

СПОСОБИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

У роботі розглядаються джерела виникнення каналів витоку інформації, класифікація методів несанкціонованого доступу, способи порушення конфіденційності, цілісності й доступності відомостей в інформаційно-телекомунікаційній системі при локальному і віддаленому доступі.

Постановка проблеми. У сучасних умовах при обробці інформації з обмеженим доступом вагому роль відіграють електронно-обчислювальні машини (ЕОМ) – ядро будь-якої інформаційно-телекомунікаційної системи (ІТС). Масштаби і сфери застосування ЕОМ такі, що виникає проблема забезпечення безпеки інформації, що циркулює в ній.

Побудова надійної й ефективної системи захисту не можлива без чіткого усвідомлення методів та засобів несанкціонованого доступу (НСД) до ІТС.

Огляд останніх досліджень і публікацій. Проблемі захисту інформації присвячена велика кількість робіт, більшість з яких носить оглядовий характер і не дає глибинного розуміння причин виникнення каналів НСД, способів та засобів його реалізації, наслідків, що тягнуть за собою такі дії зловмисників.

Формулювання завдання дослідження. У даній роботі досліджуються способи несанкціонованого доступу до ІТС, що перебувають під управлінням різних операційних систем (ОС), та засоби, які для цього використовуються на різних етапах реалізації НСД.

НСД – доступ до інформації, що здійснюється з порушенням встановлених в автоматизованій системі правил його розмежування. Він спрямований на ураження властивостей інформації (конфіденційності, цілісності або доступності) і вимагає використання різних способів та технічних засобів його реалізації. При цьому канали витоку даних утворюються як при роботі ЕОМ, так і в режимі очікування. Джерелами таких каналів є [1]:

електромагнітні поля;

струми і напруги, що наводяться в провідних системах (живлення, заземлення і з'єднання);

перевипромінювання інформації, що обробляється, на частотах паразитної генерації елементів і пристроїв технічних засобів ЕОМ, а також на частотах контрольно-вимірної апаратури.

Крім цих каналів, обумовлених природою процесів, що протікають у ЕОМ, та їхніми технічними особливостями, у комп'ютерах, що постачаються на ринок, можуть навмисно створюватися додаткові канали витоку інформації, для цього може використовуватися [1]:

розміщення в ЕОМ закладок на мовну чи оброблювану інформацію;

встановлення радіомаяків;

навмисне застосування таких конструктивно-схемних рішень, що призводять до збільшення електромагнітних випромінювань у певній частині спектра;

встановлення закладок, що забезпечують знищення ЕОМ ззовні (схемні рішення);

встановлення елементної бази, що виходить з ладу.

Методи НСД до інформації ІТС можна класифікувати, виходячи з таких ознак [1]: за вид доступу, характер дій зловмисника, багаторазовість доступу, спрямованість дій зловмисника, тяжкість наслідків.

За видом доступу всі методи можна розділити на дві великі групи. До першої відносять методи і засоби, що використовуються при локальному доступі до ІТС, а до другої – при віддаленому доступі.

За характером дій зловмисника застосовувані ним методи можуть бути спрямовані на копіювання, модифікацію, знищення чи впровадження інформації. В останньому випадку використовується особливість ІТС, відсутня в традиційних засобах накопичення відомостей, пов'язана з тим, що в таких системах зберігаються не тільки дані, але й програмні засоби, що забезпечують їхню обробку й обмін. Ця особливість інтенсивно використовується зловмисниками, які часто прагнуть одержати доступ до тієї чи іншої ІТС не заради доступу до відомостей, що зберігається в ній, а для впровадження програмної закладки, тобто для несанкціонованого створення в системі нової інформації, що становить собою активний компонент самої ІТС.

За багаторазовістю доступу виділяють методи, спрямовані на його разове та багаторазове одержання. У першому випадку завдання попередження несанкціонованих дій зловмисника значно ускладнюється, однак часто, оскільки останній не піклується про приховання факту втручання, трохи полегшується виявлення таких дій. У другому випадку завдання попередження спрощується, але ускладнюється виявлення, оскільки основну увагу порушник, що планує багаторазово проникати в ІТС, зосереджує на конспірації всіх ознак такого проникнення.

