дробів дає можливість економії жорсткої пам'яті комп'ютера, а простота обчислювальних операцій – економію часу, який необхідний для розв'язування задачі.

1. Шмойлов В.И. Периодические цепные дроби. Львов: Академический Экспресс, 1998. – 219с. 2. Шмойлов В.И., Слобода М.З. Расходящиеся непрерывные дроби.- Меркатор, Львов, 1999. – 820с. 3. Рутисхаузер Г. Алгоритм частных и разностей.- М.:ИИЛ, 1960. – 93с. 4. Копченова Н.В., Марон И.А. Вычислительная математика в примерах и задачах. М., Наука, 1972. 5. Robert Vich, Zdenek Smekal Adaptive continued fraction speech synthesis on digital signal processor.-SIP'97, New Orleans, Louisiana, USA, December 4 – 6. – 1997. – P. 163 – 168. 6. Шмойлов В.И., Чирун Л.В. Комплексные числа и непрерывные дроби.- Меркатор, Львов, 2001. – 564с. 7. Русин Б.П. Системи синтезу, обробки та розпізнавання складноструктурованих зображень.-Львів: Вертикаль, 1997. – 264с.

УДК 683.1

Д.О. Тарасов
Національний університет "Львівська політехніка"
кафедра "Інформаційні системи та мережі"

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Describes some methods of computer network information infrastructure modeling, information (data) security threat over unauthorized network investigate, protection against unauthorized network investigate and modeling methods.

Розглядаються методи побудови моделі інформаційної інфраструктури комп'ютерних мереж, загрози інформаційній безпеці, які виникають внаслідок неавторизованого аналізу інформаційної інфраструктури. Наведено методи захисту від неавторизованих спроб побудови моделі інформаційної інфраструктури.

ІНФОРМАЦІЙНА БЕЗПЕКА

Ефективність та успішність ведення тієї чи іншої діяльності залежить від оперативного обміну та аналізу інформації за допомогою комп'ютерних інформаційних систем. Більшість комп'ютерних інформаційних систем мають тимчасові або постійні з'єднання з іншими інформаційними системами та мережами.

Інформаційна система *IS* – програмно апаратний комплекс, який має постійне інформаційне з'єднання та одного адміністратора (особу або організацію відповідальну за роботу системи та реалізацію єдиної політики безпеки).

Вимога постійного інформаційного з'єднання означає що, у довільний момент часу, з імовірністю не меншій $0 < p \le 1$, компоненти інформаційної системи обмінюються інформацією.

Інформаційні системи, політика безпеки яких визначає, що у довільний момент часу, з імовірністю не меншій $0 < p \le 1$, компоненти інформаційної системи можуть обмінюватися інформацією належать до класу S^p - *p–зв'язних* інформаційних систем.

У контексті роботи, компонентами (вузлами інформаційної системи) h_i є потенційні джерела та приймачі інформації комп'ютерної мережі: комп'ютери, мережні сервіси. концентратори, маршрутизатори тощо. Компоненти характеризується можливими сервісами *Srv* (сервіс електронної пошти, HTTP сервер, FTP сервер, сервер БД, SNMP агент тощо).

$H^{IS} = \{h_i\}$ – і множина вузлів інформаційної системи *IS*.

Основними завданнями інформаційної безпеки є:

- вчасне отримання правильної інформації (забезпечення коректності вхідних даних, виявлення помилок та неточностей тощо):
- збереження цілісності інформації (у каналах зв'язку, під час опрацювання. у місцях зберігання),
- правильне використання інформації (коректність методів та алгоритмів, з правильних вхідних даних мають бути зроблені правильні висновки);
- забезпечення конфіденційності (захист від розголошення інформації, яка може спричинити прямі чи непрямі збитки: втрата репутації, зменшення ринків, збільшення конкуренції тощо)
- точне та вчасне донесення інформації до споживача (забезпечення якості інформації, точності, доступності тощо).

Отже, основними завданнями порушника інформаційної безпеки є:

- дезорганізація внутрішнього обміну інформацією між компонентами інформаційної системи (комп'ютерами та обладнанням, процесами, задачами) за допомогою інформаційних потоків I^{Int};
- дезорганізація зовнішнього обміну інформацією між компонентами інформаційної системи та сторонніми інформаційними системами за допомогою інформаційних потоків I^{Ext};
- нанесення шкоди даним (знищення, підміна інформації), які є основою для організації обміну інформацією;
- отримання конфіденційної інформації створенням нових чи використанням існуючих інформаційних потоків I^P для обміну інформацією між інформаційною системою та порушником.

