к.т.н. Мазулевський О.Є. (ВІТІ НТУУ„КПІ”)

АНАЛІЗ ПРИХОВАНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ЗАСТОСУВАННЯ

У статті показано існування прихованих каналів витоку інформації в телекомунікаційних системах із захищеними каналами, наведені визначення інформаційного потоку та на їх основі показано створення моделі прихованих каналів витоку інформації, а також способів їх знищення.

Мазулевский О.Е. Анализ скрытых каналов утечки информации в телекоммуникационных системах военного применения. *В статье показано существование скрытых каналов утечки информации в телекоммуникационных системах с защищенными каналами, приведены определения информационного потока и на их основе показано создание модели скрытых каналов утечки информации, а также способов их уничтожения.*

O. Mazulevskyj Analyses Covert Channels Of Information Leak In The Telecommunication Military Systems. *This article represents existence covert channels of information leak. Also presents definition the information flow, and on these founding represent models of covert channels information leak and method destroyed covert channels.*

Ключові слова: *прихований канал витоку інформації, інформаційний потік, модель прихованого каналу витоку інформації.*

Вступ. Останні роки все більшу важливість в громадській та державній сфері людства відіграє інформація. Трансформація людства в інформаційне суспільство призвела до появи нових методів та способів застосування інформації. Так з’явилися поняття: „інформаційна зброя”, „бойовий інформаційний простір”, „кібернетичний простір”, в яких сама інформація та її властивості відіграють ключові ролі як засобів нападу так і засобів захисту, що обумовлює важливість володіння нею. Тому збереження властивостей інформації (конфіденційності, доступності та цілісності) на даний час є однією з основних задач як в суспільній діяльності людства, так у військовій сфері.

Тому під час використання локальних інформаційно-телекомунікаційних систем (ІТС) для захисту інформації використовують різні методи, способи та засоби. Для захисту інформації в телекомунікаційних системах (ТКС) існує лише обмежена кількість методів. По-перше, це методи як побудови власної телекомунікаційної мережі із застосуванням організаційних способів захисту телекомунікаційних ліній. По-друге захист телекомунікаційних ліній засобами криптографічного захисту. Також застосовують комбінування цих підходів.

В зв’язку з гарними властивостями збереження конфіденційності та цілісності інформації, а також із-за незалежності від платформи та відносно невеликої вартості саме криптографічний спосіб набув значної популярності для забезпечення захисту інформації в ТКС. Але існують деякі недоліки, його застосування, що можуть призвести до порушення властивостей інформації, що передається в ІТС. Один з таких недоліків, це можливість порушення конфіденційності інформації. Так, при впровадженні агента в захищену локальну мережу, він може на зовні (в незахищену мережу), через приховані канали витоку інформації, проводити передачу інформації, що призведе до порушення її конфіденційності. Такі приховані канали несуть інформацію в таких параметрах захищеного трафіку, як розмір пакету так і інтенсивність інформаційного потоку, а також аналіз інтенсивності інформаційного потоку може призвести до викриття структури системи управління та етапу її функціонування, що створює загрози для інформації. В зв’язку з чим, актуальною задачею є розробка додаткової підсистеми в системі захисту інформації в ІТС, яка дозволить звести до мінімуму вплив прихованих каналів витоку інформації на конфіденційність інформації, що циркулює в ІТС.

Метою статті є розкриття сутності існування прихованих каналів витоку інформації та визначення шляхів їх руйнування в сучасних телекомунікаційних системах побудованих із застосуванням криптографічних засобів захисту інформації.

Постановка завдання. Для досягнення поставленої мети необхідно навести математичне визначення інформаційного потоку і на його основі показати модель прихованого каналу витоку інформації та визначити вразливі місця функціонування прихованих каналів та визначити способи їх руйнування.

Вперше поняття прихованого каналу (covert channel) було введено у роботі Лемпсона в 1973 році [1]. Канал називається **прихованим**, якщо він не проектувався, тобто не передбачався для передачі інформації в електронній системі. Таким чином, термін „приховані канали” більше відносяться до телекомунікаційної складової інформаційно-телекомунікаційних систем та мереж.

Аналіз досліджень та публікацій. У роботі Тсаі [2] дано наступне визначення прихованого каналу. Якщо нам дана модель не дискреційної політики безпеки M і її імплементація $I(M)$ в операційній системі, то будь-який потенційний зв’язок між двома суб’єктами $I(S_h)$ і $I(S_i)$ в $I(M)$ називається прихованим каналом, якщо цей зв’язок між суб’єктами S_h і S_i в моделі M не дозволений.

