Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

В. Б. Вишня, О. С. Гавриш, Е. В. Рижков

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Дніпро
2020

УДК 34+004 (075)
В 55

Рекомендовано до друку
Науково-методичною радою
Дніпропетровського державного
університету внутрішніх справ
(протокол № 10 від 19 червня 2019 р.)

РЕЦЕНЗЕНТИ:

доктор технічних наук, професор **Міхальов О. І.** – завідувач кафедри інформаційних технологій і систем Національної металургійної академії України;

кандидат юридичних наук **Ісмайлов К. Ю.** – завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ.

Вишня В. Б.
В 55 **Основи інформаційної безпеки** : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

ISBN 978-617-7665-08-2

Навчальний посібник призначено для вивчення дисципліни «Основи інформаційної безпеки». У ньому висвітлено питання теоретичного та практичного характеру, пов’язані з теоретичними основами інформаційної безпеки, в тому числі її нормативно-правовим забезпеченням. Надано характеристику апаратним та програмним засобам захисту інформації. Висвітлюються основи та методи криптографії, протидії комп’ютерним вірусам та захист інформації у комп’ютерних мережах.

За кожною темою передбачено контрольні запитання та надається загальний перелік використаних джерел.

Розраховано на здобувачів вищої освіти.

ISBN 978-617-7665-08-2

ЗМІСТ

Тема 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Умови безпеки інформації

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

З початку свого розвитку системи інформаційної безпеки (ІБ) розроблялися для військових відомств. Розголошення такої інформації могло призвести до численних втрат, у тому числі й людських. Тому конфіденційності (тобто нерозголошенню інформації) в перших системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням на сьогодні є захист інформації в комп'ютерних мережах.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Початковий етап розвитку комп'ютерної безпеки міцно пов'язаний із криптографією. Головні умови безпеки інформації – її доступність і цілісність. Інакше кажучи, користувач може будь-коли запросити необхідний йому набір сервісних послуг, а система безпеки повинна гарантувати при цьому його правильну роботу. Будь-який файл або ресурс системи, при дотриманні прав доступу, повинен бути доступний користувачеві в будь-який час. Якщо якийсь ресурс недоступний, то він некорисний. Інше завдання захисту – забезпечити незмінність інформації під час її зберігання або передавання. Це так звана умова цілісності.

Виконання процедур шифрування й дешифрування у будь-якій системі інформаційного процесу сповільнює передачу даних і зменшує їхню доступність, тому що користувач буде занадто довго чекати свої

«надійно захищені» дані, а це неприпустимо в деяких сучасних комп'ютерних системах. Тому система безпеки повинна в першу чергу гарантувати доступність і цілісність інформації, а потім уже (якщо треба) її конфіденційність.

Принцип сучасного захисту інформації можна виразити так – пошук оптимального співвідношення між доступністю й безпекою.

Актуальність вивчення різних аспектів інформаційної безпеки (ІБ) пов'язана із входженням України в глобалізаційні процеси, в яких постійно зростає значення інформації. По суті, йдеться про становлення інформаційного постіндустріального суспільства, однією з найголовніших ознак якого є перетворення інформації на найцінніший товар і продукт. В інформаційному суспільстві інформаційний вплив на державу, суспільство, громадянина є ефективнішим, ніж політичний, економічний, військовий. Значення інформації зростає в міру зникнення національних кордонів між державами, подолання наслідків інформаційної ізоляції пострадянського суспільства (хоча ці наслідки в багатьох сферах, зокрема науковій, не подолані дотепер). Водночас суспільство не може не турбувати інша проблема − інформаційне перенасичення, надмір недостовірної та шкідливої інформації, не зникає і загроза національній безпеці держави через інформаційне шпигунство, інформаційну агресію іноземних держав тощо.

У таких умовах Конституція України проголошує ІБ «справою всього українського народу». Звісно, це декларація, оскільки захист ІБ держави не може бути загальнонародною справою, для цього існують спеціальні державні органи. Однак прогалини та недоліки чинної системи ІБ можуть негативно позначитися на матеріальному та духовному становищі народу. 1997 року Верховна Рада України ухвалила «Концепцію національної безпеки України», яка до загроз у національній безпеці відносить «інформаційну експансію з боку інших держав, витік інформації, що становить державну таємницю, а також конфіденційної інформації, що є власністю держави». ІБ заявлена як одна з головних цілей «Національної програми інформатизації» (1998 р.) Цим питанням опікується комісія з питань ІБ при Президенті України.

Що ж таке ІБ? На жаль, жодні нормативні акти не дають визначення ІБ, поняття не має законодавчого оформлення. Є кілька неофіційних визначень, які не завжди узгоджені між собою. Одне з них можна знайти в проєкті Закону «Про інформаційний суверенітет та інформаційну безпеку України». У ньому ІБ розглядається як «захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовір-

ність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України». На думку фахівців, це визначення демонструє надмірний патерналізм держави, яка бере на себе готовність визначати, яка саме інформація є «недостовірною», «зіпсованою», «достовірною» і яку треба заборонити. Демократична держава не повинна мати монополії на інформацію та її тлумачення, а сприяти інформаційному плюралізму.

Дослідники пропонують такі характеристики ІБ:

– ІБ балансує на стику національної безпеки та інформаційної функції держави;

– питання ІБ має екстериторіальний характер, не замикається на національних кордонах;

– протистояння між бажанням держави «засекретити» якомога більший масив інформації і невід'ємним правом людини та громадянина мати вільний доступ до інформації;

– державне регулювання інформаційної сфери відбувається лише на правовій основі.

Зважаючи на це, об'єктом ІБ є інформація, важлива для функціонування держави, демократичного розвитку суспільства, інформаційні стосунки між особою, державою та суспільством, інформаційні права людини як невід'ємна складова загальнолюдських прав.

1.2. Державна політика та система технічного захисту інформації в Україні

Якою ж є політика держави у сфері ІБ? Україна − посттоталітарна країна, відтак, чимало проблем, що виникають є наявні у сфері ІБ, вкорінюються у так званий «синдром тоталітаризму», який полягає у намаганні держави, попри демократичні декларації, побудувати таку модель стосунків між державою та суспільством, за якої суспільство матиме мінімальні відомості про державу, і відповідно мінімальний вплив на прийняття політичних рішень. І при цьому держава знатиме про суспільство практично все. Якщо конкретніше, йдеться про дві небезпечні тенденції. З одного боку, ми маємо дуже низький рівень законодавчого забезпечення інформаційної сфери. Зокрема, Закон України «Про інформацію» 1992 р., навіть з доповненнями до 2005 р., застарів і не відповідає низці демократичних засад. Єдиним законом, який регулює сферу інфо-

рмації з обмеженим доступом (ІЗОД), є чинний Закон «Про державну таємницю» в редакції 1999 р. Та з іншого боку, існують величезні масиви інформації, які під дію цього Закону не підпадають, а власної законодавчої бази або не мають, або вона вкрай незадовільна. Йдеться про службову таємницю («конфіденційна інформація, що є власністю держави»), комерційну таємницю, охорону персональних даних та інше. Коли доступ до інформації обмежується не законом, а особистим рішенням посадової особи, це відкриває шляхи для чиновницького свавілля, порушення інформаційних прав громадян, необґрунтованих засекречень тощо.

Щодо державної таємниці (ДТ) держава здійснює політику поступового збільшення обсягу засекреченої інформації, хоча, на думку фахівців, це навряд чи є доцільним. Наслідком такої політики можуть бути зниження якості прийняття політичних рішень через недоступність потрібної інформації, криза влади, інформаційна ізоляція, застій в економічному, політичному та науковому житті. Наприклад, абсолютно недоречним кроком учені вважають віднесення до сфери ДТ інформації «*про наукові, науково-дослідні, конструкторські, проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва продукції, технологічних процесів, які мають важливе оборонне чи економічне значення чи суттєво впливають на зовнішньоекономічну діяльність і національну безпеку України*», оскільки держава не повинна безпідставно засекречувати інформацію «про всяк випадок», бо те, чи матиме така наукова інформація оборонне чи економічне значення, ще невідомо. Але це істотно обмежує науково-інформаційні контакти наших учених з їхніми колегами з-за кордону, не сприяє вільному обігу наукової інформації. А без свободи, поза сферою інформаційного різноманіття, інформація існувати не може.

Інформаційне право − це відносно молода галузь права, предметом якої є інформаційні відносини, що виникають у процесі обігу інформації в інформаційній сфері. За останні роки сформувався великий обсяг законодавчих актів, що регулюють інформаційну сферу, зокрема сферу ІБ та захисту інформації. Отже, до предмета вивчення інформаційного права потрапляє ІБ та нормативно-правова база, яка її гарантує. Якими ж є недоліки українського законодавства у сфері ІБ та захисту інформації? Це:

1. Невідповідність більшості законів та нормативно-правових актів, ухвалених до 1996 року, Конституції України та міжнародним нормативно-правовим актам.

2. Надмірна декларативність українських законів, певні положення

декларуються без вказівок на механізми їх реалізації.

3. Нерідко трапляються посилання на посилання, або посилання на такі норми, які неможливо застосувати.

4. Відсутність чіткої ієрархічної структури у нормативно-правовій базі (Конституція − закони − підзаконні акти та відомчі інструкції).

5. Велика кількість підзаконних актів ускладнює можливості їх застосування.

6. Випадки суперечностей між законами та відомчими інструкціями, міжнародними правовими актами та українськими законами, колізії між різними законами тощо.

7. Неузгодженість нових законів з попередніми, що спричиняє правовий хаос.

8. Наявність великого обсягу засекреченої інформації поза законодавчим полем.

9. Широкі можливості для посадових осіб безкарно і безпідставно засекречувати інформацію.

10. Незадовільна правова основа доступу громадян до інформації, що перебуває в руках державних органів.

11. Термінологічна неузгодженість (наприклад, у законодавстві відсутнє однозначне тлумачення таких термінів, як «документ», «інформація», «державні секрети», «таємна інформація», «таємниця», «інформаційна безпека», «інформаційний суверенітет», «документована інформація», є 5 різних визначень «конфіденційної інформації», 3 визначення «захисту інформації», 2 – «таємної інформації» тощо).

12. Невизначеність механізмів забезпечення відповідальності за порушення інформаційного законодавства.

13. Не розробленість, точніше відсутність законодавчої бази для таких сфер як захист персональних даних, доступ до конфіденційної інформації, що є власністю держави, комерційна таємниця та інше.

14. Відсутність інституцій, які б спеціалізувалися на питанні захисту інформації, форм запиту на отримання інформації, невизначеність механізму надання державних документів.

За подібних умов інформація про діяльність державних органів може фактично перетворитися на «державну таємницю», що суперечить принципам України як демократичної, правової, соціальної держави, та міжнародним демократичним нормам стосунків влади і громадян.

1.3. Нормативно-правова база України у сфері технічного захисту інформації

Права людини в інформаційному суспільстві: міжнародні правові акти, що стосуються інформаційних прав особи. Принцип верховенства права в інформаційній політиці держави. Важливим аспектом інформаційної діяльності демократичної держави є ієрархія пріоритетів, серед яких на першому місці стоїть міжнародне право, на другому – національне законодавство разом з Основним Законом, і вже далі − підзаконні акти, які не повинні суперечити міжнародному та національному законодавству. Як відомо, в українському законодавстві з дотриманням цієї ієрархічності не все гаразд. Часто підзаконні акти та відомчі інструкції стоять на першому місці в діяльності окремих державних органів та посадових осіб.

Які міжнародні правові акти гарантують інформаційні права та свободи людини і громадянина, зокрема право на конфіденційність та право на вільне отримання інформації? Передусім, це «Загальна Декларація прав людини» (1948 р.). Відповідно до статті 12, «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя“. Згідно з статтею 19 «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів».

Важливим документом є «Європейська конвенція про захист прав людини та основних свобод» (1950 р.), яка про інформаційні права людини говорить таке: стаття 10 «Кожен має право на вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів». У цій же конвенції міститься перелік винятків, коли права громадян можуть бути обмежені на законних підставах: «Здійснення цих свобод може бути обмежене в інтересах громадської безпеки, запобігання злочинам, охорони здоров’я, моралі, запобігання розголошенню конфіденційної інформації».

Розвиток комп’ютерних технологій призвів до масової практики автоматизованої обробки інформації в комп’ютерних мережах, в тому числі інформації персонального характеру. Виникла потреба додаткового захисту інформаційних прав людини. Цій меті має служити «Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру» (Страсбург, 28 січня 1981 р.). У Преамбулі Конвенції зазначено, що її головною метою є гарантування свободи інформації незале-

жно від кордонів, безперешкодного обігу інформації між народами. Зміст Конвенції можна проілюструвати через окремі статті.

Стаття 1 гарантує право людини на недоторканність особистого життя, яке підлягає ризику під час автоматизованої обробки персональних даних. Стаття 5 визначає якість обробки даних про особу: «Дані особистого характеру, що підлягають автоматизованій обробці: а) отримуються та обробляються сумлінно та законно; б) зберігаються для визначених та законних цілей; в) мають бути адекватними, відповідними і ненадмірними з точки зору цілей, заради яких вони зберігаються; г) мають бути точними і поновлюватися (на вимогу особи); д) зберігатися не довше, ніж це потрібно цілям збереження». Стаття 6 виокремлює особливу категорію персональних даних, які одержали назву «вразливі» або «делікатні». Це «дані особистого характеру, що свідчать про расову належність, політичні або релігійні та інші переконання, а також дані особистого характеру, що стосуються здоров'я, статевого життя, не можуть піддаватися автоматизованій обробці. Це правило стосується також особистих даних, що стосуються кримінального засудження». Стаття 8 встановлює додаткові гарантії для суб'єкта даних: а) «особі надається можливість встановлювати існування файлу особистих даних для автоматизованої обробки, особу і місцезнаходження контролера файлу; б) отримувати без затримки чи витрат підтвердження чи спростування інформації про зберігання даних особистого характеру; в) вимагати виправлення і знищення незаконно одержаних даних; г) гарантується правовий захист персональних даних». Звісно, європейське право передбачає чітке окреслення сфери винятків, їх обґрунтованість і зрозумілість. Обмежити інформаційні права громадян можна в кількох випадках: в інтересах захисту державної та громадської безпеки, валютно-кредитних інтересів держави, боротьби з кримінальними структурами, а також в інтересах захисту прав і свобод інших громадян (стаття 9). Крім того, особисті дані можна використовувати в статистичних підрахунках та наукових дослідженнях (як правило, в знеособленому вигляді).

Важливим міжнародним документом є також «Директива Європарламенту та Ради Європи стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року, метою якої є «забезпечення невтручання в особисте життя при обробці персональних даних в телекомунікаційному просторі та для забезпечення вільного переміщення таких даних». Сфера винятків будується за аналогією з попередніми європейськими актами: це громадський порядок, оборона, державна безпека (включаючи економічний добробут держави), кримінальне право.

Імплементація положень європейського права щодо захисту інформаційних прав людини та громадянина вважається необхідною умовою демократизації політико-правової системи України, її наближення до стандартів ЄС та формування громадянського суспільства.

Конституція України про інформаційні права громадян та інформаційну безпеку. Конституція (1996 р.) у статті 17 проголошує, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». Йдеться про те, що від інформаційної безпеки держави залежить доля народу, його матеріальний добробут та духовне благополуччя. Стаття 19 однозначно стверджує пріоритет Закону та Конституції перед іншими нормативними актами: «Органи державної влади та органи місцевого самоврядування, їхні посадові особи зобов'язані діяти лише в межах повноважень та у спосіб, що передбачені Конституцією та законами України». Проте громадяни мають право апелювати до Конституції як закону прямої дії, якщо посадова особа відмовляє у задоволені запиту громадянина, керуючись підзаконними актами чи внутрішніми інструкціями.

Стаття 32 гарантує, що «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації».

Стаття 34 говорить про право «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір», а також встановлює перелік винятків, коли право громадян може бути обмежено: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших

людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Як бачимо, поряд із винятками, визначеними європейськими документами, згадується кілька специфічно українських, а саме: запобігання розголошенню конфіденційної інформації та «підтримання авторитету правосуддя». При цьому найменш зрозумілим є останній виняток.

Так чи інакше, Конституція є найважливішим юридичним актом, що забезпечує інформаційні права громадян України, право на недоторканність приватного життя, та закладає основи для розробки спеціального законодавства з охорони інформаційної безпеки держави.

Основні положення Закону України «Про національну безпеку від 21 червня 2018 року». «Стратегія національної безпеки України від 26 травня 2015 року» про загрози в інформаційній сфері. Базовим чинним законом, що регулює інформаційну сферу, є Закон України «Про інформацію», прийнятий 2 жовтня 1992 р. Доцільно викласти основні положення закону. Під терміном «інформація» закон розуміє «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві» (стаття 1). Основними принципами інформаційних відносин вважаються: гарантованість права на інформацію; відкритість та доступність інформації; свобода інформаційного обміну; об'єктивність та вірогідність інформації; законність її одержання, використання, поширення та збереження (стаття 5).

Статті 17 та 18 визначають галузі та види інформації: основними галузями інформації є: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна. До видів належить: статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

Стаття 27 надає законодавче визначення терміну «документ»: «Документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві. Первинний документ – це документ, що містить в собі вихідну інформацію. Вторинний документ – це документ, що являє собою результат аналітико-синтетичної та іншої переробки одного або кількох документів».

Стаття 28 поділяє інформацію на відкриту та інформацію з обмеженим доступом (ІЗОД), а стаття 30 роз'яснює, що таке ІЗОД, встановлює режими доступу до інформації. Інформація з обмеженим доступом

за своїм правовим режимом поділяється на конфіденційну і таємну.

«*Конфіденційна інформація* – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України. До конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості:

про стан довкілля, якість харчових продуктів і предметів побуту;

про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень;

про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмеженим.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верхов-

ною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист».

Ця стаття є засадничою для роботи державних службовців з документами, що належать до категорії ІЗОД, громадян, які зацікавлені в отриманні «суспільно важливої» інформації та захисті своїх інформаційних прав, в тому числі права на конфіденційність. У наступній статті 31 якраз йдеться про право громадян на доступ до інформації, а саме: громадяни мають право «*знати у період збирання інформації, які відомості про них і з якою метою збираються, як, ким і з якою метою вони використовуються; доступу до інформації про них, заперечувати її правильність, повноту, доречність тощо.*

Державні органи та організації, органи місцевого і регіонального самоврядування, інформаційні системи яких вміщують інформацію про громадян, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом, а також вживати заходів щодо запобігання несанкціонованому доступу до неї. У разі порушень цих вимог Закон гарантує захист громадян від завданої їм шкоди використанням такої інформації.

Забороняється доступ сторонніх осіб до відомостей про іншу особу, зібраних відповідно до чинного законодавства державними органами, організаціями і посадовими особами.

Зберігання інформації про громадян не повинно тривати довше, ніж це необхідно для законно встановленої мети.

Всі організації, які збирають інформацію про громадян, повинні

до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних.

Необхідна кількість даних про громадян, яку можна одержати законним шляхом, має бути максимально обмеженою і може використовуватися лише для законно встановленої мети.

Відмова в доступі до такої інформації, або приховування її, або незаконні збирання, використання, зберігання чи поширення можуть бути оскаржені до суду».

Усі ці положення відповідають європейським правовим нормам. Держава не має права безпідставно відмовляти громадянину у задоволенні його інформаційного запиту, а термін вивчення запиту не повинен перевищувати 10 днів. Задоволення ж запиту повинно відбутися упродовж 30 днів. Громадянин має право оскаржувати в суді відмову державного органу задовольнити інформаційний запит, при цьому саме держава повинна доводити в суді законність такої відмови. Якщо суд встановив, що запитувачу відмовили незаконно, винні посадові особи притягуються до дисциплінарної та іншої, передбаченої законодавством, відповідальності.

37-ма стаття роз'яснює обмеження на доступ до тієї чи іншої інформації. Не всі інформаційні запити громадян можуть бути задоволені. До інформації, що не надається та не оприлюднюється, належать: інформація, визнана державною таємницею; конфіденційна інформація; інформація про оперативну і слідчу роботу органів прокуратури, Міністерства внутрішніх справ, Служби безпеки України, роботу органів дізнання та суду, якщо її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи; інформація, що стосується особистого життя громадян; документи, що становлять внутрішньовідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю; інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої надано запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення; інформація фінансових установ, підготовлена для контрольно-фінансових відомств.

Закон забороняє державну цензуру: «*забороняються створення*

будь-яких органів державної влади, установ, введення посад, на які покладаються повноваження щодо здійснення контролю за змістом інформації, що поширюється засобами масової інформації» (стаття 45-1). Водночас інформацією та інформаційною свободою не можна зловживати: «*інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини*» (стаття 46).

Закон гарантує рівність усіх учасників інформаційних відносин (громадяни, юридичні особи та держава), розглядає інформацію з погляду права власності. Крім того, закон визначає низку термінів, важливих у процесі інформаційних відносин: це поняття «інформація як товар», «інформаційна продукція», «інформаційна послуга».

Важливим моментом є встановлення відповідальності за розголошення інформації, яка розголошенню не підлягає (стаття 47). Однак у цій статті є важливий елемент, пов'язаний з формуванням громадянського суспільства: громадянин звільняється від відповідальності за розголошення ІЗОД, якщо він у суді зміг довести «суспільну важливість» такої інформації, тобто потреба суспільства знати цю конкретну інформацію визнана важливішою за можливі негативні наслідки її розголошення. На цьому пункті, до речі, ґрунтується легітимність роботи журналістів.

Закон «Про інформацію» 1992 р. (з доповненнями до 2005 р.) безумовно є прогресивним у плані забезпечення демократичних прав та свобод громадян, вільного обігу інформації, але до деяких його положень фахівці висловлюють зауваження. Наприклад, акцентують на відсутності у Законі концепції офіційної інформації, неконкретність положень про секретність, розмитість сфери прав та обов'язків громадян і обов'язків державних органів. До осіб, що мають право доступу до інформації, пропонують включити також жителів держави, які ще не отримали громадянства. Концепція «авторського контролю» за доступом до конфіденційної інформації вважається застарілою, принаймні, вона зникає з європейського права (йдеться про те, що власник конфіденційної інформації самостійно визначає режим доступу до неї, спосіб отримання, коло осіб, що мають доступ, захист і так далі). Також звертається увага на брак критеріїв гіпотетичної шкоди від розголошення інформації та суспільного інтересу до цієї інформації. Дослідники пропонують створити доступний реєстр усіх документів, на які поширюються положення Закону для того, щоб допомогти громадянам у пошуку потрібної їм інформації. Нарешті, найбільшій критиці підлягає поло-

ження 29-ї статті про переважне право доступу до інформації службовців під час виконання службових обов'язків. На думку фахівців, це положення суперечить принципові рівності усіх осіб у доступі до інформації. Отже, Закон «Про інформацію» потребує істотних змін та доповнень, враховуючи демократичний поступ нашої держави та вимоги часу.

Україна − суверенна держава. Тому на порядку денному – проблема захисту її інформаційного простору від негативних впливів. Це не означає запровадження цензури, мова йде лише про те, що держава, яка існує на кошти платників податків, повинна забезпечити для них належні умови для інтелектуального, фізичного, духовного розвитку. Про захист інформаційного простору держави йдеться у Законі України «Про національну безпеку України від 21.06.2018 року (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) . У першій статті 6 пункту, загрози національній безпеці України це явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України;

Державні стандарти та нормативні документи, що стосуються технічного захисту інформації (ТЗІ). До них належать такі документи: «Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення» (ДСТУ 3396.0-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт» (ДСТУ 3396.1-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення» (ДСТУ 3396.2-96).

Ці стандарти установлюють об'єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють та користуються інформацією, що підлягає технічному захисту.

Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження. Об'єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоря-

джаються ІЗОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ. Цими стандартами визначаються носії ІЗОД, середовище поширення, мета ТЗІ (див. далі), джерела загроз.

До джерел загроз належать діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Далі йдеться про канали поширення загроз, розроблення і реалізацію системи захисту інформації, контроль за ТЗІ та функції нормативних документів у сфері ТЗІ. Такими функціями, зокрема, є: проведення єдиної технічної політики; створення і розвиток єдиної термінологічної системи; функціонування багаторівневих систем захисту інформації на основі взаємоузгоджених положень, правил, методик, вимог та норм; функціонування систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації; розвиток сфери послуг у галузі ТЗІ; установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури; організація проектування будівельних робіт у частині забезпечення ТЗІ; підготовка та перепідготовка кадрів у системі ТЗІ. Нормативні документи системи ТЗІ поділяють на: нормативні документи із стандартизації у галузі ТЗІ; державні стандарти та прирівняні до них нормативні документи; нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України; нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів України органом; нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

1.4. Структура системи захисту інформації

Комплексна система захисту інформації (КСЗІ) наведена на рис. 1. Основне завдання КСЗІ полягає в блокуванні технічних каналів витоку інформації та ліквідації наслідків реалізації загроз інформації. Загрози інформації складаються з багатьох факторів, тому завдання захисту потребує комплексного підходу з використанням новітніх технічних засобів і наукових розробок. Вирішення завдань включають в себе аналіз об’єкта захисту, розробку системи виявлення каналів витоку інформації та економічне обґрунтування необхідності використання системи захисту інформації. КСЗІ являє собою діючі у єдиній сукупності законодавчі, організаційні, технічні, криптографічні та інші заходи і засоби, які забезпечують захист інформації від усіх визначених загроз і можливих каналів її витоку, і особливо каналів електромагнітного випромінювання.

