробки інформації, в тому числі інфокомунікаційні засоби та інформаційні технології, з іншого боку різко зріс обсяг інформації, яку необхідно обробити для отримання необхідних даних про противника. Крім того різко ускладнилася конкурентна боротьба. Вона набула глобального характеру, стала більш динамічною і менш прогнозованою. У цих умовах потрібні нові підходи до застосування методів та засобів розвідки у кібернетичному просторі, які дають можливість планувати проведення наступальних кібернетичних операцій з метою домінування у кібернетичному просторі над противником та заздалегідь з'ясувати та запобігти спрямованому кібернетичному впливу на критично-важливі об'єкти інформаційно-телекомунікаційних мереж (ІТМ). Тому, підвищення ефективності заходів розвідки у кібернетичному просторі противника є актуальним питанням дослідження.

**Аналіз останніх досліджень та публікацій.** Незважаючи на безліч проведених досліджень M. S. Dahiya, Howard Chivers, Monowar H. Bhuyan стосовно удосконалення методів кібернетичної розвідки, на наш час ефективного вирішення цієї проблеми немає. Тому вони потребують додаткового і більш глибокого вивчення та аналізу.

**Метою статті** є аналіз переваг та недоліків пасивного та активного методу кібернетичної розвідки ІТМ противника та визначення шляхів комплексного використання переваг кожного методу при розробці та впроваджені засобу добування розвідувальних даних ІТМ, що підвищить ефективність проведення кібернетичної розвідки в умовах обмеження часу.

**Виклад основного матеріалу.** Складовою кібернетичної розвідки (рис. 1) є комп'ютерна розвідка, при якій добування розвідувальних відомостей полягає в отриманні даних та інформації, що циркулює в засобах електронно-обчислювальної техніки, локальних та глобальних обчислювальних мережах, у тому числі з використанням несанкціонованого доступу (НСД) [2]. Кібернетична розвідка організовується і ведеться в інтересах вирішення двох груп завдань, а саме добування розвідувальних відомостей з комп'ютерних систем або інформаційних мереж (ІМ) та їх обробка за допомогою апаратно-програмних засобів (комп'ютерна розвідка), а також добування і систематизація даних про потенційні джерела кіберзагроз (розвідка кібернетичних загроз) [1]. Перша група завдань вирішується шляхом проведення комплексу узгоджених заходів щодо несанкціонованого проникнення в ІМ та комп'ютери іноземних державних та урядових організацій. Рішення другої групи завдань (добування інформації про кібернетичні загрози) припускає використання абсолютно нових джерел, технологій і технічних прийомів, а саме апаратно-математичне моделювання кібернетичних атак.

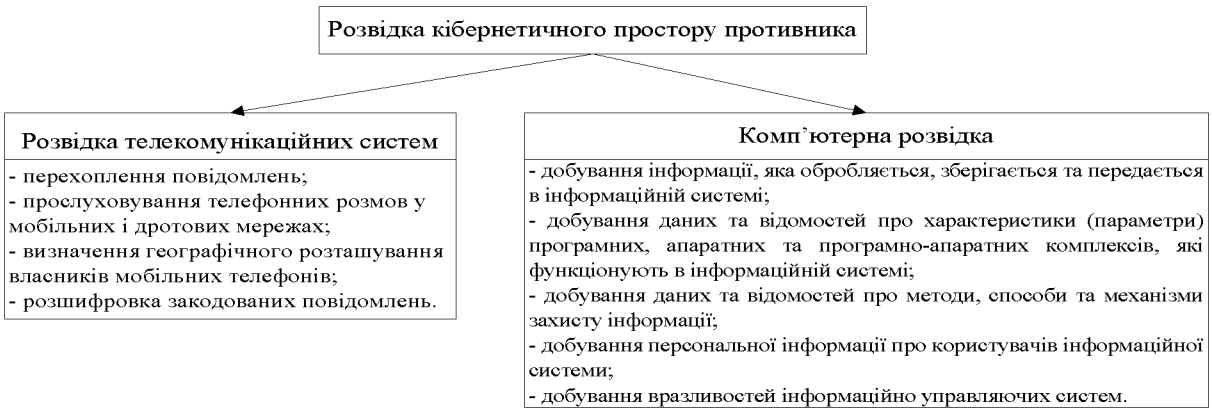


**Рис. 1. Складові кібернетичної розвідки**

Головним фактором, який впливає на процес реалізації кібернетичних атак, є засоби і методи розвідки у кібернетичному просторі, які дають можливість планувати проведення наступальних кібероперацій з метою домінування у кіберпросторі над противником та заздалегідь з'ясувати і запобігти спрямованому кібернетичного впливу на критично-важливі об'єкти ІТМ. Забезпеченням інформаційної безпеки є конфіденційність, доступність та цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від НСД. Вплив на будь-яку з цих складових можна розглядати, як кібернетичну атаку. Об'єктом атаки може бути персональна електронно-обчислювальна машина, мережевий пристрій, ІМ або інформаційна система.