Іншими словами, задача порушника інформаційної безпеки – розбиття *IS* на дві підсистеми IS^S та IS^{UnS} такі, що: адміністратор не повною мірою контролює реалізацію політики безпеки та роботу $h_i^{UnS} \in H^{UnS}$ з IS^{UnS}; h_i^{UnS} містять дані. потрібні порушнику; порушник впливає на роботу h_i^{UnS}, обмін даними IS^{UnS}.

Наприклад, заблокувавши обмін даними між IS^{S} та IS^{UnS}, порушник зменшує параметр зв'язності p інформаційної системи IS та переводить інформаційну систему до класу S^{p_1}, де $p_1<p$.

Під час дослідження інформаційної та економічної безпеки підприємств виникає питання оцінки об'ємів конфіденційної інформації доступної порушнику через комп'ютерні інформаційні мережі та прогнозування можливих втрат.

Для оцінки об'ємів конфіденційної інформації доступної порушнику необхідно визначити:

- ресурси доступні потенційному порушнику інформаційної безпеки (час, обчислювальні потужності, швидкість та пропускна здатність каналів зв'язку тощо);
- рівень кваліфікації та можливі методи дій порушника;
- яка інформація потрібна порушнику;
- яка інформація та які об'єкти інформаційної системи потребують захисту;
- яка інформація що потребує захисту може бути отримана із загальнодоступних (альтернативних) джерел;
- вартість захисту інформації.

Для реалізації завдань порушника інформаційної безпеки суттєве значення мають дані про інформаційну інфраструктуру – компоненти інформаційної системи, що відповідають за передавання та накопичення інформації, опрацювання даних, надання послуг користувачам, шляхи переміщення інформації тощо.

До критичних відомостей про інформаційну інфраструктуру відносяться:

- дані про компоненти інформаційної системи h_i;
- шляхи переміщення інформації (інформаційні потоки) l;
- пріоритетність та алгоритми опрацювання інформації;
- швидкості v та об'єми n опрацювання та передачі даних;
- доступні сервіси Srv та їх параметри;
- опис або зміст даних;
- інформацію про користувачів;
- дані про програмне та апаратне забезпечення, систему захисту інформації.

Знання інформаційної інфраструктури дозволяє порушнику:

- визначити потенційно слабкі місця системи захисту інформації (наприклад, відомі стандартні дірки у захисті) та можливі методи зламу системи захисту інформації;
- знайти критичні з точки зору працездатності інформаційної системи компоненти та дані для DoS атаки;
- точніше оцінити цікавість окремих інформаційних ресурсів.

Так, наявність схеми каналів зв'язку та їх характеристик (пропускна здатність, методи захисту, швидкість, час роботи) дозволяє планувати атаки "відмова у обслуговуванні" та робити припущення про інформаційні потоки підприємства. Аналогічно, відомості про сервіси інформаційної системи, інформаційні потоки підприємства дозволяють досить точно визначати характеристики каналів зв'язку.

Позначимо через $U = \{h\}$ множину всіх вузлів усіх інформаційних систем.

$$H^{IS} \subseteq U \qquad (1)$$

Для збирання інформації про *IS* та виконання своїх завдань, потенційний порушник використовує вузли z_i деякої p_2-зв'язної інформаційної системи (мережі) *Net*, яка характеризується множиною вузлів $H^{Net} \subseteq U$, набором сервісів та властивостями каналів зв'язку (швидкість, пропускна здатність, надійність). Прикладом *Net* є деяка зв'язна сукупність загальнодоступних інформаційних ресурсів, Internet.

Під час дослідження *Net* та *U*, порушник визначає множину тією чи іншою мірою доступних та цікавих вузлів $H^{K_{Net}} \subseteq H^{Net}$.

Аналіз $H^{K_{Net}} \subseteq H^{Net}$ дозволяє визначити множину відомих та потенційно доступних інформаційних систем $K_{Net} = \{IS_k\}$ та, можливо, взнати про існування деяких вузлів $\hat{h}_j$ інформаційних систем $IS_k \in K_{Net}$.

$$\begin{cases} \hat{h}_j \in H^{IS_k} \\ \hat{h}_j \notin H^{Net} \end{cases} \tag{2}$$

Одне із завдань захисту інформації – зменшити кількість доступних порушнику даних про $\hat{h}_j$.