За спрямованістю дій зловмисника вирізняють методи і засоби несанкціонованого одержання відомостей з ІТС, спрямовані на отримання системної інформації (файли паролів, ключів шифрування, переліки облікових записів, схеми розподілу мережних адрес тощо), а також прикладних даних.

За тяжкістю наслідків використовувані зловмисниками методи несанкціонованого одержання інформації можна розділити на безпечні (сканування портів, спроби встановлення з'єднань тощо), потенційно небезпечні (отримання доступу до вмісту підсистем збереження даних, спроби підбору паролів і т. д.), небезпечні (одержання доступу з високим рівнем повноважень, модифікація відомостей в ІТС, копіювання системної та прикладної інформації, створення власних даних тощо) і надзвичайно небезпечні (знищення інформації, блокування доступу легальних користувачів до ІТС та ін.).

Усі програмні засоби, що дозволяють несанкціоновано втрутитися в роботу системи, за своїм призначенням можна розділити на такі групи [2]:

несанкціонований запуск виконавчого коду;

несанкціоноване читання/запис файлових чи інших об'єктів;

обхід встановлених розмежувань прав доступу;

відмова в обслуговуванні (Denial of Service);

використання вбудованих недокументованих можливостей (помилки і закладки);

використання недоліків системи аутентифікації, що дозволяють шляхом реверсування, підбору чи повного перебору усіх варіантів одержати ці дані; „троянські” програми.

Діаграма, що демонструє співвідношення перерахованих методів для ОС сімейства Windows, зображена на рис. 1, для ОС сімейства UNIX – на рис. 2 [3, 4].