Передумовою успішної кібернетичної атаки є розвідка кібернетичного простору противника, яка характеризується часовим та якісним критерієм добування інформації, характеристик одного або більше віддалених комп'ютерів ІТМ противника. Добування інформації може бути використаний для побудови моделі атакуючої системи та полегшення в майбутньому спроби проникнення до неї для реалізації кібернетичного впливу. Розвідку кібернетичного простору противника можна поділити на такі етапи (рис. 2):


**Рис. 2. Етапи проведення кібернетичної розвідки**

Кожен із зазначених етапів кібернетичної розвідки має свою мету, яка в кінцевому результаті виконання розвідувальних заходів дає можливість добути бажану інформацію про противника (табл. 1), що в свою чергу є нетривіальною задачею [6].

Таблиця 1

**Добування розвідувальної інформації про противника**

| | | |
|---|---|---|
| Добування мережевої інформації | • доменне ім'я (внутрішнє, зовнішнє);<br>• топологія мережі;<br>• *IP*-адреси систем;<br>• *TCP* та *UDP* запущені сервіси; | • мережеві протоколи;<br>• точки *VPN*;<br>• списки *ACL*;<br>• *IDS*-системи |
| Добування інформації про систему | • імена користувачів;<br>• імена локальних груп;<br>• системні банери;<br>• архітектура системи; | • тип віддаленого доступу до системи;<br>• паролі користувачів. |
| Добування інформації про органи управління | • інформація про співробітників;<br>• відомості із сайту управління;<br>• керівники управління;<br>• територіальне розташування управління; | • факс та телефонний номер організації;<br>• різна таємна інформація пов'язана з органом управління |

Основними методами добування даних у кібернетичному просторі противника є технології сканування мережі (сканування адресного простору та портів з використанням активних та пасивних методів) та перехоплення мережевого трафіку з використанням методів НСД до інформації, що циркулює в ІТМ, а також використання класичних методів

соціальної інженерії (психологічне маніпулювання з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію) [3]. Додатково також може використовуватися інформація від *whois*-серверів, перегляд інформації *DNS*-серверів мережі для виявлення записів, що визначають маршрути електронної пошти (*MX*-записи). Використання методів НСД неможливо провести без попереднього дослідження мережі, в якій знаходяться різні програмно-апаратні засоби зв'язку, а також інформаційні ресурси (об'єкти впливу) противника.

Процес дослідження одного або декількох хостів мережі називається скануванням мережі, в ньому використовується метод віддаленого аналізу. Він реалізується за допомогою відправки тестових запитів, щоб встановити зв'язок та визначити перелік активних служб, які надають віддалене обслуговування, на будь-якому хості. У процесі розвідки інформаційних об'єктів противника сканування допомагає визначити ймовірні цілі атаки [5]. Сканування мережі використовується на попередньому етапі перед атакою та дає можливість отримати потрібні початкові дані про ймовірний об'єкт впливу (перелік відкритих портів та відповідно список ймовірно атакуючих додатків на сервері, які завантажені на комп'ютер) [7].

Завчасний збір відомостей можливо співвіднести з прихованим спостереженням. На сьогодні застосовуються такі методи сканування мережі [4] (рис. 3):

