УДК 004.491

Віталій Анатолійович Савченко *(д-р техн. наук, с.н.с.)*
Тарас Михайлович Дзюба *(канд. техн. наук, доцент)*
Владислав Юрійович Кива

Національний університет оборони України імені Івана Черняховського, Київ, Україна

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ КІБЕРНЕТИЧНОЇ РОЗВІДКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

В статті розглядається проблема нейтралізації загроз національній безпеці у кібернетичному просторі, що обумовлюється стрімким зростанням залежності державних та військових органів управління від використання автоматизованих систем управління, які є цілями здійснення кібернетичного впливу противника у разі ймовірного військово-політичного конфлікту.

Розглянуто способи кібернетичного впливу на інформаційно-телекомунікаційні мережі, які включають несанкціонований доступ, що завдає збитків критично важливим інформаційним системам, ресурсам або інформації загального та приватного характеру шляхом порушення конфіденційності, цілісності та працездатності інформаційно-телекомунікаційних мереж, програмного забезпечення та цифрових даних.

Стаття описує важливість 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. Розглянуто порівняльні характеристики засобів розвідки кібернетичного простору та визначено критерії щодо їх побудови. Визначено основні переваги та недоліки активного та пасивного методу добування розвідувальних даних та запропоновано комплексний підхід використання переваг кожного методу, що дасть можливість підвищити ефективність проведення кібернетичної розвідки у інформаційно-телекомунікаційних мережах.

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

Вступ

В умовах агресії Російської Федерації проти України, анексії Криму, дестабілізації суспільно-політичної обстановки на території Донецької та Луганської областей однією з найважливіших проблем стає забезпечення інформаційної безпеки України. Важливість цієї проблеми, зокрема, визначається в нових редакціях Стратегії національної безпеки України та Воєнної доктрини України, нормативно-правових актах, які визначають напрями та завдання співпраці України з НАТО та іншими міжнародними безпековими організаціями. Відповідно до Стратегії національної безпеки України, затвердженої Указом президента України від 26 травня 2015 року №287/2015, основним пріоритетом забезпечення інформаційної безпеки нашої держави є "забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії" [11].

Всі заходи політики інформаційної безпеки (відповідно до об'єктів та відповідних механізмів і технологій захисту) можна достатньо умовно розподілити на інформаційно-психологічні заходи та інформаційні заходи, які проводяться у кібернетичному просторі, під яким розуміється електронне інформаційне середовище, утворене організованою сукупністю взаємно поєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [12].

Сучасні концепції ведення воєнних дій передбачають широке використання в них кібернетичного простору. Провідні країни світу розглядають можливість проведення у кібернетичному просторі наступальних (*Offensive Cyber Operations*), оборонних (*Defensive Cyber Operations*) та розвідувальних (*Cyber Warfare Operations*) дій (операцій). Особливу роль у проведенні всіх дій (операцій) у кіберпросторі займає кіберрозвідка, яку можна визначити, як добування інформації, наявної у кібернетичному просторі, моніторинг різних інформаційно-телекомунікаційних систем і процесів, які в них протікають під час їхнього функціонування.

За час протистояння з Російською Федерацією, заходами кіберрозвідки отримувалась інформація, яка підтверджувала присутність російських військ (з порушенням норм міжнародного гуманітарного права) на території України.

Зокрема виявлялись маршрутизатори, мережеві принтери, відеокамери тощо на тимчасово

окупованих територіях, використання яких сприяло вирішенню завдань інформаційної підтримки дій наших військ (сил) в антитерористичній операції на території Донецької та Луганської областей.

Постановка проблеми. Вивчення противника з метою виявлення його можливостей і намірів є однією з найстаріших форм інформаційної діяльності. З вдосконаленням формуванням 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 те, що було проведено багато досліджень *M. S. Dahiya*, *Howard Chivers*, *Monowar H. Bhuyan* щодо удосконалення методів кібернетичної розвідки, на теперішній час справді ефективного вирішення даного роду проблеми немає. Тому вони потребують додаткового і більш глибокого вивчення та аналізу.

Мета статті. Так, як добування розвідувальних даних у ІТМ неможливий без технічного дослідження об'єкта противника, виникає необхідність у виявленні 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 дослідження

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, в тому числі із використанням несанкціонованого доступу (НСД) [2].

Кібернетична розвідка організується 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

Сьогодні кіберпростір більший, ніж Інтернет. Це взаємозалежні мережі, що містять телекомунікаційні мережі, вбудовані автоматизовані системи управління та критично важливі об'єкти інфраструктури.

