**УДК 004.056: 004.031.4**

**Д. М. Самойленко**
Національний університет кораблебудування імені адмірала Макарова,
кафедра електрообладнання суден та інформаційної безпеки

# СЕМАНТИЧНІ ЗАГРОЗИ МЕРЕЖНОМУ ІНФОРМАЦІЙНОМУ РЕСУРСУ



**Запропоновано класифікацію семантичних загроз мережним інформаційним ресурсам, спрямованих на маніпулювання їх інформаційним змістом. Описано способи реалізації семантичних загроз. Наведено можливі напрями модифікації комплексної системи захисту інформаційного ресурсу з метою протидії семантичним загрозам.**

**Ключові слова: інформаційна безпека, мережні ресурси, захист інформації, семантичні загрози.**

# SEMANTIC THREATS FOR NETWORK INFORMATION RESOURCE



**The classification of network information resource semantic threats associated with resource's information manipulation is proposed. Some attacks that realize semantic threats are described. For the semantic threats protection proposes the directions of complex network security system modification are shown.**

**Key words: information security, network resource, data protection, semantic threats.**

## Вступ

Проблема захисту мережних інформаційних ресурсів (МІР), розміщених у відкритих мережах, зокрема у мережі Інтернет, еволюціонує разом з розширенням самих мереж. Захист мережної інформації актуалізується положеннями Доктрини інформаційної безпеки України, Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" та супроводжується початком робіт зі створення Єдиної інформаційно-комунікаційної платформи Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Основні напрями розвитку типових захисних рішень для МІР можна умовно поділити на ті, що спрямовані на захист інформаційного вмісту (захист інформації), захист програмно-апаратної частини (технічний захист) та розмежування відповідальності персоналу, що забезпечує функціонування МІР (організаційний захист).

Водночас сучасний стан розвитку мережних технологій вимагає урахування новітнього типу загроз, спрямованих не стільки на порушення функціональності МІР, скільки на використання його легальних можливостей у власних (нелегітимних чи злочинних) намірах. Інколи зловмисник навіть зацікавлений у підтримці дієздатності ресурсу, на який він здійснив атаку. Аналіз подібних впливів вимагає відходу від опису загроз у термінах лише інформатики, використовуючи висновки різних комунікаційних наук.

## Аналіз останніх досліджень і публікацій

Як об'єкт небезпечного впливу довільний МІР являє собою інформаційну комп'ютерну систему. Відповідно, з погляду інформаційної безпеки, слід використати запропоноване нормативним документом [1] означення комп'ютерної системи як набору функціональних послуг. Кожна складова послуга являє собою набір функцій, що дають змогу протистояти певній множині загроз. Функціональні критерії, за якими розрізняються послуги, розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Загрози, що належать до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Загрози, що належать до несанкціонованої модифікації інформації, становлять загрози цілісності. Загрози, що належать до порушення можливості використання МІР, становлять загрози доступності. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості [1, с. 3, 4 (р. 5)].

Усі загрози так чи інакше стосуються виведення МІР з нормального робочого стану. Класичні способи здійснення атак на МІР так само спряжені із порушенням його функціонування [2].

Поширеність відкритих мереж, зростання обчислювальної потужності їх вузлів та кількості учасників супроводжується появою нових видів атак [3] та способів розвідки у мережах [4]. Зокрема з'являється можливість оцінювання рівня розвитку та економічного стану конкурента, шляхом аналізу тематики, якою він цікавиться у глобальній мережі [4].

З метою адекватної реалізації захисних рішень у програмний код МІР рішення проблем захисту мають бути знайдені на етапі проектування комплексної системи захисту інформаційного ресурсу (КСЗІР) [5]. Одним з основних етапів створення КСЗІР є встановлення, якими з можливих способів можуть здійснюватися загрози [6, с. 15 (п. 4.2.1)].

За характером впливу зазначені новітні загрози було запропоновано об'єднувати терміном "семантичні", додатково підкреслюючи той факт, що ці загрози спрямовані саме на зміст (смисл) інформації – її семантику [7].

## Постановка завдання

Метою даної роботи є виявлення, аналіз та класифікація семантичних загроз у глобальних інформаційних мережах, опис потенційних способів їх практичної реалізації у вигляді атак на мережні інформаційні ресурси, а також формування пропозицій щодо реалізації захисних заходів для зазначених загроз.