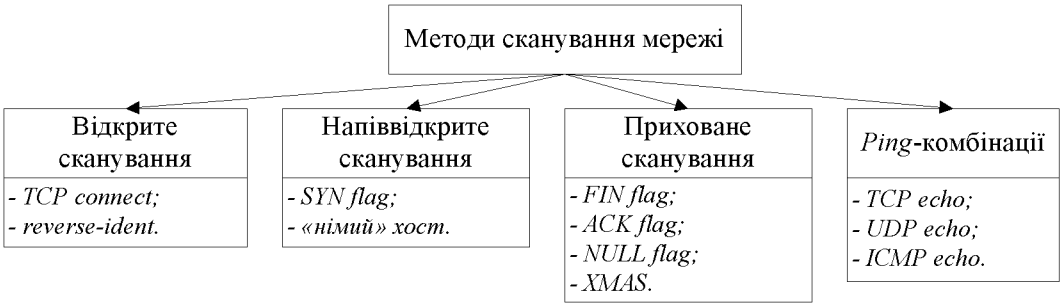


**Рис. 3. Методи сканування мережі**

Одним із важливих засобів розвідки у кібернетичному просторі є інструменти віддаленого аналізу та ідентифікації досліджуваних об'єктів противника. Проте, незважаючи на той факт, що нині питанню побудови інструментів добування розвідувальних даних приділена велика увага, головним питанням залишається – ефективне застосування інструментів розвідки кіберпростору. На сьогодні методи розвідки кібернетичного простору класифікують як активні та пасивні, кожен з яких має свої переваги та недоліки. При використанні пасивного методу збору розвідувальної інформації контакту з досліджуваним об'єктом не відбувається. При безпосередньому добуванні даних не генерується трафік, не реєструється з'єднання з хостом або сервером у системному журналі подій, а також скорочується загальна навантаженість на досліджуваний сегмент мережі при скануванні. Незважаючи на всі переваги пасивного методу добування інформації у нього є і недоліки. Для проведення пасивного аналізу завжди потрібно інтегруватися у сегмент досліджуваного об'єкта мережі для виконання ролі датчика, через який буде проходити та аналізуватися мережевий трафік, який циркулює в цьому сегменті між об'єктами розвідки (рис. 4). Або, як варіант, потребує віддаленого з'єднання з інформаційним ресурсом досліджуваного об'єкта для генерації мережевого трафіку та його подальшого аналізу для ідентифікації віддаленого об'єкта, що в свою чергу втрачає актуальність прихованого віддаленого аналізу. Також великим недоліком є велика ймовірність помилкової ідентифікації досліджуваного об'єкта, що впливає на якісні показники добутої інформації у ході проведення розвідувальних заходів.


**Рис. 4. Пасивний метод збору розвідувальних даних**

Метод активного добування розвідувальних даних полягає у безпосередньому контактуванні з досліджуваним об'єктом розвідки з використанням методів прихованого сканування, що дає можливість бути непомітним при здійсненні впливу на противника (рис. 5). Також на відміну від пасивного методу добування даних при активному добуванні ймовірність помилкової ідентифікації віддаленого об'єкта зменшується врази, що підвищує точність розвідувальної інформації та ефективність подальшого формування кібернетичного впливу на основі добутих розвідувальних даних про об'єкт дослідження.

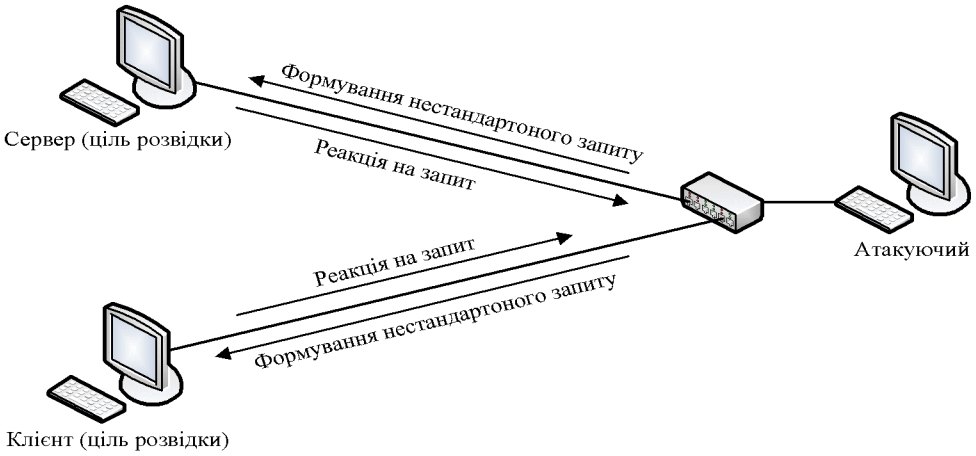


**Рис. 5. Активний метод добування розвідувальних даних**

У свою чергу, для порівняльного аналізу засобів розвідки можна застосувати такі критерії побудови програмного забезпечення [8]:

масштабованість (можливість додавання нових ресурсів, а також можливість керування єдиною розподіленою системою кібернетичної розвідки);

відкритість (можливість інтеграції в систему додаткових розроблених компонентів);

кросплатформеність (можливість перенесення додатку на різну платформу сімейства операційних систем *Windows*, *MacOS X*, *Unix*);

методи добування розвідувальних даних досліджуваного об'єкта (*TCP*, *UDP* та приховане сканування віддаленого об'єкта);

час виконання розвідувальних заходів (зменшення використання часу на добування інформації);

якість добутих розвідувальних даних (зведення до мінімуму помилкової ідентифікації об'єкта).