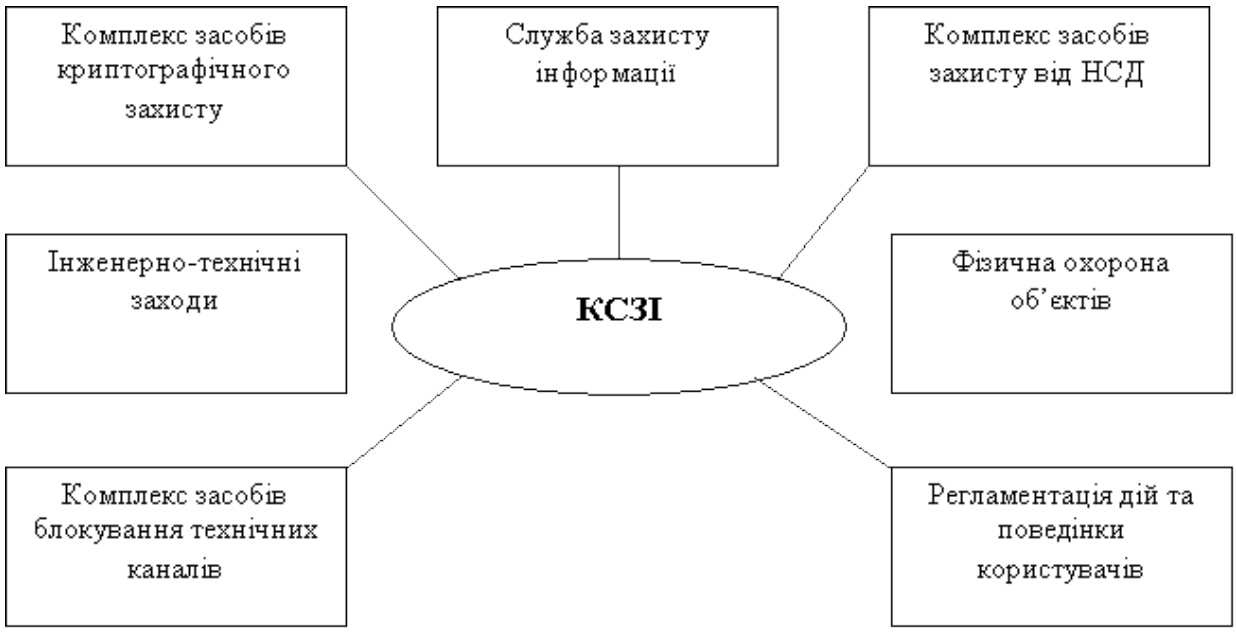

Рис. 1.1. Комплексна система захисту інформації

КСЗІ створюється поєднанням застосування технічних, фізичних та організаційних заходів. Проектування КСЗІ відбувалось на принципах побудови раціональної та ефективної системи захисту. Структура засобів КСЗІ зображена на рис. 1.2. Організаційно-правовими заходами реалізується комплекс відповідній нормативно-правовій базі держави адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності і засобів ТЗІ, а також шляхом створення служб, відповідальних за їх реалізацію. Основним завданням технічних заходів є забезпечення фізичної інформаційної безпеки.

Фізичні заходи захисту інформації створюють пристрої та споруди, проводять заходи, що утруднюють або унеможливлюють проникнення потенційних порушників у місця, де можна мати доступ до системи управління та інформації, що захищається. Пропонується застосувати фізичну ізоляцію споруди, де встановлена апаратура, від інших будівель зокрема – огородження й систематичний контроль території, організація контрольно-пропускних пунктів, обладнання вхідних дверей спеціальними замками, організація системи охоронної сигналізації.

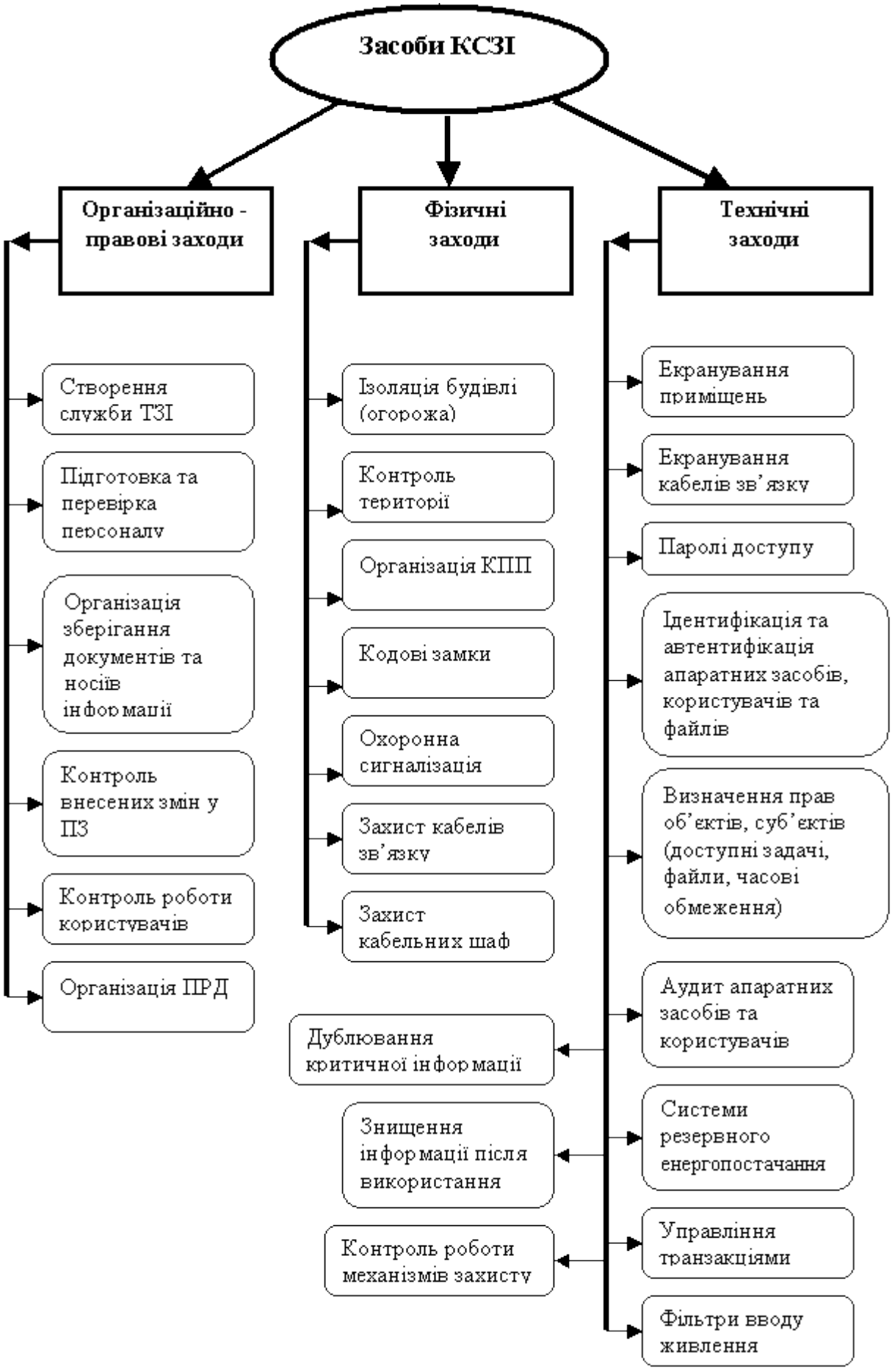

Рис. 1.2. Структура засобів КСЗІ

Застосовані ізоляція будинку, контроль території, кодові замки, контрольно-пропускний пункт (КПП), охоронна сигналізація. Від витоку інформації по каналах побічних електромагнітних випромінювань та наводок (ПЕОМ) пропонується екранування приміщень та кабелів зв'язку, по кабелях електроживлення передбачається установка фільтрів.

Контрольні запитання

1. Що входить до комплексної системи захисту інформації?
2. Заходи формування режиму інформаційної безпеки не мають рівня?
3. Що не належить до основних аспектів інформаційної безпеки?
4. Що не належить до зовнішніх загроз інформаційної безпеки?
5. До видів інформації належить?
6. Інформаційна безпека – це?
7. Коли доцільно не робити жодних дій щодо виявлених ризиків?
8. Яка категорія є найбільш ризикованою з огляду на ймовірне шахрайство та порушення безпеки?
9. Вкажіть функції управління підприємством, які підтримують сучасні інформаційні системи.
10. Основи безпеки підприємницької діяльності – це?

Тема 2. АПАРАТНІ ЗАСОБІ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Основи апаратного захисту

Проблема захисту даних стала актуальною з самого початку використання обчислювальної техніки. Втрата недокументованих електронних даних спричиняла необхідність повторного виконання необхідної обробки інформації. У деяких випадках втрата вихідних даних робила неможливою повторну обробку інформації, а отже, і втрату важливих результатів.

Саме проблема захисту даних під час передачі їх між комп'ютерами (поряд із завданням збільшення швидкості їх обробки) стала поштовхом до створення комп'ютерних мереж.

Можливо, закономірним є той факт, що саме розвиток комп'ютерних мереж став причиною надзвичайного загострення проблеми захисту даних.

Захист даних, а, отже, і захист інформації – комплексна проблема, яка є частиною національної безпеки. Необхідність вирішення проблеми захисту інформації на державному рівні викликала включення цієї проблеми до стратегії національної безпеки та прийняття Закону «Про електронний підпис». Це не останній законодавчий акт в цьому напрямі, оскільки комплексне вирішення проблеми передбачає створення єдиної правової, організаційної та матеріально-технічної бази.

На державному рівні мова йде про захист інформації державної ваги. Але і на рівні органів державного управління та місцевого самоврядування ця проблема на сьогодні досить гостра.

Чи є у вашій організації організована система захисту даних?

Коли говорять про захист даних, то мають на увазі дві основних небезпеки втрати даних: пошкодження даних і несанкціонованого доступу до них. Боротьба з обома небезпеками ведеться апаратними і програмними засобами та організаційними заходами. Нижче ми розглянемо основні засоби захисту даних, які можна використовувати у практичній діяльності.

До апаратних засобів захисту від пошкодження даних слід зарахувати використання джерел неперервного живлення, а також резервування та архівування даних.

Раптове зникнення напруги може спричинити втрату тих файлів, з

якими в момент зникнення напруги працював комп'ютер. Наприклад, як операційна система Windows, так і програми з пакету MS Office під час роботи створюють багато тимчасових файлів, які постійно використовуються програмами. Раптове зникнення напруги може спричинити втрату цих файлів і, як наслідок, «розвал» системи і втрату файлів з даними. Найгіршим випадком є вихід з ладу жорсткого диска. Хоча відновлення інформації з цього диска ще здебільшого можливе, але це може бути не в повному обсязі і коштуватиме досить дорого.

Чому коректне вимкнення комп'ютера є важливим для збереження цілості операційної системи?

Використання джерел неперервного живлення (UPS) дає можливість у разі зникнення напруги в мережі підтримувати роботу системи ще протягом 20 хв. За цей час завершиться виконання всіх програм, і комп'ютер можна буде вимкнути без втрати всіх даних. У відповідальніших випадках використовують резервне живлення або з мережі, або від автономного джерела.

Резервування інформації дає можливість у разі втрати даних повернути стан системи на момент її резервування. За такої умови резервні копії можна зберігати у захищених місцях (приміщеннях чи сейфах). Для резервування використовують або засоби постійної пам'яті (компакт-диски, стримери, переносні жорсткі диски), або жорсткі диски на іншому комп'ютері в мережі.

Для інформації невеликого обсягу цілком придатний спосіб зберігання даних у вигляді архіву на тому ж комп'ютері, на автономному носії або на іншому комп'ютері. Принципово – це те ж резервування даних, але в трансформованому (стисненому) вигляді. Для архівування використовують програми WinZIP або WinRAR. До речі, в архівованому вигляді дані легше передавати засобами електронного зв'язку в мережі. За такої умови бажано користуватись архіватором ZIP.

Чи використовується у вашій організації централізована система архівування даних?

До апаратних засобів захисту від несанкціонованого доступу найкраще використовувати засоби постійної пам'яті – компакт-диски і переносні жорсткі диски. У цьому разі дані будуть захищені навіть при пошкодженні чи втраті комп'ютера. У жодному разі для тривалого зберігання даних не слід використовувати дискети. Для цього їх надійність занадто низька.

2.2. Класифікація технічних засобів зняття інформації

До апаратних засобів захисту даних від несанкціонованого доступу належать також :

криптографічні плати, за допомогою яких дані можна зашифрувати, створити електронний підпис та аутентифікувати користувача;

магнітна картка SmartCard для зберігання секретного ключа та шифрування паролів;

пристрої ActiveCard для введення паролів, в яких паролі обчислюються на підставі уведених даних (динамічні паролі), та **SmartReader** для зчитування цих паролів. Чотиризначний пароль, що вводиться користувачем, перераховується в цих пристроях у спеціальний код.

До технічних засобів можна зарахувати і біометричні засоби, тобто: зчитування візерунка сітчатки ока, відбитків пальців, геометрії рук, динаміки підпису. Крім того, використовують також комплекси технічних засобів захисту від несанкціонованого доступу до даних, які можна згрупувати так:

захист від електромагнітного випромінювання, куди належать: використання оптоволоконних кабелів, захисної плівки на вікнах, захищених дисплеїв;

захист від поновлення знищених даних;

захист від підслуховування шляхом: встановлення фільтрів на лініях зв'язку, попередження встановлення підслуховувальних пристроїв, використання звукопоглинальних покриттів, протипідслуховувального зашумлення.

Бурхливий розвиток техніки, технології, інформатики в останні десятиліття викликав ще більш бурхливий розвиток технічних пристроїв і систем розвідки. Справді, занадто часто виявлялося вигідніше витратити N-у суму на добування, наприклад, технології, що вже існує, ніж у кілька разів більшу на створення власної. А в політиці чи у військовій справі виграш іноді виявляється просто безцінним.

У створення пристроїв і систем ведення розвідки вкладалися і вкладаються величезні кошти у всіх розвинених країнах. Сотні фірм багатьох країн активно працюють у цій галузі. Серійно виробляються десятки тисяч моделей «шпигунської» техніки. Ця галузь бізнесу давно і стійко зайняла своє місце в загальній системі економіки Заходу і має міцну законодавчу базу.

У західній пресі можна знайти дуже захопливі документи про існу-

вання і роботу міжнародної організації промислового шпигунства «Спейс Інкорпорейтед», а заодно і познайомитися зі спектром послуг, пропонованих цією компанією. Зокрема, англійська газета «Піпл» повідомляє, що серед клієнтів компанії є не тільки промисловці, але й організовані злочинні угруповання. Як і будь-який бізнес, коли він вигідний, торгівля секретами розширює поле діяльності, знаходячи для свого процвітання вигідний ґрунт.

Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно, орієнтуючись на найбільш фінансово вигідні.

У СРСР після 1917 р. ведення комерційної розвідки знаходилося під суворим контролем держави. У Радянському Союзі в цій галузі були зосереджені чудові, якщо не сказати кращі, фахівці. Видатним досягненням було і залишиться на багато років чудо технічної розвідки — будинок посольства США в Москві, перетворене у величезне «вухо», у якому кожен подих, кожен шерех був доступний для запису й аналізу. Датчики знаходили навіть у зварених сталевих конструкціях будинку, причому по щільності матеріалу вони відповідали навколишньому металу і були недоступні для рентгенівського аналізу. Ці системи були здатні функціонувати автономно десятки років. Американці змушені були відмовитися від використання цього будинку, навіть незважаючи на те, що колишній голова Комітету Державної Безпеки Вадим Бакатін передав їм схему побудови цієї системи.

Розпад СРСР і розвиток вільної ринкової економіки відродило попит на техніку подібного роду. Фахівці військово-промислового комплексу, що залишилися без роботи, не затрималися запропонувати свої послуги й у цій сфері. Спектр послуг широкий: від примітивних радіопередавачів до сучасних апаратно-програмних комплексів ведення розвідки. Звичайно, у нас немає ще великих фірм, що виробляють подібну техніку, немає і такого достатку моделей, як на Заході, але техніка наших виробників цілком за своїми даними порівняно з аналогічною західною іноді краще і дешевше. Зрозуміло, мова йде про порівняння техніки, яка є у відкритому продажу.

Природно, апаратура, використовувана спецслужбами (її кращі зразки) набагато перевершує по своїх можливостях техніку, використовувану комерційними організаціями. Як приклад – найменший і найдорожчий у світі радіомікрофон, габарити якого не перевищують чверті олівцевої гумки для стирання. Цей мініатюрний передавач живиться від ізотопного елемента і здатний протягом року сприймати і передавати на прийомний пристрій, розташований за півтора кілометра, розмову, що

ведеться в приміщенні пошепки. Крім того, уже зараз виробляються радіозакладки, що можуть записувати перехоплену інформацію, зберігати її протягом доби чи тижня, передавати в режимі швидкодії за мілісекунду, стирати запис і починати процес знову.

Сучасні злочинні угруповання мають на озброєнні новітні технічні засоби отримання, обробки та захисту інформації. Частину таких засобів як вітчизняного (наприклад, радіокапсула Р1-Р9, приймачі RH-03, RA-05, RA-07, конвертори СО-01 та інші), так і імпортного виробництва (наприклад, лазерний мікрофон HP-150 фірми “Hewlett-Packard”) дотепер можна було придбати у відкритій торгівлі. Крім того, є багато літератури, яка дозволяє практично будь-якому радіоаматору кустарно виготовити радіомікрофони та інші технічні засоби ведення розвідувальної та контррозвідувальної діяльності.

2.3. Основні групи технічних засобів ведення розвідки

1. Радіопередавачі з мікрофоном (радіомікрофони):
– з автономним живленням;
– з живленням від телефонної лінії;
– з живленням від електромережі;
– керовані дистанційно;
– що використовують функцію вмикання по голосу;
– напівактивні;
– з накопиченням інформації і передачею в режимі швидкодії.

2. Електронні пристрої знімання акустичної інформації:
– мікрофони з проводами;
– електронні стетоскопи (що прослуховують через стіни);
– мікрофони з гострою діаграмою спрямованості;
– лазерні мікрофони;
– мікрофони з передачею через мережу 220 В;
– прослуховування через мікрофон телефонної трубки;
– гідроакустичні мікрофони.

3. Пристрої перехоплення телефонних повідомлень:
– безпосереднього підключення до телефонної лінії;
– підключення з використанням індукційних датчиків (датчики Холу й інші);
– з використанням датчиків, розташованих усередині телефонного

апарату;

– телефонний радіотранслятор;
– перехоплення повідомлень сотового телефонного зв’язку;
– перехоплення пейджерних повідомлень;
– перехоплення факс-повідомлень;
– спеціальні багатоканальні пристрої перехоплення телефонних повідомлень.

4. Пристрої прийому, запису, управління:
– приймач для радіомікрофонів;
– пристрої запису;
– ретранслятори;
– пристрої запису і передачі в прискореному режимі;
– пристрої дистанційного управління.

5. Відеосистеми запису і спостереження.
6. Системи визначення місця розташування контрольованого об’єкта.
7. Системи контролю комп’ютерів і комп’ютерних мереж.

2.4. Радіомікрофони

Радіомікрофон, як випливає з назви, це мікрофон, об’єднаний з радіо, тобто з радіоканалом передачі звукової інформації. На сьогодні немає визначеної остаточно назви цих пристроїв. Їх називають радіозакладками, радіобагами, радіокапсулами, іноді – «жуками», але все-таки найбільш точною назвою варто визнати «радіомікрофон».

Радіомікрофони є найпоширенішими технічними засобами отримання акустичної інформації. Їхня популярність пояснюється, насамперед, зручністю їхнього оперативного використання, простотою застосування (не потрібно тривалого навчання персоналу), дешевизною, дуже невеликими розмірами. У найпростішому варіанті радіомікрофон складається з власне мікрофона, тобто пристрою для перетворення звукових коливань в електричні, а також радіопередавача – пристрою, що випромінює в простір електромагнітні коливання радіодіапазону (несучу частоту), промодульовані електричними сигналами з мікрофона. Мікрофон визначає зону акустичної чутливості (звичайно вона коливається від декількох до 20–30 м), радіопередавач — дальність дії радіолінії. Визначальними параметрами з погляду дальності дії для передавача є потуж-

ність, стабільність несучої частоти, діапазон частот, вид модуляції. Істотний вплив на довжину радіоканалу має, звичайно, і тип радіоприймального пристрою.

Пристрій управління не є обов'язковим елементом радіомікрофона. Він призначений для розширення його можливостей: дистанційного вмикання-вимикання передавача, мікрофона, пристрою, що записує. Можуть бути передбачені режими: ввімкнення по голосу, режим запису в реальному часі, режим прискореного відтворення тощо.

Пристрій запису, як випливає з вищесказаного, також не є обов'язковим елементом.

Розроблено і випускаються серійно сотні моделей радіомікрофонів, у тому числі не менше ніж сто типів — у Росії і СНД (в основному в Україні й у Білорусі).

Технічні дані радіомікрофонів знаходяться в таких межах:

вага ..... від 5 до 350 г

габарити ..... від 1 $см^3$ до 8 $дм^3$

частотний діапазон ..... від 27 до 900 МГц

потужність ..... від 0,2 до 500 МВт

дальність без ретранслятора ..... від 10 до 1 500 м

час безупинної роботи .....від декількох годин до декількох років.

Дальність дії, габарити і час безупинної роботи дуже залежать один від іншого. Справді, для збільшення дальності необхідно, насамперед, підвищити потужність, одночасно зростає струм, споживаний від джерела живлення, що швидше витрачає свій ресурс, а виходить, скорочується час безупинної роботи. Щоб збільшити цей час, збільшують ємність батарей живлення, але це збільшує габарити радіомікрофона. Можна збільшити тривалість роботи передавача введенням у його склад пристрою дистанційного управління (вмикання-вимикання), однак це також збільшує габарити. Крім того, потрібно мати на увазі, що збільшення потужності передавача полегшує можливість його виявлення.

Одним з перспективних напрямків збільшення скритності і часу ефективного використання є застосування дистанційного ввімкнення. Прикладами є вироби TRM-1530 і TRM-1532. Це радіомікрофони з живленням від батарей, габаритами 87х54х70 мм, вагою близько 100 г, із ЧМ передавачем діапазону 380–400 МГц або 100–150 МГц і дальністю до 300 м. Дистанційне вмикання-вимикання дозволяє довести час ефективної роботи виробу до 1 року за умови безупинної роботи 280-300 год. Подібна апаратура, але більш великих габаритів, починає надходити в продаж і від вітчизняних виробників.

Дуже перспективним є застосування радіомікрофонів з активацією від звуку — музики, мови і т.д., наприклад, модель STG-4001: включення увімкнення пристрою відбувається від звуку, вимикання — автоматично через 5 с після зникнення звуку. Застосування функції ввімкнення по голосу дозволило довести час ефективної роботи до 300 год. Прилад має дуже прийнятні розміри — 20х38х12 мм, вага з батареями — 18 г забезпечує дальність до 500 м, частоти — 130–150 МГц. Варто підкреслити, що такі радіомікрофони досить важко знайти.

У складних випадках можлива побудова системи передавачів. Наприклад, під час руху об'єкта по шляху проходження заздалегідь розміщуються радіомікрофони, що працюють на різних частотах. Спостереження ведеться за допомогою багатоканального приймача. Можлива побудова схеми з використанням передавача-ретранслятора. Потужність радіомікрофона робиться дуже невеликою (для збільшення часу роботи і підвищення скритності), а на невеликій відстані, наприклад, у сусідньому приміщенні, установлюється передавач-ретранслятор, габарити і потужність якого піддаються набагато меншим обмеженням.

Як уже зазначалося вище, дальність дії радіопередавачів визначається якостями радіоприймальних пристроїв, насамперед, чутливістю. Як приймачі часто використовують побутові радіоприймальні пристрої. У цьому разі кращим є застосування магнітол, тому що з'являється можливість одночасного ведення запису. До недоліків таких пристроїв належать низька чутливість і можливість настроювання сторонніх осіб на частоту передавача. Частково ці недоліки можна усунути перебудовою частотного діапазону, у тому числі за допомогою конверторів, а також переналагодженням підсилювачів для підвищення чутливості. Достоїнством таких систем є низька вартість, а також те, що вони не викликають підозр. Але все-таки кращим варто вважати застосування спеціальних прийомних пристроїв.

2.5. Основні методи прослуховування телефонних ліній

Цінність інформації, переданої по телефонних лініях, а також існуюче переконання про масовий характер такого прослуховування викликає найбільше занепокоєння в організацій і приватних осіб за збереження конфіденційності своїх переговорів саме по телефонних каналах. Для захисту своїх секретів необхідно знати методи, за допомогою яких можуть бути здійснені операції по перехопленню. Але при цьому потрібно врахувати, що організація масового прослуховування (в існуванні якої

переконані дуже багато людей) неможлива з причин технічного і фінансового характеру. Справді, для аналізу записаних повідомлень потрібно тримати чималу кількість людей і техніки. Крім того, для організації прослуховування в даний час потрібна санкція суду. Більш ймовірна організація прослуховування без санкції, у комерційних чи інших цілях. Ймовірність витоку інформації по телефонних каналах становить від 5 до 20 %.

В цей час на ринку СНД є сотні типів пристроїв перехоплення телефонних повідомлень як вітчизняного, так і імпортного виробництва.

Можна виділити шість основних зон прослуховування:

- телефонний апарат;
- лінія від телефонного апарата, включаючи розподільну коробку;
- кабельна зона;
- зона АТС;
- зона багатоканального кабелю;
- зона радіоканалу.

Найбільш ймовірна організація прослуховування перших трьох зон, бо саме в цих зонах найлегше підключитися до телефонної лінії. Фахівці, що займаються захистом інформації, підтверджують, що найчастіше використовується прослуховування за допомогою рівнобіжного апарата. Здебільшого для цього навіть не потрібно прокладати додаткові проводи — телефонна мережа настільки заплутана, що завжди є лінії, які не використовуються. Крім того, неважко підключитися в парадній до розподільної коробки. Підключення в третій зоні менш поширено, бо потрібно проникати в систему телефонних комунікацій, що складається з труб із прокладеними усередині них кабелями, а також розібратися в цій системі і визначити потрібну пару серед сотень інших. Однак не слід вважати, що це нездійсненне завдання, оскільки існує вже необхідна для цього апаратура. Як приклад можна навести американську систему «Кріт». За допомогою спеціального індуктивного датчика, що охоплює кабель, знімається передана по ньому інформація. Для установки датчика на кабель використовуються колодязі, через які проходить кабель. Датчик у колодязі закріплюється на кабелі і для утруднення виявлення проштовхується в трубу, що підводить. Сигнал записується на диск спеціального магнітофона. Після заповнення диска видається сигнал, і агент за сприятливих умов заміняє диск. Апарат може записувати інформацію, передану одночасно по 60 каналах. Тривалість безупинного запису становить 115 год. Такі пристрої знаходили в Москві. Для різних типів підземних кабелів розроблені різні датчики: для симетричних високочастотних — індуктивні для відводу енергії з коаксіальних кабелів, для кабелів з надлишковим

тиском — пристрої, що виключають його зниження. Деякі прилади забезпечуються радіопередавачем для передачі записаних повідомлень чи перехоплення їх у реальному масштабі часу.

У технічному плані найпростішим способом є контактне підключення.

Можливо тимчасове підключення до абонентської проводки за допомогою стандартної «монтерської трубки». Однак підключення такого типу легко виявляється за допомогою найпростіших засобів контролю напруги телефонної мережі. Зменшити ефект спадання напруги можна підключенням слухавки через резистор 0,6–1кОм. Підключення здійснюється за допомогою дуже тонких голочок і тонких проводів, що прокладаються в якій-небудь існуючій чи виготовленій щілині. Щілина може бути зашпакльована і пофарбована так, що візуально визначити підключення дуже важко.

Відомий спосіб підключення до ліній зв'язку апаратури з компенсацією спадання напруги. Істотними недоліками контактного способу підключення є порушення цілісності проводів і вплив підключеного пристрою на характеристики ліній зв'язку. З метою усунення цього недоліку застосовується індуктивний датчик, виконаний у вигляді трансформатора. Існують також датчики, принцип роботи яких заснований на ефекті Холу.