## Семантичні загрози та атаки

Здебільшого технології семантичних загроз відпрацьовані у галузях, віддалених від мережного програмування: "чорний PR", інформаційні війни, сугестія, провокування агресії тощо. Відповідно способи реалізації семантичних загроз можна розглядати як адаптування розглянутих технологій до інформаційної сфери.

За способом впливу на МІР пропонується розрізняти загрози прямої і непрямої дії. Загрози прямої дії спрямовані безпосередньо на сам МІР: його наповнення, можливості, зміст. Непрямі загрози не зачіпляють МІР безпосередньо, спрямовуючись на інформацію про ресурс чи його власника, розміщену на інших ресурсах (не лише мережних).

Загрози прямої дії слід розрізняти за характером впливу на відкриті та приховані. Відкриті загрози супроводжуються появою у складі МІР нових об'єктів, що несуть певне семантичне повідомлення, доступне довільному користувачеві МІР. Приховані загрози передбачають розміщення таємного повідомлення, як правило, з використанням стеганографічних технологій, або приховане використання функцій МІР. Слід додатково зауважити, що йдеться не про "злам" МІР і підміну інформації чи функцій (що є загрозою цілісності), а про використання його легальних функціональних можливостей та дозволене розміщення чи заміну об'єктів.

Розглянемо детальніше атаки різних видів.

Прямі відкриті загрози. Дія зловмисника (атака): розміщення об'єкта, що несе у собі семантичне повідомлення. Атака використовує можливість МІР розміщувати коментарі, відгуки чи завантаження авторських зображень. Принципи, закладені в атаку, основані на висновках сучасної психології та її розділу – сугестії, що вивчає волю та почуття людини. Використання відповідно побудованих фраз чи зображень здатне вплинути на вибір користувача, передбачити чи спрогнозувати його подальші дії. Ознаки сугестивного впливу вже є у Інтернеті [8]. Потенційну небезпеку атаки можна охарактеризувати цитатою з дослідження [9]: "У наш час теоретично цілком можливо створення комп'ютерного психічного вірусу, який … буде призводити до порушень роботи оператора. Він зможе, наприклад "не бачити" певну інформацію, здійснювати заздалегідь заплановану помилку або без причини наносити шкоду базі даних, знеструмлювати комп'ютер".

Способи захисту від описаної атаки так само слід шукати у психології. Побудова керувальних сугестивних фраз підкоряється певним правилам, законам [9]. Відповідно, існує можливість виявлення ознак потенційного впливу аналізом повідомлень від користувачів перед їх візуалізацією. Оскільки правила побудови мають семантичний відтінок – визначаються не самі слова, а зміст, що ними передається, – система їх аналізу має бути побудована за експертним принципом з виділенням відповідних ознак.

Прямі приховані загрози. Атака: залучення МІР до зловмисних дій. Ця атака можлива у тому випадку, коли засобами МІР передбачено можливість формування запитів до інших ресурсів на зразок перевірки їх справжності, завантаження чи відображення об'єктів, розміщених на інших ресурсах. Зловмисник може сформувати запит, що містить очевидні ознаки якоїсь класичної атаки, наприклад, ін'єкції коду. Також можливе створення потоку запитів, що у поєднанні з залученням до потоку інших МІР матиме усі ознаки розподіленої атаки відмови в обслуговуванні (DDoS-атаки).

Негативні наслідки зазначеного впливу слідуватимуть за результатами реакції з боку МІР, до якого було спрямовано класичну атаку. Як правило, ресурси, які були "помічені" у спробах атаки, вносяться до "чорних списків", що супроводжується подальшим їх блокуванням. В окремих випадках інформація щодо виявлених атак передається до антивірусних компаній, що може спричинити глобальні мережні санкції проти залучених до семантичної атаки МІР.

Протидія зазначеному впливу може полягати у використанні фільтрів для вихідних запитів, цілком аналогічно до фільтрування на ознаку атак вхідних запитів. За наявності вхідного фільтра у вигляді окремого модуля його можна безпосередньо використати для перевірки запиту, що відправляється до іншого МІР.

Атака: використання МІР для прихованої комунікації. Непряма участь МІР полягає у створенні засобів інформаційного обміну між зловмисниками. Використання глобальних мереж терористами для прихованого обміну інформацією неодноразово висвітлювали у пресі [10–11]. Повідомлення приховували засобами цифрової стеганографії, вбудовувалась у зображення, які розміщувались на популярних легальних МІР, доступних у різних країнах.