З погляду порушника, IS_k – "чорна скринька", яка характеризується вхідними точками (шлюзами) g_i.

$$g_i \in Gate(IS_k, Net) \tag{3}$$

$$Gate(IS_k, Net) \subseteq H^{IS_k} \bigcap H^{Net} \tag{4}$$

Множина всіх відомих порушнику вузлів системи IS_k має вигляд

$$H_K^{IS_k} = Gate(IS_k, Net) \bigcup \{\hat{h}_j\}. \tag{6}$$

МЕТОДИ ОТРИМАННЯ ДАНИХ ПРО ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ

У літературі, методи отримання інформації про складові віддалених інформаційних систем (тип обладнання, версії ОС та ПЗ, доступні сервіси тощо) називаються fingerprinting. Існує багато видів програмного забезпечення для отримання даних про інформаційну інфраструктуру віддалених ІС.

Щодо необхідності контакту дослідника з ІС – об'єктом дослідження вирізняють контактні та безконтактні методи. Відносно до непомітності методи збирання інформації поділяють на активні (active fingerprinting) і пасивні (passive fingerprinting).

Активні використовують особливості відповідей різних типів систем на певні дії (запити дослідника). Аналізуючи особливості відповідей, можна по типу відповіді визначити тип системи.

Пасивні використовують інформацію, отриману від ІС, без активізації (попередньої) механізмів розповсюдження інформації ІС. Пасивні методи не передбачають обмін інформацією між дослідником та ІС і засновані на прослуховуванні мереж.

Безконтактні методи передбачають отримання інформації про IS_k з деякого третього джерела. Як правило деякого офіційно доступного для дослідника інформаційного ресурсу IS_m. Прикладами IS_m є Інтернет, "дружня" для IS_k інформаційна система тощо. Отже, усувається взаємодія дослідника та IS_k. Контактні методи передбачають взаємодію між дослідником та IS_k.

На рис. 1 наведено методи отримання даних про інформаційну інфраструктуру та основні види інформації, яку отримують за допомогою відповідних методів.

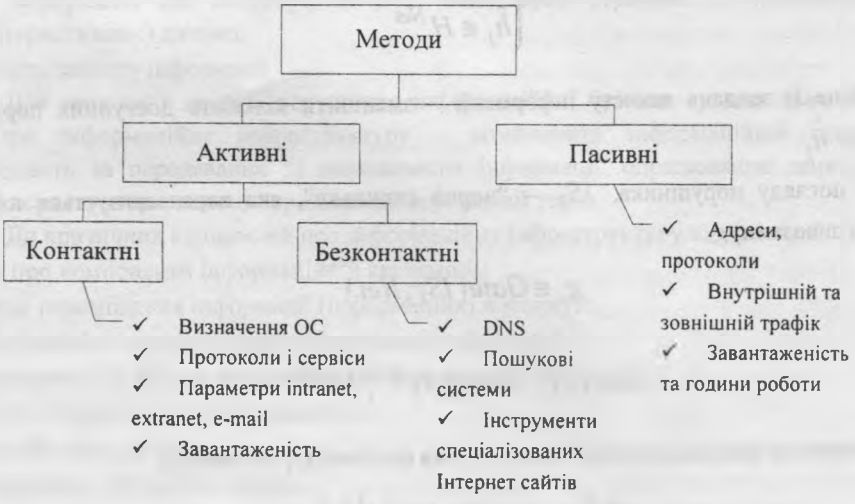

Рис. 1. *Методи отримання інформації про компоненти віддалених інформаційних систем*

АКТИВНІ МЕТОДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Активні електронні методи отримання даних про інформаційну інфраструктуру передбачають контакт між ІС порушника та ІС – об'єктом дослідження (наприклад, обмін інформаційними пакетами через комп'ютерні мережі).

Типова схема такого методу – ІС порушника надсилає по мережі запит деякому існуючому чи потенційно доступному публічному сервісу ІС (наприклад, Web чи поштовому серверу) з метою отримати відповідь та визначити факт існування, параметри та завантаженість сервіса.

Особливістю електронних методів отримання даних є те, що порушник може використовувати проміжну мережну станцію (вузол) у якості адресанта цільового запита.