Вартість подібних пристроїв коливається від 20 до 250 $. Як записувальні пристрої застосовуються стандартні диктофони, спеціальні мініатюрні типу OLIMPUS L-400, а також стаціонарні багатоканальні диктофони, наприклад АД-25-1. Як правило, схема прослуховування організована так, що магнітофон включається з появою сигналу в лінії.

Як приклад мініатюрного магнітофона можна навести модель N2502, рекламовану як магнітофон, що неможливо знайти за допомогою сучасних детекторів записувальної техніки. У цьому магнітофоні є гнізда для підключення зовнішнього мікрофона, пульта дистанційного управління і головних телефонів.

Як правило, спеціальні багатоканальні магнітофони для запису телефонних переговорів використовуються в складі спеціальної апаратури для контролю особливо режимних робіт. У цьому разі використовуються спеціальні прийоми, що дозволяють по ключових словах переривати чи записувати телефонну розмову. Такий акустичний контроль може бути організований за допомогою наявних на ринках США, Німеччини і Японії спеціальних багатоканальних магнітофонів, призначених для стаціонарного запису телефонних переговорів і розрахованих на значну (від 10 до 100) кількість каналів.

2.6. Телефонні радіотранслятори

Телефонні радіотранслятори надзвичайно популярні і являють собою радіоподовжувач для передачі телефонних розмов по радіоканалу. Більшість телефонних закладок автоматично включаються при піднятті слухавки і передають інформацію на пункт перехоплення і запису. Джерелом живлення для радіопередавача є, як правило, напруга телефонної мережі, бо в цьому разі не потрібно ні батарейок, ні вбудованого мікрофона, розміри ретранслятора можуть бути дуже невеликими. Недоліком подібних пристроїв є те, що вони можуть бути виявлені по радіовипромінюванню.

Малогабаритний кварцовий передавач AD-31 призначений для контролю телефонної лінії. Дальність дії — до 300 м і більше. Діапазон частот: 350–450 МГц. Має канали А, В чи С. Вмикається в розрив телефонної лінії. Габарити — 18 х 38 х 10 мм, вага — 15 г.

Компактний ЧМ-передавач FD-45-4 для контролю телефонної лінії закамуфльований у телефонну розетку. Дальність дії — до 150 м. Габаритні розміри — 22х16х12 мм. Вага — 210 г.

Щоб зменшити можливість виявлення радіовипромінювання, застосовують той самий спосіб, що й у разі із радіомікрофоном — зменшують потужність випромінювання передавача, встановленого на телефонній лінії. А в безпечному місці встановлюють більш потужний ретранслятор, що перевипромінює сигнал на іншій частоті й у зашифрованому вигляді.

Варто врахувати, що не можна виключати можливість застосування радіопередавачів, що використовують псевдошумові сигнали і(чи) працюючих «під шумами». У цьому разі виявлення радіозакладок ще більш ускладнюється.

Для маскування телефонні радіотранслятори випускаються у вигляді конденсаторів, фільтрів, реле й інших стандартних вузлів і елементів, що входять до складу телефонної апаратури.

Існують ретранслятори, виготовлені у вигляді мікрофона слухавки (наприклад, модель CRISTAL фірми Sipe). Подібні вироби дуже легко і швидко можна установити в телефонний апарат, який цікавить.

Тут не можна не зауважити, що дуже часто не потрібно проробляти навіть і такі прості операції. Дуже поширені телефонні апарати з кнопковим номеронабиранням типу ТА-Т, ТА-12. Завдяки особливостям своєї конструкції вони перевипромінюють інформацію на десятках частот СВ, КВ і УКВ діапазону на відстань до 200 м.

Ще більш просто підслухати розмову, якщо використовується телефон з радіоподовжувачем, що являє собою дві радіостанції: одна змонтована в трубці, інша — у самому телефонному апараті. У цьому разі потрібно тільки налаштувати приймач на необхідну частоту. Для подібних цілей виготовляються і спеціальні розвідувальні приймачі. Наприклад, приймач «Мініпорт» фірми «Роді і Шварц» з діапазоном частот 20–1000 МГц. Цей приймач має невеликі габарити (188 х 7 1х 212 мм), універсальне живлення й вбудований процесор. Запам'ятовуючий пристрій може зберігати в пам'яті до 30 значень частот і здійснювати сканування в заданому діапазоні з перемінним кроком.

2.7. Системи прослуховування повідомлень, переданих по стільникових, пейджингових каналах і по факсу

Стільниковою називається система зв'язку, що складається з деякої кількості осередків, що, з'єднуючись між собою, утворять мережу, соту. Кожен осередок може працювати з визначеною кількістю абонентів одночасно. Стільникові мережі мають можливість нарощування, а також можуть стикуватися одна з одною. Радіус дії базової стільникової станції становить 5–15 км, а перехоплення повідомлень у цьому разі може проводитися на відстані до 50 км. Як приклад реалізації подібної системи можна навести стільникові системи спостереження Cellmate-lOB і Cellscan.

Cellmate-lOB контролює одночасно до 10 телефонних номерів, тобто один осередок стільникового зв'язку. Є можливість програмувального перебору осередків. Потрібна розмова може визначатися по голосу абонента чи по змісту розмови. Перехоплені один раз номера за бажанням переводяться програмою в особливий режим спостереження. Вбудований запам'ятовуючий пристрій запам'ятовує останні параметри настроювання. Запис починається автоматично, коли об'єкт спостереження починає користуватися телефоном. Інформація про номери телефонів, параметри настроювання, ідентифікації по голосу зчитується з кольорового рідкокристалічного дисплея, так само визначаються коди доступу.

Система Cellscan аналогічна за функціями Cellmate-lOB і також розміщується в аташе-кейсі. Вважається, що кількість програмувальних номерів не обмежена. У режимі сканування на дисплей виводиться інформація про 895 каналів. Спостерігається вся телефонна система, і вибираються канали, по яких відбуваються дзвінки. За допомогою ком-

плекту стільникових карт визначається район, у якому відбувається підозріла розмова, ідентифікований сканером по змісту чи голосу. Можна відключити канали, на яких ви не хочете здійснювати перехоплення. Використовується дороблений стільниковий телефон OKI, що може застосовуватися і як звичайний стільниковий телефон, вага системи — 9 кг.

Сучасні системи стільникового зв'язку можуть використовувати різні системи кодування і(чи) перебудову частоти по випадковому принципу. Існують і спеціальні комплекти радіоперехоплення з можливістю аналізу зашифрованих повідомлень, наприклад, Sigint/Comint Spektra фірми Hollandes Signal, але подібна апаратура дуже дорога. У Росії розроблені і пропонуються програмно-апаратні системи перехоплення пейджингових повідомлень. До складу подібної системи входять дороблений сканер (AR-3000A, IC-7100 і ін.), пристрій перетворення, комп'ютер і спеціальне програмне забезпечення. Система дозволяє здійснювати прийом і декодування текстових і цифрових повідомлень, переданих у системі радіопейджингового зв'язку і зберігати всі прийняті повідомлення (з датою і часом передачі) на твердому диску персонального комп'ютера. При цьому може здійснюватися фільтрація потоку повідомлень, виділення даних, адресованих конкретним абонентам.

Перехоплення факсів-повідомлень принципово не відрізняється від перехоплення телефонних повідомлень.

Наостанок наведемо приклад організації прослуховування Агентством національної безпеки США, що має в 6 разів більше службовців, ніж ЦРУ. 4 120 могутніх центрів прослуховування на базах у Німеччині, Туреччині, Японії і т.д., а також на кораблях, підводних човнах, літаках і супутниках збирають і аналізують майже всю інформацію, передану електронним способом, включаючи випромінювання систем сигналізації автомобілів, квартир і так далі.

2.8. Використання телефонної лінії для прослуховування приміщень

Телефонна лінія використовується не тільки для передачі телефонних повідомлень, але і для прослуховування приміщення. Щоб ввімкнути подібний пристрій, потрібно набрати номер абонента. Перші два гудки «ігноруються» пристроєм, тобто телефон не дзвонить. Після цього необхідно покласти слухавку і через визначений час (30–60 с) подзвонити знову. Тільки після цього система включається в режим прослухо-

вування.

Аналогічно працюють, наприклад, пристрої ST-01 ELSY, UM103. Ціна таких пристроїв — від 15 (вітчизняні) до 250 $ (закордонні). Як приклад одного з таких пристроїв є пристрій БОКС-Т. Цей пристрій дозволяє контролювати приміщення з будь-якої точки земної кулі по телефону. Для цього досить набрати номер телефону, де вже встановлений прилад «Бокс-Т», і включити мікрофон. Для вимикання досить покласти слухавку.

Необхідно мати на увазі, що існують такі системи передачі акустичної інформації з телефонних ліній, що дозволяють прослуховувати приміщення без установки якого-небудь додаткового устаткування. Також використовуються недоліки конструкції телефонного апарата: акустичні коливання впливають на якір дзвоника, що, коливаючись, викликає появу в котушці мікрострумів модульованих дросельною системою, що наводиться в котушці та у цьому разі може досягати декількох мілівольтів. Дальність цієї системи не перевищує (через загасання) декількох десятків метрів. Прийом здійснюється на якісний підсилювач низької частоти.

Другий варіант системи пов’язаний з реалізацією ефекту «нав’язування». Коливання частотою від 150 кГц і вище подаються на один провід телефонної лінії, до другого проводу приєднується приймач. Земля передавача і приймача з’єднані між собою або із загальною землею, наприклад, водогінною мережею.

Через елементи схеми телефонного апарата високочастотні коливання надходять на мікрофон, навіть якщо він відключений від мережі, і модулюються мовою. Детектор приймача виділяє мовну інформацію. Через істотне загасання ВЧ сигналу у двопроводовій лінії дальність також не перевищує декількох десятків метрів (без ретранслятора).

2.9. Спеціальні пристрої прослуховування

Спрямовані мікрофони

Звичайні мікрофони здатні реєструвати людську мову на відстані, що не перевищує декількох десятків метрів. Для збільшення дистанції, на якій можна робити прослуховування, практикують застосування спрямованого мікрофона.

Іншими словами, цей пристрій збирає звуки тільки з одного напрямку, тобто має вузьку діаграму спрямованості. Такі пристрої широко застосовуються не тільки в розвідці, але і журналістами, мисливцями,

рятувальниками і т.д.

Можна виділити два основних типи спрямованих мікрофонів:

– з параболічним відбивачем;
– резонансний мікрофон.

Мікрофон з параболічним відбивачем

У мікрофоні з параболічним відбивачем власне мікрофон розташований у фокусі параболічного відбивача звуку.

Спрямований параболічний мікрофон з підсилювачем AD-9 концентрує звуки, що йдуть, і підсилює їх. Простий у використанні і настроюванні. У комплект входить мікрофон, підсилювач, кабель і головні телефони. Електроживлення — від батареї 9 В.

Випускаються кілька моделей. Загальним у конструкції всіх цих мікрофонів є наявність рукоятки пістолетного типу, параболічного відбивача діаметром близько 40 мм і підсилювача. Діапазон сприйманих частот становить від 100–250 Гц до 15–18 кГц. Усі мікрофони мають автономне живлення і мають рознімання для підключення до магнітофона. Гостра «голчаста» діаграма спрямованості дозволяє за відсутності перешкод контролювати людську мову на відстані до 1200 м. У реальних умовах (в умовах міста) можна розраховувати на дальність до 100 м.

Резонансний мікрофон

Резонансний мікрофон заснований на використанні явища резонансу в металевих трубках різної довжини. Наприклад, в одній з модифікацій такого мікрофона використовується набір з 37 трубок довжиною від 1 до 92 см.

Звукові хвилі, що приходять до приймача по осьовому напрямку, приходять до мікрофона в однаковій фазі, а з бічних напрямків (через відмінну швидкість поширення звукових хвиль у металі, а також різної довжини трубок) — виявляються зрушеними по фазі.

З погляду схованого контролю звуку застосування спрямованих мікрофонів утруднено через найчастіше неприйнятні їхні габарити і джерела акустичних перешкод. Крім того, для того щоб не бути прослуханим в автомобілі, досить просто підняти скло.

Лазерні мікрофони

У разі, якщо ви підняли скло чи закрили кватирку в автомобілі, може бути використаний лазерний мікрофон. Перші їхні зразки були прийняті на озброєння американськими спецслужбами ще в 60-ті роки.

Як приклад розглянемо лазерний мікрофон HP-150 фірми Hewlett-

Packard з дальністю дії до 1000 м. Він сконструйований на основі гелій-неонового чи напівпровідникового лазера з довжиною хвилі 0,63 мкм (тобто у видимому діапазоні; сучасні пристрої використовують невидимий ІЧ діапазон).

Промінь лазера, відбитий від скла приміщення, у якому ведуться переговори, виявляється промодульованим звуковою частотою. Прийнятий фотоприймачем відбитий промінь детектується, звук підсилюється і записується. Приймач і передавач виконані роздільно, є блок компенсації перешкод. Вся апаратура розміщена в кейсі і має автономне живлення. Подібні системи мають дуже високу вартість (більше ніж 10 тис. $) і, крім того, вимагають спеціального навчання персоналу і використання комп'ютерної обробки мови для збільшення дальності.

Існує досвідчена вітчизняна система ЛСТ-ЛА2 з дальністю зняття менше 100 м і досить скромною вартістю. Слід зазначити, що ефективність застосування такої системи зростає зі зменшенням освітленості оперативного простору.

Гідроакустичні датчики

Звукові хвилі поширюються у воді з дуже невеликим загасанням.

Гідроакустики військово-морських сил навчилися прослуховувати шепіт у підводних човнах, що знаходяться на глибині десятків метрів. Цей же принцип можна застосовувати, використовуючи рідину, що знаходиться в системах водопостачання і каналізації. Таку інформацію можна перехоплювати в межах будинку, але радіус прослуховування буде дуже сильно залежати від рівня шумів, особливо у водопроводі. Переважно використовувати датчик, встановлений у батареї опалення. Ще більш ефективним буде використання гідроакустичного передавача, встановленого в батареї приміщення, що прослуховується.

Надвисокочастотні та інфрачервоні передавачі

Для підвищення скритності в останні роки стали використовувати інфрачервоний канал. Як передавач звуку від мікрофона використовується напівпровідниковий лазер. Наприклад, розглянемо пристрій TRM-1830. Дальність дії вдень становить 150 м, уночі — 400 м, час безупинної роботи — 20 год. Габарити не перевищують 26 х 22 х 20 мм. До недоліків інфрачервоного (ІЧ) - каналу подібної системи можна віднести необхідність прямої видимості між передавачем і приймачем і вплив перешкод.

Підвищити скритність одержання інформації можна також за допомогою використання каналу надвисокочастотного (НВЧ) -діапазону —

більше 10 гГц. Передавач, виконаний на діоді Ганна, може мати дуже невеликі габарити. Забезпечується дальність більше 100 м. До переваг такої системи можна віднести відсутність перешкод, простоту і відсутність у цей час ефективних засобів контролю. До недоліків варто віднести необхідність прямої видимості, хоча й у меншому ступені, тому що НВЧ-сигнал може все-таки обгинати невеликі перешкоди і проходить (з ослабленням) крізь тонкі діелектрики, наприклад, штори на вікнах.

Стетоскопи

Стетоскоп являє собою вібродатчик, підсилювач і головні телефони.

Вібродатчик спеціальною мастикою прикріплюється до стіни, стелі і тому подібне. Розміри датчика, на прикладі пристрою DTI, становлять 2,2 х 0,8 см, діапазон частот — 300–3000 Гц, вага — 126 г, коефіцієнт підсилення — 20 000.

За допомогою подібних пристроїв можна здійснювати прослуховування розмови через стіни товщиною до 1 м. Стетоскоп може оснащуватися проводовим, радіо чи іншим каналом передачі інформації. Основною перевагою стетоскопа можна вважати труднощі виявлення, тому що він може встановлюватися в сусідніх приміщеннях.

Існують стетоскопи, у яких чуттєвий елемент, підсилювач і радіопередавач об’єднані в одному корпусі. Вони мають дуже невеликі габарити і дозволяють не тільки прослуховувати розмови через стіни, віконні рами, двері, але і передавати інформацію по радіоканалу. Мають високу чутливість і забезпечують гарну розбірливість мовного сигналу. Як правило, робоча частота становить 470 МГц. Дальність передачі — до 100 м. Час безупинної роботи — 24 год, розміри — 40 х 93 мм.

Більшість фахівців прогнозують постійне збільшення випадків застосування стетоскопів, що насамперед пояснюється зручністю застосування подібної техніки, а також тим, що їх надзвичайно важко знайти.

2.10. Системи і пристрої відеоконтролю

Системи і пристрої відеоконтролю одержали могутній імпульс свого розвитку в зв’язку зі створенням мініатюрних відеокамер і відеомагнітофонів. Якщо історія застосування фотокамер у розвідці нараховує 90–100 років, то застосування відеотехніки стримувалося неприйнятними її ваговими та габаритними характеристиками. На сьогодні габарити відеокамер (без відеомагнітофонів) часто можуть бути менше, ніж габа-

рити наймініатюрніших фотокамер. Тим часом застосування відеотехніки в розвідці часто має переваги, недосяжні за допомогою фото- і кінотехніки. Насамперед, це те, що за допомогою відеотехніки легко здійснити запис, передачу на великі відстані й оперативний аналіз зорової і звукової інформації в реальному масштабі часу.

У спрощеному вигляді система відеоспостереження складається з відеокамери, відеомагнітофона і(чи) передавача.

Мікровідеокамери

Відеокамери, що застосовуються для оперативної діяльності, мають, в основному, імпортне походження. Вітчизняні камери по габаритних характеристиках придатні поки тільки для систем відеоконтролю (службові приміщення, відеодомофони, магазини і так далі). Зупинимося більш докладно на характеристиках деяких конкретних моделей камер закордонного виробництва. Найбільший інтерес у цьому разі має опис безкорпусних відеокамер.

Об’єктив і електронна схема управління розміщаються на одній платі розміром 4,2 х 4,2 см. Стандартний об’єктив має фокусну відстань 3,6 мм. З цим об’єктивом камера має габарити 4,2 х 4,2 х 2,1 см і кут огляду 92°. З точечним об’єктивом габарити становлять 4,2 х 4,2 х 1,2 см, кут огляду — 88°.

Незалежно від типу об’єктива, камера має такі характеристики: мінімальна освітленість — 0,4 лм, розподільна здатність — 380 ліній, живлення — 12 В, вага — 12 г.

Ці і подібні камери можуть монтуватися як разом з об’єктивом, так і з винесеним об’єктивом. Маскування може бути всіляким: у розетках електроживлення, радіоприймачах, настінному і настільному годинниках, одязі, окулярах, датчиках пожежної сигналізації, приладах освітлення і так далі.

Відеокамери можуть забезпечуватися різними змінними об’єктивами. Потрібно мати на увазі, що деякі матеріали, застосовувані для маскування об’єктів (типу «чорне скло»), пропускають тільки невелику частину спектра і можуть успішно працювати при сонячному освітленні, при освітленні ІЧ прожектором або звичайними лампами накалювання, але їхнє застосування неможливе при освітленні об’єкта люмінесцентними чи галогенними лампами.

Становить інтерес опис відеокамери з передавачем. Наприклад, це може бути OVS-25-5.

Розподільна здатність цієї камери — 380 ліній. Чутливість — 0,5 лм, об’єктив з фокусною відстанню 1,6 мм і автоматичним регулюван-

ням діафрагми. Вбудований передавач працює в діапазоні 400–500 МГц і має потужність 40 МВт. Живлення – 12 В, споживаний струм – 120 мА. Габарити – 3,8 х 4,5 х 5,9 см, вага — 120 г.

2.11. Пристрої дистанційного управління, відеодетектор руху

Пристрій управління служить для наведення камери на заданий об’єкт, умикання-вимикання передавача, відеомагнітофона, інфрачервоного освітлювача. У найпростішому випадку цей пристрій задає швидкість і кут сканування. Розглянемо поворотний пристрій OVS-32, управління яким здійснюється за допомогою пульта.

Спеціальний поворотний пристрій для відеокамер має такі можливості:

– Кут повороту автоматичного сканування становить 180° чи задається за допомогою пульта управління.

– Плавна і безшумна робота поворотного механізму.

– Можливість кріплення на стіні за допомогою спеціального кронштейна.

Максимальне навантаження — 7 кг, габаритні розміри — 146 х 124 мм, вага — 1,4 кг.

Відеодетектор руху служить для активізації апаратури при зміні положення на об’єкті, що спостерігається.

Інфрачервоні освітлювачі (ІЧ)

Застосування ІЧ-освітлювачів буває необхідно під час роботи в умовах недостатньої видимості, а також, якщо для маскування об’єктива відеокамери застосовані непрозорі у видимому діапазоні матеріали. Інфрачервоні освітлювачі можуть випускатися або окремо, або вбудованими в відеокамери. Як приклад ІЧ-освітлювача з камерою можна навести виріб фірми SANYO — VDC-9212. Ця чорно-біла відеокамера може працювати в повній темряві.

Розподільна здатність — 400 ліній, габарити — 10 х 5 см. Окремо виконаний ІЧ-освітлювач використовує випромінюючий елемент на основі галієво-алюмінієвого арсеніду (GaALAs) зі спектром випромінювання в межах 880 нм, поміщений в алюмінієвий корпус. Споживаний струм — 600 мА. Габарити — 10 х 5 х 4,5 см.

Мініатюрні відеомагнітофони

Найпоширенішим режимом відеоспостереження є режим з одночасним записом на відеомагнітофон. Найбільш широко для цих цілей застосовуються відеомагнітофони, розраховані на роботу з 8 мм відеокасетою. Відеомагнітофони мають, як правило, функцію дистанційного управління, звук записується в режимі стерео. Деякі моделі оснащені відеомонітором. Наведемо характеристики деяких моделей таких відеомагнітофонів. OVS-9 має дві швидкості запису, час запису — до 5 год. Живлення здійснюється від убудованого акумулятора чи зовнішнього джерела живлення напругою 7,5 В. Споживана потужність — 4 Вт, габарити — 148 х 130 х 62 мм, вага — 670 г.

Модель OVS-9-1 являє собою відеомагнітофон OVS-9 з убудованим кольоровим плоским монітором. Монітор зручний під час монтажу і настроюванні схованих відеокамер, а також для контролю діючих відеосистем і перегляду знятого відеоматеріалу. Габарити — 150 х 135 х 70 мм, вага — 700 г.

Бездротові лінії передачі і прийому відеоінформації. Узагальнена схема бездротової лінії передачі і прийому відеоінформації складається з блоків приймача і передавача, лінії передачі-прийому відеозображення і звуку.

Робоча частота комплекту моделі WVL-90 становить від 904 до 928 МГц. Лінія в змозі передавати кольорове чи чорно-біле зображення на відстань від 300 до 900 м, залежно від типу використовуваної антени (вбудована плоска чи зовнішня антена високого посилення типу WVLA-902), відношення сигнал/шум не менше ніж 45 дб. Живлення від зовнішнього джерела живлення – 10–25 В, споживаний струм передавача – не менше ніж 50 мА, приймача — не менше ніж 20 мА. Габарити передавача – 23 х 6,3 х 9,5 см, приймача – 23 х 70 х 12 см.

2.12. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації

Одним зі шляхів боротьби з несанкціонованим доступом до каналів передачі інформації є заміна аналогових каналів на цифрові. Цифрові канали передачі даних більш надійні, ніж традиційні, аналогові. Цифрові канали легше захистити за допомогою різноманітних радіоелектронних засобів, наприклад за допомогою комп’ютерних засобів. Такими захищеними цифровими каналами можуть бути і телефон, і радіо.

Найбільший рівень скритності і перешкодозахищеності мають волоконо-оптичні лінії зв'язку. Навмисне перекручування і потаємне перехоплення інформації, переданої по цих лініях зв'язку, в цей час практично неможливі. Крім того, ці канали зв'язку мають дозволяють передавати дуже великі об'єми даних.

Звичайно, для охорони інформації варто використовувати і традиційні засоби – сейфи, коди і так далі. Приміщення доцільно періодично перевіряти на наявність «жучків» й іншої шпигунсько-розвідувальної «живності». У кімнатах не повинно бути жодних сторонніх електронних приладів, а в переговорних – узагалі жодних. На вікнах – важкі і щільні штори, на склі – спеціальні плівки. Переговорні кімнати – без вікон. Похмура картина? Але така мінімальна плата за обмеження чужого доступу до своїх секретів. Інформація часто того варта!

Доцільно, і навіть необхідно, використовувати відповідні випромінювачі перешкод як в акустичних, так і в радіодіапазонах.

Випромінювачі акустичних перешкод – це, наприклад, різні вібратори, встановлювані в місцях можливого розміщення електронних «жучків».

Перешкоди в радіодіапазонах – це спеціальні передавачі, що передають сигнали перешкод у широкій смузі частот. При цьому використовуються як АМ-, так і ЧМ-сигнали.

Подібні засоби оборони, наприклад, випромінювачі перешкод, не менш різноманітні, ніж засоби нападу.

І, звичайно, для виявлення схованих радіопередавальних засобів гарні різні детектори і сканери, що дозволяють виявити активні пристрої.

Дуже ефективні нелінійні локатори. Ці складні і дорогі апарати дозволяють виявляти сховані електронні пристрої. Принцип роботи нелінійних локаторів заснований на ефекті генерації напівпровідниковими p-n-переходами власних ВЧ-коливань при їхньому опроміненні зовнішніми ВЧ-коливаннями, вироблюваними цими пошуковими засобами. Тобто подібно традиційному локатору нелінійний локатор спочатку випромінює згенеровану послідовність високочастотних (ВЧ) -коливань у напрямку можливого розташування схованої електронної схеми, потім «слухає». Опромінені p-n-переходи випромінюють ВЧ-коливання і тим самим видають наявність схеми, навіть неактивної! Залишається нагадати, що будь-який електронний пристрій містить мікросхеми, транзистори, діоди, а отже, і p-n-переходи. Сучасні нелінійні локатори дозволяють шукати напівпровідникові елементи навіть у залізобетонній стіні на глибині в кілька десятків сантиметрів!

З огляду на роль комп'ютерів як сучасних інформаційних центрів

для збереження, обробки і передачі/прийому інформації необхідно відповідним чином захищати їх від несанкціонованого доступу до конфіденційної інформації.

Для захисту інформації в комп'ютерах, як мінімум, необхідно використовувати паролі для доступу до системи. Звичайно, це не дає 100 % гарантії, але ускладнює доступ. Існують різні апаратні і програмні засоби для обмеження доступу до комп'ютера і кодування інформації, що там знаходиться. Правда, і це не забезпечує повної гарантії, але значно підвищує рівень захисту. Часто такого рівня буває досить. При «розкритті» пароля зловмиснику потрібен час, іноді значний. Можливо, йому будуть потрібні програмні й апаратні засоби. Усе це утрудняє його діяльність. Очевидно, що тривалий час «розкриття» і необхідність використання апаратно-програмних засобів не тільки охороняють секрети, але і заважають збереженню інкогніто викрадача.