Кібернетичні атаки на критичні об'єкти інфраструктури стають серйозною загрозою для діяльності державних і військових органів управління [9]. Простий і швидкий доступ до мережі з одного боку автоматизує діяльність роботи з інформацією, а з іншого боку робить дану інформацію більш вразливою для кіберзлочинців. Сьогодні противник (хакер) вміло і добре оснащений різними інструментами злому, що дає йому можливість легко використовувати будь-які

вразливості в інформаційній системі для здійснення НСД (кібератаки) [3].

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 (вплив). 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 наступні етапи (рис. 2):

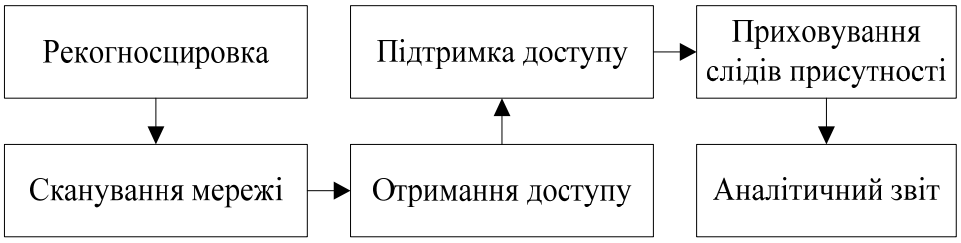

Рис. 2. Етапи проведення кібернетичної розвідки

Рекогносцировка

Рекогносцировка відноситься к підготовчому етапу, де суб'єкт атаки прагне добути інформацію про ціль до початку здійснення кібератаки. В залежності від факторів які впливають на добування розвідувальних даних про противника рекогносцировка може бути двох видів:

активна рекогносцировка – включає активну взаємодію з об'єктом атаки з безпосереднім використанням будь-яких засобів, наприклад телефонні дзвінки в службу підтримки певного органу для отримання певної інформації;

пасивна рекогносцировка – включає отримання інформації без безпосередньої взаємодії з об'єктом кібернетичного впливу, наприклад пошук інформації на викинутих документах, записках, накопичуваних пристроях, комп'ютерах.

Сканування мережі

Сканування відноситься до етапу попередньої атаки на противника, коли атакуючий сканує мережу для отримання певної інформації проведеної в ході рекогносцировки. Сканування може включати в себе сканування портів, *IP*-адрес, топології мережі, сервісів, вразливостей та визначення типу операційної системи.

Отримання доступу

Отримання доступу відноситься до точки входу в систему, де атакуючий отримує доступ до операційної системи або додатків на комп'ютері. Атакуючий може підвищити привілеї, щоб отримати повний контроль над системою, що дає можливість у подальшому приєднатися до проміжних систем, які підключені до неї.

Атакуючий може отримати доступ на рівні операційної системи, рівні додатків або мережевому рівні, прикладом може бути злом паролів, переповнення буфера, відмова у обслуговуванні.

Підтримка доступу

Підтримка доступу відноситься до етапу, де атакуючий намагається зберегти доступ до системи. Атакуючий може використати вразливості нульового дня (*0-day*) з використанням *Backdoor*, *Trojan*, *RootKit*.

Атакуючий може завантажувати, вивантажувати або маніпулювати даними додатків або конфігурацією над атакуючою системою, а також використовувати систему для запуску нових кібератак.

Приховування слідів присутності

Приховування слідів присутності відноситься до етапу, де атакуючий намагається здійснити атаку не замiченою та не перехопленою, видаливши докази котрі могли б привести його до кримінального переслідування.

Аналітичний звіт

Всі добуті розвідувальні дані аналізуються та формуються певні пропозиції та висновки, щодо реалізації кібернетичного впливу на противника. Аналітичний звіт являє собою опис ретельного дослідження противника, а також описує результативні показники та підсумки у кількісному та якісному вимірі, які є пріоритетними в оцінці ефективності проведення розвідувальних заходів під час добування інформації про противника.

Кожен з вище зазначених етапів кібернетичної розвідки має свою ціль та мету, яка в кінцевому результаті виконання розвідувальних заходів дає можливість добути бажану інформацію про противника (табл. 1), що в свою чергу є нетривіальною задачею [8].