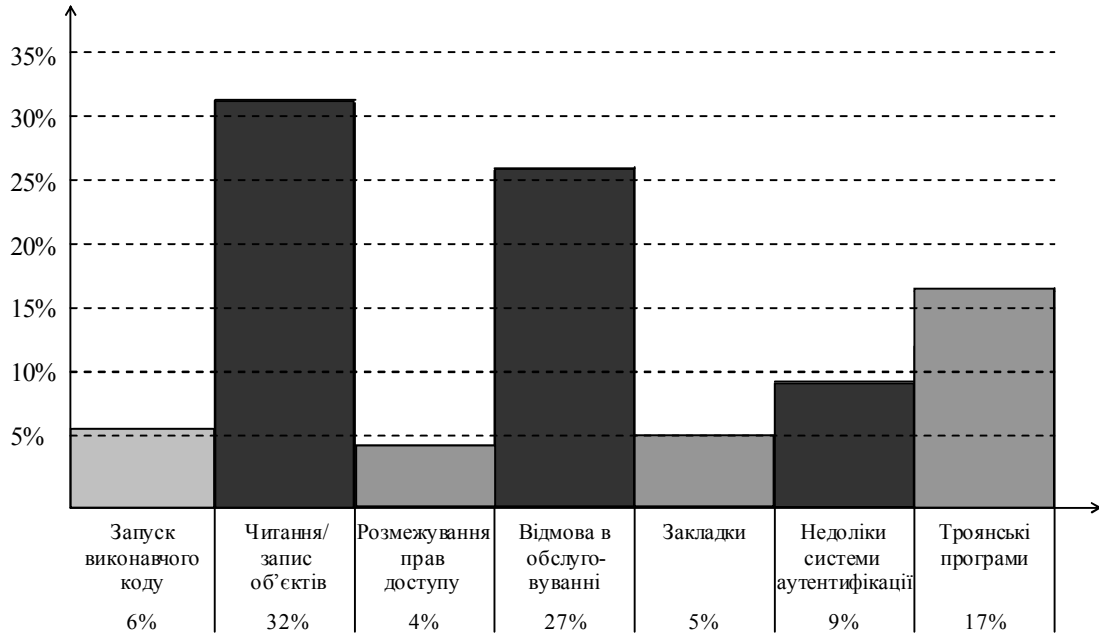


Рис. 1. Співвідношення методів НСД для ОС сімейства Windows

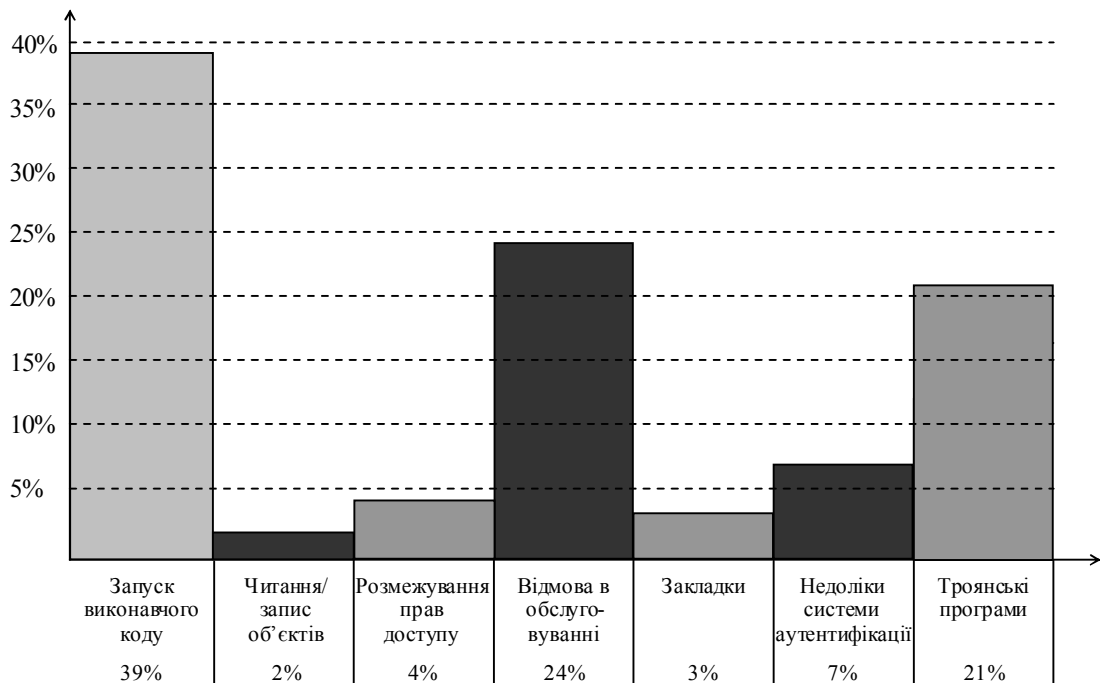


Рис. 2. Співвідношення методів НСД для ОС сімейства UNIX

Способи несанкціонованого запуску виконавчого коду

До даної групи відносяться методи, що ґрунтуються на переповненні буфера для вхідних даних (переповнення стека) і наступній передачі управління на виконавчий код, що занесений при цьому в стек. Для переповнення стека використовується той факт, що

часто при виконанні функцій роботи з рядками, змінними середовища виконання тощо розробники програмного забезпечення не турбуються про перевірку розмірності вхідних даних. А це призводить до виходу за межі масивів, виділених для роботи.

Велика кількість прикладів, що реалізують цю групу методів, розрахована на ОС сімейства UNIX. При цьому переповнення буфера можливе в найрізноманітніших додатках і системних утилітах. Найбільш часто воно використовується для віддаленого запуску виконавчого коду за допомогою обробників мережних запитів і протоколів (*ftp, telnet, pop3* та ін.).

Переповнення буфера можна використовувати й у локальному контексті для того, щоб збільшити свої привілеї чи одержати доступ на рівні адміністратора системи (*root*).

Прикладами реалізації цієї групи методів НСД є такі програми: *Zgv_exploit.c, Kmemthief.c, Imapd_exploit.c* та ін.

Для ОС сімейства UNIX ця група має найбільшу кількість опублікованих прикладів для НСД до системи (майже 40%). Для MS Windows застосування цих методів також можливе, але в основному це призводить тільки до перебоїв прикладного чи системного рівня, що віднесені до іншої групи. Відзначимо, що загальна кількість прикладів, які використовують переповнення буфера для цілей, відмінних від виведення системи з ладу, не перевищує 10%.