Оскільки всі наведені вище терміни, що стосуються прихованої передачі інформації, відрізняються нюансами додатків, ми будемо без обмеження спільності називати способи прихованої передачі інформації прихованими каналами. Повертатися до вихідних термінів ми будемо в тих особливих випадках, коли виділення відповідних каналів випливає з контексту.

Розглянемо важливі поняття для більш глибокого розуміння прихованих каналів витоку інформації. Першим таким поняттям є „Інформаційний потік”.

Найпростіший підхід до визначення інформаційного потоку можна знайти в TCSEC („Помаранчева книга”, 1985 р.) [3].

Визначення 1. Якщо здійснюється доступ на читання (*read*) суб’єкта S до об’єкта O, то потік інформації йде від O до S. Якщо S має доступ на запис (*write*) до O, то інформаційний потік спрямований від S до O. Транзитивне замикання ланцюгів доступу (навіть без урахування часу) являє собою складний інформаційний потік.

Більш звичне визначення інформаційного потоку вводиться через середню взаємну інформацію. Об’єкт O в інформаційній системі являє собою кінцеву множину допустимих записів у даній мові, а станом об’єкта O є конкретний запис з цього кінцевої множини, яка знаходиться в інформаційній системі в даний момент часу з ім’ям O. Нехай X та Y два об’єкти в інформаційній системі і припустимо, що в даний момент часу стани об’єктів X та Y визначаються спільним розподілом ймовірностей $P(x, y)$ на кінцевій множині пар (x, y), $x \in X$, $y \in Y$, $P(x, y) \geq 0$, $\sum_{y \in Y,\, x \in X} P(x, y) = 1$.

Позначимо $P_X(x) = \sum_{y \in Y} P(x, y)$ і аналогічно $P_Y(y) = \sum_{x \in X}(x, y)$.

Середньою взаємною інформацією об’єктів X та Y називається величина

$$I(X, Y) = \sum_{y \in Y,\, x \in X} P(x, y) log_2 \frac{P(x, y)}{P_X(x) P_Y(y)}$$

Визначення 2. Інформаційний потік між об’єктами X і Y існує, якщо середня взаємна інформація $I(X, Y) > 0$.

Можна довести, що існування інформаційного потоку еквівалентно умові, що існує пара (x, y) така, що $P(x, y) \neq P_X(x)\, P_Y(y)$.

Ясно, що коли існує інформаційний потік від X до Y, то існує такий же інформаційний потік від Y до X.

Відзначимо, що дане визначення потоку еквівалентно завданню спільного розподілу на множинах станів об’єктів X та Y за умови, що заходи, індуковані на X та Y, не є незалежними.

Розглянемо ще одне визначення інформаційного потоку. У деяких роботах для аналізу прихованих каналів вводиться поняття залежності. З точки зору нашого аналізу будь-яка залежність породжує канал передачі даних. Тому ми розглядаємо поняття залежностей як один із способів визначення інформаційного потоку.

Визначення 3. Інформаційним потоком від об’єктів {*S*} до об’єкта *T* можна вважати трійку (*T*, {*S*}, *G*), де *T* змінює свій стан, якщо {*S*} змінює свій стан за умови, що логічний вираз *G* приймає значення істина.

До цього визначення відносяться всі види функціональних зв’язків, в яких значення *T* є функція від деякого набору змінних, куди входить {*S*}.

Узагальненням даної схеми є модель інформаційного потоку як кінцевого автомату, в якому джерело повідомлення посилає вхідне слово на вхід автомата, а одержувач повідомлення бачить вихідну послідовність автомата. Наступним узагальненням є модель прихованого каналу, як імовірнісного автомату, і модель детермінованого автомату з випадковим входом.

Враховуючи, що більшість політик безпеки виражаються через інформаційні потоки розглянемо поняття „Політика безпеки” згідно TCSEC [3].

Визначення 4. Політика безпеки це набір норм, правил і практичних прийомів, які регулюють управління, захист і розподіл цінної інформації [3].

