УДК 004.9

к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)

МІСЦЕ ТА РОЛЬ МЕРЕЖЕВОЇ РОЗВІДКИ В МОДЕЛЯХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

У статті розглядається поняття, цілі та задачі мережевої розвідки віддалених інформаційних вузлів як інструмента отримання домінуючої переваги над супротивником в процесах інформаційного протиборства.

Любарский С.В. Место и роль сетевой разведки в моделях информационного противостояния. *В статье рассмотрено понятие, цели и задачи сетевой разведки удаленных информационных узлов как инструмент получения доминирующего превосходства над противником в процессах информационного противостояния.*

S .Lubarskii The place and role of intelligence in the network model, the information counter. *The article deals with the concept, objectives and tasks of network intelligence remote information nodes as a tool for obtaining a dominant advantage over the enemy in the process of information confrontation.*

Ключові слова: *інформаційне протиборство, мережева розвідка, об’єкт інформаційного дослідження.*

Науковий прогрес і впровадження його результатів суттєво змінюють умови існування людства. На зміну військовим діям із застосуванням зброї приходить час інформаційного протиборства. Якість та терміни отримання інформації – показник складності ведення війни. Чим актуальніше інформація, якою володіє командир, тим більші його переваги в порівнянні з його супротивником.

Саме з цієї причини європейські концепції інформаційного протиборства військових конфліктів 90-х років минулого століття нині піддаються серйозному перегляду. Так, класифікація напрямів ведення інформаційного протиборства, що запропонована М. Лібікі [1], в цілому виглядає цілком логічною. Проте, її основним недоліком є суміщення функціональних напрямів (боротьба з системами управління, економічна боротьба) і методів (електронна боротьба, психологічне протиборство, атаки інформаційних зловмисників) інформаційного протиборства.

Подальші дослідження в даній області значною мірою були спробою створити досконалу систему, щоб почати реалізацію прикладних програм досягнення інформаційного домінування.

Деякі експерти провідних європейських держав для кращого розуміння проблеми запропонували концептуальну модель інформаційного протиборства [2], що представлена на рисунку 1.

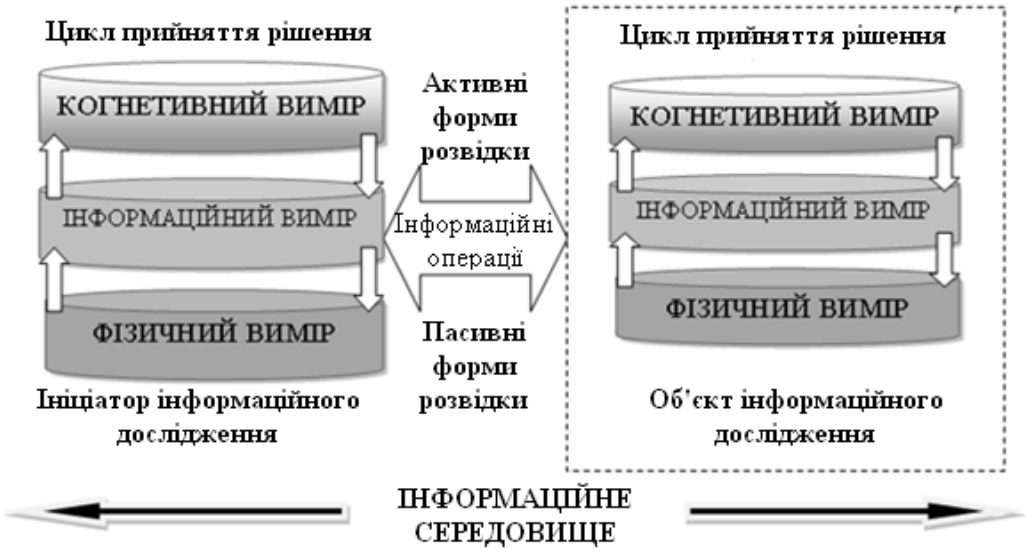

Рис. 1. Концептуальна модель інформаційного протиборства

Фізичний вимір – це матеріальний світ, де ведуться класичні бойові дії. У ньому інформація і комунікаційні системи (інфраструктура) відіграють роль забезпечення.

Інформаційний вимір – це той простір, де інформація створюється, обробляється, розподіляється і зберігається. Він зв’язує фізичний і когнітивний виміри і використовується для отримання, як інформації, що надходить, так і вихідної інформації. Інформація циркулює в так званому „контурі” *observation orientation decision action* (*OODA*) – спостереження, орієнтація, ухвалення, дія. Рішення приймаються з урахуванням інформації, що поступає з фізичного оточення (розвідка, рекогностування і спостереження), і через інформаційний вимір (бази даних, віддалені сервери та вузли комп’ютеризованої мережі спеціального призначення) здійснюють вплив на реальний світ.