Способи несанкціонованого читання/запису файлових чи інших об'єктів

До другої групи можна віднести методи, що ґрунтуються на неправильній інтерпретації прикладними і системними програмами вхідних параметрів. У результаті вони дають доступ до об'єктів, не перерахованих у списках санкціонованого доступу.

Неправильна інтерпретація вхідних параметрів пов'язана з некоректною програмною реалізацією їхньої обробки. Це відбувається тому, що програми, які обробляють дані запити, є або системними утилітами, або прикладними програмами, запущеними в контексті безпеки системи. Завдяки цьому вони мають безпосередній доступ до будь-яких файлових (й інших) об'єктів і можуть надати цей доступ користувачам, котрі не мають достатніх прав для безпосередньої роботи з ними.

Найбільшого поширення набула реалізація даних методів для ОС сімейства MS Windows. В основному помилки зустрічаються в таких стандартних інтернет-додатках, що включені до складу ОС, як IIS (Internet Information Server), поштові клієнти (MS Mail, Exchange) та ін.

Досить велику кількість помилок даного роду можна зустріти в системних утилітах, що реалізують взаємодію за мережними протоколами прикладного рівня (*NETBIOS* та ін.).

Численні помилки зустрічаються в реалізації Java-апплетів, VB-скриптів у браузерях фірм Microsoft і Netscape. Через них за допомогою відповідних апплетів можна одержати НСД до файлових об'єктів. А оскільки обидві фірми випускають свої браузери не тільки для ОС сімейства MS Windows, але й для UNIX, то помилки в більшості випадків дублюються у версіях програмного забезпечення для різних платформ. Варто відзначити, що проблема апплетів відноситься, власне, не до мови Java, а до її реалізації, наприклад, Microsoft Java VM.

Способи обходу встановлених розмежувань прав доступу

До третьої групи можна віднести методи, що ґрунтуються на недоробках (точніше сказати, навмисному створенні так званих „дір”) у ядрі та системних утилітах ОС, що

дозволяють програмними методами обходити встановлені розмежування доступу до об'єктів системи.

Приклади помилок, що складають цю групу, нечисленні, тому що вимагають детального аналізу роботи механізмів ОС (функції API) і відповідної кваліфікації порушника. Потрібно також враховувати, що при розгляді комерційних ОС даний аналіз досить ускладнений, оскільки виробники, зі зрозумілих причин, у край неохоче документують внутрішню архітектуру систем.

Як приклад для даної групи можна привести відому програму „*GetAdmin*”, що реалізує одержання адміністраторських прав, використовуючи некоректну роботу функції *NTAddAtom*, яка дозволяє записувати значення в будь-яку область адресного простору.

У системі Windows NT є деякий глобальний прапор *NtGlobalFlag*, що має адресу 0x801XXXXX. Зміною одного з бітів цього прапора можна перетворити Windows NT у Windows NT Checked Build. У результаті право *SeDebugPrivilege* не буде необхідним для впровадження в системні процеси. Далі, упроваджуючи свій виконавчий код (для чого потрібний був привілей *SeDebugPrivilege*) у системні процеси, можна обійти будь-які обмеження, пов'язані з політикою безпеки.

Способи НСД, що призводять до відмови в обслуговуванні (DoS)

Велику частину цієї групи складають методи, основані на недостатній надійності реалізації стека мережних протоколів ОС. Перебої в її роботі досягаються надсиланням груп пакетів з некоректними заголовками, параметрами тощо.

Прикладами подібних програм є:

teardrop; jolt/jolt2; lornuke; winnuke; winfreez; win95ping та ін.

Іншу частину цієї групи складають методи, що не використовують деталі реалізації стека мережних протоколів конкретної ОС. Вони провокують відмову в обслуговуванні шляхом надмірного завантаження каналу. Найпростішим прикладом може бути надсилання великої кількості пакетів із джерела, що володіє більш швидкісним каналом, приймачу, що володіє менш швидкісним каналом. У такий спосіб цілком вичерпується ресурс приймача, призводячи до його повної чи часткової відмови в обслуговуванні.