Наприклад, всі інформаційні потоки в системі (в тому числі потенційні) поділяються на дві непересічні підмножини: дозволені й недозволені потоки. Тоді система захисту повинна забезпечувати підтримку дозволених потоків і перешкоджати забороненим потокам. До політик такого класу належить багаторівнева політика безпеки (MLS, Multi-Layer Security). MLS прийнята всіма розвиненими державами світу. У секретному повсякденному діловодстві державний сектор також дотримується цієї політики.

Решітка цінностей (SC) є основою політики MLS. Лінійно упорядкована множина грифів секретності „нетаємно” < „таємно” < „цілком таємно” є найпростішим прикладом такої решітки цінності. У більш загальному випадку до грифів секретності додаються підмножини тематичних категорій із заданого набору категорій. У цьому випадку також виходить решітка цінностей, в якій деякі елементи впорядковані. Наприклад, елементи такої решітки порівняні як: „секретно, кадри, фінанси” < „цілком таємно, кадри, фінанси, матеріальне забезпечення”.

Враховуючи, що класифікація інформаційних ресурсів - це відображення з множини об’єктів системи *O* в множину вузлів *SC* решітки цінностей, то відображення з: $O \to SC$ вважається заданим, якщо $c(Y)$ більше або дорівнює $c(X)$, то *Y* - більш цінний об’єкт, ніж *X*. Кожен об’єкт системи класифікується рівнем секретності і множиною тематичних категорій.

Визначення 5. Інформаційний потік $X \to Y$ вважається дозволеним, згідно MLS, тоді і тільки тоді, коли $c(Y)$ більше або дорівнює $c(X)$ в решітці SC.

Таким чином політика MLS має справу з множиною інформаційних потоків в системі і ділить їх на дозволені й недозволені дуже простою умовою. Однак ця простота стосується інформаційних потоків, яких у системі величезна кількість, тому наведене вище визначення неконструктивне.

Розглянемо клас систем з двома видами доступів *read* і *write* (хоча можуть бути й інші доступи, але вони або не визначають інформаційний потік, або виражаються через *write* і *read*). Нехай процес *S* в ході вирішення свого завдання послідовно звертається до об’єктів O_1, O_2, ..., O_l (деякі з них можуть виникнути в ході вирішення задачі). Нехай

$$S \xrightarrow{r} O_{i_1},\ \dots,\ S \xrightarrow{r} O_{i_k},\ S \xrightarrow{W} O_{j_1},\ \dots,\ S \xrightarrow{W} O_{j_{l-k}} \qquad (1)$$

Тоді з визначення MLS випливає, що при виконанні умов $c(S) \geq c\left(O_{i_t}\right),\ t = 1, \dots, k$, відповідні потоки інформації, що визначаються доступом *read*, йтимуть в дозволеному політикою MLS напрямку, а при $c(S) \leq c\left(O_{i_t}\right),\ t = 1, \dots, k$, потоки, що визначаються доступом *write*, теж будуть йти в дозволеному напрямку. В результаті виконання завдання процесом *S*, інформаційні потоки, які з ним пов’язані, задовольняють політиці MLS. Такого якісного аналізу виявляється достатньо, щоб класифікувати майже всі

процеси і прийняти рішення про дотримання чи недотримання політики MLS. Якщо десь політика MLS порушується, то відповідний доступ не дозволяється. Причому дозвіл ланцюга (1) зовсім не означає, що суб’єкт S не може створити об’єкт O такий, що $c(S) > c(O)$. Однак він не може записати туди інформацію. При передачі управління потік інформації від процесу S або до нього переривається (хоча в нього інші процеси можуть записувати або зчитувати інформацію як в об’єкт). При цьому, якщо правила напрямку потоку при *read* і *write* виконуються, то MLS дотримується, якщо ні, то відповідний процес не отримує доступ. Таким чином, ми приходимо до управління потоками через контроль доступів. В результаті для певного класу систем отримаємо конструктивний опис політики MLS.

Визначення 6. У системі з двома доступами *read* і *write* політика MLS визначається наступними правилами доступу:

$$X \xrightarrow{r} Y \ll=\gg c(X) \geq c(Y),$$
$$X \xrightarrow{w} Y \ll=\gg c(X) \leq c(Y).$$

Нехай є послідовний ланцюг інформаційних потоків $O_1 \rightarrow O_2 \rightarrow O_3 \rightarrow \ldots \rightarrow O_k$. Тоді якщо кожен з потоків дозволений, то властивості решітки дозволяють стверджувати, що дозволений наскрізний потік $O_1 \rightarrow O_k$. Дійсно, якщо інформаційний потік на кожному кроці дозволений, то $c(O_i+1) \geq c(O_k)$ то за властивостями транзитивності решітки $c(O_1) \leq c(O_k)$ наскрізний потік є дозволеним.