Таблиця 1

Добування розвідувальної інформації про противника

Добування мережевої інформації	• доменне ім'я (внутрішнє, зовнішнє); • топологія мережі; • *IP*-адреси систем; • *TCP* та *UDP* запущені сервіси;	• мережеві протоколи; • точки *VPN*; • списки *ACL*; • *IDS*-системи.
Добування інформації про систему	• імена користувачів; • імена локальних груп; • системні банери; • архітектура системи;	• тип віддаленого доступу до системи; • паролі користувачів.
Добування інформації про органи управління	• інформація про співробітників; • відомості з сайту управління; • керівники управління; • територіальне розташування управління;	• факс та телефонний номер організації; • 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) [5].

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 [7]. 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'ютері) [10].

Завчасний збір відомостей можливо співвіднести з прихованим спостереженням. На даний час застосовуються наступні методи сканування мережі [6] (рис.3):

Рис. 3. Методи сканування мережі

Також важливу роль у добуванні розвідувальних даних відіграє перехоплення мережевого трафіку , що циркулює в мережі. Даний метод добування даних дає можливість перехопити та проаналізувати мережевий трафік, що циркулює між різними вузлами сегменту мережі. Для перехоплення мережевого трафіку використовуються так звані аналізатори трафіку (сніфери). Аналіз мережевого трафіку дозволяє вивчити логіку роботи розподіленої системи, тобто отримати характеристики подій, які відбуваються в системі, а також перелік команд, які відправляються один одному, а також перехопити потік даних, якими обмінюються об'єкти розподіленої системи, прикладом перехоплення даних можуть бути ім'я та логін користувача, які пересилаються у не зашифрованому вигляді.

Перехоплення мережевого трафіку може здійснюватися наступними методами :

звичайним прослуховуванням мережевого інтерфейсу;

підключення та перехоплення трафіку в розриві каналу;

відгалуженням (програмним або апаратним) трафіку та спрямування його копії на підготовлений сніфер;

через аналіз побічних електромагнітних випромінювань та відновлення таким чином прослуховування трафіку;

через атаку на канальному (*MAC - spoofing*) або мережевому рівні (*IP - spoofing*), що призводить до перенаправлення трафіку об'єкта дослідження або всього трафіку сегменту на сніфер з наступним поверненням трафіку до належної адреси.

Відповідно після проведення дослідження об'єкта противника, використовуються наступні методи НСД:

безпосередній доступ до об'єкта з конфіденційною інформацією (наприклад, за допомогою керованого користувачем додатком, читаючи дані з файлу або записуючи їх в нього);

створення програмних та технічних засобів, виконуючих доступ до об'єкту в обхід засобів захисту (наприклад, з використанням випадково або навмисно залишених розробником цих засобів, так званих люків);

модифікація засобів захисту для здійснення НСД (наприклад, вбудовування програмних закладок) ;

впровадження в технічні засоби обчислювальної техніки або автоматизованих систем програмних або технічних механізмів, які порушують структуру і функції даних засобів для здійснення НСД (наприклад, шляхом завантаження на комп'ютер незахищеної операційної системи);

ручний або програмний підбір паролів шляхом їх повного перебору або за допомогою словника;

підключення до лінії зв'язку та перехоплення доступу до комп'ютерної системи після відправлення пакета завершення сеансу легального користувача, який працював у віддаленому режимі;

видача себе за легального користувача з застосуванням викраденої інформації або отриманої обманим шляхом (за допомогою соціальної інженерії);

створення умов для зв'язку у комп'ютерній мережі легального користувача з терміналом зловмисника, який видає себе за легального об'єкта комп'ютерної системи (наприклад, одного з її серверів);

створення умов для виникнення в роботі комп'ютерної системи збоїв, які можуть призвести до відключення засобів захисту інформації або порушення правил політики безпеки;

ретельне вивчення захисту системи та виявлення помилкових ділянок в програмних засобах захисту інформації у комп'ютерній системі, вбудовування програмних закладок, що дає можливість здійснити НСД до системи.

Одним із важливих засобів розвідки у кібернетичному просторі є інструменти віддаленого аналізу та ідентифікації досліджуваних об'єктів противника. Проте, незважаючи на той факт, що у теперішній час питання побудови інструментів добування розвідувальних даних приділена велика увага, головним питанням залишається – ефективне застосування інструментів розвідки кіберпростору.

У теперішній час, 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. Не дивлячись 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 даному 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 добувані 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.