Непряма участь МІР у інформаційному обміні злочинців не є безпосереднім недоліком цього ресурсу, проте може зашкодити іміджу МІР чи його власника. Захист від подібного впливу полягає у перевірці усіх об'єктів, що розміщуються, на ознаки стегоінтервенції. Цілком можливі заходи активного захисту – оброблення завантажених об'єктів методами, за якими руйнується стего і не спотворюється основна інформація.

Загрози непрямої дії. Атака: інформаційне підкорення (моделювання). Атака інспірується прагненням контролювати інформаційні процеси та розширювати область інформаційного впливу. Інформаційне підкорення може розглядатись як алгоритм, який здатен підібрати такі вхідні дані для інформаційної системи, які дають змогу задіяти у ній бажані внутрішні алгоритми або активувати процеси створення цих алгоритмів [12].

Інформаційний вплив на МІР стає можливий через поширеність тенденції введення системи захисту за інтелектуальним принципом. Однією з вимог до інтелектуальних систем є навчання – зміна порядку застосування алгоритмів чи змісту самих алгоритмів у процесі спостереження, аналізу вхідних даних. Інакше кажучи, якщо система здатна навчатись, її можна "навчити поганому".

Як рекомендації щодо захисту можна запропонувати створення динамічної структури як самого МІР, так і його захисного комплексу. Введення до програмної структури МІР поліморфного коду, засобів інтелектуального аналізу даних та моделювання поведінки, за якої однакові вхідні дані можуть спричиняти різні реакції з подібним, проте відмінним, кінцевим результатом. МІР з постійною структурою, навіть з такою, що передбачає інтелектуальний аналіз вхідних даних, залишається "нерухомою" системою – системою з однаковою реакцію на однакові вхідні дані. Саме цю передбачуваність можна використати з метою інформаційного маніпулювання.

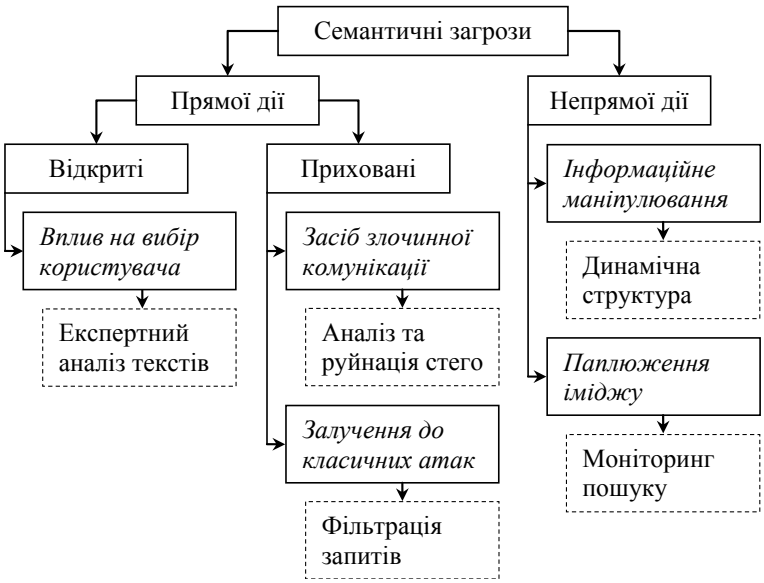
Атака: паплюження іміджу передбачає створення негативного образу МІР чи його власника у мережі. Як правило, атака використовує функції автозаповнення пошукових сервісів. Атаки

супроводжуються судовими позивами [13, 14], спричиненими тим, що пошукова форма "дописувала" образливу інформацію до прізвищ позивачів. Для цього зловмисник може створити потік пошукових запитів, підвищуючи популярність небажаних запитів і тим самим паплюжачи імідж МІР чи його власника.

Пошукові сервіси можуть самі по собі бути використані як засоби підготовки атаки прямої дії чи класичної атаки. При введені у пошуковий рядок фрагмента програмного коду, вразливого до атаки, виведуться результати про МІР, у яких цей код знайдено. У бюлетені NIST зазначено, що такий пошук складав 4 % мережних атак [15].

Захист від атак непрямої дії вбачається у веденні бази даних моніторингу відгуків пошукових сервісів на запити, що містять ключові елементи МІР чи відомості його власників. Зміни у результатах пошуку відносно збереженої у базі даних інформації можуть розцінюватись як ознаки атаки, про що має бути повідомлений адміністратор безпеки МІР.