MLS-політика в сучасних системах захисту реалізується через мандатний контроль (через мандатну політику). Структура мандатного контролю, яка задовольняє деяким додатковим вимогам, називається монітором звернень. Мандатний контроль ще називають обов’язковим, так як через нього проходить кожне звернення суб’єкта до об’єкта, якщо суб’єкт і об’єкт перебувають під захистом системи безпеки.

Організовується мандатний контроль наступним чином. Кожен об’єкт O має позначку з інформацією про клас $c(O)$. Кожен суб’єкт також має мітку, що містить інформацію про те, який клас доступу $c(S)$ він має. Мандатний контроль порівнює мітки і задовольняє запит суб’єкта S до об’єкта O на читання, якщо $c(S) \geq c(O)$ і задовольняє запит на запис, якщо $c(S) \leq c(O)$.

Відповідно до викладеного, мандатний контроль реалізує політику MLS. Однак мандатний контроль – це не єдиний спосіб управління інформаційними потоками в комп’ютерних системах.

В системі з багаторівневою політикою безпеки, в якій інформаційні потоки зведені до доступів, можливі потоки більш загального типу з розглянутих раніше, які можуть порушувати політику безпеки MLS. Наприклад, будь-який інформаційний потік між непорівнянними вузлами решітки або зверху вниз, який існує, але не виражається через доступи *read* і *write*, буде порушувати політику безпеки MLS навіть при коректній реалізації мандатної контролю доступів. У найпростішому випадку, до якого будемо звертатися далі, в розділеній системі, принаймні, на два рівня *High* та *Low*, то в системі прийнята багаторівнева політика безпеки, розділена на інформаційні потоки знизу вгору (від *Low* до *High*) і забороняє потоки зверху вниз, то порушник може використовувати прихований канал для передачі інформації від програмно-апаратного агента в середовищі *High* до програмно-апаратного агенту в середовищі *Low*. При цьому прихований канал повинен захищати порушника від системи захисту, підтримуючої багаторівневу політику, засновану на визначенні потоків через доступи *read* і *write*. Тобто прихований канал повинен бути невидимий для монітора звернень, системі аудиту, аналітику, який досліджує захищеність системи і т.д.

Потоки в MLS дозволені тільки між порівнянними вузлами знизу вгору. Дана політика захищає конфіденційність інформації. Точно так само, як багаторівнева політика, визначається політика захисту цілісності Байба, тільки дозволеними в даній політиці є всі потоки між порівнянними вузлами, спрямовані вниз.

Припустимо, що небезпеки для порушення секретності не існує, а єдина мета політики безпеки – захист від порушень цілісності інформації. Нехай, як і раніше, в інформацію внесена решітка цінностей SC. У цьому зв’язку будь-який інформаційний потік $X \to Y$ може впливати на цілісність об’єкта Y. Якщо в Y більш цінна інформація, ніж в X, то такий потік при порушенні цілісності Y принесе більш відчутний збиток, ніж потік у зворотному напрямку від більш цінного об’єкта Y до менш цінному X. Байба запропонував в якості політики безпеки для захисту цілісності наступне.

Визначення 7. У політиці Байба інформаційний потік $X \to Y$ дозволений тоді і тільки тоді, коли $c(Y) \le c(X)$.

Можна показати, що в широкому класі систем ця політика еквівалентна наступній.

Визначення 8. Для систем з доступами *write* і *read* політика Байба дозволяє доступ в наступних випадках:

$$S \overset{r}{\to} O \;\Leftrightarrow\; c(S) \le c(O),$$
$$S \overset{w}{\to} O \;\Leftrightarrow\; c(S) \ge c(O).$$

Очевидно, що для реалізації цієї політики також підходить мандатний контроль. Точно так само як і раніше при виконанні мандатної контролю доступів *read* і *write* можливе порушення політики Байба за допомогою прихованих каналів (інформаційних потоків більш загального типу).