Визначення операційної системи

Найбільш широко подані засоби визначення назви та версії операційної системи заданого вузла. Деякі засоби дозволяють визначати не лише версію дистрибутиву, а і версії окремих компонент, мережних драйверів, системних бібліотек та виправлень (Service Pack, Hot Fix). У роботі такі засоби використовують як стандартні засоби ідентифікації операційних систем, так і не документовані платформно-залежні особливості роботи драйверів та системних бібліотек.

Основна частина подібних інструментів орієнтована на роботу у мережах з протоколом TCP/IP.

Достовірне визначення ОС дозволяє навіть некваліфікованому порушнику застосувати типові широковідомі засоби порушення безпеки. Досвідчений порушник може використати цю інформацію для адаптації існуючих засобів до конкретних недоліків.

Найпростішим захистом від засобів визначення ОС є:

- обмеження доступу до внутрішньої мережі за допомогою міжмережних екранів (firewall);
- максимальне зменшення кількості вузлів g_i та їх сервісів;
- використання систем визначення атак (Intrusion Detection System, IDS).

Ці методи захисту типові та мінімально необхідні для захищених ІС. Їх використання збільшує захищеність всіх вузлів ІС. Використання IDS робить систему захисту гнучкою та дозволяє оперативно реагувати на можливі загрози.

Визначення протоколів та сервісів

Для визначення працюючих сервісів віддалених ІС та протоколів для зв'язку з сервісами використовують сканування портів та прослуховування мереж.

Окремі з активних методів не мають чіткого юридичного тлумачення як нелегальні (переслідуються законом), або легальні, навіть без врахування розбіжностей у закононавстві країни дослідника та країни місцезнаходження ІС. До таких методів належить і сканування портів.

Сканування портів полягає у відсиланні вузлу запитів та прослуховуванні відповідей на порти (TCP та UDP) з деякого діапазону. Результат – визначення доступності сервісів, їх завантаженості тощо.

Методи блокування визначення працюючих сервісів аналогічні захисту від визначення ОС.

Аналіз відповідей поштових серверів

Для аналізу роботи системи електронної пошти порушник може використати електронні листи з помилковими та правильними адресами в межах домена об'єкту досліджень.

Результатом аналізу будуть дані про:

- наявність, IP-адреси та фізичне розміщення поштових серверів;
- маршрути та швидкості передавання інформації;
- завантаженість поштової системи;
- наявність користувачів електроної пошти та операційної системи.

Політика безпеки повинна містити правило реакції на листи типу спам (spam, небажана кореспонденція) та листи з помилковими адресами.

Прикладом реакції на спам є централізована фільтрація листів без доставки спаму до адресатів. Доцільно організувати збір адрес спамерів від користувачів.

Прикладом реакції на листи з помилковими адресами є відсутність автоматичної відповіді автору листа про неправильну поштову адресу. Тобто не відправляти лист з описом помилки "користувач *123@xyz.com* не існує".

ПАСИВНІ МЕТОДИ ОТРИМАННЯ ДАНИХ ПРО ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ

Пасивні методи використовують прослуховування мереж з метою дослідження:

1. Інформаційної структури підприємства, зокрема:
- протоколів, сервісів;
- основних, резервних та службових маршрутів руху інформації;
- пропускну здатність каналів зв'язку;
- інтенсивність мережного трафіку та документообігу окремих вузлів та сервісів;
- георафічне розсташування обладнання та підрозділів;
- внутрішню та зовнішню адресацію та множину доменів.
2. Наявного обладнання та програмного забезпечення.
3. Персональної інформації щодо працівників, напрямків роботи, місцезнаходження, номери телефонів тощо.
4. Працездатності сервісів (працюють 7*24, з періодичними збоями, з некоректною роботою окремих функцій тощо).
5. Провайдерів, хостерів, та інших партнерів.
6. Конфіденційної інформації, яка доступна через недоліки адміністрування та недоліки політики безпеки.

Зібрана інформація дозволяє зробити припущення про можливі методи доступу до ресурсів інформаційної ситеми, місце збереження інформації.

Наприклад, інформація про номери телефонів може бути використана для визначення розміщення пристроїв, які, можливо, підключені до внутрішньої мережі підприємства та мають вихід у загальні телефонні мережі.

Збирання інформації може відбуватися не безпосередньо на вузлах *IS*, а на вузлах $z_i \in H^{Net}$. Як правило, z_i та *IS* розділяє невелика кількість комутацій IP пакетів. Це пов`язано з особливостями метода та складністю непомітного керування маршрутизацією у гетерогенних інформаційних системах.