Але при обмеженні доступу до конфіденційної комп'ютерної інформації за допомогою стандартних, вбудованих засобів захисту необхідно виявляти визначену обережність. Так, наприклад, нерідко доступ до комп'ютерної інформації обмежують за допомогою пароля, що встановлюють у системному біосі. Введення цього пароля необхідний відразу після ввімкнення комп'ютера. Однак забрати цей пароль можна скиданням системного біоса за допомогою короткого замикання на кілька секунд батарейки на материнській платі. Правда, доступ до материнської плати можливий тільки після розкриття системного блоку, для чого, як правило, досить однієї викрутки. Звичайно, замикання батарейки призведе до очищення всіх системних установок, але повернути їх зовсім неважко. Однак можливий і інший шлях вирішення проблеми пароля, невідомого для порушника. Дійсно, нерідко існують так звані технологічні паролі. Введення одного з таких паролів замість невідомого дозволяє одержати безперешкодний доступ у систему комп'ютера. Так, наприклад, для комп'ютерів з BIOS фірми Award, зокрема Award Modular BIOS v4.50, один з таких паролів – послідовність J256. І, до речі, це не єдиний пароль! Таких «паролів-всюдиходів» існує цілий список, доступний через комп'ютерні мережі широкому колу комп'ютерних ентузіастів і хакерів. Імовірно, маються аналогічні паролі і для BIOS інших фірм. Отже, для надійного захисту комп'ютера краще скористатися спеціалізованими апаратно-програмними засобами обмеження доступу до конфіденційної інформації.

Як уже зазначалося, комп'ютер у процесі роботи випромінює радіохвилі в широкому частотному діапазоні. І інформацію, що несуть ці радіохвилі, можна перехопити і розшифрувати. Однак рівень радіови-

промінювання комп'ютера в радіодіапазонах: СХ-, КХ-, УКХ-, телевізійних і т.д. можна значно зменшити. Це досягається виконанням низки досить простих організаційних заходів.

Для ослаблення радіовипромінювання комп'ютерів доцільно, як мінімум, використовувати комп'ютери, вузли й елементи, сертифіковані на рівень радіовипромінювання. Особливо це стосується комп'ютерних корпусів, що забезпечують значне ослаблення радіовипромінювання. Як правило, комп'ютери відомих брендових фірм і, звичайно, їхні корпуси й елементи відповідають досить сталим нормам на супутнє роботі комп'ютера радіовипромінювання. Ці норми встановлюють міжнародні стандарти.

З огляду на те, що частина радіовипромінювання відбувається через електропроводи мережі живлення, підключення системних блоків і моніторів комп'ютерів доцільно робити через спеціальні пристрої безперебійного живлення (ПБЖ) чи, як мінімум, через подовжувачів типу Pilot. ПБЖ не тільки здійснює захист даних за рахунок короткочасної підтримки енергоживлення у разі його порушення в електромережі, але і завдяки особливостям своєї конструкції забезпечує значне ослаблення радіовипромінювання комп'ютера через електромережу. І ПБЖ, і Pilot мають у своєму складі спеціальні фільтри високочастотних перешкод – ВЧ-фільтри. Ці фільтри не тільки знижують рівень радіовипромінювання комп'ютера через проводи силової електромережі, але і підвищують стійкість роботи комп'ютера за рахунок ослаблення ВЧ-перешкод і коротких імпульсів струму, які надходять з електромережі в комп'ютер.

ВЧ-фільтри для радіоапаратури прості, але досить ефективні, можуть бути виготовлені самостійно.

Слід зазначити, що досить часто кабелі вже мають убудовані фільтри. Однак додаткові фільтри зменшують рівень радіовипромінювань через мережу електроживлення і збільшують ступінь захисту. При користуванні комп'ютерами доцільно застосовувати захисні екрани із заземленням. Дійсно, скло таких екранів має дуже тонкий електропровідний шар, який через спеціальний електропровід підключається до «землі», звичайно через корпус комп'ютера. Цей електропровідний шар є гарним екраном для електростатичного і перемінного електромагнітного полів. Отже, використання подібних захисних екранів істотно підвищує і рівень захисту інформації від несанкціонованого доступу, здійснюваного дистанційно за допомогою різноманітних радіозасобів.

Ефективність використаних засобів можна оцінити за рівнем випромінювання комп'ютера. Як такі засоби доцільно застосовувати спеціалізовані засоби. Однак у суто пізнавальних, навчальних, цілях мо-

жуть бути використані і згадані телевізор з антеною й антенним підсилювачем.

Отже, *послабити радіовипромінювання комп'ютера можна суттєво, але неможливо його виключити цілком.*

Подальше підвищення ступеня захисту досягається через застосування спеціальних апаратно-програмних засобів, наприклад тих, що змінюють по спеціальних алгоритмах порядок виведених рядків на екран монітора під час формування зображення. Для користувача комп'ютера, що знаходиться за таким монітором, функціонування цих засобів непомітно і, звичайно, не заважає роботі. Для зловмисника, що перехопив радіовипромінювання, але не знає відповідного коду, інформація залишається недоступною. Тут під кодом розуміється послідовність виведення комп'ютерних даних на екран монітора. Підбір коду можливий, але вимагає часу, сил, устаткування і, звичайно, засобів.

Погіршити розшифровку інформації з радіовипромінювання системних блоків комп'ютерів і підключених до них моніторів можна і за допомогою їхнього раціонального розміщення. Очевидно, що компактне розміщення декількох комп'ютерів утрудняє їхню дистанційну локалізацію і селекцію комп'ютерної інформації. Спільне випромінювання групи комп'ютерів створює взаємний ефект, що маскує. До того ж, чим більш ідентичні спектри випромінювань комп'ютерів і чим компактніше вони розташовані, тим вище цей ефект. Отже, для захисту інформації доцільно, якщо можна, використовувати однакові компактно розміщені комп'ютери – системні блоки і монітори. Слід зазначити, що різні монітори і системні блоки комп'ютерів не забезпечують такого взаємного ефекту, що маскує, як однакові пристрої. Дійсно, з хору значно легше виділити голос, що відрізняється від інших. Тут – аналогічно. Різні системні блоки і монітори відрізняються один від іншого різними спектрами радіовипромінювання, а це полегшує процес селекції інформації.

Звичайно, цей організаційний метод не знімає проблему радіовипромінювання комп'ютерів. Зменшувати радіовипромінювання необхідно, але зменшувати його вплив у всіх комп'ютерах, що входять до складу групи. І в першу чергу в тих, чия інформація важливіше, і, звичайно, таємніша. Інші комп'ютери будуть забезпечувати своєрідне «прикриття» випромінюванням, що маскує.

На додаток до викладених рекомендацій слід зазначити, що значною мірою проблему випромінювання моніторів комп'ютерів можна вирішити заміною традиційних моніторів, заснованих на принципі високочастотного розгорнення зображення на екрані електроннопроменевої трубки на більш сучасні монітори з рідкокристалічними (РК) екра-

нами. РК-монітори характеризуються значно меншим рівнем випромінювань: радіо й інших. На жаль, ці пристрої набагато дорожче. Але ціни на рідкокристалічні монітори швидко знижуються, що поступово робить їх більш доступними. Тому можна припускати, що в найближчі кілька років монітори цього типу будуть більш поширеними, ніж у цей час, і проблема випромінювання моніторів трохи зменшиться.

2.13. Основні стаціонарні засоби захисту інформації

Вібросистема WNG-006

Комплект призначений для постановки перешкод системам перехоплення інформації, що працює по віброакустичному каналі витоку.

Комплект складається з блока формування перешкоди і датчиків. Блок формує електричний сигнал, промодульований випадковим чином. Датчик перетворить електричний сигнал, переданий по кабелю від блока формування перешкоди, у вібросигнал. Датчик жорстко кріпиться на поверхні, що захищається, і перекриває площі від 1 до 1,5 кв. м.

Габарити датчика – циліндр діаметром 50 і висотою 10 мм.

Живлення блока формування перешкоди – мережеве 220 В / 50 Гц.

Фільтр «Граніт-8»

Фільтр призначений для блокування витоку акустичної інформації по телефонній лінії при покладеній трубці телефонного апарата.

Основні технічні й експлуатаційні характеристики:

— Виріб призначений для роботи на навантаження 600 Ом +/-10 % у безупинному режимі.

— Загасання в смузі частот 0,15–10 кГц при рівні вхідного сигналу 10 В не більше ніж 3 дБ.

— Загасання при вхідній напрузі 10 В на частоті 50 Гц не менше

ніж 6 дБ, на частоті 100 кГц не менше ніж 10 дБ.

— Габаритні розміри виробу не більше ніж 95х60х25 мм.

— Маса фільтра не більше ніж 0,2 кг.

Пристрій захисту від диктофонів і радіомікрофонів «Буран-2»

Виріб «Буран-2» призначено для запобігання несанкціонованого запису акустичної інформації в приміщенні на диктофон та ретрансляції інформації за допомогою радіомікрофона. Придушення здійснюється шляхом постановки нечутної для вуха людини перешкоди.

Виріб виконаний у вигляді трьох функціонально і конструктивно закінчених модулів: формувача перешкодного сигналу, антенного вузла і вузла живлення. Усі вузли розміщені на шасі, вбудованому в аташе-кейсі.

Основні технічні й експлуатаційні характеристики:

— Дальність придушення – 1,5 м.

— Ширина головного пелюстка на рівні 3 дБ – 45–60°.

— Напруга живлення від автономного джерела – 30–32 В.

— Споживаний струм від автономного джерела – < 900 ма.

— Живлення – від мережі 220 В / 50 Гц (і від акумуляторів).

Стаціонарний цифровий виявник диктофонів PTKD-018

У новій системі PTRD-018, побудованій на основі мікропроцесора 80C251 SB, застосовані найсучасніші принципи виявлення диктофонів, що дозволяють охопити до 16 посадкових місць. Дальність виявлення за сприятливих умов – 1,5 м для кожного датчика. Системою можна керувати за допомогою комп’ютера, який підключається через порт RS-232, що дає змогу інтегрувати PTRD-018 у глобальну систему захисту.

Генератор «білого шуму» IVNG-022

Цей пристрій дозволить ефективно забезпечити захист переговорів від систем промислового шпигунства, що прослуховують.

Прилад випромінює так званий «білий шум» в основному спектрі звукових частот, що забезпечує маскування розмови і робить практично неможливим її розуміння після передачі будь-якими типами систем, що прослуховують. Прилад впливає безпосередньо на вхідні низькочастотні системи, що підслуховують (мікрофони), незалежно від особливостей їх схемотехніки і принципів передачі інформації цих пристроїв.

Генератор шуму «Гном-3»

Генератор шуму «Гном-3» «маскує» у перешкоді корисну інформацію, що міститься в побічних електромагнітних випромінюваннях.

Основні технічні й експлуатаційні характеристики.

Рівень шумового сигналу на вихідних розніманнях генератора в діапазоні частот:

— від 10 до 150 кГц (f прийм.= 200 Гц) – не менше ніж 70 дБ;
— від 150 кГц до 30 МГц (f прийм.= 9 кГц) – не менше ніж 70 дБ;
— від 30 до 400 МГц (f прийм.=120 кГц) – не менш 75 дБ;
— від 400 до 1 гГц (f прийм.= 120 кГц) – не менше ніж 45 дБ.

Ослаблення рівня сигналу в піддіапазонах частот:

— від 10 до 150 кГц – не менше ніж 30 дБ;
— від 150кГц до 30 МГц – не менше ніж 30 дБ;
— від 30 300 МГц – не менше ніж 20 дБ.

Ентропійний коефіцієнт шуму – не менше ніж 0,8.

СТО-24 «Хуртовина»

Прилад призначений для контролю параметрів телефонних ліній для виявлення несанкціонованого гальванічного підключення електронних засобів знімання інформації (ЗЗІ), а також для/або виключення утруднення нормальної роботи цих засобів. Прилад призначений для роботи на телефонних лініях міських АТС, а також може бути модифі-

кований для роботи на міні АТС.

Прилад дозволяє:

1) придушувати послідовно підключені електронні ЗЗІ, що мають «м'який» радіоканал передачі (не мають кварцової стабілізації частоти):

— значно знизити потужність передавача (відношення «сигнал/шум») паралельно підключених ЗЗІ, що мають «твердий» радіоканал (кварцова стабілізація частоти) передачі;

2) знизити ефективність застосування паралельно підключених ЗЗІ, що мають «м'який» канал, за рахунок зсуву і зміни спектра сигналу:

— вмикати пристрої, що прослуховують, якими управляють по сигналу звукового діапазону, на передачу і запис шуму замість інформації за рахунок створення активної шумоподібної перешкоди в різних режимах роботи телефонного апарата: якщо слухавку знято; якщо слухавку покладено;

— установлювати пасивне загородження прийому сигналів мовного діапазону з телефонної лінії за допомогою індукційних датчиків шляхом зменшення відношення сигнал/шум не менше ніж у 3 рази;

— установлювати пасивне загородження поширенню в лінії високочастотних сигналів несучих частот радіопередавачів;

— забезпечувати загасання в смузі частот 0,15...15 кГц при рівні вхідного сигналу 10 В не більше ніж 3 дБ;

— забезпечувати загасання на – 50 кГц при рівні сигналу 10 В – не менше ніж 60 дБ, на – 100 кГц не менше ніж 100 дБ.

Основні технічні й експлуатаційні характеристики:

— живлення генератора перешкоди від телефонної лінії – 60 В;

— струм споживання в режимі захисту – 500 мкА;

— живлення від акумулятора – 9 В;

— погрішність виміру U ± 0,2;

— розмах шумового сигналу прямокутної форми 4,5...5 У;

— габарити 12,5 х 68 х 40 мм.

2.14. Пошукове устаткування

Професійний багатополосний радіоприймач AR-3000A

Має рідкокристалічний індикатор, на якому відображається рівень сигналу (у дБ), частота прийнятого сигналу, вид модуляції, номер каналу пам'яті, режим роботи й інше. Може працювати разом з IBM/PC у разі наявності програмного забезпечення. Можливе підключення магнітофона, акустичних систем, навушників.

Основні технічні й експлуатаційні характеристики:

— частотний діапазон: 100 кГц – 2 036 МГц;

— види модуляції: USB, LSB, CW, AM, NFM, WFM;

— кількість каналів пам'яті: 4 банки (по 100 каналів);

— чутливість:

Діапазон	Вид модуляції			
	SSB/CW	AM	NFM	WFM
1 Мгц - 2.5 Мгц	1.0мВ	3.2 мкВ	-	-
2.5 мГц-1.8 ГГц	0.25 мкВ	1.0 мкВ	0.35 мкВ	1.0 мкВ
1.8 ГГц-2 ГГц	0.75 мкВ	3.0 мкВ	1.25 мкВ	3.0 мкВ

— аудіовихід: 4 – 8 Ом;

— напруга: 13,8 В (через блок живлення від мережі 110/220 В);

— розміри: 138 х 80 х 200 мм.

Портативний нелінійний радіолокатор «АТ-6»

Призначений для виявлення пристроїв, що містять напівпровідникові елементи: транзистори, діоди, мікросхеми.

Основні технічні й експлуатаційні характеристики:

— живлення виробу здійснюється як від мережі перемінного струму

частотою 50 Гц, напругою 220 В, так і від джерела постійного струму напругою 12 В;

— потужність, споживана виробом від джерела живлення, не перевищує:

4 Вт в імпульсному режимі;

— час безупинної роботи виробу не більше ніж 8 год;

— вага блока портативного нелінійного радіолокатору не перевищує 2 кг;

— передавач працює в імпульсному режимі на частоті 905+1 МГц;

— тривалість імпульсу не більше ніж 1,5 мкс;

— частота проходження імпульсів;

— в імпульсному режимі 400+50 Гц;

— у режимі, що обгинає 20+1 кГц;

— частота настроювання дорівнює подвоєній частоті передавача;

— реальна чутливість при співвідношенні сигнал\шум не менше ніж 6 дБ і при вихідній напрузі 0,1 В (амплітудне значення) – не гірше 10 – 11 дБ;

— регулювання посилення приймача здійснюється плавно в діапазоні 0–30 дБ;

— узагальнена ширина діаграми спрямованості за рівнем 0,5. Розмах не більше ніж 90°.

Контрольні запитання

1. Чи є гарантія, що конкретна інформація доступна лише тим особам, для яких вона призначена?
2. Під політичними факторами загроз інформаційній безпеці розуміють?
3. Основними організаційно-технічними факторами загроз інформаційній безпеці є?
4. У групу антропогенних джерел загроз безпеки інформації входять?
5. До техногенних джерел загроз належать?
6. До стихійних джерел загроз належать?
7. Які основні функції апаратних засобів захисту інформації?
8. Який випромінювач не включає комплекс віброакустичного захисту?
9. До електронних пристроїв знімання акустичної інформації належать?
10. Які пристрої є обов’язковими у радіомікрофонах?

Тема 3. ЗАХИСТ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Історично перші електронні обчислювальні машини (ЕОМ) поставлялися без єдиної програми, що управляє, і користувачі повинні були самі створювати програмні засоби, що охоплюють всі аспекти вирішуваного завдання. З накопиченням досвіду використання ЕОМ спочатку почали з'являтися програми для допомоги програмістові, потім – програми-утиліти загального застосування, які могли використовувати користувачі під час вирішення різних завдань. Поступово ці програми почали структуруватися і організовуватися так, щоб виконувати основні функції взаємодії користувача з апаратними засобами ЕОМ. Це привело до появи операційної системи (ОС).

Операційна система – спеціально організована сукупність програм, яка управляє ресурсами системи (ЕОМ, обчислювальної системи) для найбільш ефективного їх використання і забезпечує інтерфейс користувача з ресурсами.

Механізми захисту операційних систем. Під механізмами захисту ОС розумітимемо всі засоби і механізми захисту даних, що функціонують у складі ОС.

Операційні системи, у складі яких функціонують засоби і механізми захисту даних, в літературі часто називають захищеними системами.

Моделі доступу до даних. Через те, що ОС можна подати як сукупність даних, для яких також необхідно забезпечити надійний захист, під безпекою ОС розумітимемо такий стан ОС, при якому неможливе випадкове або навмисне порушення функціонування ОС, а також порушення безпеки ресурсів системи, що знаходяться під управлінням ОС. Вкажемо такі особливості ОС, які дозволяють виділити питання забезпечення безпеки ОС в особливу категорію:

– управління всіма ресурсами системи;
– наявність вбудованих механізмів, які прямо або побічно впливають на безпеку програм і даних, ОС, що працюють в середовищі;
– забезпечення інтерфейсу користувача з ресурсами системи;
– розміри і складність ОС.

Через ці особливості забезпечення безпеки ОС відігравало і продовжує відігравати важливу роль в процесі розвитку обчислювальної тех-

ніки.

Більшість ОС мають дефекти з погляду забезпечення безпеки даних в системі, що, як вже наголошувалося, зумовлено виконанням завдання забезпечення максимальної доступності системи для користувача.

Контроль доступу до даних. Під час створення механізмів контролю доступу необхідно, перш за все, визначити суб'єктів і об'єктів доступу. **Суб'єктами** можуть бути, наприклад, користувачі, завдання, процеси і процедури. **Об'єктами** – файли, програми, семафори, директорії, термінали, канали зв'язку, пристрої, і так далі. Суб'єкти можуть одночасно розглядатися і як об'єкти, тому у суб'єкта можуть бути права на доступ до іншого суб'єкта. У конкретному процесі в певний момент часу суб'єкти є активними елементами, а об'єкти – пасивними.

Для здійснення доступу до об'єкта суб'єкт повинен мати відповідні повноваження. Повноваженням є будь-який символ, володіння яким надає суб'єктові певні права доступу стосовно об'єкта ділянка захисту визначає права доступу деякого суб'єкта до безлічі об'єктів, що захищаються, і є сукупністю всіх повноважень цього суб'єкта.

Під час функціонування системи необхідно мати змогу створювати нові суб'єкти і об'єкти. Під час створення об'єкта одночасно створюється і повноваження суб'єктів щодо використання цього об'єкта. Суб'єкт, що створив таке повноваження, може скористатися ним для здійснення доступу до об'єкта або ж може створити декілька копій повноваження для передачі їх іншим суб'єктам.

Безпосередня реалізація контролю прав доступу зазвичай виконується за допомогою матриць доступу.

3.1. Ідентифікація, встановлення справжності

Класифікувати характеристики для встановлення достовірності можливо за мал. 3.1.

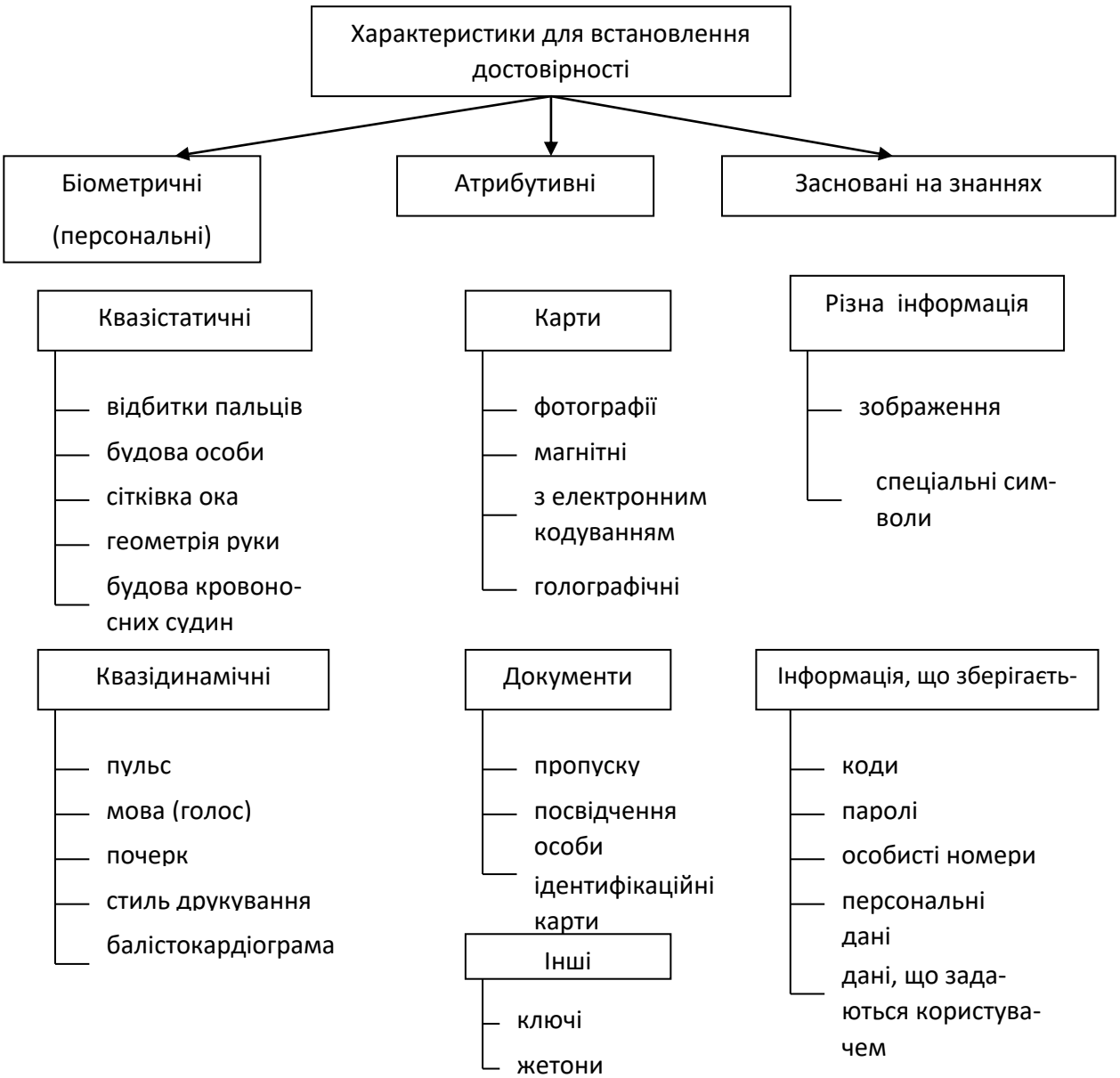

Рис. 3.1. Класифікація характеристик, використовуваних для встановлення достовірності

Особливо помітні успіхи в розробці і реалізації методів встановлення достовірності досягнуті в Японії в рамках проєкту обчислювальних машин п’ятого покоління. У технічній літературі

описані пристрої встановлення достовірності суб'єктів в реальному масштабі часу за почерком, по голосу і за відбитками пальців.

Встановлення достовірності за почерком здійснюється, наприклад, за допомогою спеціальної ручки-датчика. За допомогою цього пристрою встановлення достовірності використовують методи зіставлення контурів, аналізу специфічних штрихів і гістограм.

Під час встановлення достовірності по голосу використовують такі параметри: тембр, висота звуку, акцент, інтонація, сила звуку і швидкість мовлення. Встановлення достовірності по голосу засноване на спектральних методах і, як правило, не залежить від змісту мовлення.

Встановлення достовірності за відбитками пальців здійснюється шляхом звірення пред'явлених відбитків пальців з еталонними. За допомогою цього пристрою використовують методи зіставлення бінарних образів і проєкцій для характерних крапок і напрямків штрихів відбитків пальців.

Акціонерним товариством «ЛЕК УК» (м. Санкт-Петербург) розроблено і реалізовано систему встановлення достовірності на основі пластикових карток, на які кодова інформація записується і зчитується лазерно-голографічними методами. Такі карти можуть використовуватися в двох режимах: ключа і персонального ідентифікаційного коду (ПІК). У режимі ключа картка служить для відкриття спеціальних голографічних електронно-механічних замків, що встановлюються на об'єктах, що захищаються. У режимі ПІК картка використовується для обмеження доступу до терміналів обчислювальної системи і даних, що в ній зберігаються. Для цього на картку заноситься ПІК користувача, що займає від 64 до 256 біт.

Найбільш поширеними для встановлення достовірності на сьогодні є методи паролювання.

3.2. Методи паролювання

*Метод простого паролювання***.** Методи паролювання вимагають, щоб користувач увів рядок символів (пароль) для порівняння з еталонним паролем, що зберігається в пам'яті системи. Якщо пароль відповідає еталонному, то користувач може працювати із системою. Розглядаючи різні методи паролювання, використовуватимемо такі позначення: З – повідомлення системи; П – повідомлення, що вводиться користувачем; ОК – повідомлення системи про правильне встановлення достовірності.

Метод простого пароля полягає у введенні користувачем одного пароля з клавіатури.

Приклад: паролем є слово «ПАРОЛЬ».