Більш складним прикладом є так званий „флудер-множник”. При відправленні на віддалений хост повідомлення, що складається з 20 байт IP-заголовка, у полі Protocol якого міститься значення 00 (що відповідає *IPPROTO_RAW*), віддалена система (чи найближчий до системи, що провокується, маршрутизатор) надасть відповідь повідомленням *ICMP-Destination Unreachable-Protocol Unreachable*, довжиною від 68 до 84 байт. Очевидно, що замінюючи Source Address на адресу об'єкта системи, що атакується, провокується потік з коефіцієнтом множення 4.

Слід зазначити, що програми даної групи безпосередньо не порушують безпеку системи, яка атакується, а просто виводять її з ладу. Але можна уявити собі приклад більш складних атак, коли методами, що призводять до відмови від обслуговування, можна усувати реально діючі в системі вузли, а потім від їхнього імені одержувати НСД до захищених даних.

Способи використання вбудованих недокументованих можливостей

До таких закладок відносяться:

вбудовані інженерні паролі для входу до системи;

спеціальні можливості (послідовність дій) для недокументованих дій (наприклад, в одній з екранних заставок фірми Microsoft є мережний код);

закладки в різноманітних прикладних додатках тощо.

Прикладом використання вбудованого інженерного пароля може бути широко відомий пароль фірми Award "*AWARD_SW*", що дозволяє одержати весь спектр прав для роботи з BIOS.

Способи НСД, що використовують недоліки системи аутентифікації

До шостої групи можна віднести методи, що дозволяють шляхом реверсування, підбору чи повного перебору усіх варіантів одержати дані про аутентифікацію (пароль). Ці програми ґрунтуються на недоліках алгоритмів кодування (хешування) паролів на ресурси, що захищаються, або на вхід в операційну систему.

Прикладом може бути реалізація захисту розподілених ресурсів у Windows 9x, де при розмежуванні доступу на рівні ресурсу пароль зберігається в реєстрі (HKLM\Software\Microsoft\Windows\Current Version\Network\ LanMan\<ІМ'Я КАТАЛОГУ>, у ключі ParmlEnc), зашифрований за допомогою алгоритму, що легко піддається розшифруванню, тому досить просто можна одержати вихідний пароль.

Також невдалий сам алгоритм аутентифікації в Windows 9x через NETBIOS. Якщо клієнт вводить замість повного паролю відкритим текстом тільки його перший символ (байт), то при збігу цього символу пароль вважається правильним.

Слід зазначити, що існує велика кількість програм (не тільки для ОС сімейства MS Windows), призначених для перебору паролів за різними алгоритмами, що враховують недоліки реалізації систем їх аутентифікації та вибору. До таких програм відносяться: *IOphcrack*; *pwlhack*; *pwlview*; *John the Ripper* та ін.

„Троянські” програми

Це програми, що прописуються в автозавантаження ОС або підміняють собою їх системні компоненти (утиліти) і виконують несанкціоновані дії. Для того, щоб така програма з'явилася в системі, користувач повинен сам (навмисно або ні) запустити її на виконання.

Зазвичай „троянські” програми поширюються під виглядом корисних утиліт (у тому числі вони можуть бути в наявності й у некомерційних засобах додаткового захисту інформації), посилаються поштою як приєднані замасковані виконавчі файли, скрипти, встановлюються зловмисником на комп'ютері, що захищається, вручну тощо. Після першого запуску програма замінює собою частину системних файлів чи просто додає себе в список завантаження і надає порушнику доступ до системи або ресурсів, що захищаються. Класифікація та механізм роботи „троянських” програм детально розглянутий у [5].

Прикладом підмінюючої програми є динамічна бібліотека клієнта Novell NetWare для ОС Windows NT "*FPNWCLNT.DLL*", що перехоплює і зберігає передані паролі у відкритому вигляді. Інші програми з цієї групи: *Back Orifice*; *Net Bus*; *Priority* та ін.