Крім зазначених політик слід назвати клас політик захисту зв’язку, в яких інформаційний потік, що передається від відправника до одержувача, не повинен бути перехоплений або спотворений при різних припущеннях щодо можливостей противника по спотворенню інформаційних потоків або з перехоплення частини переданої інформації, або навпаки, по спробах вклинитися в переданий інформаційний потік. Сюди слід віднести ряд стеганографічних схем, в яких основне завдання створити інформаційний потік, „невидимий” для спостерігача, з певним набором можливостей.

Ще одним прикладом є ситуація, коли виробник продає користувачеві комп’ютерну систему для обробки даних, при цьому виробник вмонтував програмно-апаратного агента для аналізу даних, які обробляються покупцем. Дана система може бути зроблена таким чином, що програмно-апаратний агент відповідає рівню *High*, а легальний обчислювальний процес проходить на рівні *Low*. Для передачі агентом інформації назовні системи необхідно побудувати прихований канал між верхнім і нижнім рівнями з виходом в зовнішнє середовище (наприклад, в Інтернет). Аналогічно агент повинен отримувати інструкції з нижнього рівня приховано, оскільки вхідні повідомлення для легального обчислювального процесу і агента приходять по одному каналу.

Для підтримки політики безпеки використовуються механізми захисту, що перешкоджають порушенню політики безпеки. Одним із способів порушення політики безпеки є створення прихованих інформаційних потоків, що не виявляються системами захисту. У разі багаторівневої політики приховані канали передають інформацію з верхніх рівнів конфіденційності на нижній рівень так, щоб механізми захисту не могли перешкоджати порушенню політики захисту конфіденційності. У політиці Байба прихований канал з нижнього рівня на верхній може передати команду „Троянському коню” на знищення або модифікацію інформаційних ресурсів, цілісність яких захищає дана політика.

У зв’язку з цим виникла проблема аналізу прихованих каналів усюди, де виникають обмеження на інформаційні потоки. Будь-який такий аналіз передбачає вирішення чотирьох взаємопов’язаних завдань:

1. Виявлення прихованих каналів;

2. Оцінка пропускної здатності прихованих каналів і оцінка небезпеки, яку несе їх приховане функціонування;

3. Виділення сигналу або одержання якої-небудь інформації, переданої по прихованим каналах;

4. Протидія реалізації прихованого каналу аж до його знищення.

Розглянемо приклади прихованих каналів. Традиційно приховані канали характеризуються як канали по пам’яті або канали за часом. У роботі Кемерера [4] визначаються приховані канали по пам’яті, як такі канали, в яких інформація передається через доступ відправника на запис і одержувача на читання до одних і тих же ресурсів або об’єктів. Прихований канал за часом характеризується доступом відправника і одержувача до одного і того ж процесу або атрибуту, що може змінюватися в часі.

Як і раніше будемо вважати, що система розділена, принаймні, на два рівня *High* і *Low* і в системі прийнята багаторівнева політика безпеки, що розділяє інформаційні потоки знизу вгору (від *Low* до *High*) і забороняє потоки зверху вниз. Порушник може використовувати прихований канал для передачі інформації від програмно-апаратного агента в середовищі *High* до програмно-апаратного агенту в середовищі *Low*. При цьому прихований канал повинен захищати порушника від системи захисту, підтримуючої багаторівневу політику.

Найпростішим прихованим каналом по пам’яті є можливість показу на рівні *Low* назв директорій і файлів, створених на рівні *High*. У даному випадку інформація може передаватися в іменах файлів, які вибираються відповідно до заздалегідь визначеним кодом, в атрибутах файлів, в яких інформація може кодуватися, розмірами файлів, датами зміни файлів і т.д. І, нарешті, існування файлу з даними, який своєю назвою несе біт інформації з верхнього рівня на нижній.

Іншим прикладом каналу по пам’яті є кодування інформації, що зберігається в налаштуваннях будь-яких ресурсів загального користування суб’єктів рівнів *High* і *Low*. Налаштування, проведені на рівні *High*, доступні спостереженню на рівні *Low* і, отже, можуть нести інформацію, виражену заздалегідь визначеним кодом.

Приховані канали за часом вперше стали серйозно розглядатися з 1976 р., коли один з творців захищеної операційної системи Multics Миллен продемонстрував своїм колегам прихований канал за часом, реалізований на ізольованих машинах *High* і *Low* [5]. Обидві машини були приєднані до деяких загальних ресурсів *ROM*, інших каналів або зв’язків між ними не було. У підсистемах *High* і *Low* перебували „Троянські коні”. На рівні *High* „Троянський кінь” при натисканні букв на клавіатурі модулював спеціальним кодом інтервали часів зайнятості бібліотеки *ROM*. Час зайнятості бібліотеки верхнім рівнем сканувати запитами до бібліотеки „троянським конем” нижнього рівня. Одержаний прихований канал за часом дозволяв в реальному часі друкувати інформацію, що отримується через прихований канал з клавіатури підсистеми рівня *High*.