З: Введіть пароль

П: ПАРОЛЬ

З: ОК

Метод вибірки символів. Полягає в запиті системою певних символів пароля, вибираних випадково.

Приклад: паролем є слово «ПАРОЛЬ».

З: Введіть пароль: 2, 5

П: АЛ

З: ОК

Метод вибірки символів не дозволяє порушникові визначити значення пароля за одноразовим спостереженням символів, що вводяться користувачем.

Метод паролів одноразового використання. Припускає наявність списку з N паролів, що зберігається в системі. Під час кожного звернення до системи користувач уводить черговий пароль, який після закінчення роботи викреслюється системою із списку.

Основним недоліком розглянутого методу є неоднозначність пароля. Наприклад, у разі нештатного закінчення роботи користувача система може вважати пароль вже використаним, а користувач – ні.

Метод груп паролів. Ґрунтується на тому, що система для кожного користувача може зажадати паролі з двох груп. Перша група включає паролі, які є відповідями на загальні для всіх користувачів запитання, наприклад, ім’я, адреса, номер телефону і тому подібне. Друга група включає паролі – відповіді на запитання, які встановлюються адміністратором системи під час реєстрації користувача для роботи із системою. Ці питання сформульовані персонально для кожного користувача, наприклад, улюблений колір, дівоче прізвище матері і тому подібне. При кожному зверненні користувача система випадково вибирає по декілька питань з кожної групи. Недоліком розглянутого методу є те, що системі буде потрібно значний об’єм пам’яті для зберігання запитань і відповідей для великої кількості користувачів.

Метод функціонального перетворення. Припускає, що користувачеві під час реєстрації для роботи в системі повідомляється деяке перетворення, яке він може виконати подумки. Паролем у цьому разі є результат такого перетворення.

Даний метод заснований на використанні деякої функції, яка

повинна відповідати таким вимогам:

- для заданого числа або слова X легко обчислити Y = F (X);
- знаючи X і Y, складно або неможливо визначити функцію Y = F (X).

Необхідною умовою виконання даних вимог є наявність у функції F (X) динамічно змінюючихся параметрів, наприклад, поточних дат, часу, номера дня тижня або віку користувача.

Користувачеві повідомляється:

- вихідний пароль - слово або число X, наприклад, число 31;
- функція F (X), наприклад, Y = (X mod 100) * D + W, де (X mod 100) -

операція взяття залишку від цілочисельного ділення X на 100, D - поточний

номер дня тижня, а W - поточний номер тижня в поточному місяці;

- періодичність зміни пароля, наприклад, кожен день, кожні три

дня або кожного тижня.

Паролями користувача для послідовності встановлених періодів дій одного пароля будуть відповідно X, F (X), F (F (X)), F (F (F (X))) і т.д., тобто для і-го періоду дії одного пароля паролем користувача буде $F^{i-1}(X)$. Тому для того щоб обчислити черговий пароль після закінчення періоду дії використовуваного пароля, користувачеві не потрібно пам’ятати початковий пароль, важливо лише не забути функцію парольного перетворення і пароль, який використовується до теперішнього моменту часу.

Для ускладнення пароля в методі функціонального перетворення як аргументи можуть використовуватися числа місяця, час доби або їх комбінації.

Під час роботи з паролями потрібно дотримуватись таких правил:

– паролі повинні зберігатися в пам’яті тільки в зашифрованому вигляді;

– символи пароля при введенні їх користувачем не повинні з’являтися в явному вигляді;

– паролі повинні періодично змінюватися;

– паролі не повинні бути простими.

Для перевірки складності паролів зазвичай використовують спеціальні контролери паролів.

Контролер паролів дозволяє перевірити вразливість паролів. Контролер здійснює спроби злому пароля за такою методикою.

1.Перевірка використання як пароль вхідного імені користувача, його ініціалів і їх комбінацій. Наприклад, для користувача Daniel V.

Klein (автор контролера) контролер пробуватиме паролі DVK, DVKDVK, DKLEIN, LEINK, DVKLEIN, DANIELK, DVKKVD, DANIEL-KLEIN і так далі.

2.Перевірка використання як пароль слів з різних словників (60 000 слів):

– чоловічі і жіночі імена (16 000 імен);
– назви країн і міст;
– імена персонажів мультфільмів, кінофільмів;
– спортивні терміни (назви спортивних команд, імена спортсменів, спортивний жаргон і тому подібне);
– числа (цифрами і прописом, наприклад, 2 000, TWELVE);
– рядки букв і цифр (наприклад, AA, AAA, AAAA і так далі);
– біблійні імена і назви;
– біологічні терміни;
– жаргони і лайливі слова;
– послідовність символів у порядку їх розташування на клавіатурі (наприклад, QWERTY, ASDF, ZXCVBN і так далі);
– імена комп'ютерів (з файлу/etc/hostc в ОС Unix);
– персонажі і місця події з творів Шекспіра;
– іноземні слова, що часто вживаються;
– назви астероїдів.

3.Перевірка різних перестановок слів з п. 2, включно із:

– заміною першої букви на прописну;
– заміною всіх букв на прописні;
– інверсією всього слова;
– заміною букви «О» на цифру «0» і навпаки (цифру «1» на букву «l» і так далі);
– перетворенням слів на множину.

Всього відповідно до п. 3 контролер здійснює перевірку на збіг приблизно з одним мільйоном слів.

4. Перевірка різних перестановок слів з п. 2, не розглянутих в п. 3:

– заміна однієї рядкової букви на прописну (наприклад, michel-miChel і тому подібне – близько 400 000 слів);
– заміна двох рядкових букв на прописні (близько 1 500 000 слів);
– заміна трьох рядкових букв на прописні і так далі.

5. Для іноземних користувачів перевірка слів на мові користувача.

6. Перевірка пар слів.

Виконані експерименти показали, що цей контролер дозволив визначити 10 % паролів з п'яти символів, 35 % паролів з шести

символів, 25 % паролів з семи символів і 23 % паролів з восьми символів. Такі високі результати пояснюються тим, що більшість користувачів використовують прості паролі. Цим скористався Роберт Моріс – автор «мережевого черв'яка», що заразив мережу «Інтернет» у 1988 році. Модуль вірусу Моріса здійснював випробування облікових паролів з імен користувачів, та підставляв облікові імена користувачів в зворотному порядку, а також паролі з шаблону, що складається з 432 загальновідомих слів.

В окремих випадках Моріс зумів отримати до 10 % паролів, у тому числі і низки системних паролів.

Наведені приклади дозволяють назвати такі способи зниження вразливості паролів:

– не використовувати як пароль слова, що перевіряються контролером Кляйна;

– перевіряти паролі перед їх використанням контролерами паролів;

– часто змінювати паролі;

– під час формування пароля використовувати розділові знаки і різні регістри;

– використовувати не осмислені слова, а набори букв (наприклад, перших букв будь-якої відомої користувачеві фрази).

З прикладів, наведених під час розгляду контролера паролів, видно, що найважливішими характеристиками пароля є його довжина і період зміни (або період життя). Природно, що чим більше довжина пароля, тим більше зусиль доведеться докласти порушникові для його визначення. Чим більше період життя пароля, тим більше вірогідне його розкриття.

Контрольні запитання

1. У чому полягає Метод паролювання «Вибірка символів»?
2. Яких правил потрібно дотримуватися під час роботи з паролями?
3. Які завдання безпеки реалізуються з допомогою програмних засобів захисту?
4. Для чого призначені контролери паролів?
5. Що таке технологічний пароль?

Тема 4. ПРОГРАМНІ ЗАСОБИ, ЩО МІСТЯТЬ НЕБЕЗПЕКУ

4.1. Перехоплювачі паролів першого роду

Перехоплювачі паролів *першого роду* діють по наступному алгоритму. Зловмисник запускає програму, яка імітує запрошення користувачеві для входу в систему, і чекає введення. Коли користувач вводить ім'я і пароль, закладка зберігає їх в доступному для зловмисника місці, після чого закінчує роботу і здійснює вихід з системи користувача-зловмисника (у більшості операційних систем вихід користувача з системи можна здійснити програмно). Після закінчення роботи закладки на екрані з'являється справжнє запрошення для входу користувача в систему.

Користувач, що став жертвою закладки, бачить, що він не увійшов до системи, і що йому знову пропонується ввести ім'я і пароль. Користувач припускає, що під час введення пароля відбулася помилка, і вводить ім'я і пароль повторно. Після цього користувач входить в систему, і подальша його робота протікає нормально. Деякі закладки, що функціонують за цією схемою, перед закінченням роботи видають на екран правдоподібне повідомлення про помилку, наприклад: «Пароль введений неправильно. Спробуйте ще раз».

Основною перевагою цього класу перехоплювачів паролів є те, що написання подібної програмної закладки не вимагає від зловмисника жодної спеціальної кваліфікації. Будь-який користувач, що вміє програмувати хоча б мовою BASIC, може написати таку програму за лічені години. Єдина проблема, яка може тут виникнути, полягає в програмній реалізації виходу користувача з системи. Проте відповідний системний виклик документований для всіх операційних систем, відомих авторові. Якщо зловмисник не полінується уважно вивчити документацію щодо операційної системи, то він вирішить цю проблему дуже швидко.

Перехоплювачі паролів першого роду є найбільш небезпечні для тих операційних систем, в яких запрошення користувачеві на вхід має дуже простий вигляд. Наприклад, у більшості версій ОС UNIX це запрошення виглядає так: login: user; password:

Завдання створення програми, що підробляє таке запрошення, тривіальне.

Захист від перехоплювачів паролів першого роду.

Ускладнення зовнішнього вигляду запрошення на вхід в систему дещо утрудняє вирішення завдання перехоплення паролів, проте не створює для зловмисника жодних принципових труднощів. Для того щоб істотно утруднити впровадження в систему перехоплювачів паролів першого роду, необхідні складніші заходи захисту. Прикладом операційної системи, де такі заходи реалізовані, є Windows NT.

У Windows NT звичайна робота користувача і автентифікація користувача при вході в систему здійснюються на різних *робочих полях* (desktops). Робочим полем Windows NT є сукупність вікон, одночасно видимих на екрані. Тільки процеси, вікна яких розташовані на одному робочому полі, можуть взаємодіяти між собою, використовуючи засоби Windows GUI. Поняття робочого поля Windows NT близьке до поняття терміналу UNIX.

Процес Winlogon, що одержує від користувача ім’я і пароль, виконується на окремому робочому полі (*робочому полі автентифікації*). Жодний інший процес, у тому числі і перехоплювач паролів, не має доступу до цього робочого поля. Тому запрошення користувачеві на вхід в систему, що виводиться перехоплювачем паролів першого роду, може розташовуватися тільки на робочому полі прикладних програм, де виконуються всі програми, запущені користувачем.

Перемикання екрана комп’ютера з одного робочого поля на інше здійснюється при натисненні комбінації клавіш Ctrl-Alt-Del. Win32 – підсистема Windows NT – обробляє цю комбінацію по-особливому: повідомлення про натиснення Ctrl-Alt-Del посилається тільки процесу Winlogon. Для всіх інших процесів, зокрема для всіх прикладних програм, запущених користувачем, натиснення цієї комбінації клавіш непомітно.

При старті системи на екран комп’ютера спочатку відображається робоче поле автентифікації. Проте користувач вводить ім’я і пароль не відразу, а тільки після натиснення Ctrl-Alt-Del. Коли користувач закінчує сеанс роботи з системою, на екран також виводиться робоче поле автентифікації, і, так само як і у попередньому випадку, новий користувач може ввести пароль для входу в систему тільки після натиснення Ctrl-Alt-Del.

Якщо в систему упроваджений перехоплювач паролів першого роду, то для того, щоб він зміг перехопити пароль користувача, він повинен принаймні обробити натиснення користувачем Ctrl-Alt-Del. Інакше

при натисненні користувачем цієї комбінації клавіш відбудеться перемикання на робоче поле автентифікації, робоче поле прикладних програм стане неактивним, і перехоплювач паролів просто не зможе нічого перехопити – повідомлення про натиснення користувачем клавіш надходитимуть на інше робоче поле. Проте для всіх прикладних програм факт натиснення користувачем Ctrl-Alt-Del завжди залишається непоміченим. Тому пароль буде сприйнятий не програмною закладкою, а процесом Winlogon.

Звичайно, перехоплювач паролів може імітувати не перше запрошення операційної системи, де користувачу пропонується натиснути Ctrl-Alt-Del, а те запрошення, яке висвічується після натиснення користувачем цієї комбінації. Проте в звичайних умовах (за відсутності програмної закладки) це друге запрошення автоматично відміняється за достатньо короткий час (від 30 с до 1 хв, залежить від версії Windows NT). Якщо друге запрошення є на екрані комп'ютера тривалий час, цей факт повинен насторожити користувача. Крім того, як показує досвід, користувачі, що тривалий час працюють з Windows NT, звичкають починати роботу з системою з натиснення Ctrl-Alt-Del незалежно від того, що відображається на екрані.

Захист Windows NT від перехоплювачів паролів першого роду досить надійний. Мабуть, під час розробки заходів захисту операційної системи від перехоплювачів паролів першого роду слід орієнтуватися на механізм, подібний вищеописаному. Слід звернути особливу увагу на такі дві умови, виконання яких обов'язкове для забезпечення надійного захисту від перехоплювачів паролів першого роду:

1. Програма, одержуючи від користувача ім'я і пароль під час входу в систему, виконується на ізольованому терміналі (*терміналі автентифікації*), недоступному прикладним програмам.
2. Факт перемикання призначеної для користувача консолі на термінал автентифікації непомітний прикладним програмам. Прикладні програми не можуть заборонити перемикання консолі на термінал автентифікації.

Якщо операційна система не підтримує ці можливості (а жодна операційна система, відома авторові, крім Windows NT, ці можливості не підтримує), захищеність системи від перехоплювачів паролів першого роду можна підвищити адміністративними заходами. Кожен користувач системи повинен бути проінструктований, що якщо він кілька разів поспіль не може увійти до системи з першого разу, він повинен звернутися до адміністратора.

4.2. Перехоплювачі паролів другого роду

Перехоплювачі паролів другого роду перехоплюють всі дані, що вводяться користувачем з клавіатури. Прості програмні закладки такого типу просто скидають всі ці дані на жорсткий диск комп'ютера або в будь-яке інше місце, доступне зловмисникові. Досконаліші закладки аналізують перехоплені дані і відсівають інформацію, що свідомо не має відношення до паролів. Декілька подібних закладок було в різний час написано для операційної системи MS-DOS, деякі з них використовувалися на практиці, причому дуже ефективно.

Цими закладками є резидентні програми, які перехоплюють одне або декілька переривань процесора, що мають відношення до роботи з клавіатурою. Інформація про натиснуту клавішу і введений символ використовується закладками для своїх цілей.

У кінці 1997 року на хакерських серверах в Інтернеті з'явилися перехоплювачі паролів другого роду для Windows3.x і Windows95. Приклади їх використання зловмисниками для здійснення несанкціонованого доступу поки не зустрічалися на практиці. У телеконференціях в Інтернеті (newsgroups) кілька разів зустрічалися повідомлення про атаки Windows95 перехоплювачами паролів другого роду. Проте ця інформація жодного разу не підтверджувалася.

Створення подібних програмних закладок не потребує великих зусиль. Програмні інтерфейси Win16 і Win32 підтримують спеціальний механізм фільтрів (hooks), який може бути використаний для перехоплення паролів користувачів. За допомогою цього механізму прикладні програми і сама операційна система вирішують цілу низку завдань, у тому числі і завдання підтримки національних розкладок клавіатури. Будь-який русифікатор клавіатури, що працює в середовищі Windows, перехоплює всю інформацію, що вводиться користувачем з клавіатури, у тому числі й паролі. Нескладно написати русифікатора так, щоб він, крім основних функцій, виконував би і функції перехоплювача паролів. Написання програми локалізації клавіатури є достатньо простим завданням. У багатьох довідниках і підручниках з програмування це завдання описано детально, в деяких виданнях наведені початкові тексти простого русифікатора клавіатури. До того ж, Windows підтримує ланцюжки фільтрів, за допомогою яких декілька програм можуть одночасно діставати доступ до інформації, що вводиться з клавіатури, і обробляти її так, як вважають за потрібне, у разі потреби передаючи оброблену інформацію далі по ланцюжку. Можна вбудувати перехоплювач па-

ролів в ланцюжок фільтрів перед русифікатором або після нього так, що вся інформація, що вводиться користувачем з клавіатури, проходить і через русифікатор, і через перехоплювач паролів. В цьому разі завдання написання програмної закладки, що перехоплює паролі користувачів Windows, стає настільки простим, що практично не вимагає від автора закладки спеціальної кваліфікації.

Здебільшого правильне таке твердження: «*Якщо операційна система допускає перемикання розкладки клавіатури при введенні пароля, то для цієї операційної системи можна написати перехоплювач паролів другого роду»*. Дійсно, якщо для операційної системи існує програма локалізації розкладки клавіатури, і якщо ця програма використовується при введенні пароля, після незначної зміни початкового тексту ця програма перетворюється на перехоплювач паролів другого роду. Якщо ця програма написана на мові програмування С, то достатньо додати в програму чотирьох операторів приблизно такого вигляду:

```
StoreFile = fopen (FileName, «a+b»);
fseek (StoreFile, 0, SEEK_END);
fputc (NewSymbol, StoreFile);
fclose (StoreFile).
```

Для деяких операційних систем можна обійтися трьома операторами.

Захист від перехоплювачів паролів другого роду

Для організації захисту від перехоплювачів паролів другого роду необхідно добитися виконання в операційній системі таких трьох умов:

1. Перемикання розкладки клавіатури під час введення пароля неможливе. Інакше завдання створення перехоплювача паролів другого роду істотно спрощується.

2. Конфігурація ланцюжка програмних модулів, що беруть участь в отриманні операційною системою пароля користувача, доступна тільки адміністраторам системи.

3. Доступ на запис до файлів цих програмних модулів надається тільки адміністраторам системи.

Для підвищення стійкості системи захисту до помилок адміністраторів можна сформулювати останню умову так: доступ на запис до файлів програмних модулів, що беруть участь в отриманні пароля користувача, не надається нікому. Доступ на запис до атрибутів захисту цих файлів надається тільки адміністраторам. Будь-які звернення з метою запису до цих файлів, а також до їх атрибутів захисту, реєструються в системному журналі аудиту.

Якщо в системі виконується третя умова в другому формулюванні, адміністрування операційної системи в частині обслуговування клавіатури (зокрема, установка і зміна розкладок клавіатури), дещо ускладнюється.

Для того щоб вказані умови виконувалися, необхідно, щоб підсистема захисту операційної системи підтримувала розмежування доступу і аудит.

Для більшості сучасних операційних систем всі умови, крім першої, можуть бути забезпечені організаційними заходами. Перша умова в неросійськомовних версіях операційних систем зазвичай виконується автоматично. Для більшості російськомовних версій операційних систем (зокрема, для російської версії Windows NT 4.0) добитися виконання цієї умови неможливо – можливість створювати користувачів з російськими іменами закладена в програмне забезпечення операційних систем. У всіх англомовних версіях Windows NT і у всіх відомих авторові версіях UNIX можливе створення і підтримка політики безпеки, за якої виконуються всі три вказані умови.

Якщо забезпечити виконання першої умови в цій операційній системі неможливо, потрібно добитися виконання другої і третьої умов. Виконання цих умов значно підвищує захищеність системи від перехоплювачів паролів другого роду.

4.3. Перехоплювачі паролів третього роду

До перехоплювачів паролів *третього роду* належать програмні закладки, що повністю або частково підміняють собою підсистему автентифікації операційної системи. Оскільки завдання створення такої програмної закладки набагато складніше, ніж завдання створення перехоплювача паролів першого або другого роду, цей клас програмних закладок з’явився зовсім недавно. Існують дві демонстраційні версії перехоплювачів паролів третього роду (обидві для Windows NT). Випадки застосування зловмисниками перехоплювачів паролів третього роду поки не зустрічалися.

Перехоплювач паролів третього роду може бути написаний для будь-якої операційної системи. Складність створення такого перехоплювача паролів залежить від складності алгоритмів, що реалізовуються підсистемою автентифікації, складності інтерфейсу між її окремими модулями, а також від ступеня документованості підсистеми автентифікації операційної системи. Загалом завдання створення перехоплювача паролів третього роду набагато складніше, ніж завдання створення пе-

рехоплювача паролів першого або другого роду. Мабуть, цим і пояснюється невелика кількість програмних закладок цього класу. Проте через широке розповсюдження операційної системи Microsoft Windows NT, що містить достатньо могутні вбудовані засоби захисту від перехоплювачів паролів першого і другого роду, використання перехоплювачів паролів третього роду з метою здійснення несанкціонованого доступу можливе найближчим часом.

Захист від перехоплювачів паролів третього роду

Оскільки перехоплювачі паролів третього роду частково беруть на себе функції підсистеми захисту операційної системи, перехоплювач паролів третього роду під час впровадження в систему повинен виконати принаймні одну з таких дій:

- підмінити собою один або декілька системних файлів;
- упровадитися в один або декілька системних файлів по одному з «вірусних» алгоритмів;
- використовувати підтримувані операційною системою інтерфейсні зв'язки між програмними модулями підсистеми захисту для вбудовування себе в ланцюжок програмних модулів.
- використовувати для тієї ж мети низькорівневі інтерфейсні зв'язки операційної системи, використовувані підсистемою захисту для вирішення своїх завдань.

Кожна з цих дій залишає в операційній системі сліди, які можуть бути виявлені за допомогою таких заходів захисту:

1. Дотримання адекватної політики безпеки. Підсистема автентифікації повинна бути найзахищенішим місцем операційної системи. Заходи, необхідні для підтримки адекватної політики безпеки, дуже розрізняються для різних операційних систем.

У разі дотримання адекватної політики безпеки впровадження в систему перехоплювача паролів третього роду, як і будь-якої іншої програмної закладки, неможливе. Проте, оскільки адміністратори, як і всі люди, схильні допускати помилки у своїй роботі, підтримка адекватної політики безпеки протягом тривалого часу є практично нездійсненним завданням. Крім того, дотримання адекватної політики безпеки захищає тільки від проникнення програмної закладки в систему. Як тільки перехоплювач паролів упроваджений в систему, заходи щодо підтримки політики безпеки стають безглуздими – за наявності в системі програмної закладки політика безпеки не може бути адекватною. Тому необхідні додаткові заходи захисту.

2. Контроль цілісності виконуваних файлів операційної системи. Необхідно контролювати не тільки файли, що входять до складу підсистеми захисту, але і бібліотеки, що містять низькорівневі функції операційної системи.

3. Контроль цілісності інтерфейсних зв'язків усередині підсистеми захисту, а також інтерфейсних зв'язків, використовуваних підсистемою захисту для вирішення низькорівневих завдань.

Створення абсолютно надійного захисту проти перехоплювачів паролів третього роду є неможливою, оскільки машинний код перехоплювачів паролів третього роду виконується не в контексті користувача, а в контексті операційної системи, перехоплювач паролів третього роду може вживати заходи, що утрудняють його виявлення адміністраторами системи, зокрема:

- перехоплення системних викликів, які можуть використовуватися адміністраторами для виявлення програмної закладки для підміни інформації;
- фільтрація реєстрованих повідомлень аудиту.

Мабуть, відбувається «боротьба щита і меча», коли для будь-якої відомої атаки може бути створений надійний захист від неї, і для будь-якого відомого захисту може бути реалізована атака, що дозволяє його ефективно долати.

4.4. Принципи роботи троянських програм

Троянські коні (логічні бомби). До троянських коней належать програми, що завдають будь-які руйнівні дії, тобто залежно від будь-яких умов або під час кожного запуску, що знищує інформацію на дисках, виводить систему з ладу і тому подібне.

Більшість відомих троянських коней є програмами, які «підробляються» під будь-які корисні програми, нові версії популярних утиліт або доповнення до них. Дуже часто вони розсилаються по BBS-станціях або електронних конференціях. Порівняно з вірусами «троянські коні» не дуже поширені з достатньо простих причин: вони або знищують себе разом з рештою даних на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

До «троянських коней» також можна віднести «дропери» вірусів – заражені файли, код яких підправлений так, що відомі версії антивірусів не визначають вірусу у файлі. Наприклад, файл шифрується будь-яким спеціальним способом або упаковується унікальним архіватором, що не

дозволяє антивірусу «побачити» зараження.

Слід зазначити також «злі жарти» (hoax). До них належать програми, які не завдають комп'ютеру будь-якої прямої шкоди, але виводять повідомлення про те, що така шкода вже завдана, або буде завдана за будь-яких умов, або попереджають користувача про неіснуючу небезпеку. До «злих жартів» належать, наприклад, програми, які «лякають» користувача повідомленнями про форматування диска (хоча жодного форматування насправді не відбувається), детектують віруси в незаражених файлах (як це робить широко відома програма ANTITIME), виводять дивні вірусоподібні повідомлення (драйвер диска CMD640X від якогось комерційного пакету) і так далі – залежно від почуття гумору автора такої програми. Мабуть, до «злих жартів» належить також рядок «CHOLEEPA» в другому секторі вінчестерів фірми Seagate.

До такої ж категорії «злих жартів» можна віднести також свідомо помилкові повідомлення про нові супервіруси. Такі повідомлення періодично з'являються в електронних конференціях і зазвичай викликають паніку серед користувачів.

4.5. Принципи роботи утиліт скритого адміністрування

Троянські коні цього класу за своєю суттю є достатньо могутніми утилітами віддаленого адміністрування комп'ютерів у мережі. За своїми функціями вони багато в чому нагадують різні системи адміністрування, що розробляються і поширюються різними фірмами-виробниками програмних продуктів.

Єдина особливість цих програм примушує класифікувати їх як шкідливі троянські програми – це відсутність попередження про інсталяцію і запуск. При запуску Троя встановлює себе в системі і потім стежить за нею, водночас користувачеві не видається жодних повідомлень про дії Трої в системі. До того ж, посилання на Трої може бути відсутнім в списку активних застосувань. Як наслідок, «користувач» цієї троянської програми може і не знати про її наявність в системі, тоді як його комп'ютер відкритий для дистанційного управління.

Будучи встановленими на комп'ютер, утиліти прихованого управління дозволяють робити з комп'ютером все з будь-якими можливостями, що запрограмував автор: приймати/відсилати файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перезавантажувати комп'ютер і так далі. І як наслідок, ця Троя може бути використана для виявлення і передачі конфіденційної інформації, для запус-

ку вірусів, для знищення даних і тому подібне – уражені комп'ютери виявляються відкритими для зловмисних дій хакерів.

Intended-віруси. До таких вірусів належать програми, які на перший погляд є стовідсотковими вірусами, але не здатні розмножуватися внаслідок помилок. Наприклад, вірус, який при зараженні «забуває» помістити в початок файлів команду передачі управління на код вірусу, або записує в неї неправильну адресу свого коду, або неправильно встановлює адресу перехоплюваного переривання (що здебільшого «завішує» комп'ютер) і так далі.