Когнітивний вимір існує в людській свідомості. У ньому інформація, що поступає, відповідно до тих або інших моделей сприйняття обробляється, приймаються рішення, формуються ідеї і спрямування.

Така концептуальна модель може служити базою для визначення сфери інформаційного протиборства конкуруючих суб’єктів і цілей інформаційного домінування.

Поки що не прийнято єдиного твердження терміну „інформаційне протиборства”, але інтуїтивно вважається, що *інформаційне протиборство* – це цілеспрямовані дії зі створення інформаційної переваги, за допомогою руйнування інформації, інформаційних систем протилежної сторони, при цьому одночасно відбувається процес захисту власної інформації і інформаційних систем.

Все вище зазначене укладається в концепцію *інформаційної війни*, що спрямована в забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом нашої власної інформації та інформаційних систем.

Інформаційна війна націлена на всі можливості і фактори уразливості, що неминуче виникають при зростаючій залежності від інформації, а також на використання інформації у всіляких конфліктах. Об’єктом уваги стають інформаційні системи (включаючи відповідні лінії передач, центри обробки інформації та людські фактори цих систем), а також інформаційні технології, що використовуються в системах озброєнь. Інформаційна війна має наступальні і оборонні складові, але починається з цільового проектування і розробки власної архітектури командування, управління, комунікацій, комп’ютерів і розвідки. Це, в свою чергу, забезпечує особам, що приймають рішення, відчутну перевагу інформації у всіляких конфліктах.

Основними складовими інформаційної війни в межах інформаційного протиборства можна вважати:

– психологічні операції – це планова пропагандистська і психологічна діяльність, що проводиться в мирний або воєнний час, і розрахована на іноземні ворожі, дружні або нейтральні аудиторії з тим, щоб впливати на їх ставлення та поведінку в сприятливому напрямку для досягнення як політичних, так і військових національних цілей держави;

– дезінформація – надає супротивнику помилкову інформацію про власні сили і наміри;

– фізичне руйнування – може бути частиною інформаційного протиборства, якщо має місце руйнівний вплив на елементи інформаційних систем супротивника;

– інформаційні атаки – пряме спотворення інформації без видимої зміни суті, в якій вона знаходиться;

– інформаційна розвідка – є комплекс заходів щодо отримання і обробки даних про існуючого або ймовірного супротивника, його військові ресурси, бойові можливості і уразливості, а також про потенційний театр військових дій.

В даний час світове співтовариство серйозно стурбоване станом захисту національних інформаційних ресурсів у зв’язку з розширенням доступу до них через відкриті інформаційні мережі типу *Internet*. Інформаційне зброя, що базується на самих передових інформаційних і

телекомунікаційних технологіях, технологіях інформаційної розвідки, сприяє вирішенню цього завдання і прокладає світовий політичний фарватер.

Проте, в численних публікаціях з цієї тематики не вистачає означень тлумачення суті, завдань і методів інформаційної розвідки, що і обумовлює актуальність даної проблеми.

Ряд авторів, що спеціалізуються на теорії і практиці економічної розвідки (званою також конкурентною, діловою, комерційною, *competitive intelligence*, business *intelligence* та ін.), визначають інформаційну розвідку як аналітичну обробку величезної кількості даних з різноманітних відкритих джерел інформації, причому, як публічних мереж, так і мереж спеціального призначення. Суть інформаційної розвідки вони бачать в пошуку і передачі інформації з відкритих комп’ютерних систем, і мереж з наступною її верифікацією та аналітичною обробкою.

Аналітична розвідка була визначена, як розвідувальний пошук, технічна розвідка, комплексне вивчення матеріалів прихованого спостереження і оперативної установки, а також аналіз повідомлень, публікацій і виступів в засобах масової інформації, статистичних даних, відомостей автоматизованих банків даних. Інформаційна розвідка розглядалася при цьому як один з видів аналітичної розвідки, цілеспрямовано використовуваної для моніторингу комп’ютерних систем.

Термін „мережева розвідка” (МР) уперше з’явився в нормативних документах для позначення особливої форми діяльності оперативно-пошукових, аналітичних підрозділів.