Розглянемо ще один приклад прихованого каналу за часом. Нехай у програмно-апаратній схемі, що реалізує інтерфейс RS-232 між *Low* і *High*, немає передавача на рівні *High* і немає приймача на рівні *Low*. Разом з тим для передачі байт з нижнього рівня на верхній машина верхнього рівня виставляє сигнал готовності до прийому інформації. Черговий байт передається тільки тоді, коли виставлений сигнал готовності прийому. Тоді затримка у виставленні сигналу після чергового переданого байта вважається таймером на нижньому рівні і може таким чином передавати інформацію від програмно-апаратного агента на верхньому рівні до програмно-апаратного агенту на нижньому рівні. Для цього агент на верхньому рівні кодує повідомлення різними по довжині інтервалами затримки виставлення сигналу, а агент на нижньому рівні зчитує ці повідомлення за допомогою таймера.

Прихований канал передачі інформації через Інтернет будується за допомогою вписування повідомлення замість останнього біта оцифрованого зображення, яке передається в якості легального повідомлення. Оскільки останній біт мало впливає на якість зображення, передача інформації виявляється прихованою від суб’єкта, провідного перехоплення і допускає передачу тільки легальних зображень. Добре відомий метод боротьби з даним методом стеганографії, що полягає у зміні формату зображення,

наприклад, за допомогою компресії. Даний метод знищує прихований канал зазначеного виду.

Ще одним прикладом прихованого каналу в аналогічній задачі є прихований канал в TCP/IP протоколі. Поле ISN в TCP-протоколі служить для організації зв’язку клієнта з віддаленим сервером. Розмір цього поля 32 біта. Використовуючи це поле в 5 пакетах, було приховано передано слово Hello.

Особливо слід виділити два приклади каналів за часом, що використовують можливості змінювати тривалості зайнятості в роботі центрального процесора. У першому прикладі відправник інформації змінює час зайнятості CPU протягом кожного фрагмента часу, виділеного для його роботи. Наприклад, для передачі 0 і 1 одна довжина проміжку часу кодує 1, а інша – 0. В іншому випадку відправник використовує проміжки часу між зверненнями до процесора.

Розглянемо моделі прихованих каналів та їх аналіз. Моделі прихованих каналів використовуються для розробки методів виявлення прихованих каналів або, навпаки, для обґрунтування неможливості виявити подібні канали. Традиційний метод виявлення прихованих каналів спирається на модель залежності. Як визначалося вище залежності представляють із себе трійки (T, $\{S\}$, G), в яких зміна параметра T визначається зміною вихідних параметрів $\{S\}$, коли логічний вираз G приймає значення істина.

Нехай у розглянутому раніше прикладі прихованого каналу при використанні односпрямованого каналу RS-232 умова G приймає значення істина, коли при передачі з’являється фіксований байт. У цьому випадку S є час затримки виставлення сигналу про можливість прийому наступного байта. Агент нижнього рівня вимірює час затримки виставлення сигналу на таймері T тільки тоді, коли переданий байт, що звертає логічний вираз G в істину. Пошук даного прихованого каналу спостерігачем за часом затримки виставлення сигналу значно складніше, ніж у наведеному раніше прикладі. Однак, статистичними методами сам факт такої передачі можна розпізнати.

З методом залежностей тісно пов’язаний метод пошуку прихованих каналів на основі матриці поділюваних ресурсів. У цьому методі передбачається, що система повністю описується змінними a, b, c, d, ... Аналіз операцій OP_1 проводиться в матриці таким чином. Рядки матриці відповідають атрибутам поділюваних ресурсів (у нашому прикладі a, b, c, d, ...). Стовпці матриці відповідають операціям системи (OP_1 в прикладі). Значення в клітинах матриці відповідають діям оператора над відповідним атрибутом.