До категорії «intended» також належать віруси, які з наведених вище причин розмножуються тільки один раз – з «авторської» копії. Заразивши який-небудь файл, вони втрачають здібність до подальшого розмноження.

З'являються *intended-віруси* найчастіше при невмілій перекомпіляції якого-небудь вже існуючого вірусу або внаслідок недостатнього знання мови програмування, або внаслідок незнання технічних тонкощів операційної системи.

Конструктори вірусів. Конструктор вірусів – це утиліта, призначена для виготовлення нових комп'ютерних вірусів. Відомі конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати початкові тексти вірусів (ASM-файли), об'єктні модулі й/або безпосередньо заражені файли.

Деякі конструктори (VLC, NRLG) забезпечені стандартним віконним інтерфейсом, де за допомогою системи меню можна вибрати тип вірусу, об'єкти (COM і/або EXE), що вражаються, наявність або відсутність самошифровки, протидію розшифрувальнику, внутрішні текстові рядки, вибрати ефекти, що супроводжують роботу вірусу і тому подібне. Інші конструктори (PS-MPC, G2) не мають інтерфейсу і зчитують інформацію про тип вірусу з конфігураційного файлу.

Поліморфні генератори. Поліморні-генератори, як і конструктори вірусів, не є вірусами у прямому значенні цього слова, оскільки в їх алгоритмі не передбачено функції розмноження, тобто відкриття, закриття і запис у файли, читання і запис секторів і так далі. Головною функцією подібних програм є шифрування тіла вірусу і генерація того, що розшифровує відповідно.

Зазвичай поліморфні генератори розповсюджуються їх авторами без обмежень у вигляді файлу-архіву. Основним файлом в архіві будь-якого генератора є об'єктний модуль, що містить цей генератор. У всіх генераторах, що зустрічалися, цей модуль має зовнішню (external) функцію – виклик програми генератора.

Отже, авторові вірусу, якщо він бажає створити справжній поліморний-вірус, не доводиться довго працювати над кодами власного шифрувальника. На бажання він може підключити до свого вірусу будь-який відомий поліморний-генератор і викликати його з коду вірусу. Фізично це досягається так: об'єктний файл вірусу з'єднується з об'єктним файлом генератора, а в початковий текст вірусу перед командами його запису у файл вставляється виклик поліморного-генератора, який створює коди того, що розшифровує і шифрує тіло вірусу.

4.6. Комп'ютерні віруси і механізми боротьби з ними

Шкідливі програми і, перш за все, віруси є дуже небезпечними для інформації в комп'ютерних системах (КС). Недооцінювання цієї небезпеки може мати серйозні наслідки для інформації користувачів. Шкодить використанню всіх можливостей КС і надмірне перебільшення небезпеки вірусів. Знання механізмів дії вірусів, методів і засобів боротьби з ними дозволяє ефективно організувати протидію вірусам, звести до мінімуму вірогідність зараження і втрат від їх дії.

Термін «комп'ютерний вірус» був введений порівняно недавно – в середині 80-х років. Малі розміри, здатність швидко поширюватися, розмножуючись і упроваджуючись в об'єкти (заражаючи їх), негативна дія на систему – всі ці ознаки біологічних вірусів властиві і шкідливим програмам, що отримали з цієї причини назву «Комп'ютерні віруси». Водночас із терміном «вірус» під час роботи з комп'ютерними вірусами використовуються й інші медичні терміни: «зараження», «місце існування», «профілактика» й інші.

«Комп'ютерні віруси» – це невеликі виконувані або такі, програми що мають властивість до самовідтворення (реплікації) в КС. Віруси можуть виконувати зміну або знищення програмного забезпечення або даних, що зберігаються в КС. Під час розповсюдження віруси можуть себе модифікувати.

4.7. Класифікація комп'ютерних вірусів

На сьогодні у світі налічується більше 50 тисяч тільки зареєстрованих комп'ютерних вірусів. Оскільки переважна більшість сучасних шкідливих програм мають здібність до саморозмноження, то часто їх зараховують до комп'ютерних вірусів. Всі комп'ютерні віруси мо-

жуть бути класифіковані за такими ознаками [4, 20]:

– за місцем існування;
– за способом зараження;
– за ступенем небезпеки деструктивних (шкідницьких) дій;
– за алгоритмом функціонування.

За місцем існування в КС, комп'ютерні віруси поділяють на:

– *мережеві;*
– *файлові;*
– *завантажувальні;*
– *комбіновані.*

Місцем існування *мережевих* вірусів є елементи комп'ютерних мереж. *Файлові* віруси розміщуються у виконуваних файлах. *Завантажувальні* віруси знаходяться в завантажувальних секторах (областях) зовнішніх пристроїв, що записуються у (boot-секторах). Іноді завантажувальні віруси називають бутовими. *Комбіновані* віруси розміщуються в декількох місцях існування. Прикладом таких вірусів є завантажувальні файлові віруси. Ці віруси можуть розміщуватися як в завантажувальних секторах накопичувачів на магнітних дисках, так і в тілі завантажувальних файлів.

За *способом зараження місця існування* комп'ютерні віруси поділяють на:

– *резидентні;*
– *нерезидентні.*

Резидентні віруси після їх активізації повністю або частково переміщаються з місця існування (мережа, завантажувальний сектор, файл) в оперативну пам'ять ЕОМ. Ці віруси, використовуючи, як правило, привілейовані режими роботи, дозволені тільки операційній системі, заражають місце існування і при виконанні певних умов реалізують деструктивну функцію. На відміну від резидентних *нерезидентні* віруси потрапляють в оперативну пам'ять ЕОМ тільки на час їх активності, протягом якого виконують деструктивну функцію і функцію зараження. Потім віруси повністю покидають оперативну пам'ять, залишаючись в місці існування. Якщо вірус поміщає в оперативну пам'ять програму, яка не заражає місце існування, то такий вірус вважається *нерезидентним.*

Арсенал деструктивних або шкідливих можливостей комп'ютерних вірусів дуже великий. Деструктивні можливості вірусів залежать від цілей і кваліфікації їх створювача, а також від особливостей комп'ютерних систем.

За *ступенем небезпеки для інформаційних ресурсів* користувача

комп'ютерні віруси можна поділити на:

– *нешкідливі віруси;*

– *небезпечні віруси;*

– *дуже небезпечні віруси.*

*Нешкідливі к*омп'ютерні віруси створюють автори, у яких не має мети завдати будь-якого збитку ресурсам КС. Ними, як правило, керує бажання показати свої можливості програміста. Іншими словами, створення комп'ютерних вірусів для таких людей – своєрідна спроба самоствердження. Деструктивна дія таких вірусів зводиться до виводу на екран монітора безневинних текстів і картинок, виконання музичних фрагментів і тому подібне.

Проте при всій нешкідливості таких вірусів, як здається, вони завдають певного збитку КС. По-перше, такі віруси витрачають ресурси КС, тією чи іншою мірою знижуючи її ефективність функціонування. По-друге, комп'ютерні віруси можуть містити помилки, що викликають небезпечні наслідки для інформаційних ресурсів КС. Крім того, під час модернізації операційної системи або апаратних засобів КС віруси, створені раніше, можуть призводити до порушень штатного алгоритму роботи системи.

До *небезпечних* належать віруси, які істотно знижують ефективність КС, але не призводять до порушення цілісності і конфіденційності інформації, яка зберігається в пристроях, що запам'ятовують. Наслідки цих вірусів можуть бути ліквідовані без особливих витрат матеріальних і тимчасових ресурсів. Прикладами таких вірусів є віруси, що займають пам'ять ЕОМ і канали зв'язку, але не блокують роботу мережі; віруси, що призводять до повторного виконання програм, перезавантаження операційної системи або повторної передачі даних по каналах зв'язку і тому подібне.

Дуже небезпечними слід вважати віруси, що порушують конфіденційність, знищують, необоротно модифікують (у тому числі і шифрування) інформацію, а також віруси, які блокують доступ до інформації, призводять до відмови апаратних засобів і шкодять здоров'ю користувачів. Такі віруси стирають окремі файли, системні області пам'яті, форматують диски, дістають несанкціонований доступ до інформації, шифрують дані і тому подібне.

Відомі публікації, в яких згадуються віруси, що викликають несправності апаратних засобів. Передбачається, що на резонансній частоті рухомі частини електромеханічних пристроїв, наприклад в системі позиціонування накопичувача на магнітних дисках, можуть бути зруйновані. Саме такий режим і може бути створений за допомогою

програми-вірусу. Інші автори стверджують, що можливе завдання режимів інтенсивного використання окремих електронних схем (наприклад, великих інтегральних схем), за яких настає їх перегрів і вихід з ладу.

Використання в сучасних ЕОМ постійної пам'яті з можливістю перезапису сприяло появі вірусів, які змінюють програми BIOS, що призводить до необхідності заміни постійних пристроїв, які запам'ятовують.

Можливі також дії на психіку людини – оператора ЕОМ за допомогою підбору відеозображення, що видається на екран монітора з певною частотою (кожен двадцять п'ятий кадр). Вбудовані кадри цієї відеоінформації сприймаються людиною на підсвідомому рівні. Як наслідок, можливе нанесення серйозного збитку психіці людини. У 1997 році 700 японців потрапили до лікарні з ознаками епілепсії після перегляду комп'ютерного мультфільму по телебаченню. Припускають, що саме таким способом була випробувана можливість дії на людину за допомогою вбудовування 25-го кадру .

Відповідно до особливостей алгоритму функціонування віруси можна поділити на два класи:

віруси, що не змінюють місце існування (файли і сектори) під час поширення;

віруси, що змінюють місце існування під час поширення.

У свою чергу, віруси, що не змінюють місце існування, можуть бути поділені на дві групи:

–віруси-«супутники» (compaпion);

–віруси-«черви» (worm).

Віруси-«супутники» не змінюють файли. Механізм їх дії полягає у створенні копій виконуваних файлів. Наприклад, в MS DOS такі віруси створюють копії для файлів, що мають розширення .EXE. Копії привласнюється те ж ім'я, що і виконуваному файлу, але розширення змінюється на .COM. При запуску файлу із загальним ім'ям операційна система першим завантажує на виконання файл з розширенням .COM, який є програмою-вірусом. Файл-вірус запускає потім і файл з розширенням .EXE.

Віруси-«черви» потрапляють в робочу станцію з мережі, обчислюють адреси розсилки вірусу по інших абонентах мережі і здійснюють передачу вірусу. Вірус не змінює файлів і не записується в завантажувальні сектори дисків. Деякі віруси-«черви» створюють робочі копії вірусу на диску, інші – розміщуються тільки в оперативній пам'яті ЕОМ.

За складністю, ступенем досконалості і особливостями маскування алгоритмів віруси, що змінюють місце існування, поділяють на:

студентські;

«стелс»-віруси (віруси-невидимки);

поліморфні.

До студентських належать віруси, створювачі яких мають низьку кваліфікацію. Такі віруси, як правило, є нерезидентними, часто містять помилки, досить просто виявляються і віддаляються. «Стелс»-віруси і поліморфні віруси створюються кваліфікованими фахівцями, обізнаними з принципом роботи апаратних засобів і операційної системи, а також мають навички роботи з машинно-орієнтованими системами програмування.

«Стелс»-віруси маскують свою присутність в місці існування шляхом перехоплення звернень операційної системи (ОС) до уражених файлів, секторам і переадресують ОС до незаражених ділянок інформації. Вірус є резидентним, маскується під програми ОС, може переміщатися в пам'яті. Такі віруси активізуються при виникненні переривань, виконують певні дії, у тому числі і по маскуванню, і тільки тоді управління передається на програми ОС, оброблювальні ці переривання. *«Стелс»-віруси* мають здатність протидіяти резидентним антивірусним засобам.

Поліморфні віруси не мають постійних пізнавальних груп – сигнатур. Звичайні віруси для розпізнавання факту зараження місця існування розміщують у зараженому об'єкті спеціальну пізнавальну двійкову послідовність або послідовність символів (сигнатуру), яка однозначно ідентифікує зараженість файлу або сектора. Сигнатури використовуються на етапі поширення вірусів для того, щоб уникнути багатократного зараження одних і тих же об'єктів, оскільки при багатократному зараженні об'єкта значно зростає вірогідність виявлення вірусу. Для усунення демаскуючих ознак поліморфні віруси використовують шифрування тіла вірусу і модифікацію програми шифрування. За рахунок такого перетворення поліморфні віруси не мають збігів коду.

Будь-який вірус, незалежно від приналежності до певних класів, повинен мати три функціональні блоки: блок зараження (поширення), блок маскування і блок виконання деструктивних дій. Поділ на функціональні блоки означає, що до певного блока належать команди програми вірусу, що виконують одну з трьох функцій, незалежно від місця знаходження команд в тілі вірусу.

Після передачі управління вірусу, як правило, виконуються певні функції блока маскування. Наприклад, здійснюється розшифрування тіла вірусу. Потім вірус здійснює функцію впровадження в незаражене

місце існування. Якщо вірусом повинні виконуватися деструктивні дії, то вони виконуються або безумовно, або при виконанні певних умов.

Закінчує роботу вірусу завжди блок маскування. При цьому виконуються, наприклад, такі дії: шифрування вірусу (якщо функція шифрування реалізована), відновлення старої дати зміни файлу, відновлення атрибутів файлу, коректування таблиць ОС і інше.

Останньою командою вірусу виконується команда переходу на виконання заражених файлів або на виконання програм ОС.

Для зручності роботи з відомими вірусами використовуються каталоги вірусів. У каталог поміщаються такі відомості про стандартні властивості вірусу: ім'я, довжина, файли, що заражаються, місце впровадження у файл, метод зараження, спосіб впровадження в ОП для резидентних вірусів, ефекти, що виникають, наявність (відсутність) деструктивної функції і помилки. Наявність каталогів дозволяє під час опису вірусів указувати тільки особливі властивості, опускаючи стандартні властивості і дії.

Файлові віруси та їх структура. Файлові віруси можуть упроваджуватися тільки у виконувані файли: командні файли (файли, що складаються з команд операційної системи), призначені для користувача і системні програми в машинних кодах, а також в документи (таблиці), що мають макрокоманди. Макрокомандами або макросами є виконувані програми для автоматизації роботи з документами (таблицями). Тому такі документи (таблиці) можна розглядати як виконуваний файл.

Для International Business Machines (IBM) – сумісних комп'ютерів вірус може упроваджуватися у файли таких типів: командні файли (BAT), завантажувальні драйвери (SYS), програми в машинних (двійкових) кодах (EXE, COM), документи Word (DOC) з версії 6.0 і вище, таблиці EXCEL (XLS). Макровіруси можуть упровадитися і в інші файли, що містять макрокоманди.

Файлові віруси можуть розміщуватися на початку, в середині і в кінці файлу, що заражається (рис. 4.1).

Незалежно від місця розташування вірусу в тілі зараженого файлу після передачі управління файлу першими виконуються команди вірусу.

У початок файлу вірус упроваджується одним з трьох способів. Перший з них полягає в переписуванні початку файлу в його кінець, а на місце, що звільнилося, записується вірус. Другий спосіб припускає зчитування вірусу і зараженого файлу в оперативну пам'ять, об'єднання їх в один файл і запис його на місце файлу. При третьому способі зараження вірус записується в початок файлу без збереження вмісту. У цьому разі заражений файл стає непрацездатним.

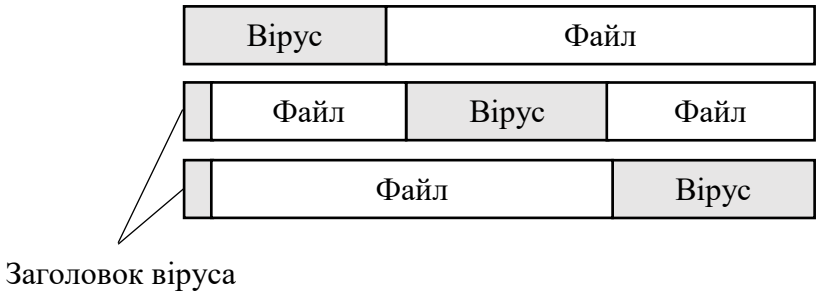

Рис. 4.1. Варіанти розміщення вірусів у файлах

У середину файлу вірус може бути записаний також різними способами. Файл може «розсуватися», а в місце, що звільнилося, може бути записаний вірус. Вірус може упроваджуватися в середину файлу без збереження ділянки файлу, на місце якого поміщається вірус. Є і більш екзотичні способи впровадження вірусу в середину файлу. Наприклад, вірус Mutant застосовує метод стиснення окремих ділянок файлу, при цьому довжина файлу після впровадження вірусу може не змінитися.

Найчастіше вірус упроваджується в кінець файлу. За такої умови, як і у випадку з впровадженням вірусу в середину файлу, перші команди файлу замінюються командами переходу на тіло вірусу.

Алгоритм роботи файлового вірусу. Незважаючи на різноманіття файлових вірусів, можна виділити дії і порядок їх виконання, які є під час реалізації більшості вірусів цього класу. Цей узагальнений алгоритм може бути поданий у вигляді такої послідовності кроків:

Крок 1. Резидентний вірус перевіряє, чи заражена оперативна пам’ять, і у разі потреби заражає її. Нерезидентний вірус шукає незаражені файли і заражає їх.

Крок 2. Виконуються дії із збереження працездатності програми, у файл якої упроваджується вірус (відновлення перших байт програми, настройка адрес програм і так далі).

Крок 3. Здійснюється деструктивна функція вірусу, якщо виконуються відповідні умови.

Крок 4. Передається управління програмі, у файлі якої знаходиться вірус.

У разі реалізації конкретних вірусів склад дій і їх послідовність можуть відрізнятися від наведених в алгоритмі.

Особливості макровірусів. Особливе місце серед файлових вірусів мають макровіруси. Макровірусами є шкідливі програми, написані на макромовах, вбудованих в текстові редактори, електронні таблиці й ін-

ше.

Для існування вірусів у конкретній системі (редакторові) необхідно, щоб вбудована в неї макромова мала такі можливості:

– прив'язку програми на макромові до конкретного файлу;
– копіювання макропрограм з одного файлу в інший;
– отримання управління макропрограмою без втручання користувача.

Таким умовам відповідають редактори MS Word, MS Office, Ami Pro, табличний процесор MS Excel. У цих системах використовуються макромови Word Basic і Visual Basic.

При виконанні певних дій над файлами, що містять макропрограми (відкриття, збереження, закриття тощо), автоматично виконуються макропрограми файлів. Водночас управління отримують макровіруси, які зберігають активність доти, доки активний відповідний редактор. Тому під час роботи з іншим файлом в «зараженому редакторові» він також заражається. Тут простежується аналогія з резидентними вірусами по механізму зараження. Для отримання управління макровіруси, що заражають файли MS Office, як правило, використовують один з прийомів:

– у вірусі є автомакрос (виконується автоматично, під час відкриття документа, таблиці);
– у вірусі перевизначений один із стандартних макросів, який виконується під час вибору певного пункту меню;
– макрос вірусу автоматично викликається на виконання під час натиснення певної клавіші або комбінацій клавіш.

Перший макровірус WinWord.Concept, що вражає документи Word, з'явився літом 1995 року. Шкідлива функція цього вірусу полягає в зміні формату документів текстового редактора Word у формат файлів-стилів. Інший макровірус WinWord.Nuclear вже не такий нешкідливий. Він дописує фразу з вимогою заборони ядерних випробувань, що проводяться Францією в Тихому океані. Крім того, цей вірус щорічно 5 квітня намагається знищити важливі системні файли.

Завантажувальні віруси. Заражають завантажувальні Boot-сектори гнучких дисків і Boot-сектори або Master Boot Record (MBR) жорстких дисків, рис. 4.2.

Завантажувальні віруси є резидентними. Зараження відбувається під час завантаження операційної системи з дисків.

Після включення ЕОМ здійснюється контроль її працездатності за допомогою програми, записаної в постійному пристрої, що запам'ятовує. Якщо перевірка закінчилася успішно, то здійснюється зчитування першого сектора з гнучкого або жорсткого диска. Порядок ви-

користання дисководів для завантаження задається користувачем за допомогою програми Setup. Якщо диск, з якого виконується завантаження ОС, заражений завантажувальним вірусом, то зазвичай виконуються такі кроки:

Крок 1. З першого сектора диска завантажувальний вірус (частина вірусу) отримує управління, зменшує об'єм вільної пам'яті і зчитує з диска тіло вірусу.

Крок 2. Вірус переписує сам себе в іншу ділянку ОП, найчастіше – в старші адреси пам'яті.

Крок 3. Встановлюються необхідні вектори переривань (вірус резидентний).

Крок 4. При виконанні певних умов виконуються деструктивні дії.

Крок 5. Копіюється Boot-сектор в ОП і передається йому управління.

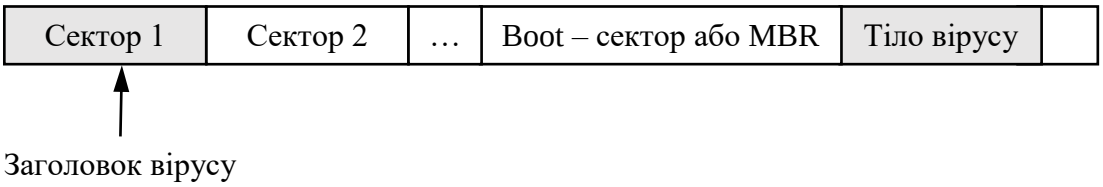

Рис. 4.2. Розміщення завантажувального вірусу на диску

Якщо вірус був активізований з гнучкого диска, то він записується в завантажувальний сектор жорсткого диска. Активний вірус, постійно знаходячись в ОП, заражає завантажувальні сектори всіх гнучких дисків, а не тільки системні диски.

Зараження робочих гнучких дисків завантажувальними вірусами виконується з розрахунку на помилкові дії користувача ЕОМ у момент завантаження ОС. Якщо встановлений порядок завантаження ОС спочатку з гнучкого диска, а потім – з жорсткого, то за наявності гнучкого диска в накопичувачі буде перший сектор з гнучкого диска. Якщо диск був заражений, то цього достатньо для зараження ЕОМ. Така ситуація найчастіше виникає під час перезавантаження ОС після «зависань» або відмов ЕОМ.

Віруси і операційні системи. Програми-віруси створюються для ЕОМ певного типу, що працюють з конкретними ОС. Для одних ОС створені тисячі вірусів. Як приклад можна навести ОС MS DOS, що встановлюється на сумісні персональні комп'ютери.

Для ОС Unix, OS/2, Windows і деяких інших ОС відома невелика кількість вірусів. Привабливість ОС для створювачів вірусів визначається такими чинниками:

–поширеність ОС;

–відсутність вбудованих антивірусних механізмів;

–відносна простота;

–тривалість експлуатації.

Всі наведені чинники характерні для MS DOS. Наявність антивірусних механізмів, складність систем і відносно малі терміни експлуатації роблять завдання створення вірусів важко вирішуваним. Тому автори вірусів для Windows, OS/2 часто вдаються до використання з цих операційних систем MS DOS для впровадження вірусів.

Головним недоліком MS DOS є можливість повного і безконтрольного доступу будь-якої активної програми до всіх системних ресурсів ЕОМ, включаючи і модулі самої ОС.

Операційна система Microsoft Windows 3.1 і її модифікація Microsoft Windows for Workgroups 3.11 не є самостійними ОС, а більше схожі на дуже великі програми MS DOS. У цих ОС введені обмеження на доступ до ОП. Кожна програма дістає доступ тільки до свого віртуального простору ОП. Доступ же до дисків, файлів і портів зовнішніх пристроїв не обмежений. Зберігають працездатність і завантажувальні віруси, розроблені для MS DOS, оскільки вони отримують управління ще до завантаження Microsoft Windows 3.1, в цей період часу їх дії нічим не обмежені.

Слабкість захисних функцій ОС Microsoft Windows 95/98 також пояснюється сумісністю з MS DOS. Ця ОС має таку ж стійкість до дії вірусів, як і Microsoft Windows 3.1. До того ж, у цій ОС набули поширення і макровіруси.

Значно краще захищена від вірусів операційна система OS/2. Ця система повністю незалежна від MS DOS. Всі програми, що виконуються в OS/2, працюють в окремих адресних просторах, що повністю виключає можливість взаємного впливу програм. Існує можливість заборонити робочим програмам (несистемним) мати доступ до портів периферійних пристроїв. Якщо ЕОМ з Microsoft OS/2 використовується як файл-сервера ШМ LAN Server, то за допомогою драйвера 386 HPFS можна вказувати права доступу до каталогів і файлів. Можна також захистити каталоги від запису у файли, що містяться в них. У цій системі є можливість виконання програм MS DOS. Але в OS/2 для вірусів, створених для MS DOS, значно менше можливостей.

4.8. Методи і засоби боротьби з вірусами

Через масове поширення вірусів, серйозність наслідків їх дії на ресурси КС виникла потреба розробки і використання спеціальних антивірусних засобів і методів їх застосування. Антивірусні засоби застосовуються для вирішення таких завдань:

– виявлення вірусів в КС;

– блокування роботи програм-вірусів;

– усунення наслідків дії вірусів.

Виявлення вірусів бажано здійснювати на стадії їх впровадження або, принаймні, до початку здійснення деструктивних функцій вірусів. Необхідно зазначити, що не існує антивірусних засобів, що гарантують виявлення всіх можливих вірусів.

У разі виявлення вірусу необхідно відразу ж припинити роботу програми-вірусу, щоб мінімізувати збиток від його дії на систему.

Усунення наслідків дії вірусів здійснюється у двох напрямках:

– видалення вірусів;

– відновлення (якщо треба) файлів, областей пам’яті.

Відновлення системи залежить від типу вірусу, а також від часу виявлення вірусу щодо початку деструктивних дій. Відновлення інформації без використання дублюючої інформації може бути нездійсненним, якщо віруси при впровадженні не зберігають інформацію, на місце якої вони поміщаються в пам’ять, а також якщо деструктивні дії вже почалися, і вони передбачають зміни інформації.

Для боротьби з вірусами використовуються програмні і апаратно-програмні засоби, які застосовуються в певній послідовності і комбінації, утворюючи методи боротьби з вірусами. Можна виділити методи виявлення вірусів і методи видалення вірусів.

Відомі такі методи виявлення вірусів:

– сканування;

– виявлення змін;

– евристичний аналіз;

– використання резидентних сторожів;

– вакцинація програм;

– апаратно-програмний захист від вірусів.

Сканування – один з найпростіших методів виявлення вірусів. Сканування здійснюється програмою-сканером, яка проглядає файли у пошуках пізнавальної частини вірусу – сигнатури. Програма фіксує наявність вже відомих вірусів, за винятком поліморфних вірусів, які за-

стосовують шифрування тіла вірусу, змінюючи при цьому кожного разу і сигнатуру. Програми-сканери можуть зберігати не сигнатури відомих вірусів, а їх контрольні суми. Програми-сканери часто можуть видаляти виявлені віруси. Такі програми називають поліфагами.