МР виступає в якості комплекс заходів щодо отримання і обробки даних про віддалену інформаційну систему (об’єкт інформаційного дослідження), її ресурсів, засобів захисту, використаних пристроїв і програмного забезпечення і їхні вразливості. Також визначаються технології організації МР (рис. 2) та ступінь глибини інформаційного дослідження.

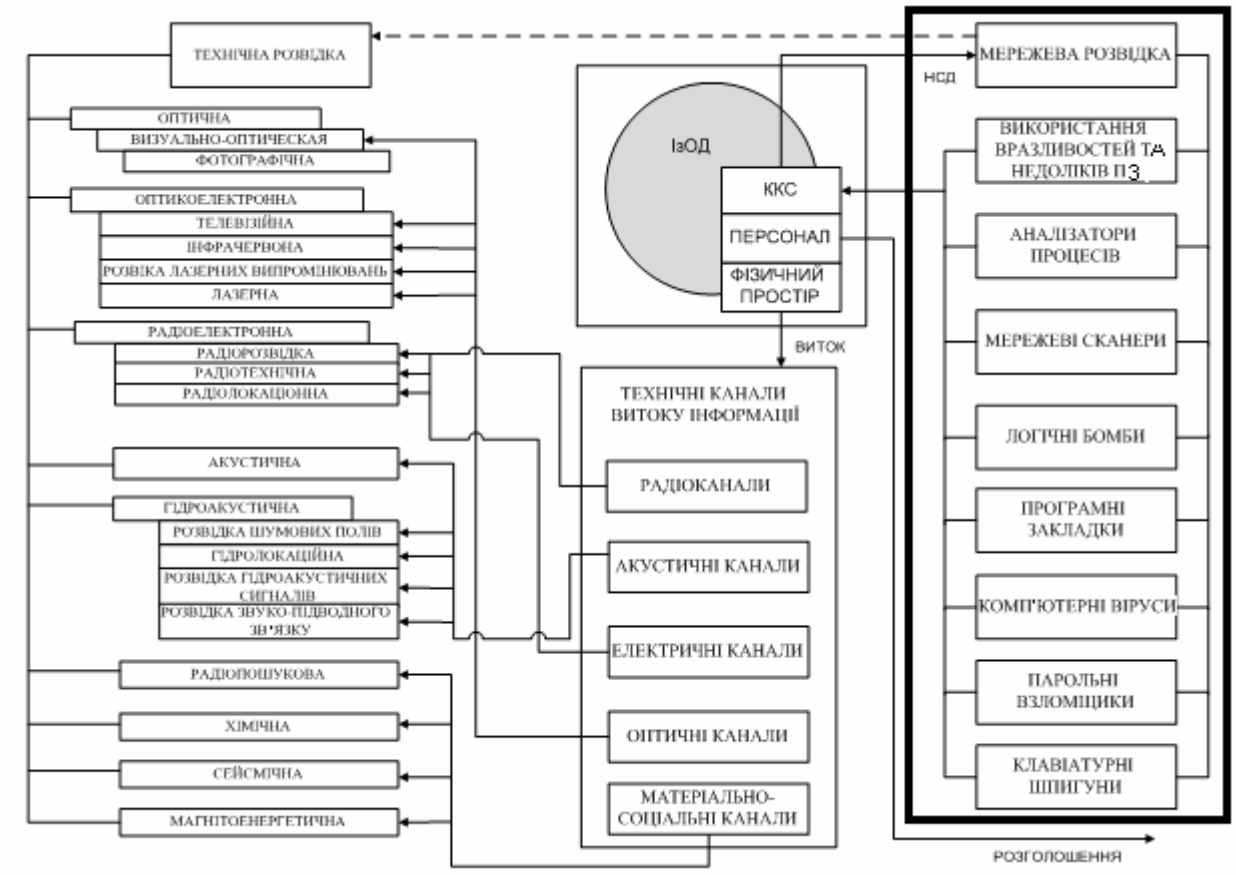

Рис. 2. Роль і місце МР в добуванні інформації з типового об’єкта інформаційного дослідження

Предметом дослідження МР є не побічні (небажані) ефекти, що неминуче супроводжують функціонування технічних засобів інформаційних систем (ІС) і утворюють неумисні канали витоку інформації, а різні види комп’ютерної інформації, що є результатом якраз штатного функціонування ІС і реалізації їх основного призначення – збору, аналізу, обробки, зберігання, передачі інформації та інше.