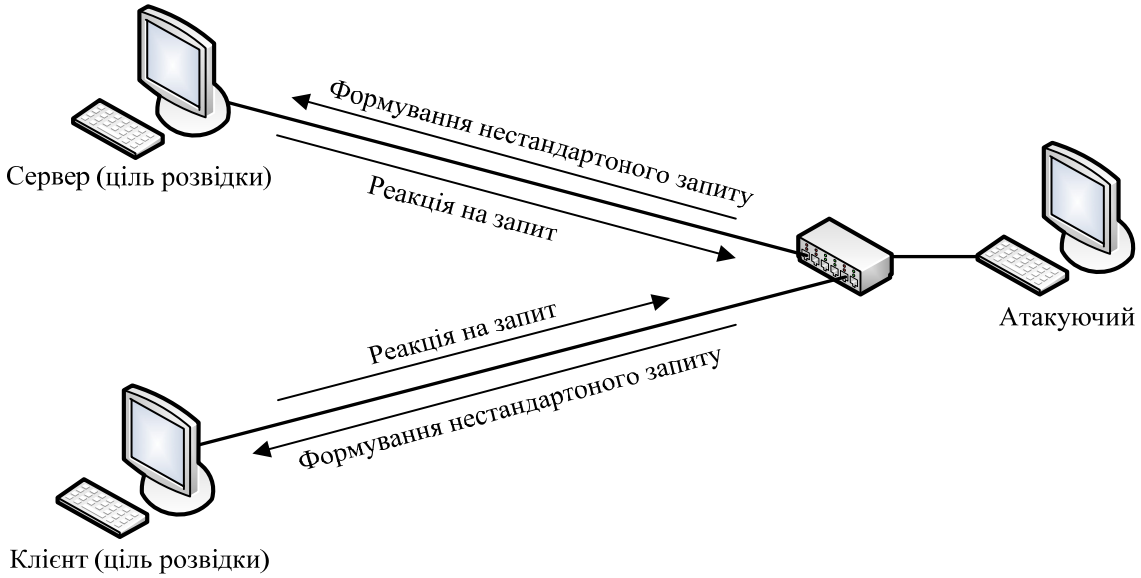

Рис. 5. Пасивний метод добування розвідувальних даних

У свою чергу, для порівняльного аналізу засобів розвідки можна застосувати наступні критерії побудови програмного забезпечення [13]:

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 у повній мірі 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*	*WinScan*	*WUPS*	*Fscan*
Кросплатформеність	-	-	-	+	-	-	-	-	-	-
Відкритість	-	-	-	+	-	-	-	-	-	-
TCP сканування	+	+	-	+	+	+	+	+	-	+
UDP сканування	-	-	+	+	+	-	-	-	+	+
Приховане сканування	-	-	-	+	-	-	-	-	-	-

Висновки й перспективи подальших досліджень

Виходячи з вищезазначених порівняльних характеристик, можливо зробити висновок, що найбільш сприятливим засобом кібернетичної розвідки є *nmap*, який дозволяє 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 даний 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 розробці 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.

Для цього необхідно провести низку досліджень щодо розробки ефективного засобу добування розвідувальних даних використовуючи шляхи комплексного використання переваг активного та пасивного методу сканування ІТМ, в основу функціонування якого необхідно покласти розподілену систему раціонального розподілу (взаємодії) функцій між програмними модулями добування розвідувальних даних та вирішити наступні завдання:

розробити алгоритм роботи розподіленої системи добування розвідувальних даних;

розробити алгоритм передачі даних у розподіленій системі;

розробити інструмент (додаток) розподіленого добування розвідувальних даних.

Література

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. Surveying** Port Scans and Their Detection Methodologies. [Електронний ресурс]. Режим доступу до ресурсу : http://www.comjnl.oxfordjournals.org. **4. Network** reconnaissance [Електронний ресурс]. Режим доступу ресурсу : https://www.cs.york.ac.uk. **5. Offensive** Cyber 2012 [Електронний ресурс]. Режим доступу ресурсу : https://cyberwar.nl. **6. Detection** and characterization of port scan attacks. Technical report [Електронний ресурс]. Режим доступу до ресурсу : https://www.scholar.google.com.ua. **7. Idle** port scanning and non-interference analysis of network protocol stacks using model checking [Електронний ресурс]. Режим доступу до ресурсу : https://www.usenix.org. **8. Cyber** Reconnaissance: An Alarm before Cyber Attack [Електронний ресурс]. Режим доступу до ресурсу : http://www.ijcaonline.org. **9. A Roadmap** for Cyber security Research [Електронний ресурс]. Режим доступу до ресурсу : http://www.dhs.gov. **10. Practical** automated detection of stealthy portscans [Електронний ресурс]. Режим доступу до ресурсу : http://dl.acm.org. **11. Указ** Президента України від 26 травня 2015 року №287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" **12. Військовий** стандарт 01.004.004 (Видання 1) Воєнна політика, безпека та стратегічне планування: Інформаційна безпека держави у воєнній сфері. – К.: ЦУМС ЗС України, 2014. **13. Л. Константайн** Разработка программного обеспечения. – СПб.: Питер, 2004. – 592 с.