Наступне питання, яке виникає в таких завданнях, чи можна створити „невидимі” для контролюючого суб’єкта приховані канали. У роботі А. Груші [6] доведено, що якщо супротивник знає схему контролю в системі захисту, то в комп’ютерному середовищі при виконанні певних умов можлива побудова невидимого для системи захисту каналу керування програмно-апаратним агентом. При цьому „невидимість” розуміється в абсолютному значенні, тобто доводиться неможливість виявлення такого каналу будь-якими методами і засобами. Також в роботі А. Груші за умови знання противником системи захисту доводиться можливість побудови „невидимого” прихованого каналу при спілкуванні програмно-апаратних агентів у відкритому середовищі між собою. Отримані в цій роботі результати також носять абсолютний характер, тобто доводиться, що прихований канал неможливо виявити будь-якими методами і засобами.

При використанні методу залежностей слід зазначити наступне:

– запропонований апарат і деякі його реалізації (наприклад, метод матриць поділюваних ресурсів є конструктивним інструментом пошуку прихованих каналів;

– не всі приховані канали можуть бути описані за допомогою даного методу.

Зокрема, існують приховані статистичні канали, які не виявляються за допомогою методу виявлення залежностей. Наприклад, якщо T і S пов’язані між собою статистичної залежністю, то метод залежностей може не виявити детермінований зв’язок між цими параметрами. Нехай у розглянутому раніше прикладі прихованого каналу при

однонаправленому інтерфейсі RS-232 умова *G* і раніше відповідала появі у передачі фіксованого байта. У випадках, коли *G* істина, агент на рівні *High* генерує випадкову величину з розподілом P_1, якщо він хоче передати вниз одиницю. Якщо агент хоче передати нуль або не передає повідомлення взагалі, то затримка виставлення сигналу відбувається відповідно до розподілу P_0. Агент нижнього рівня накопичує середні значення інтервалів затримки тільки при передачі зазначеного вище байта. Ідентифікація одиниці або нуля проводиться агентом нижнього рівня за допомогою статистичного критерію. При цьому контролюючий суб’єкт, що спостерігає за затримками виставлення сигналу на верхньому рівні, не знає при якому байті відбувається зміна розподілу часу затримки. Тому можливості виявлення даного каналу контролюючим суб’єктом значно нижче можливості агента нижнього рівня розпізнати сигнал, який передається [7].

Однією з найважливіших завдань аналізу прихованих каналів є оцінка їх пропускної здатності. Пропускна здатність прихованих каналів обчислюється методами теорії інформації. Часто пропускна здатність прихованих каналів вимірюється відношенням кількості приховано переданої інформації до кількості інформації в легальному процесі або контейнері. Наприклад в звичайному цифровому зображенні, що містить 1,5 мегабайт інформації, маніпуляцією останнього біта безпечно можна передати 192 кілобайт прихованого повідомлення. З іншого боку, прихований канал потайного копіювання „цікавого” файлу на дискету має пропускну здатність, рівну обсягу копійованого файлу.

В силу того, що приховані канали володіють, як правило, невеликою пропускною здатністю, може скластися думка, що вони не представляють небезпеки. Часто в таких випадках встановлюється поріг на пропускну здатність, нижче якого канал не вважається небезпечним. Однак, не слід забувати, що оцінки пропускної здатності, носять асимптотичний характер і підхід, пов’язаний з сталим обмеженням пропускної здатності, може виявитися неефективним в реальних системах.

Ще одним прикладом прихованих каналів витоку інформації можливо запропонувати наявність такого негативного явища більш відомого як „прихований вплив” з одного боку або „фізично неіснуючих прихованих каналів витоку інформації”. Представимо таку ситуацію коли рішення на верхньому рівні доступу приймається на основі відкритої інформації зібраної на нижньому рівні доступу. Тобто якщо зловмиснику відома вихідна інформація нижнього рівня та відомий алгоритм прийняття рішення на верхньому рівні, то зловмисник може зробити висновок про прийняте рішення на верхньому рівні. Таке явище можна розглядати з двох сторін. Так зі сторони зловмисника по-перше при можливості впливу на інформацію нижнього рівня можливо провести нав’язування необхідної інформації для вироблення на верхньому рівні прогнозованого висновку (ефект прихованого впливу). По-друге, не проводячи впливу на інформацію нижнього рівня зловмисник може зробити припущення про висновок прийнятий на верхньому рівні (ефект роботи фізично неіснуючого прихованого каналу витоку інформації). Цей приклад дає можливість зробити висновки. Перший, в тому, що застосування багаторівневої політики безпеки не є залогом повної безпеки, так як секретна інформація верхнього рівня може стати відомою на нижньому рівні незалежно від способу реалізації багаторівневої політики. Другий, що найбільш загальне ймовірнісне трактування інформаційного потоку не дозволяє просто розділити множину інформаційних потоків на дозволені і недозволені.