Основним методом ведення МР є несанкціонований доступ (НСД) до комп’ютерної інформації, що циркулює в ІС. Проте, в термінах комп’ютерної безпеки йдеться не про технічну розвідку і про канали витоку інформації, а, відповідно, про погрози конфіденційності комп’ютерній інформації і про приховані (таємні) канали проникнення в комп’ютеризовані мережі спеціального призначення, які можуть проявлятися, як на фізичному рівні (фізичний доступ до елементів ІС, розкрадання носіїв інформації і так далі), так і на логічному рівні (відключення або обхід системи захисту, захоплення привілеїв, помилкова маршрутизація потоків даних, збір інформації та інше).

В мережевій розвідці, як і в технічній розвідці, можуть застосовуватися, як пасивне перехоплення інформації (прийом і аналіз мережевого трафіка, сканування жорсткого диска та ін.), так і активні методи добування комп’ютерної інформації, за допомогою, наприклад, впровадження в об’єкти інформаційного дослідження вірусів, „троянських” програм, або логічних бомб, що спрацьовують при активізації певних умов або ініціюються сигналами ззовні.

Інструментами організації МР об’єктів інформаційного дослідження можна вважати:

– засоби знищення, перекручення чи розкрадання інформаційних масивів;

– засоби подолання систем захисту;

– засоби обмеження допуску законних користувачів до ресурсів інформаційної системи;

– засоби дезорганізації роботи технічних засобів, комп’ютерних систем.

– комп’ютерні віруси, здатні розмножуватися, впроваджуватися в програми, передаватися за мережевими протоколами, виводити з ладу системи управління і т. п.;

– логічні бомби – програмні закладні пристрої, які заздалегідь впроваджують у інформаційно-керуючі центри військової або цивільної інфраструктури, щоб за сигналом або у встановлений час привести їх в дію;

– засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації у каналах державного, військового, економічного та громадського управління;

– засоби нейтралізації тестових програм;

– різного роду помилки, що свідомо вводяться в програмне забезпечення об’єкта інформаційного дослідження.

Етапами для здійснення несанкціонованого проникнення в об’єкт інформаційного дослідження є наступні:

– вибір мережі дослідження, сервера, інформаційного простору;

– сканування, тестування, збір інформації про об’єкт у відповідності до цільової настанови інформаційного дослідження;

– обробка даних, вибір уразливої точки для проникнення в об’єкт;

– експлуатація вразливості, проникнення в об’єкт;

Подальші дії далі ініціатора інформаційного дослідження залежать від завдання, поставленого перед ним і можуть носити буд-який характер: зміна інформації; витягненння інформації за встановленими критеріями важливості; перевищення повноважень доступу до ресурсів об’єкта; утримання системи у потрібному функціональному стані.

На даний момент існують наступні *методологічні підходи щодо організації мережевої розвідки* (рис. 3):

1. *Перехоплення мережевого трафіка.* Для виконання даних завдань застосовуються наступні методи:

– *мережевий сніфінг*. Для сніфінга мереж *Ethernet,* зазвичай, використовуються мережеві карти, що переведені в режим прослуховування. Прослуховування мережі *Ethernet* вимагає підключення комп’ютера із запущеною програмою-сніфером до сегмента мережі, після чого ініціатору інформаційного дослідження стає доступним весь мережевий трафік, що відправляється і отримується комп’ютерами в даному мережевому сегменті. Ще простіше виконати перехоплення трафіка радіо-мереж, що використовують бездротові мережні посередники, – в цьому випадку не потрібно навіть шукати місце для підключення до кабелю. Або ж може бути встановлено з’єднання до телефонної лінії, що зв’язує комп’ютер із сервером Інтернету;

Рис. 3. Методи організації мережевої розвідки

–*неправдиві запити ARP.* Для перехоплення мережевого трафіка між хостами *A* і *B* ініціатору інформаційного дослідження нав’язує цим хостам свою *IP*-адресу, щоб *A* і *B* використовували цю фальсифіковану *IP*-адресу при обміні повідомленнями;

–*неправдива маршрутизація.* Для перехоплення мережевого трафіка між хостами *A* і *B* ініціатору інформаційного дослідження нав’язує цим хостам свою *IP*-адресу, щоб *A* і *B* використовували цю фальсифіковану *IP*-адресу при обміні повідомленнями;

–*перехоплення TCP-з’єднання.* Ініціатор інформаційного дослідження шляхом генерації і відсилання на атакованих хост *TCP*-пакетів перериває поточний сеанс зв’язку з хостом. Далі, користуючись можливостями протоколу *TCP* з відновлення перерваного *TCP*-з’єднання, він перехоплює перерваний сеанс зв’язку і продовжує його замість відключеного клієнта.