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ КИБЕРНЕТИЧЕСКОЙ РАЗВЕДКИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

***Виталий Анатольевич Савченко** (д-р техн. наук, с.н.с.)*
***Тарас Михайлович Дзюба** (канд. техн. наук, доцент)*
Владислав Юрьевич Кива

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассматривается проблема нейтрализации угроз национальной безопасности в кибернетическом пространстве, которая обусловливается стремительным ростом зависимости государственных и военных органов управления от использования автоматизированных систем управления, которые являются целями осуществления кибернетического воздействия противника в случае вероятного военно-политического конфликта.

Рассмотрены способы кибернетического воздействия на информационно-телекоммуникационные сети, включающие несанкционированный доступ, что наносит ущерб критически важным информационным системам, ресурсам или информации общего и личного характера путем нарушения конфиденциальности, целостности и работоспособности информационно-телекоммуникационных сетей, программного обеспечения и цифровых данных.

Статья описывает важность 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. Рассмотрены сравнительные характеристики средств разведки кибернетического пространства и определены критерии для их построения. Определены основные преимущества и недостатки активного и пассивного метода добычи разведданных и предложен комплексный подход использования преимуществ каждого метода, что позволит повысить эффективность проведения кибернетической разведки в информационно-телекоммуникационных сетях.

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

THE ANALYSIS OF EXISTING CYBERNETIC INTELLIGENCE METHODS OF INFORMATION AND TELECOMMUNICATION NETWORKS

***Vitalii A. Savchenko** (Doctor of Technical Sciences, Senior Research Fellow)*
***Taras M. Dziuba** (Candidate of Technical Sciences, Associate Professor)*
Vladyslav Y. Kyva

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The article surveys the necessity of taking the measures to neutralize threats to national security in cyberspace, which are specified with the rapid growth of dependence of state and military authorities on the using of various automated control systems, which are the targets of the realization of cyber impact of enemy in case of a possible military-political conflict between countries.

Every second, the dynamic processes take place in the cyberspace which are characterized some cybernetic activities – an action that provides access to various information resources or intelligence activities with the using of software and information networks for the purpose of collecting information about information systems and resources of enemy.

Cyber influence is considered, which includes unauthorized access, which causes damage to critical information systems, to resources or general information and personal appointment by a breach of confidentiality, integrity and efficiency of information and information and telecommunication networks software, digital data, which provides a range of consumer services (telecommunication or information services).

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. It is considered comparative characteristics of intelligence in cyberspace and it is determined the main criteria for their construction. The main advantages and disadvantages of active and passive method of intelligence gathering and integrated approach are proposed with the benefits of each method, which will allow increasing the efficiency of cybernetic intelligence in information and telecommunication networks.

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

References

1. Cyber Operations: Air Force Doctrine Document 3-12, Available at : http://www.fas.org **2. Features** of national security in high-tech society. [*Osoblivosti zabezpechennya natsionalnoyi bezpeki u visokotehnologichnomu suspilstvi*], Available at : http://www.kbuapa.kharkov.ua **3. Surveying** Port Scans and Their Detection Methodologies, Available at : http://www.comjnl.oxfordjournals.org **4. Network** reconnaissance, Available at : https://www.cs.york.ac.uk **5. Offensive** Cyber 2012, Available at : https://cyberwar.nl **6. Detection** and characterization of port scan attacks. Technical report, Available at : https://www.scholar.google.com.ua **7. Idle** port scanning and non-interference analysis of network protocol stacks using model checking, Available at : https://www.usenix.org **8. Cyber** Reconnaissance: An Alarm before Cyber Attack, Available at : http://www.ijcaonline.org **9. A Roadmap** for Cyber security Research, Available at : http://www.dhs.gov **10. Practical** automated detection of stealthy portscans, Available at : http://dl.acm.org **11. Decree** of the President of Ukraine from May 26, 2015 №287 / 2015 On the decision of the National Security and Defense Council of Ukraine on May 6, 2015 "On the Strategy of National Security of Ukraine" **12. Military** Standard 01.004.004 (Edition 1) military policy, security and strategic planning, information security in the military sphere (2014), Kyiv, CDMS Armed Forces of Ukraine. **13. Larry Constantine (**2004) Software development. [*Rozrobka programnogo zabezpechennya*], StP, Peter, 592 p.

Отримано: 29.09.2015 р.