Метод сканування застосовний для виявлення вірусів, сигнатури яких вже виділені і є постійними. Для ефективного використання методу необхідне регулярне оновлення відомостей про нові віруси.

Метод виявлення змін ґрунтується на використанні програм-ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких зазвичай розміщуються віруси. Під час періодичного виконання програм ревізорів порівнюють характеристики, що зберігаються, і характеристики, що отримуються при контролі областей дисків. За наслідками ревізії програма видає зведення про згадану наявність вірусів.

Зазвичай програми-ревізори запам'ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, характеристики всіх контрольованих файлів, каталогів і номери дефектних кластерів. Можуть контролюватися також об'єм встановленої оперативної пам'яті, кількість підключених до комп'ютера дисків і їх параметри.

Головною перевагою методу є можливість виявлення вірусів всіх типів, а також нових невідомих вірусів. Досконалі програми-ревізори виявляють навіть «стелс»-віруси. Наприклад, програма-ревізор Adinf, розроблена Д. Ю. Мостовим, працює з диском безпосередньо по секторах через BIOS. Це не дозволяє використовувати «стелс»-вірусам можливість перехоплення переривань і «підставки» для контролю області пам'яті, потрібної вірусу.

Є у цього методу і недоліки. За допомогою програм-ревізорів неможливо визначити вірус у файлах, які надходять у систему вже зараженими. Віруси будуть виявлені тільки після поширення в системі.

Програми-ревізори непридатні для виявлення зараження макровірусами, оскільки документи і таблиці дуже часто змінюються.

Евристичний аналіз порівняно недавно почав використовуватися для виявлення вірусів. Як і метод виявлення змін, цей метод дозволяє визначати невідомі віруси, але не вимагає попереднього збору, обробки і зберігання інформації про файлову систему.

Суть евристичного аналізу полягає в перевірці можливих місць існування вірусів і виявлення в них команд (груп команд), характерних для вірусів. Такими командами можуть бути команди створення резидентних модулів в оперативній пам'яті, команди прямого звернення до

дисків, минаючи ОС. Евристичні аналізатори у разі виявлення «підозрілих» команд у файлах або завантажувальних секторах видають повідомлення про можливе зараження. Після отримання таких повідомлень необхідно ретельно перевірити ймовірно заражені файли і завантажувальні сектори всіма наявними антивірусними засобами. Евристичний аналізатор є, наприклад, в антивірусній програмі Doctor Web.

Метод використання *резидентних сторожів* заснований на застосуванні програм, які постійно знаходяться в оперативній пам'яті ЕОМ і відстежують всі дії решти програм.

У разі виконання будь-якою програмою підозрілих дій (звернення для запису в завантажувальні сектори, приміщення в ОП резидентних модулів, спроби перехоплення переривань і тому подібне) резидентний сторож надсилає повідомлення користувачу. Програма-сторож може завантажувати на виконання інші антивірусні програми для перевірки «підозрілих» програм, а також для контролю всіх файлів, що надходять ззовні (із змінних дисків, по мережі).

Істотним недоліком цього методу є значний відсоток помилкових тривог, що заважає роботі користувача, викликає роздратування і бажання відмовитися від використання резидентних сторожів. Прикладом резидентного сторожа є програма Vsafe, що входить до складу MS DOS.

Під *вакцинацією програм* розуміється створення спеціального модуля для контролю її цілісності. Як характеристика цілісності файлу зазвичай використовується контрольна сума. У разі зараження вакцинованого файлу, модуль контролю виявляє зміну контрольної суми і повідомляє про це користувача. Метод дозволяє виявляти всі віруси, у тому числі і незнайомі, за винятком «стелс»-вірусів.

Найнадійнішим методом захисту від вірусів є використання *апаратно-програмних антивірусних засобів.* В цей час для захисту ЕОМ використовуються спеціальні контролери і їх програмне забезпечення. Контролер встановлюється в роз'єм розширення і має доступ до загальної шини. Це дозволяє йому контролювати всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких в звичайних режимах роботи не допускається. Отже, можна встановити захист на зміну головного завантажувального запису, завантажувальних секторів, файлів конфігурації, виконуваних файлів й інше.

При виконанні заборонених дій будь-якою програмою контролер надсилає відповідне повідомлення користувачу і блокує роботу комп'ютера.

Апаратно-програмні антивірусні засоби мають низку переваг

перед програмними:

– працюють постійно;

– виявляють всі віруси, незалежно від механізму їх дії;

– блокують недозволені дії, роботи вірусу або некваліфікованого користувача.

Недолік у цих засобах один – залежність від апаратних засобів. Зміна останніх призводить до необхідності заміни контролера.

Прикладом апаратно-програмного захисту від вірусів є комплекс Sheriff.

Методи видалення наслідків зараження вірусами. Під час видалення наслідків зараження вірусами здійснюється видалення вірусів, а також відновлення файлів і областей пам'яті, в яких знаходився вірус. Існує два методи видалення наслідків дії вірусів антивірусними програмами.

Перший метод припускає відновлення системи після дії відомих вірусів. Розробник програми-фага, що видаляє вірус, повинен знати структуру вірусу і його характеристики розміщення в місці існування.

Другий метод дозволяє відновлювати файли і завантажувальні сектори, заражені невідомими вірусами. Для відновлення файлів програма відновлення повинна завчасно створити і зберігати інформацію про файли, отриману в умовах відсутності вірусів. Маючи інформацію про незаражений файл і використовуючи зведення про загальні принципи роботи вірусів, здійснюється відновлення файлів. Якщо вірус піддав файл незворотнім змінам, то відновлення можливе тільки з використанням резервної копії або з дистрибутива. У разі їх відсутності існує тільки один вихід – знищити файл і відновити його вручну.

Якщо антивірусна програма не може відновити головний завантажувальний запис або завантажувальні сектори, то можна спробувати це зробити вручну. У разі невдачі слід відформатувати диск і встановити ОС.

Існують віруси, які, потрапляючи в ЕОМ, стають частиною його ОС. Якщо просто видалити такий вірус, то система буде непрацездатною.

Одним з таких вірусів є вірус One Half. Під час завантаження ЕОМ вірус поступово зашифровує жорсткий диск. При зверненні до вже зашифрованих секторів резидентний вірус One Half перехоплює звернення і розшифровує інформацію. Видалення вірусу призведе до неможливості використовувати зашифровану частину диска. При видаленні такого вірусу необхідно спочатку розшифрувати інформацію на диску. Для цього необхідно знати механізм дії вірусу.

Профілактика зараження вірусами комп'ютерних систем. Щоб забезпечити ЕОМ від дії вірусів, користувач, перш за все, повинен мати уявлення про механізм дії вірусів, щоб адекватно оцінювати можливість і наслідки зараження КС. Головною ж умовою безпечної роботи в КС є дотримання низки правил, які апробовані на практиці і показали свою високу ефективність.

Правило перше. Використання програмних продуктів, що отримані законним шляхом. Вірогідність наявності вірусу в піратській копії набагато більша, ніж в офіційно отриманому програмному забезпеченні.

*Правило друге***.** Дублювання інформації. Перш за все, необхідно зберігати дистрибутивні носії програмного забезпечення. При цьому запис на носії, що допускає виконання цієї операції, повинен бути, якщо можливо, заблокований. Слід особливо поклопотатися про збереження робочої інформації. Переважно регулярно створювати копії робочих файлів на знімних машинних носіях інформації із захистом від запису. Якщо створюється копія на незнімному носієві, то бажано її створювати на інших ВЗУ або ЕОМ. Копіюється або весь файл, або зміни, що тільки вносяться. Останній варіант застосовний, наприклад, під час роботи з базами даних.

Правило третє. Регулярно використовувати антивірусні засоби. Перед початком роботи доцільно виконувати програми-сканери і програми-ревізори. Антивірусні засоби повинні регулярно оновлюватися.

*Правило четверте***.** Особливо обережними слід бути у разі використання нових знімних носіїв інформації і нових файлів. Нові дискети обов'язково повинні бути перевірені на відсутність завантажувальних і файлових вірусів, а отримані файли – на наявність файлових вірусів. Перевірка здійснюється програмами-сканерами і програмами, що здійснюють евристичний аналіз. Під час першого виконання виконуваного файлу використовуються резидентні сторожі. Під час роботи з отриманими документами і таблицями доцільно заборонити виконання макрокоманд засобами, вбудованими в текстові і табличні редактори (MS Word, MS Excel), до завершення повної перевірки цих файлів.

Правило п'яте. Під час роботи в розподілених системах або в системах колективного користування доцільно нові змінні носії інформації і файли, що вводяться в систему, перевіряти на спеціально виділених для цієї мети ЕОМ. Доцільно для цього використовувати автоматизоване робоче місце адміністратора системи або особи, що відповідає за безпеку інформації. Тільки після всесторонньої антивірусної перевірки дисків і файлів вони можуть передаватися користувачам системи.

Правило шосте. Якщо не передбачається здійснювати запис інфо-

рмації носія, то необхідно заблокувати виконання цієї операції. На магнітних дискетах 3,5 дюйма для цього досить відкрити квадратний отвір.

Постійне дотримання всіх наведених рекомендацій значно зменшить вірогідність зараження програмними вірусами і захистить користувача від безповоротних втрат інформації.

У особливо відповідальних системах для боротьби з вірусами необхідно використовувати апаратно-програмні засоби (наприклад, Sheriff).

Порядок дій користувача у разі виявлення зараження ЕОМ вірусами.

Навіть при скрупульозному виконанні всіх правил профілактики можливість зараження ЕОМ комп'ютерними вірусами повністю виключити не можна. І якщо вірус все ж таки потрапив в КС, то наслідки його перебування можна звести до мінімуму, дотримуючись певної послідовності дій.

Про наявність вірусу в КС можуть свідчити такі події:

– поява повідомлень антивірусних засобів про зараження або про передбачуване зараження;

– явні прояви наявності вірусу, такі як повідомлення, що видаються на монітор або принтер, звукові ефекти, знищення файлів й інші аналогічні дії, які однозначно вказують на наявність вірусу в КС;

– неявні прояви зараження, які можуть бути викликані й іншими причинами, наприклад, відмовами апаратних і програмних засобів КС.

До неявних проявів наявності вірусів в КС можна віднести «зависання» системи, уповільнення виконання певних дій, порушення адресації, відмови пристроїв і тому подібне.

Отримавши інформацію про передбачуване зараження, користувач повинен переконатися в цьому. Вирішити таку задачу можна за допомогою всього комплексу антивірусних засобів. Переконавшись в тому, що зараження відбулося, користувачеві слід виконати таку послідовність кроків:

Крок 1. Вимкнути ЕОМ для знищення резидентних вірусів.

Крок 2. Здійснити завантаження еталонної операційної системи із змінного носія інформації, в якій відсутні віруси.

Крок 3. Зберегти на змінних носіях інформації важливі для вас файли, які не мають резервних копій.

Крок 4. Використовувати антивірусні засоби для видалення вірусів і відновлення файлів, областей пам'яті. Якщо працездатність ЕОМ відновлена, то здійснюється перехід до кроку 8, інакше – до кроку 5.

Крок 5. Здійснити повне стирання і розмітку (форматування) незнімних зовнішніх пристроїв, що запам'ятовують. У ЕОМ для цього можуть бути використані програми MS-DOS FDISK і **FORMAT.** Програма

форматування **FORMAT** не видаляє головний завантажувальний запис на жорсткому диску, в якому може знаходитися завантажувальний вірус. Тому необхідно виконати програму **FDISK** з недокументованим параметром **MBR,** створити за допомогою цієї ж програми розділи і логічні диски на жорсткому диску. Потім виконується програма **FORMAT** для всіх логічних дисків.

Крок 6. Відновити ОС, інші програмні системи і файли з дистрибутивів і резервних копій, створених до зараження.

Крок 7. Ретельно перевірити файли, збережені після виявлення зараження, і, у разі потреби, видалити віруси і відновити файли.

Крок 8. Завершити відновлення інформації всесторонньою перевіркою ЕОМ за допомогою всіх антивірусних засобів, що є у розпорядженні користувача.

За умови виконання рекомендацій щодо профілактики зараження комп'ютерними вірусами, а також за умови вмілих і своєчасних дій у разі зараження вірусами збиток інформаційним ресурсам КС може бути мінімальним.

4.9. Пакетні фільтри

Останнім часом найбільш популярними серед засобів захисту інформаційних ресурсів в Інтернеті є міжмережеві екрани (Firewall або брандмауери). Міжмережевий екран розміщується на шлюзі між локальною мережею і мережею «Інтернет». Крім інших функцій, брандмауер може проглядати IP-пакети і залежно від адреси відправника і одержувача пропускати або не пропускати пакети, що намагаються проникнути в систему.

Міжмережевий екран (МЕ) розташовується на межі мережі і регулює доступ до корпоративних ресурсів. Цей пристрій аналізує і збирає інформацію про зовнішні пакети і сеанси в мережі (залежно від типу брандмауера), згідно прийнятих правил: пропустити або не пропустити конкретний пакет і дозволити або не дозволити організувати конкретний сеанс.

МЕ поділяють на три основні класи:

– фільтри пакетів;
– шлюзи сеансового рівня;
– шлюзи рівня застосувань.

Системи фільтрації пакетів просівають кожен IP-пакет через сито визначених користувачем правил і визначають права пакету на прохід у

внутрішню частину мережі. Шлюзи рівня застосувань у відповідь на кожен запит, що надходить, про надання сервісу організовують зовнішній мережевий сеанс; вони ж відкривають відповідний внутрішній сеанс для санкціонованого доступу і передають пакети між зовнішніми і внутрішніми з'єднаннями. Загалом, шлюзи застосувань, порівняно з фільтрами пакетів, забезпечують ретельніший контроль за сеансом, але, як наслідок, вони вимагають застосування і могутніших обчислювальних потужностей. Системи обох типів призначені для того, щоб захистити мережу від небезпек, що знаходяться зовні.

На думку експертів, брандмауери повинні мати три важливі особливості, а саме:

– весь трафік повинен проходити через одну крапку;

– брандмауер зобов'язаний контролювати і реєструвати весь трафік, що проходить;

– платформа МЕ повинна бути неприступна для атак.

Фільтри пакетів виконують оцінку даних на основі IP-інформації, що наявна в заголовку пакета, а точніше в адресі відправника і одержувача пакета. Фільтр не тільки зчитує IP-заголовок, але і зіставляє отриману інформацію зі списком правил фільтрації для дозволу або заборони передачі пакета. У правилах фільтрації наявні поля IP-адрес, типи протоколів, номери портів відправника і одержувача. Перш ніж дозволити пакету продовження передбачуваного для нього маршруту, фільтри пакетів порівнюють вказані в ньому дані із зумовленими значеннями. Загалом фільтри пакетів є найкращим вирішенням МЕ, але, завдяки своєму умінню перевіряти пакети різних протоколів, є і найгнучкішими інструментами вирішення поставленого завдання. Крім того, фільтри працюють швидко, оскільки для ухвалення рішення вони просто проглядають інформацію про пакет. Проте фільтри пакетів мають декілька істотних недоліків: вони не в змозі відстежувати конкретний мережевий сеанс і не в змозі запобігти атаці з імітацією IP-адреси.

Імітація IP-адреси буває, коли хакер привласнює IP-адресу законного користувача – часто ним є внутрішня адреса того, хто має доступ до ресурсів. Оскільки фільтри пакетів «проглядають» інформацію про IP-адресу, то вони допускають пакет з дозволеною адресою в мережу незалежно від того, звідки ініційований сеанс і хто ховається за адресою. Проте вдосконалена версія цього механізму, відома як динамічна фільтрація пакетів, дозволяє аналізувати адресу, з якої хтось намагається здійснити доступ, і здійснює «пінгування» (ping) для перевірки цієї адреси. Очевидно, якщо зловмисник використовує внутрішню IP-адресу компанії ззовні, то ping не досягне відправника пакета і сеанс не отри-

має продовження. Динамічну фільтрацію пакетів підтримують продукти типу WatchGuard Security System компанії Seattle Software Labs і BorderWare Firewall Server, компанії Secure Computing (цей продукт був придбаний Secure разом з компанією Border Network Technologies з Торонто).

Компанії Seattle Software Labs, Cisco і Checkpoint Software Technologies також підтримують технологію перетворення мережевої адреси, яка забезпечує звичайну фільтрацію пакетів із спотворенням. Під час проходження пакета через брандмауер його IP-адреса замінюється якоюсь іншою, вибраною з відрізку адрес. Така заміна дозволяє приховати внутрішні адреси від зловмисника за межами мережі. Інші типи брандмауерів, наприклад шлюзи рівня застосування і шлюзи рівня каналу, мають цю ж властивість за замовчанням.

Контрольні запитання

1. За яким алгоритмом діють перехоплювачі паролів другого роду?
2. За яким алгоритмом діють перехоплювачі паролів першого роду?
3. За яким алгоритмом діють перехоплювачі паролів третього роду?
4. Що не належить до «шкідливих програм»?
5. Сигнатура вірусу – це?
6. Комп’ютерні віруси не класифікують за?
7. Назвіть складові частини сучасного антивірусу.
8. Віруси, які постійно знаходяться в оперативній пам’яті, називаються?
9. До явних проявів роботи вірусу належать?
10. Головною характеристикою троянської програми є?

Тема 5. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Проблемою захисту інформації шляхом її перетворення займається криптологія (kryptos – таємний, logos – повідомлення). Вона має два напрямки: криптографію і криптоаналіз. Цілі цих двох напрямків прямо протилежні.

Криптографія займається пошуком, дослідженням і розробкою математичних методів перетворення інформації, основою яких є шифрування, а криптоаналіз – дослідженням можливості розшифровки інформації.

Основні напрямки використання криптографічних методів – це передача конфіденційної інформації через канали зв'язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, збереження інформації (документів, баз даних) на носіях у зашифрованому вигляді.

5.1. Криптографічні методи захисту

Сучасна криптографія вивчає і розвиває такі напрямки:

– симетричні криптосистеми (зі секретним ключем);
– несиметричні криптосистеми (з відкритим ключем);
– системи електронного підпису;
– системи управління ключами.

Сучасні криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа. Однак на практиці будь-який шифр, який використовується в тій або іншій криптосистемі, піддається розкриттю з визначеною трудомісткістю. Через це, виникає необхідність оцінки криптостійкості шифрів, які застосовуються, в алгоритмах криптоперетворення.

Допомагаючи зберегти зміст повідомлення в таємниці, криптографію можна використовувати для забезпечення:

– аутентифікації;
– цілісності;
– незаперечності.

Під час аутентифікації одержувачу повідомлення потрібно переконатися, що воно виходить від конкретного відправника. Зловмисник не

може надіслати фальшиве повідомлення від будь-якого імені.

Під час визначення цілісності одержувач повідомлення в змозі перевірити, чи були внесені які-небудь зміни в отримане повідомлення під час його передачі. Зловмисникові не дозволено замінювати дійсне повідомлення на фальшиве.

Незаперечність необхідна для того, щоб відправник повідомлення не зміг згодом заперечувати, що він не є автором цього повідомлення.

В цей час аутентифікація, що здійснюється користувачем, забезпечується за допомогою:

– смарт-карт;

– засобів біометрії;

– клавіатури комп'ютера;

– криптографії з унікальними ключами для кожного користувача.

Основною сферою застосування смарт-карт є ідентифікація користувачів мобільними телефонами.

Біометрія заснована на анатомічній унікальності кожної людини. Біометричні системи ідентифікації наведені на рис. 5.1.

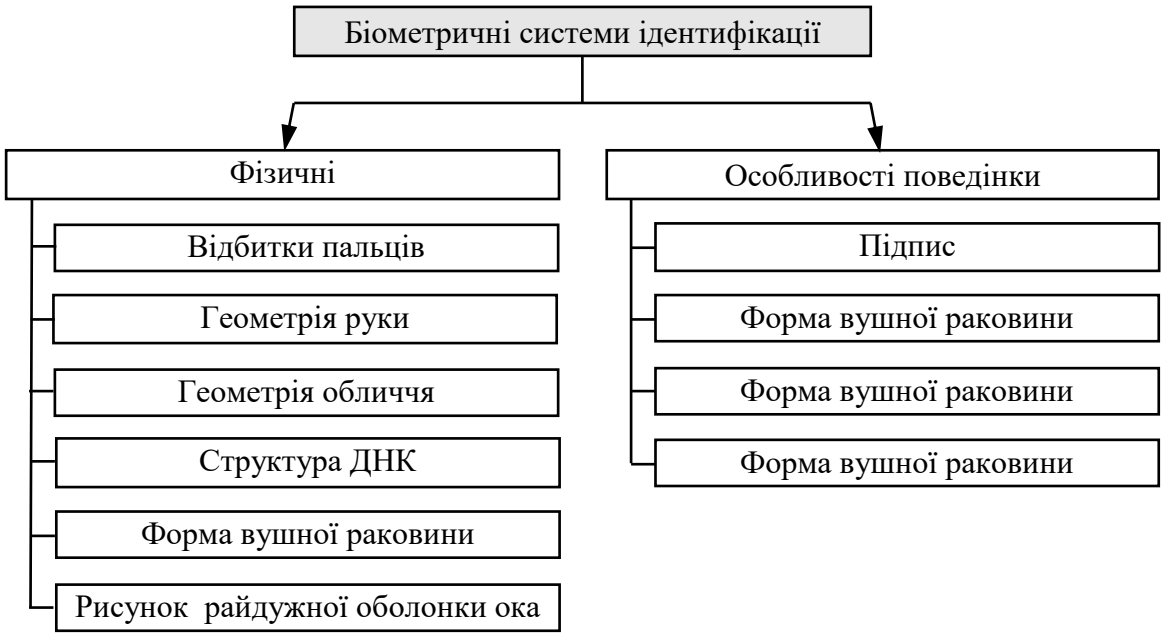

Рис. 5.1. Біометричні системи ідентифікації

Цілісність інформації забезпечується за допомогою криптографічних контрольних сум і механізмів управління доступом і привілеями. Як криптографічна контрольна сума для виявлення навмисної або випадкової модифікації даних використовується код аутентифікації повідом-

лення – MAC (Message Autentification Code).

Для виявлення несанкціонованих змін у переданих повідомленнях можна застосувати:

– електронно-цифровий підпис (ЕЦП), заснований на криптографії з відкритим і закритим ключами;

– програми виявлення вірусів;

– призначення відповідних прав користувачам для управління доступом;

– точне виконання прийнятого механізму привілеїв.

Незаперечність повідомлення підтверджується електронно-цифровим підписом.

Характеристика алгоритмів шифрування. У цей час спостерігається різке зростання об'ємів інформації (у тому числі і конфіденційної), яка передається по відкритих каналах зв'язку. Тому все більш актуальною стає проблема захисту переданої інформації. Незважаючи на те, що конкретні реалізації систем захисту інформації можуть істотно відрізнятися одна від іншої через розбіжність методів і алгоритмів передачі даних, усі вони повинні забезпечувати вирішення триєдиного завдання:

– конфіденційність інформації (доступність її тільки для того, кому вона призначена);

– цілісність інформації (її достовірність і точність, а також захищеність від навмисних і ненавмисних перекручувань);

– готовність інформації (використання в будь-який момент, коли в ній виникає потреба).

Успішне вирішення перерахованих завдань можливе як за рахунок використання організаційно-технічних заходів, так і за допомогою криптографічного захисту інформації.

Організаційно-технічні заходи містять у собі фізичну охорону об'єктів конфіденційної інформації, застосування спеціального адміністративного персоналу і цілу низку інших дорогих технічних заходів для захисту важливих даних.

Криптографічний захист здебільшого є більш ефективним і дешевим. Конфіденційність інформації у цьому разі забезпечується шифруванням переданих документів або всього трафіка.

Процес криптографічного захисту даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги, а саме: висока продуктивність, простота, захищеність і так далі. Програмна реалізація більш практична, допускає значну гнучкість у використанні. До сучасних криптографічних систем захисту інформації висувають такі вимоги:

– зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

– кількість операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинна бути не менше, ніж загальна кількість можливих ключів;

– кількість операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинна мати чітку нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);

– знання алгоритму шифрування не повинне впливати на надійність захисту;

– незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення навіть під час використання того ж ключа;

– структурні елементи алгоритму шифрування повинні бути незмінними;

– додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;

– довжина шифрованого тексту повинна дорівнювати довжині вихідного тексту;

– не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;

– будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;

– алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Криптографічний алгоритм, названий алгоритмом шифрування, являє собою деяку математичну функцію, яка використовується для шифрування і розшифрування. Точніше таких функцій дві: одна застосовується для шифрування, а інша – для розшифрування.

Розрізняють шифрування двох типів:

– симетричне (із секретним ключем);

– несиметричне (з відкритим ключем).

У разі симетричного шифрування (рис. 5.2) створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв'язку. Адресат, запустивши ту ж шифрувальну програму з

отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.

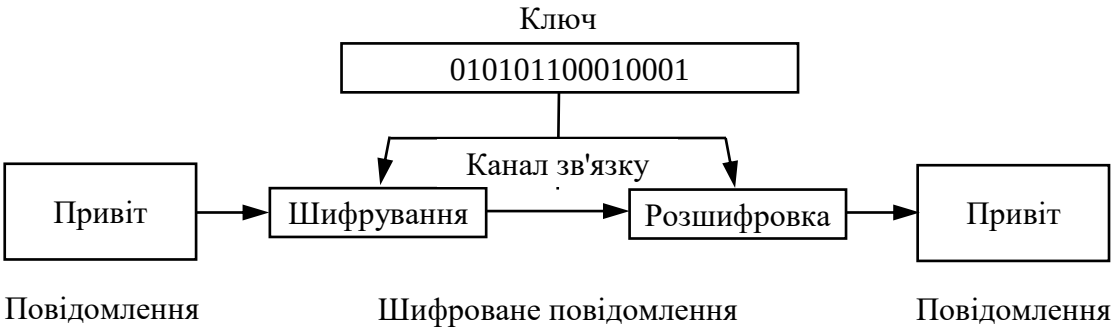

Рис. 5.2. Симетричне шифрування

Несиметричне шифрування складніше, але і надійніше. Для його реалізації (рис. 5.3) потрібні два взаємозалежних ключі: відкритий і закритий. Одержувач повідомляє всім, хто бажає, свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифроване повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. Підвищена надійність несиметричного шифрування потребує складнішого обчислення, тому процедура розшифровки займає більше часу.

Коли надійність криптографічного алгоритму забезпечується за рахунок збереження в таємниці суті самого алгоритму, такий алгоритм шифрування називається обмеженим. Обмежені алгоритми становлять значний інтерес з погляду історії криптографії, однак зовсім непридатні у сучасних вимогах, які висуваються до шифрування. Адже, в цьому разі, кожна група користувачів, які бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми шифрування.