Перехоплення мережевих даних являє собою найбільш ефективний метод мережевої розвідки, що дозволяє ініціатору мережевого дослідження отримати практично всю інформацію, що циркулює по мережі. Найбільше практичне розвиток отримали засоби сніфінга, тобто прослуховування мереж; однак не можна обійти увагою і методи перехоплення мережевих даних, що виконуються за допомогою втручання в нормальне функціонування мережі з метою перенаправлення трафіка на хост інформаційного дослідження, в особливості методи перехоплення TCP-з’єднань. Однак, на практиці останні згадані методи поки ще не отримали достатнього розвитку і потребують вдосконалення.

2. *Ідентифікація мережевих сервісів.* Класичним методом ідентифікації мережевих сервісів („fingerprinting”) став збір так званих „банерів”. Банером називається стандартне запрошення сервісу (*FTPd, HTTPd, SMTPd, TELNETD, IDENTD*). З інформації, укладеної в

банері, нерідко можна отримати дані про версію сервісу і операційну систему, що його використовує.

3. *Сканування портів.* На сьогодні цей підхід, щодо збору інформації про віддалений об’єкт інформаційного дослідження користується найбільшою популярністю. За допомогою сканування визначаються порти, через які працюють мережеві сервіси, їх стан (відкриті або закриті), а також тип мережевого протоколу, що використовується. На підставі цих даних є можливість дізнатися про тип операційної системи, яка використовується. Крім того, інформація про стан портів дозволяє судити про те, які атаки можуть обійти захист і досягти потрібної мети.

Ідентифікація сервісів (*service detection*), як правило, здійснюється шляхом виявлення відкритих портів (*port scanning*). Такі порти дуже часто пов’язані з сервісами, заснованими на протоколах *TCP* або *UDP*. Наприклад, відкритий 80-й порт відповідає наявності *Web*-сервера, 25-й порт – поштового *SMTP*-сервера, 31337-й – серверу троянського коня *BackOrifice*, 12345 або 12346-й – серверу троянського коня *NetBus* і т. д. Для ідентифікації сервісів і сканування портів можна використовувати різні програми, такі як *nmap* або *netcat*.

Вибравши мету інформаційного дослідження його ініціатор визначає запущені на об’єкті сервіси та відкриті порти, що дозволить визначити потенційно вразливі місця і звузити кількість можливих атак. Для сканування портів використовуються різні програми, що відрізняються реалізацією даного механізму.

Процес організації мережевої розвідки передбачає собою реалізацію наступних фаз:

1. Планування і обумовлення цільових завдань – складання „завдань розвідки”, підготовка плану збору інформації, постановка завдань виконавцям інформаційного дослідження і контроль за ходом його виконання. Дана фаза включає вибір контуру мережевого дослідження: мережі, сервера, інформаційного простору.

2. Організація збору інформації – отрмання інформації за існуючими технологічними прийомами. Дана фаза базується на сканування, тестування та інших методах збору інформації про ціль. Можливими шляхами отримання даних можуть бути: отримання інформації від *whois*-серверів; перегляд інформації *DNS*-серверів мережі для виявлення записів, що визначають маршрути електронної пошти (*MX*-записи); інформація про електронну пошту, представлені на сайті об’єкта дослідження.

3. Обробка даних – первинна обробка зібраної інформації, надання їй певної форми (може включати, наприклад, лінгвістичний переклад або переформатування комп’ютерних даних, вибір вразливої точки для проникнення в об’єкт інформаційного дослідження).

4. Експлуатація уразливості, проникнення в систему.

5. Подальші дії ініціатора інформаційного дослідження залежать від поставленого завдання, будь то зміни інформації, несанкціоноване копіювання даних, підвищення повноважень і утримання системи.

6. Аналіз та синтез отриманих даних.

Враховуючи вище зазначене, *організація мережевої розвідки може бути зведена до аналізу, формалізації і реалізації процесів наступних етапів*:

1. *Аналіз передумов* отримання інформаційного контакту з об’єктом інформаційного дослідження.

2. *Впровадження в об’єкт інформаційного дослідження* на основі виявлених вразливостей.

3. *Встановлення каналу передачі даних* з центром управління інформаційним дослідженням.

4. *Аналіз отриманої інформації* центром інформаційного дослідження. Організація інформаційного впливу на об’єкт інформаційного дослідження.

Технологічно цільва настанова даних етапів може бути реалізована на основі дворівневих та багаторівневих клієнт-серверних інформаційних систем, мультиагентних систем.