Особливої уваги заслуговують технології *локального* і *віддаленого* несанкціонованого доступу до ІТС.

На **локальному рівні** найбільш розповсюджені такі методи НСД:

викрадення (носіїв, окремих компонентів ІТС, копіювання інформації з диска);

використання сеансу легального користувача (через його неухважність або підібраний пароль);

використання облікового запису легального користувача для розширення повноважень в ІТС;

завантаження альтернативної операційної системи.

На відміну від локального рівня палітра методів і засобів несанкціонованого отримання інформації з ІТС при **віддаленому доступі** значно ширша і дуже залежить від використовуваної ОС, налаштування параметрів безпеки тощо.

Для опису методів і засобів НСД до системи при віддаленому доступі скористаємося схемою віддаленого проникнення в ІТС [1], яку застосовує більшість злоумисників (рис. 3).



Рис. 3. Схема НСД до ІТС при віддаленому доступі

На етапі **збору інформації** злоумисник визначає пул IP-адрес робочих станцій (PC), що входять до складу ІТС організації та доступні з мережі загального користування.

До засобів, що використовуються на даному етапі, відносяться стандартні утиліти Unix *whois*, *traceroute* (у Windows – *tracert*), *nslookup*, *host* та їхні аналоги, імпортовані в інші ОС, а також подібні засоби, що мають більш „дружній” інтерфейс (Web-орієнтовані варіанти *whois*, *VisualRoute*, *Sam Spade* тощо).

За допомогою таких засобів можна з’ясувати:

тип мережного підключення організації;

імена й адреси серверів доменних імен;

схему підключення маршрутизаторів і брандмауерів;

реальні імена, телефони й адреси електронної пошти адміністратора підключення;

схему розподілу IP-адрес всередині мережі організації та імена окремих вузлів.

Сканування дозволяє виявити реально працюючі PC досліджуваної організації, доступні в Інтернеті, визначити тип і версію ОС, під керуванням яких вони працюють, а також одержати перелік портів TCP і UDP, відкритих на виявлених PC.

Для цього використовуються такі програмні засоби: *ping*, *fping*, *Pinger*, *icmpeum*, *nmap*, *strobe*, *netcat*, *NetScantTools Pro 2000*, *SuperScan*, *NTOScanner*, *WinScan*, *ipeye*, *Windows UDP Port Scanner*, *Cheops* і безліч інших.

У більшості сучасних мережних ОС для вирішення завдання **ідентифікації доступних ресурсів** існують такі інструментальні засоби: *net*, *nbtstat* і *nbtscan* у Windows NT/2000/XP і *telnet*, *finger*, *rwho*, *rusers*, *rpcinfo* і *rpcdump* у Unix. Крім того, злоумиснику можуть стати в нагоді такі утиліти, як: *nltest*, *rmtshare*, *srvcheck*, *srvinfo* і *snmputil* (Windows NT/2000/XP Resource Toolkit), а також хакерські утиліти *DumpSec*, *Legion*, *NAT*, *enum*, *user2sid*, *sid2user* і *netcat*.

У результаті проведених дій зловмисник отримує інформацію про доступні в мережі диски і папки, про користувачів і групи, що мають доступ до даної РС, а також про додатки, що виконуються на ній, включаючи інформацію про їхні версії.

На етапі *отримання доступу* можуть здійснюватись такі операції:

перехоплення паролів;

підбір паролів для доступу до спільно використовуваних мережних ресурсів;

одержання файлу паролів;

використання програм злому, що забезпечують інтерактивний доступ до РС шляхом переведення працюючих на ній додатків у позаштатний режим;

соціальний інжиніринг.

Для виконання цих операцій можуть застосовуватись такі засоби, як: *NAT, SMBGrind, L0phtcrack, NT RAS, winhlp32, IiSHack* (Windows NT/2000/XP), *Brutus, brute_web.c, pop.c, middlefinger, TeeNet* (Unix) і безліч спеціалізованих програм злому, розрахованих на застосування проти конкретних додатків.