Описані семантичні загрози, відповідно до запропонованої класифікації, атаки, що їх реалізують, а також зміст захисних заходів можна згрупувати, як це наведено на рисунку.




*Семантичні загрози МІР, атаки та напрями захисту*

Виділені мережні загрози та атаки, що їх реалізують, не можна вважати такими, що утворюють вичерпну множину семантичних загроз МІР. Розширення наведеного переліку загроз, виявлення атак, що їх реалізують, пропозиція та випробування захисних заходів як у складі програмного коду МІР, так і як заходів організаційного характеру, актуалізують перспективи подальших досліджень у обраному напрямі.

## Висновки

Запропоновано класифікацію семантичних загроз за способом та характером впливу на мережний інформаційний ресурс. Описано атаки, що реалізують семантичні загрози.

Наведено рекомендації щодо впровадження додаткових функцій у комплексні системи захисту інформаційного ресурсу для запобігання семантичним загрозам.

Перспективи подальших розвідок вбачаються у розширенні переліку семантичних загроз та атак, а також відповідних до них захисних заходів.

*1. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22. 2. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения / Марсель*

*Низамутдинов. – СПб.: БХВ-Петербург, 2005. – 432 с. ISBN 5-94157-599-8. 3. Якобчук Д. Современные WEB-угрозы и уязвимости. Тенденции, прогнозы. / Д. Якобчук, А. Головин, Ю. Головин // XVI международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. – К.: ООО "ИП ЭДЕЛЬВЕЙС", НИЦ "ТЕЗИС" НТУУ "КПИ", 2013. – с. 129–130. 4. Іванченко І. С. Розвідка у глобальній мережі / І. С. Іванченко, В.О. Хорошко // Матеріали II міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". – Львів: Вид-во Української академії друкарства. – 2013. с. 135. 5. Дудикевич В. Діагностика у сфері технічного захисту інформації. / В. Дудикевич, Т. Крет // Матеріали II Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". – Львів: Вид-во Української академії друкарства. – 2013. – С. 164–165. 6. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53. 7. Самойленко Д. М. Семантична модель загроз мережного інформаційного ресурсу / Самойленко Д. М., Спатар С. С. // Матеріали всеукраїнської науково-технічної конференції з міжнародною участю "Автоматика та електротехніка". – Миколаїв: Вид-во НУК, 2013. – С. 185–188. 8. Шашков И. А. Суггестивное речевое воздействие как манипулятивнаяс трategия виртуального религиозного дискурса / И. А. Шашков. – Режим доступу http://archive.nbuv.gov.ua/portal/natural/vdpu/Movozn/2010_16/ article/59.pdf. 9. Смирнов И. Психотехнологии: Компьютерный психосемантический анализ и психокоррекция на неосознаваемомуровне. / Смирнов И., Безносюк Е., Журавлёв А. – М.: Издательскаягруппа "Прогресс"–"Культура", 1995. – 416 с. 10. Kelley J. Terroristins truction shidden online / JackKelley // USA TODAY. Режим доступу http://usatoday30.usatoday.com/tech/news/2001-02-05-binladen-side.htm (дата звернення: 05.10.13). – Назва з екрана. 11. Kolata G. VeiledMessagesofTerroristsMayLurkinCyberspace / GinaKolata // TheNewYorkTimes. Режим доступу http://www.nytimes.com/2001/10/30/science/physical/ 30STEG.html?pagewanted=all (дата звернення: 05.10.13). – Назва з екрана. 12. Расторгуев С. П. Формула информационной войны. / Расторгуев С. П. – М.: Радио и связь, 1999. – 222 с. 13. Японский суд требует от Google запретить автозаполнение в поисковике / Режим доступу http://cybersecurity.ru/net/147287.html (дата звернення: 29.09.13). – Назва з екрана. 14. Германия просит Google изменить функцию поиска / Економічна правда від 14.05.2013. Режим доступу http://www.epravda.com.ua/rus/ news/2013/05/14/374715/ (дата звернення: 29.09.13). – Назва з екрана. 15. Леннон Э. Компьютерные атаки: что это такое и как защититься от них / Э. Леннон Бюллетень лаборатории информационных технологий NIST (перевод Владимира Казенноваkvn@wplus.net). http://citforum.ru/internet/securities/secatt.shtml (дата звернення: 04.10.13). – Назва з екрана.*