Технологія мультиагентних систем для організації мережевої розв*ідки*, в свою чергу, має ряд суттєвих переваг перед іншими підходами, що виражаються в наступному:

– концепція агента забезпечує зручний і потужний спосіб опису складної програмної суті, яка здатна діяти з певною мірою автономності з метою виконання завдань від імені користувача;

– інформаційний агент – ,,автономний, інтерактивний і одночасно виконуючий декілька функцій об’єкт, що має внутрішній стан і інформаційний обмін”;

– визначення функцій агентів і менеджерів в стандартах *OSI* досить добре узгоджуються з визначеннями систем *SNMP*. Щоб центр управління і агент змогли взаємодіяти, кожен повинен мати певні знання один про одного. Ці знання модель *OSI* називає контекстом додатка (*Application Context, AC*). *AC* описує елементи прикладного рівня стека *OSI*, які використовуються агентами і центром управління;

– парадигма мультиагентного проектування полягає в тому, що програмні агенти для досягнення мети (виконання деякої цільової настанови) можуть переміщатися з одного об’єкта інформаційного дослідження на іншій. Агенти виконують свою роботу локально на тому сервері або робочій станції, на якій вони в даний момент знаходяться. Обмін повідомленнями між вузлами по мережі агенти, як правило, не використовують.

Тому для реалізації цільової настанови організації мережевої розвідки на основі мультиагентного підходу були сформульовані наступні *часткові задачі дослідження* (рис.4):

– аналіз методів і реалізація технологічних рішень щодо впровадження в об’єкт інформаційного дослідження;

– аналіз методів і реалізація технологічних рішень щодо встановлення з’єднання агенту об’єкта інформаційного дослідження з центром управління;

– аналіз методів і реалізація технологічних рішень щодо управління агентом об’єкту інформаційного дослідження з віддаленого центру управління.

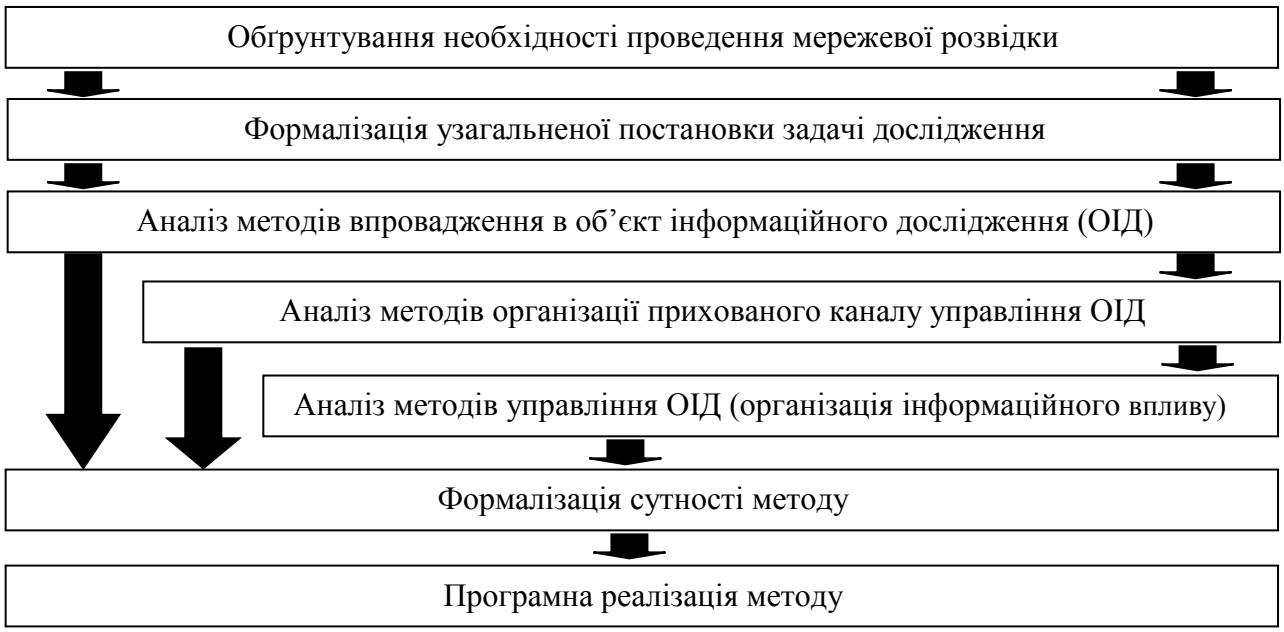

Рис. 4. Часткові задачі дослідження

Специфіка часткових задач дослідження обумовила запропонувати методику для організація чіткої політики проведення інформаційного дослідження віддалених вузлів комп’ютеризованої мережі спеціального призначення з подальшим аналізом отриманої інформації та виявленням можливості інформаційного керування (впливу). Сутність етапів методики та можливих методів реалізації представлені на рисунку 5.