Тепер розглянемо боротьбу з прихованими каналами. Перехоплення інформації, переданої по прихованим каналах, представляє велику складність. Здається, що тут виникають тільки технологічні складнощі, пов’язані з реєстрацією та аналізом швидкоплинних процесів в комп’ютерних системах. Разом з тим доведено, що можливе створення виробником закладок в апаратних системах, які можуть спілкуватися між собою „невидимо” для більшості засобів захисту [7].

У разі використання методів стеганографії рішення задачі виділення прихованих повідомлень видається більш оптимістичним. Прикладом успішного виявлення

стеганографічних вставок є використання прихованого каналу в полі ISN протоколу TCP, що згадувалося вище.

Найбільш ефективним способом боротьби з прихованими каналами є їх руйнування.

Наприклад, у наведеному вище прикладі прихованого каналу витоку інформації при використанні інтерфейсу RS-232 побудованого між рівнями *High* і *Low* пристрій, що транслює байти і випадково змінює затримку виставлення сигналу на верхньому рівні, видиму на нижньому рівні, дозволяє повністю знищити детермінований прихований канал за часом і істотно зіпсувати прихований статистичний канал. А для знищення прихованих каналів витоку інформації в телекомунікаційних системах на основі криптографічно захищених каналів доцільно використовувати засоби які будуть маскувати (приховувати) дійсне значення інформаційного обміну між ІТС та на основі статистичного аналізу властивостей трафіку порушувати властивості його статистичних закономірностей без порушення працездатності ТКС.

З викладеного вище можливо зробити **висновки**:

1. Приховані канали витоку інформації існують, навіть якщо виробник складових ІТС не передбачав їх в системі. Не є винятком системи з реалізацією багаторівневої політики безпеки.

2. В локальних інформаційних системах руйнування прихованих каналів витоку інформації може вирішуватися не тільки інженерно-технічними засобами, а і організаційними та формальними засобами. На державному рівні це обумовлено створенням комплексної системи захисту інформації.

3. В телекомунікаційних системах, які виходять за межі контрольованої зони, навіть при застосуванні криптографічних систем захисту каналів, існують приховані канали витоку інформації по часу. Боротьба з ними організаційними та формальними способами вимагає непропорційних матеріальних витрат.

4. Застосування засобів маскування дійсного трафіку з руйнуванням його статистичних характеристик призводить до руйнування таких прихованих каналів витоку інформації. Тому розробка подібної системи засобів є актуальною науковою задачею, що і буде подальшим напрямом досліджень автора. Що значно дешевше впровадження організаційних та формальних засобів захисту інформації каналів телекомунікаційних систем, навіть захищених криптографічними засобами захисту інформації.

ЛІТЕРАТУРА

1. B.W. Lampson – A Note of the Confinement Problem. – Communications of ACM, v. 16, n. 10, Oct. 1973.

2. C.-R. Tsai , V.D. Gligor , C.S. Chandersekaran – A Formal Method for the Identification of Covert Storage Channels in Source Code – IEEE Transactions on Software Engineering, v.16:6, 1990.

3. Trusted Computer System Evaluation Criteria, DoD, 1985. („Помаранчева книга”, 1985 p.).

4. R. A. Kemmerer and T. Taylor. A modular covert channel analysis methodology for trusted dg/ux. In Proceedings of ACSAC’96, 1996.

5. Secure computer system: unified exposition and multics interpretation prepared for Deputy for Command and Management systems, Electronic Systems Division, am Force Systems Command, United States Air Force, Hanscom Air Force Base, Bedford, project no. 522b prepared by the Mitre Corporation Bedford, Massachusetts, contract no. f19628-76-c-0001, march 1976.

6. Грушо А.А., Тимонина Е.Е. Роль скрытых каналов при построении защиты в распределенных компьютерных системах // Математика и безопасность информационных технологий: Материалы конференции в МГУ 23 – 24 октября 2003 г. М.: МЦНМО, 2004. с. 276 – 281.

7. http://www.nestor.minsk.by/sr/2003/01/30111.html.