Розширення повноважень дозволяє зловмиснику не тільки одержати повний доступ до РС, що його зацікавила, але й внести себе в список легальних адміністраторів, а також одержати адміністративний доступ до інших РС організації. Для цього застосовуються ті ж засоби злому і підбору паролів, що і при доступі на локальному рівні.

Дослідження системи і впровадження. Одержавши доступ на адміністративному рівні, зловмисник вивчає всі наявні на зламаній РС файли і, знайшовши потрібну інформацію, завершує несанкціонований сеанс зв'язку або, якщо така інформація відсутня чи метою проникнення було не їх одержання, а саме проникнення, приступає до вивчення інших доступних йому як адміністратору РС зламаної ІТС.

Приховання слідів. Одержання адміністративного доступу дає можливість, за необхідності, сховати сліди проникнення.

До методів **створення таємних каналів**, за допомогою яких зловмисник може одержувати багаторазовий доступ до необхідної РС, відносяться:

створення власних облікових записів;

розробка завдань, що автоматично запускаються системним планувальником (*cron* в Unix, *AT* в Windows NT/2000/XP);

модифікація файлів автозапуску (*autoexec.bat* у Windows 98, папка *Startup*, системний реєстр в Windows, файли *rc* в Unix);

впровадження програмних закладок, що забезпечують віддалене управління зламаною РС (*netcat, remote.exe, VNC, Back Orifice*);

впровадження програмних закладок, що перехоплюють потрібну зловмиснику інформацію або імітують роботу корисних програм.

Висновки. Таким чином, методи НСД, що описані в більшості груп, використовують різні недоліки ОС та системних додатків і дозволяють при цілком сконфігурованих і працюючих вбудованих в ОС механізмах захисту здійснювати НСД.

Аналізуючи подану статистику загроз, видно, що велика їхня частина пов'язана саме з недоліками засобів захисту ОС, серед яких, у першу чергу, можуть бути виділені:

некоректна реалізація механізму управління доступом при розмежуванні доступу до об'єктів системних процесів і користувачів, що мають права адміністратора;

відсутність забезпечення замкнутості (цілісності) програмного середовища.

Проведені дослідження показали, що більшість методів НСД обумовлені реалізованим в ОС концептуальним підходом, який полягає в розподіленому адмініструванні механізмів захисту.

Для підвищення захищеності ІТС від НСД необхідно, по-перше, створювати механізми додаткового захисту ОС, а по-друге, реалізувати централізовану схему адміністрування механізмів захисту, в рамках якої буде здійснюватись протидія НСД користувача до інформації.

СПИСОК ЛІТЕРАТУРИ

1. Ленков С. В. Методы и средства защиты информации: в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко. – К. : Арий, 2008.
Т.1: Несанкционированное получение информации. – 2008. – 464 с.
2. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю.Щеглов. – СПб. : Наука и техника, 2004. – 384 с.: ил.
3. Распределение поведений в последнем обновлении антивирусных баз [Электронный ресурс]. – Режим доступа : www.kaspersky/ru/viruswatchlite.
4. Рейтинг вредоносных программ [Электронный ресурс]. – Режим доступа : www.securitist.com/ru/analysis.
5. Умінський В. В. Технології сучасних деструктивних програм / В. В.Умінський // Збірник наукових праць ВІТІ НТУУ „КПІ”. – Вип. 1. – К. : ВІТІ НТУУ „КПІ”, 2009. – С. 137 – 141.

Подано 06.11.09

В. В. Воротников, В. В. Уминский, О. И. Пинчук СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫМ СИСТЕМАМ

В работе рассматриваются источники возникновения каналов утечки информации, классификация методов несанкционированного доступа, способы нарушения конфиденциальности, целостности и доступности сведений в информационно-телекоммуникационной системе при локальном и удаленном доступе.

V. V. Vorotnikov, V. V. Uminskiy, O. I. Pinchuk METHODS OF UNAUTHORIZED DIVISION TO THE INFORMATION-TELECOMMUNICATIONS SYSTEMS

The sources of origin ductings of loss information, classification of unauthorized access methods, methods violation of confidention integrity and availability of information in the information-telecommunication system at local and remote access consider in-process.