Передумовою виконання етапів методики виступає підготовча фаза, що передбачає аналіз можливих шляхів отримання даних про об’єкт інформаційного дослідження:

– отримання інформації від whois-серверів;
– отримання інформації *DNS*-серверів контуру мережі, що досліджується;
– отримання інформації про існуючі мережеві сервіси (налаштування, гостьові облікові записи, протоколи, доступність сервісу з різних підмереж, наявність функціонування сервісу на нестандартних портах, визначення рівня доступу до сервісу);
– ехо-тестування, сканування портів;
– збір та аналіз інформації за об’єкт дослідженя на основі даних соціальних мереж.

Найбільш актуальними підходами у реалізації першого етапу методики є методи, що пов’язані з різного роду ін’єкціями в об’єкт інформаційного дослідження. Дані методи (*SQL*-ін’єкція, *PHP*-ін’єкція) передбачають впровадження сторонніх команд або даних в працюючу систему з метою зміни ходу роботи системи, а в результаті – отримання доступу до закритих функцій та інформації, або дестабілізації роботи системи в цілому. Найбільш популярна така атака в мережі Інтернет, але також може бути проведена через командний рядок системи.

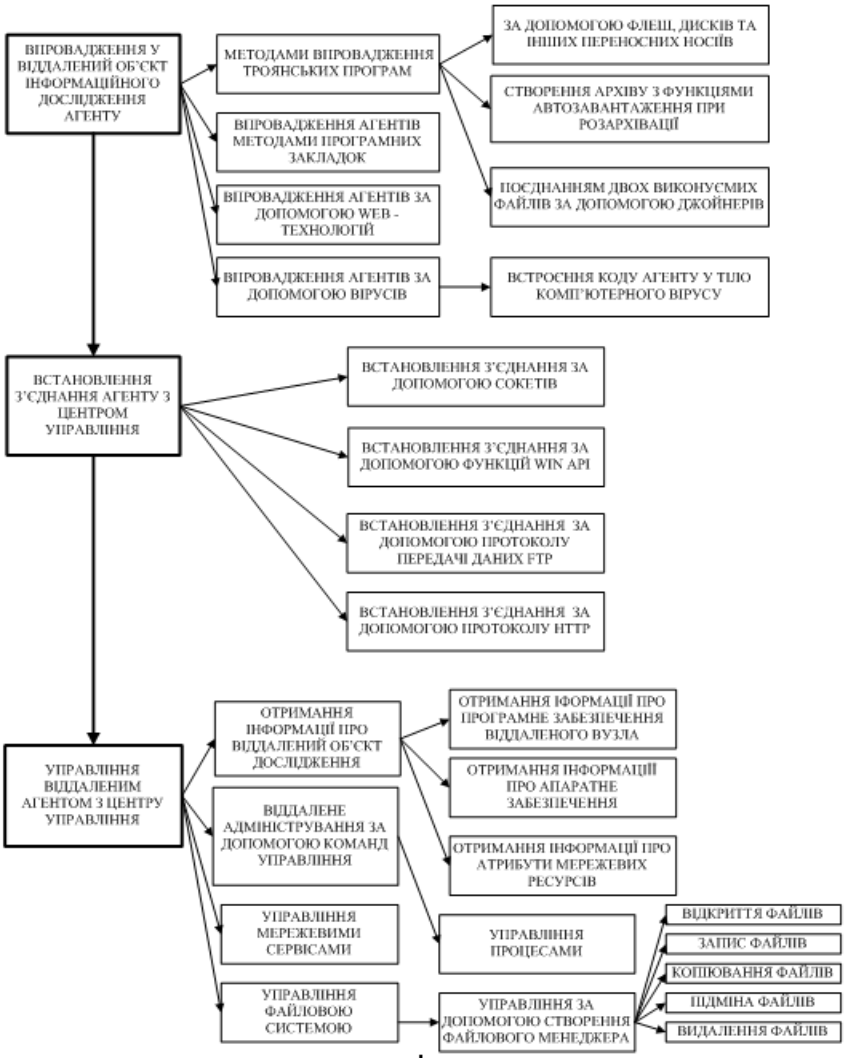

Рис. 5. Методика проведення мережевої розвідки віддалених інформаційних вузлів комп’ютеризованої мережі спеціального призначення