Основними методами захисту є:

- фізичне обмеження доступу до інформаційних мереж;
- блокування змін маршрутів переміщення даних;
- використання криптографічного захисту каналів зв'язку та технологій VPN.

БЕЗКОНТАКТНІ МЕТОДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

До типових безконтактних методів дослідження інформаційної інфраструктури належать:

- аналіз інформації DNS;
- використання пошукових систем;

- використання інструментальних засобів та баз даних спеціалізованих сайтів.

Використання безконтактних методів ґрунтується на попередньо зібраній деяким вузлом $q_i \in H^{Net}$ з вузлів $h_i \in H^{IS_k}$ інформації. Інформація про H^{IS_k} може бути зібрана

- за запитом користувача, протягом кількох хвилин;
- за запитом користувача, протягом певного часу, збирають дані та надають результати користувачу;
- незалежно від наявності чи відсутності запитів користувачів щодо того чи іншого h_i.

У своїй роботі q_i використовують легальні методи доступу до h_i, зібрана інформація, як правило, доступна не лише для користувача ініціатора запиту а і іншим користувачам *Net*. Актуальність (вік) отриманої інформації коливається від 1 дня до кількох місяців.

Аналіз інформації DNS

Аналіз інформації DNS дозволяє визначити адреси шлюзів, сервіси електронної пошти, внутрішні сервери DNS, місце хостінгу тощо.

На рис. 2 наведено схему комп'ютерної мережі, яку побудували фахівці Matta Security Limited. Для побудови схеми використовувалась інформація DNS, відповідей серверів електронної пошти (як правило на листи з неіснуючими результатами).

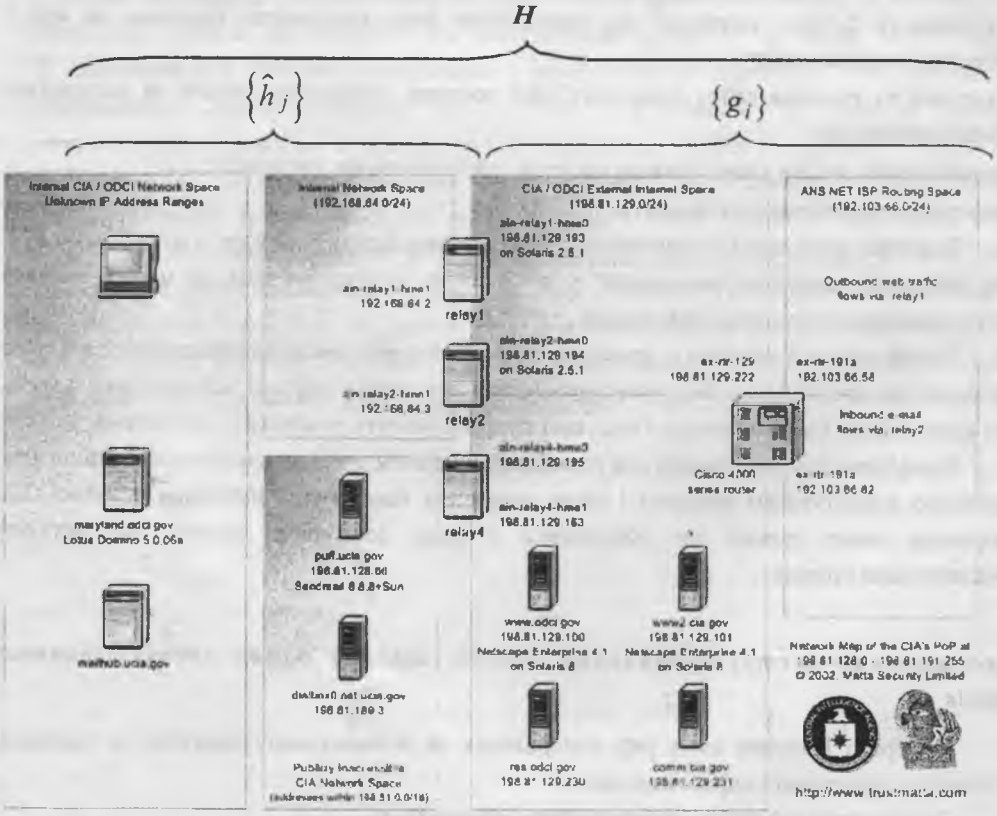

Рис. 2. *Схема комп'ютерної мережі, побудована з використанням інформації з Інтернет*

Для захисту від дослідження структури мережі шляхом аналізу інформації DNS потрібно блокувати доступ до записів внутрішніх DNS серверів з зовні, захищати DNS сервери мережним екраном.