Проте аналіз досліджень та публікацій, а також досвід експлуатації засобів кібернетичної розвідки (табл. 2) показує, що жодний з них повною мірою не відповідає наведеним критеріям.

Таблиця 2

**Порівняльний аналіз засобів кібернетичної розвідки**

| Характеристики | Засоби розвідки кібернетичного простору | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *Strobe* | *Tcp_scan* | *Udp_scan* | *Nmap* | *Netcat* | *SuperScan* | *IpEye* | *WUPS* | *Fscan* |
| Кросплатформеність | - | - | - | + | - | - | - | - | - |
| Відкритість | - | - | - | + | - | - | - | - | - |
| *TCP* сканування | + | + | - | + | + | + | + | - | + |
| *UDP* сканування | - | - | + | + | + | - | - | + | + |
| Приховане сканування | - | - | - | + | - | - | - | - | - |

**Висновки.** Виходячи із зазначених порівняльних характеристик, можливо дійти висновку, що найбільш сприятливим засобом кібернетичної розвідки є *Nmap*, який дає змогу на достатньому рівні провести розвідувальні заходи, щодо дослідження віддаленого об'єкта противника.

Водночас, враховуючи переваги зазначеного засобу добування розвідувальних даних над іншими, слід відмітити, що в умовах обмеження часу цей інструмент віддаленої ідентифікації досліджуваного об'єкта не здатний у короткі проміжки часу добути бажану розвідувальну інформацію про противника.

Тому це обумовлює актуальність подальших досліджень, які полягають у розробленні та впровадженні розподіленої системи кібернетичної розвідки досліджуваного об'єкта противника, що дасть

можливість скоротити використання часу на виконання добування розвідувальної інформації у ході проведення розвідувальних заходів.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cyber Operations: Air Force Doctrine Document 3-12 [Електронний ресурс]. Режим доступу до ресурсу : http://www.fas.org
2. Особливості забезпечення національної безпеки у високотехнологічному суспільстві [Електронний ресурс]. Режим доступу до ресурсу : http://www.kbuapa.kharkov.ua
3. Offensive Cyber 2012 [Електронний ресурс]. Режим доступу ресурсу : https://cyberwar.nl
4. Detection and characterization of port scan attacks. Technical report [Електронний ресурс]. Режим доступу до ресурсу : https://www.scholar.google.com.ua
5. Idle port scanning and non-interference analysis of network protocol stacks using model checking [Електронний ресурс]. Режим доступу до ресурсу : https://www.usenix.org
6. Cyber Reconnaissance: An Alarm before Cyber Attack [Електронний ресурс]. Режим доступу до ресурсу : http://www.ijcaonline.org
7. Practical automated detection of stealthy portscans [Електронний ресурс]. Режим доступу до ресурсу : http://dl.acm.org
8. Л.Константайн Разработка программного обеспечения. – СПб.: Питер, 2004. – 592 с.

Стаття надійшла до редакції 11.11.2017

**Кива В. Ю.;**
**Дрозд Ю. С.**
Научный центр дистанционного обучения Национального университета обороны Украины имени Ивана Черняховского, Киев

## Анализ существующих методов кибернетической разведки информационно-телекоммуникационных сетей

**Резюме.** В статье рассмотрен вопрос важности обеспечения национальной безопасности государства в кибернетическом пространстве. Обоснована актуальность и необходимость проведения разведывательных мероприятий в кибернетическом пространстве противника. Определены этапы, составляющие и методы кибернетической разведки в кибернетическом пространстве, а также критические данные, которые необходимо добыть в ходе проведения разведывательных мероприятий для обеспечения командования информацией о противнике.

**Ключевые слова:** национальная безопасность, кибернетическое пространство, кибернетическая разведка, кибернетическое влияние, несанкционированный доступ, исследования противника, средства разведки, информационно-телекоммуникационные сети.

**V. Kyva;**
**Y. Drozd**
Science center of advanced distributed learning National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv

## Analysis of existing methods cybernetic intelligence of information and telecommunication networks

**Resume**. This article describes the importance of national security in the cyberspace. It is justified the urgency and the necessity of intelligence activities in cyberspace of the enemy in this article. It is defined the stages, components and the methods of cybernetic intelligence in cyberspace and critical data is identified which must be collected in the realization of intelligence activities for providing the headquarters with information gathered about the enemy.

**Keywords:** national security, cyberspace, cybernetic intelligence, cybernetic impact, unauthorized access, research of enem, intelligence tools, information and telecommunication networks.