Завданням другого етапу є реалізація методів, що спрямовані на створення або перехоплення каналу зв’язку між двома системами (об’єкту інформаційного дослідження та центру збору та аналізу інформації про об’єкт інформаційного дослідження) з подальшим

отриманням доступ до всієї інформації, що передається. При отриманні доступу на такому рівні ініціатор інформаційного дослідження може модифікувати інформацію потрібним йому чином, щоб досягти своїх цілей. Мета даного етапу – створення каналу для крадіжки або фальсифікації переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити.

Після того як агент встановив з’єднання з центром управління виникає необхідність управління агентом та отримання інформації про віддалений об’єкт інформаційного дослідження. Це передбачає аналіз та обґрунтування методологічних підходів за наступними напрямками досліджень:

- отримання інформації про віддалений об’єкт інформаційного дослідження;
- віддалене адміністрування за допомогою команд управління;
- управління мережевими сервісами;
- управління файловою системою.

Типова схема несанкціонованого отримання інформації віддалених об’єктів на основі методів організації мережевої розвідки представлена на рисунку 6.

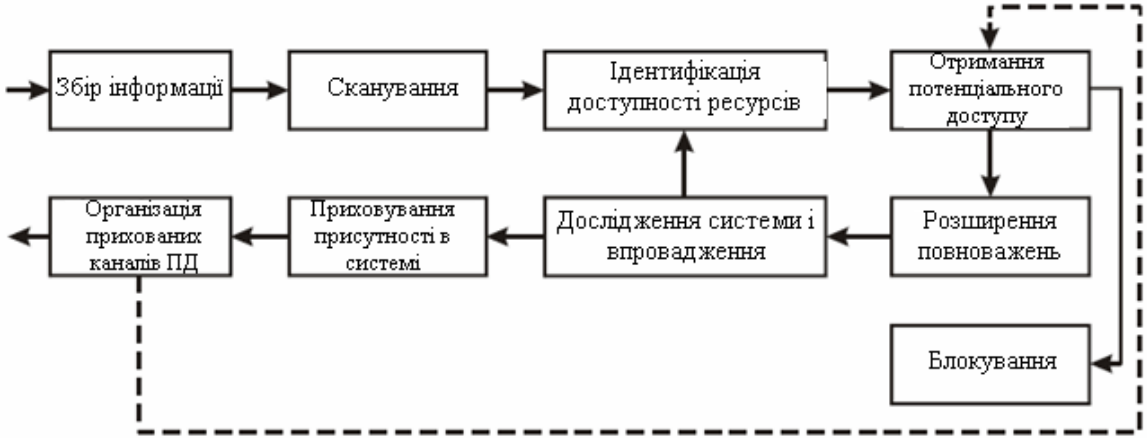

Рис. 6. Схема несанкціонованого отримання інформації віддалених об’єктів на основі методів організації мережевої розвідки

Висновки. Таким чином, аналіз сучасних підходів та технологічних рішень щодо механізмів збору інформації про комп’ютеризовані системи супротивника надає змогу констатувати, що значення мережевої розвідки постійно зростає. З одного боку, це пов’язано з інформаційним протистоянням у сучасних мережоцентричних війнах, а з іншого, з бурхливим розвитком інформаційних технологій. Сьогодні завдання мережевої розвідки стимулюють розвиток систем управління знаннями, глибинного аналізу даних і текстів, з іншого боку найбільш розвинені з цих систем в явному вигляді містять аналітичні блоки, спеціально орієнтовані на завдання мережевої розвідки.

Для прийняття оперативних та ефективних рішень, особливо в контурах комп’ютеризованих систем спеціального призначення, необхідно використання комплексних систем, які дозволяють компонувати і узагальнювати інформацію про об’єкт досліджень, отриману з різних джерел із застосуванням різних технологій.

Подальший напрямок досліджень буде зосереджений на грунтовному описі етапів організації мережевої розвідки для комп’ютеризованих систем спеціального призначення.

ЛІТЕРАТУРА

1. *Martin Libicki*. What is information warfare? / M. Libicki // National Defence University, ACIS Paper, Washington, D.C., 1995.

Манойло А. В. Объекты и субъекты информационного противоборства // Манойло А. В. – М.:

Електронний ресурс Сайт „Cryptography.ru”. http://www.cryptography.ru/.