Використання пошукових систем

Не якісно реалізована політика безпеки сайту дозволяє цілеспрямовано шукати "дірки" у захисті за допомогою звичайних пошукових систем. Пошукові системи за допомогою своїх роботів зчитують, індексують та зберігають інформацію з різних web-сторінок, автоматично шукають нові сторінки за допомогою посилань (links) з існуючих. За допомогою пошукових систем досить легко шукати не лише web-сторінки з заданим текстом, а і:

- текстову інформацію у інших форматах (DOC, PDF, PS, RTF тощо), на інших мовах;
- файли та файлові архіви (у тому числі на FTP серверах);
- оцифровані зображення, аудіо та відео записи.

Часто у результатах запиту наданих пошуковою системою (і її кеші) міститься більше інформації ніж передбачається адміністратором сайту. Це, у першу чергу, стосується:

- сторінок та файлів "закритих" від відвідувачів лише відсутністю посилань на них з головної сторінки сайту;
- сторінок та розділів сайту "закритих" від доступу пошукових систем за допомогою файлів robots.txt;
- незахищених файлів з паролями до ресурсів сайту (сторінок, каталогів);
- інформації про користувачів сайту.

Відомим прикладом є отримання користувачами Інтернет файлів зі службового FTP сайту Microsoft, який був "невідомий" у Інтернет та, у зв'язку з цим, не мав обмежував доступ відвідувачів до цінної інформації.

Інший типовий приклад – адміністрування сайту або інших інформаційних ресурсів за допомогою спеціального інструментарію адміністратора у вигляді web-сторінок, адреса яких відома лише адміністратору. Пошукові системи можуть розкрити ці механізми.

Конфіденційна інформація яка розміщена на деякій сторінці сайту може залишитися доступною користувачам Інтернет і після виявлення помилки та знищення сторінки. Ця інформація може деякий час зберігатися у кеші пошукових систем, які встигли проіндексувати сторінку.

Використання інструментальних засобів та баз даних спеціалізованих сайтів

У мережі Інтернет існує ряд комерційних та безкоштовних проектів по наданню технічної та аналітичної інформації про h_i.

До технічної інформації у першу чергу відносяться:

- IP та DNS адреси ресурсу;
- інформація про домени, їх адміністратора та власника;
- місце хостінгу;
- маршрут та швидкості переміщення IP пакетів від q_i до h_i;
- версії програмного забезпечення h_i : ОС, Web сервера тощо;
- наявність заданих користувачів електронної пошти.

До аналітичної інформації належать:

- результати аналізу захищеності h_i ;
- детальна інформація про працездатність h_i протягом часу t.

Методи захисту від неавторизованого дослідження мережі спеціалізованими сайтами ґрунтуються на захисті від активних методів дослідження інформаційної інфраструктури.

1. Вертузаев М.С., Вертузаев А.М. Некоторые аспекты виртуальной разведки // Бизнес и безопасность. – №6 – 2002. – С. 54 – 57. 2. Катренко А.В., Тарасов Д.О. Безпека систем управління розподіленими інформаційними ресурсами// Защита информации. Зб. наук. пр. КМУГА, Київ. – 1999. – С. 165 – 170. 3. Катренко А.В., Тарасов Д.О. Слабкі ланки захисту інформації в інформаційних системах// Науково-технічний журнал "Захист інформації". – №3. – 2000. – С. 58 – 63. 4. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с. 5. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997. – 368 с. 6. Планов С.А. Силы и средства экономической разведки // Бизнес и безопасность. – №4. – 2002. – С. 2 – 3. 7. Тарасов Д.О., Обмеження доступу з мережі до БД // Вісн. Львівського університету. Серія прикладна математика та інформатика. – 1999. – Вип. 1. – С. 213 – 216. 8. Altsoph. Алгоритмы анализа удаленной системы. http://www.bugtraq.ru. 30 с. 2001. 9. Frederick Avolio and Marcus Ranum. A Network Perimeter With Secure Internet Access. In Internet Society Symposium on Network and Distributed System Security, pages 109 – 119. Internet Society, February 2-4 1994. 10. Internet-based Counterintelligence. White paper (tech rep). Matta Security Limited. http://www.trustmatta.com. *11.pp. 2002.*