У сучасній криптографії зазначені вище проблеми вирішуються за допомогою використання ключа, який потрібно вибирати серед значень, що належать безлічі (ключовий простір). Функції шифрування і розшифрування залежать від цього ключа. Деякі алгоритми шифрування використовують різні ключі для шифрування і розшифровування. Це означає, що ключ шифрування відрізняється від ключа розшифровування.

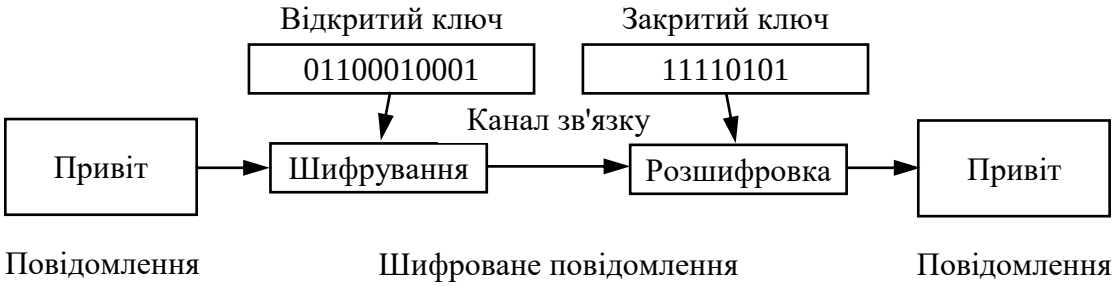

Рис. 5.3. Несиметричне шифрування

Надійність алгоритму шифрування з використанням ключів досягається за рахунок їх належного вибору і наступного збереження в секреті. Це означає, що такий алгоритм не потрібно тримати в таємниці. Можна організувати масове виробництво криптографічних засобів, в основу функціонування яких покладений цей алгоритм. Навіть знаючи криптографічний алгоритм, зловмисник не зможе прочитати зашифровані повідомлення, оскільки він не знає секретний ключ, використаний для його зашифровування.

Симетричні алгоритми шифрування поділяють на:

– потокові;
– блокові.

Алгоритми, у яких відкритий текст обробляється побітно, називаються потоковими алгоритмами або потоковими шифрами. В інших алгоритмах відкритий текст розбивається на блоки, що складаються з декількох біт. Такі алгоритми називаються блоковими або блоковими шифрами. У сучасних комп’ютерних алгоритмах блокового шифрування довжина блока звичайно складає 64 біти. Симетричні алгоритми у разі виявлення в них будь-яких слабкостей можуть бути дороблені шляхом внесення невеликих змін, а для несиметричних – така можливість відсутня.

Симетричні алгоритми працюють значно швидше, ніж алгоритми з відкритим ключем. На практиці несиметричні алгоритми шифрування часто застосовуються в сукупності з симетричними алгоритмами: відкритий текст зашифровується симетричним алгоритмом, а секретний ключ цього симетричного алгоритму зашифровується на відкритому ключі несиметричного алгоритму. Такий механізм називають цифровим конвертом (digital envelope). Найчастіше в цей час застосовують такі алгоритми шифрування:

– DES (Data Encryption Standard);
– Blowfish;
– IDEA (International Decryption-Encryption Algorithm);

– ГОСТ 28147-89;
– RSA (автори: Rivest, Shamir і Alderman);
– PGP.

У симетричних криптоалгоритмах (DES, ДСТ, Blowfish, RC5, IDEA) для шифрування і розшифрування інформації використовується той же секретний ключ. Перевагами таких алгоритмів є:

– простота програмної та апаратної реалізації;
– висока швидкість роботи в прямому і зворотному напрямках;
– забезпечення необхідного рівня захисту інформації під час використання коротких ключів.

До основних недоліків цих криптоалгоритмів варто віднести збільшення витрат щодо забезпечення додаткових заходів таємності під час поширення ключів, а також те, що алгоритм із секретним ключем виконує своє завдання тільки в умовах повної довіри кореспондентів один одному.

У несиметричних криптоалгоритмах (RSA, PGP, ECC) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв'язку, що дозволяє по одному ключу обчислити інший. За допомогою відкритого ключа практично будь-який користувач може зашифрувати своє повідомлення або перевірити електронно-цифровий підпис. Розшифрувати таке повідомлення або поставити підпис може тільки власник секретного ключа. Такі алгоритми дозволяють реалізувати протоколи типу цифрового підпису, забезпечують відкрите поширення ключів і надійну аутентифікацію в мережі, стійкій навіть до повного перехоплення трафіка.

5.2. Основи криптоаналізу

Криптоаналіз (від давньогрец. κρυπτός – прихований і аналіз) – наука про методи розшифровування зашифрованої інформації без призначеного для такої розшифровки ключа.

Термін був введений американським криптографом Уїльямом Ф. Фрідманом 1920 року. Неформально криптоаналіз називають також зломом шифру.

Здебільшого під криптоаналізом розуміють з'ясування ключа; криптоаналіз включає також методи виявлення уразливості криптографічних алгоритмів або протоколів.

Спочатку методи криптоаналізу ґрунтувалися на лінгвістичних закономірностях природного тексту і реалізовувалися з використанням тільки олівця й паперу. В криптоаналізі застосовують математичні ме-

тоди, для реалізації яких використовують спеціалізовані криптоаналітичні комп'ютери.

Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають криптографічного атакою на цей шифр. Криптографічну атаку, в ході якої розкрити шифр вдалося, називають зломом або розкриттям.

Брюс Шнайер виділяє 4 основних і 3 додаткових методи криптоаналізу, припускаючи знання криптоаналітика алгоритму шифру :

Атаки на основі шифротексту. Припустимо, криптоаналітик має деяку кількість шифротекстів, отриманих в результаті використання одного і того ж алгоритму шифрування. У цьому разі криптоаналітик може зробити тільки атаку на основі шифротексту. Метою криптографічної атаки в цьому разі є знаходження якомога більшої кількості відкритих текстів, відповідних наявним шифротекстам, або, що ще краще, знаходження використовуваного під час шифрування ключа.

Вхідні дані для подібних атак криптоаналітик може отримати в результаті простого перехоплення зашифрованих повідомлень. Якщо передача здійснюється по відкритому каналу, то реалізація завдання щодо збору даних порівняно легка і тривіальна. Атаки на основі шифротексту є найслабшими і найнезручнішими.

Атака на основі відкритих текстів і відповідних шифротекстів. Нехай у розпорядженні криптоаналітика є не тільки шифротексти, але і відповідні їм відкриті тексти. Тоді існує два варіанти постановки завдання: 1) знайти ключ, використаний для перетворення відкритого тексту в шифротекст; 2) створити алгоритм, здатний дешифрувати будь-яке повідомлення, закодоване за допомогою цього ключа.

Отримання відкритих текстів відіграє вирішальну роль у здійсненні цієї атаки. Відкриті тексти витягують з різних джерел. Так, наприклад, можна здогадатися про вміст файлу по його розширенню.

У разі злому листування можна зробити припущення, що лист має у вигляді:

«Привітання»
«Основний текст»
«Заключна форма ввічливості»
«Підпис».

Отже, атака може бути організована шляхом підбору різних видів «Привітання» (наприклад, «Привіт!», «Добрий день» і т. д.) і/або «Заключною формою ввічливості» (таких як «З повагою», «Щиро Ваш» тощо). Легко помітити, що ця атака сильніша, ніж атака на основі одного лише шифротексту.

Атака на основі підібраного відкритого тексту. Для здійснення такого типу атаки криптоаналітику необхідно мати не тільки якусь кількість відкритих текстів та отриманих на їх основі шифротекстів, до того ж у цьому разі криптоаналітик повинен мати можливість підібрати кілька відкритих текстів і отримати результат їх шифрування.

Завдання криптоаналітика повторюють завдання для атаки на основі відкритого тексту, тобто отримати ключ шифрування, або створити алгоритм дешифрування для даного ключа.

Отримати вхідні дані для такого виду атаки можна, наприклад, так: створити і відправити підроблене НЕ зашифроване повідомлення нібито від одного з користувачів, які зазвичай користуються шифруванням.

У деяких випадках можна отримати відповідь, в якій буде зашифрований текст, що цитує зміст підробленого повідомлення.

Під час здійснення атаки подібного типу криптоаналітик має можливість підбирати блоки відкритого тексту, що за певних умов може дозволити отримати більше інформації про ключі шифрування.

Атаки на основі адаптаційно підібраного відкритого тексту. Атака такого типу є більш зручним окремим випадком атаки на основі підібраного відкритого тексту. Зручність атаки на основі адаптаційно підібраного відкритого тексту полягає в тому, що крім можливості вибирати шифрований текст, криптоаналітик може прийняти рішення про шифрування того чи іншого відкритого тексту на основі вже отриманих результатів операцій шифрування. Інакше кажучи, під час атаки на основі підібраного відкритого тексту криптоаналітик вибирає всього один великий блок відкритого тексту для подальшого шифрування, а потім на основі цих даних починає зламувати систему. У разі організації адаптаційної атаки криптоаналітик може отримувати результати шифрування будь-яких блоків відкритого тексту, щоб зібрати цікаві для нього дані, які будуть враховані при виборі наступних відправлених на шифрування блоків відкритого тексту і так далі. Через наявність зворотного зв’язку атака на основі адаптаційно підібраного шифротексту має перевагу перед усіма перерахованими вище типами атак.

5.3. Стеганографія

Стеганографія — (з грец. *στεγανός* — прихований + *γράφω* — пишу) — тайнопис, при якому повідомлення, закодоване так, що не виглядає як повідомлення — на відміну від криптографії. Отже, непосвячена людина принципово не може розшифрувати повідомлення — бо не знає про факт його існування.

Якщо криптографія приховує зміст повідомлення, то стеганографія приховує сам факт існування повідомлення.

Історія. Перший запис про використання стеганографії зустрічається в трактаті Геродота «Історія», що належить до 440 року до н. е. У трактаті були описані два методи приховування інформації. Демарат відправив попередження про майбутній напад на Грецію, записавши його на дерев'яну підкладку воскової таблички до нанесення воску. Другий спосіб полягав у такому: на поголену голову раба записувалося необхідне повідомлення, а коли його волосся відростало, він вирушав до адресата, який знову голив його голову і зчитував доставлене повідомлення.

У Китаї листи писали на смужках шовку. Для приховування повідомлень смужки з текстом листа згортали в кульки, покривали воском і потім посильні їх ковтали.

У XV ст. чернець Трітеміус (1462–1516), який займався криптографією і стеганографією, описав багато різних методів прихованої передачі повідомлень. Пізніше, в 1499 році, ці записи були об'єднані в книгу «Steganographia».

Метод приховування інформації за допомогою мікроточки з'явився відразу ж після винаходу Дагером фотографічного процесу, і вперше у військовій справі був використаний під час Франко-прусської війни (1870 р.), але широкого застосування до Другої світової війни цей метод не мав.

У березні 2000 р. 17-річна американська школярка Вівіана Риска (Viviana Risca) створила алгоритм, який може «ховати» повідомлення в генну послідовність ДНК. На конкурсі молодих вчених компанії Intel Science Talent Search вона продемонструвала технологію впровадження комп'ютерних повідомлень в генну послідовність молекули.

Методи. Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі дізнатися про його існування. Одна з перших згадок про застосування тайнопису датується V ст. до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносилась шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія ґрунтується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Сімейна цифрова фотографія може містити комерційну інформацію, а файл із записом сонати

Гайдна — приватний лист.

Але найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканність документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи:

– додатковий захист — засоби захисту є доповненням до основних програмних і апаратних засобів комп'ютерної системи;

– вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потреби, але під час його реалізації можуть виникнути проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таке доповнення характеристик способів захисту зумовлено тим, що в реальній системі їх комбінують.

Класифікація стеганографії. Наприкінці 90-х років виділилося кілька напрямків стеганографії:

– класична стеганографія;
– комп'ютерна стеганографія;
– цифрова стеганографія;
– мережева стеганографія.

Класична. Одним з найпоширеніших методів класичної стеганографії є використання симпатичних чорнил (невидимих). Зазвичай процес запису здійснюється так: перший шар — наноситься важливий запис невидимими чорнилами, другий шар — запис видимими чорнилами, який нічого не означає.

Текст, записаний такими чорнилами, проявляється лише за певних умов (нагрівання, освітлення, хімічний проявник і т. д.).

Ці чорнила винайдені були ще в I ст. н. е. Філоном Александрійським. Їх використовували як в середньовіччі, так і в новітній час, наприклад, у листах революціонерів з російських в'язниць. Написаний звичайним молоком текст на папері між рядків видимого тексту проявляється під час нагрівання над полум'ям (зазвичай свічки).

Існує також чорнило з хімічно нестабільним пігментом. Написане цими чорнилами виглядає як написане звичайною ручкою, але через певний час нестабільний пігмент розкладається, і від тексту не залишається і сліду. Хоча у разі використання звичайної кулькової ручки текст можливо відновити по деформації паперу, цей недолік можна усунути за допомогою м'якого пишучого вузла, на зразок фломастера.

Симпатичними чорнилами можуть слугувати найрізноманітніші речовини: лимонна кислота, віск, яблучний сік, молоко, сік цибулі, слина, пральний порошок, аспірин, крохмаль з різними хімічними чи фізичними «декодерами»: температура, сода, йод, сіль, залізо, ультрафіолетове світло, для воску навіть крейда чи зубний порошок.

Комп'ютерна стеганографія. Напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Наприклад, це стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних форматів файлів, підміна символів у назвах файлів, текстова стеганографія і так далі. Наведемо деякі приклади:

– Використання зарезервованих полів комп'ютерних форматів файлів. Суть методу полягає в тому, що частина поля розширень, не заповнена інформацією про розширення, за замовчуванням заповнюється нулями. Відповідно ми можемо використовувати цю «нульову» частину для запису своїх даних. Недоліком цього методу є низький ступінь скритності і малий обсяг переданої інформації.

– Метод приховування інформації в невикористовуваних місцях гнучких дисків. Під час використання цього методу інформація записується в невживані частини диска, наприклад, на нульову доріжку. Недоліки: маленька продуктивність, передача невеликих за обсягом повідомлень.

– Метод використання особливих властивостей полів форматів, які не відображаються на екрані. Цей метод ґрунтується на спеціальних «невидимих» полях для отримання виносок, покажчиків. Наприклад, написання чорним шрифтом на чорному тлі. Недоліки: маленька продуктивність, невеликий обсяг переданої інформації.

– Використання особливостей файлових систем — при зберіганні на жорсткому диску файл завжди (не враховуючи деяких ФС, наприклад, ReiserFS) займає кластерів (мінімальних адресуються обсягів інформації). Наприклад, у раніше широко використовуваної файлової системи FAT32 (використовувалася в Windows98/Me/2000) стандартний розмір кластера — 4 Кб. Відповідно для зберігання 1 Кб інформації на диску виділяється 4 Кб інформації, з яких 1Кб потрібен для зберігання файлу, а інші 3 Кб ні на що не використовуються — відповідно їх можна використовувати для зберігання інформації. Недолік цього методу:

легкість виявлення.

Цифрова стеганографія. Розвиток засобів цифрової обчислювальної техніки дав поштовх для розвитку комп'ютерної стеганографії, яка ґрунтується на вбудовуванні секретного повідомлення в цифрові дані, що, як правило, мають аналогову природу (аудіозаписи, зображення, відео). Можливе також вбудовування інформації в текстові та скомпресовані файли.

Цифрова стеганографія — напрямок класичної стеганографії, заснований на захованні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Але, як правило, ці об'єкти є мультимедійними об'єктами (зображення, відео, аудіо, текстури 3D-об'єктів), і внесення спотворень, які знаходяться нижче межі чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів.

Крім того, в оцифрованих об'єктах, тобто таких, що спочатку мають аналогову природу, завжди наявний шум квантування; також при відтворенні цих об'єктів з'являється додатковий аналоговий шум і нелінійні спотворення апаратури – все це сприяє більшій непомітності прихованої інформації.

Мережева стеганографія. Останнім часом популярні методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Такі методи одержали назву «мережева стеганографія». Цей термін вперше ввів Кжиштоф Шиперський (Krzysztof Szczypiorski) у 2003 р. Типові методи мережевої стеганографії включають зміну властивостей одного з мережевих протоколів. Крім того, може використовуватися взаємозв'язок між двома або більше різними протоколами для більш надійного приховування передачі секретного повідомлення. Мережева стеганографія охоплює широкий спектр методів, зокрема:

– WLAN стеганографія ґрунтується на методах, які використовуються для передачі стеганограм у бездротових локальних мережах (Wireless Local Area Networks). Практичний приклад WLAN стеганографії — система HICCUPS (Hidden Communication System for Corrupted Networks).

– LACK стеганографія — приховування повідомлень під час розмов з використанням IP-телефонії. Наприклад: використання пакетів, що затримуються, або навмисно пошкоджуються та ігноруються приймачем (цей метод називають LACK — Lost Audio Packets Steganography), або приховування інформації в полях заголовка, які не використовуються.

– VoIP (англ. voice over IP) — технологія передачі медіа даних в реальному часі за допомогою сімейства протоколів TCP/IP. IP-

телефонія — система зв'язку, при якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується в цифровий вигляд), компресується і пересилається по цифрових каналах зв'язку до іншого абонента, де проводиться зворотна операція — декомпресія, декодування і відтворення. Розмова відбувається у формі аудіопотоків за допомогою протоколів RTP (Real-Time Transport Protocol).

– LACK — це метод стеганографії для IP-телефонії, який модифікує пакети з голосовим потоком. Він використовує те, що в типових мультимедійних комунікаційних протоколах, таких як RTP, надмірно затримані пакети вважаються приймачем марними і відкидаються.

Принцип функціонування LACK полягає у такому: передавач (Аліса) вибирає один з пакетів з голосового потоку і його корисне навантаження замінює бітами таємного повідомлення — стеганограмою, яка вбудовується в пакет. Потім обраний пакет навмисно затримується. Кожного разу, коли надмірно затриманий пакет досягає отримувача, незнайомого з стеганографічною процедурою, він відкидається. Однак якщо отримувач (Боб) знає про прихований зв'язок, то замість видалення отриманих RTP пакетів, він вилучає приховану інформацію.

Алгоритми. Існуючі алгоритми вбудовування таємної інформації можна поділити на декілька підгруп:

– працюючі з самим цифровим сигналом. Наприклад, метод LSB (Least Significant Bit);

– «впаювання» прихованої інформації. У цьому разі відбувається накладення приховуваного зображення (звуку, іноді тексту) поверх оригіналу. Часто використовується для вбудовування ЦВЗ (цифровий водяний знак);

– використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші не використовувані зарезервовані поля файлу.

За способом вбудовування інформації стегоалгоритми можна поділити на лінійні (адитивні: А17, А18, Ь18Б, А21, А25), нелінійні та інші.

LSB (Least Significant Bit, найменший значущий біт) — суть цього методу полягає в заміні останніх значущих бітів у контейнері (зображення, аудіо або відеозапису) на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини.

Принцип цього методу полягає в такому: припустимо, є 8-бітне зображення в градаціях сірого. 00h (00000000b) позначає чорний колір, FFh (11111111b) — білий. Усього є 256 градацій. Також припустимо, що повідомлення складається з 1 байта — наприклад, 01101011b. Під час використання 2 бітів в описах пікселів нам буде потрібно 4 пікселі. Припустимо,

вони чорного кольору. Тоді пікселі, що містять приховане повідомлення, виглядатимуть так: 00000001 00000010 00000010 00000011. Тоді колір пікселів зміниться: першого — на 1/255, другого і третього — на 2/255 і четвертого — на 3/255. Такі градації не тільки непомітні для людини, а й можуть взагалі не відобразитися при використанні низькоякісних пристроїв виведення. У ролі базового контейнера пропонується використовувати файли BMP-зображень високої роздільності з глибиною кольору 24 та 32 біти, таємне зображення може мати розширення .BMP, .GIF, .PNG, .JPEG.

Недоліком методу LSB є чутливість до розміру зображення, тобто чим менший розмір зображення, тим більше будуть відрізнятися два сусідні пікселі, тому пропонується використовувати зображення з великою роздільністю. Також метод «видає себе» при побітовому перегляді зображення, де чітко видно області зображення, в які «вбудовано» таємну інформацію. Попри це, метод запису Least Sagnificant Bit є досить популярним, стійким та простим під час реалізації.

Підвиди LSB-алгоритмів для растрових зображень без палітри. BlindHide (приховування наосліп). Найпростіший алгоритм: дані записують, починаючи з верхнього лівого кута зображення до правого нижнього — піксель за пікселем. Приховані дані програма записує у бітах кольорів пікселя. Приховані дані розподіляються у контейнері нерівномірно. Якщо приховані дані не заповнять повністю контейнер, то лише верхня частина зображення буде засміченою.

HideSeek (заховати-знайти). Цей алгоритм у псевдовипадковий спосіб розподіляє приховане повідомлення у контейнері. Для генерації випадкової послідовності використовує пароль. Дещо «розумніший» алгоритм, але все ж не враховує особливостей зображення-контейнера.

FilterFirst (попередня фільтрація). Виконує фільтрацію зображення-контейнера — пошук пікселів, у які записуватиметься прихована інформація (для яких зміна розрядів буде найменш помітною для ока людини).

BattleSteg (стеганографія морської битви). Найскладніший і найдосконаліший алгоритм. Спочатку виконує фільтрацію зображення-контейнера, після чого прихована інформація записується у «найкращі місця» контейнера у псевдовипадковий спосіб (подібно, як у HideSeek).

Інші методи приховування інформації в графічних файлах орієнтовані на формати файлів з втратою, наприклад, JPEG. На відміну від LSB вони більш стійкі до геометричних перетворень. Це виходить за рахунок варіювання в широкому діапазоні якості зображення, що призводить до неможливості визначення джерела зображення.

Цифрові водяні знаки (ЦВЗ). Найчастіше стеганографія використо-

вується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканність документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Цифровий водяний знак (ЦВЗ) — технологія, створена для захисту авторських прав мультимедійних файлів та інтелектуальної власності контейнера (Intellectual Property). Зазвичай цифрові водяні знаки невидимі. Однак ЦВЗ можуть бути видимими на зображенні або відео. Зазвичай ця інформація являє собою текст або логотип, який ідентифікує автора.

Стеганографія застосовує ЦВЗ, коли сторони обмінюються секретними повідомленнями, впровадженими в цифровий сигнал. Використовується як засіб захисту документів з фотографіями — паспортів, водійських посвідчень, кредитних карток з фотографіями.

ЦВЗ можна також використовувати для виявлення потенційних піратів: під час продажу в зображення вбудовують інформацію про час продажу та інформацію про покупця. Ключовою відмінністю ЦВЗ від звичайного приховання інформації є наявність активного противника. Наприклад, використовуючи ЦВЗ для захисту авторського права, активний противник намагатиметься видалити чи змінити вбудовані ЦВЗ. Тому основною вимогою є стійкість вбудованих даних до атак. Таємність не є настільки важливою, як у прихованій комунікації.

Контрольні запитання

1. Дайте такі визначення:
а) поняття криптологія;
б) поняття криптоаналіз.
2. Які є основні види атак та методи криптоаналізу?
3. Що таке стеганографія?
4. Що таке цифровий водяний знак (ЦВЗ)?
5. Приватний ключ використовується для?
6. Що не належить до основних елементів стеганосистеми?
7. Дайте визначення стеганодекодеру.
8. Дайте визначення прекодеру.
9. Дайте визначення верифікації в криптографії.
10. Дайте визначення криптосистемі PGP.

Тема 6. БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Інформаційно-комунікаційні технології, що з'явилися у другій половині XX ст., суттєво змінили життя людства. Саме вони створили передумови формування інформаційного суспільства, в якому визначальну роль відіграють інформація та нові знання. Саме в такому суспільстві ми з вами сьогодні живемо.

Перші ЕОМ були призначені лише для швидкої обробки числових даних. Згодом обчислювальна техніка стала широко використовуватися в наукових дослідженнях, виробництві, освіті, побуті тощо. У користувачів віддалених один від одного комп'ютерів виникла потреба у швидкому обміні даними. Для цього було запропоновано об'єднати комп'ютери в єдину систему і в такий спосіб передавати дані від одного комп'ютера до іншого. Так були створені комп'ютерні мережі.

Комп'ютерна мережа — це сукупність комп'ютерів та інших пристроїв, зв'язаних каналами передавання даних.

Комп'ютерні мережі забезпечують спільний доступ до даних. У мережі виділяють комп'ютери, на яких розміщують великі масиви даних, а користувачі інших комп'ютерів мережі одержують доступ до них. Це дає можливість, наприклад, людям, які працюють над одним проєктом, використовувати дані, створені іншими, тобто працювати над проєктом одночасно.

За допомогою комп'ютерної мережі є можливим спільне користування периферійними пристроями: принтерами, сканерами, модемами тощо. Невигідно мати їх біля кожного персонального комп'ютера, наприклад, у комп'ютерному класі або в банку.

Комп'ютерні мережі також дозволяють у короткі терміни розв'язувати складні інженерні задачі. У 2006 р. у Києві відкрито Центр суперкомп'ютерних обчислень. Найпотужніший суперкомп'ютер в Україні дозволяє вітчизняним ученим здійснювати обробку великих масивів даних, що зберігаються в різних організаціях, швидше виконувати складні обчислення. Створення комп'ютерних мереж відкрило нові можливості для електронного зв'язку. Сьогодні люди, що мають комп'ютери, можуть спілкуватися між собою, незважаючи на віддаль і час. З появою комп'ютерних мереж комп'ютер став своєрідним вікном у величезний світ інформації.

Основне призначення всіх комп'ютерних мереж — це спільний доступ до мережевих ресурсів (апаратного забезпечення комп'ютерів, пе-

риферійних пристроїв), спільне використання даних та швидкий обмін ними, спільне використання програмного забезпечення.

6.1. Короткі відомості про комп'ютерні мережі

*Мережева взаємодія***.** Мережева взаємодія передбачає віддалений доступ до мережевих ресурсів та відбувається за технологією. Залежно від повноважень комп'ютери в мережі розподіляються на сервери та клієнтів. Клієнт — це комп'ютер користувача, який здійснює запит, сервер – комп'ютер, що обробляє цей запит і відповідає на нього. Звертаємо вашу увагу: сервером та клієнтом називаються як комп'ютери в мережі, так і програмне забезпечення, що працює на цих комп'ютерах.

Централізовані мережі. У централізованих мережах виділяється один потужний комп'ютер — виділений сервер, що виконує основні функції з організації роботи мережі. Такі мережі ще називають «клієнт-виділений сервер». Усі клієнти отримують доступ до ресурсів мережі через сервер.

На сервері встановлюється спеціальна операційна система (наприклад, 52 г). Операційна система дозволяє організувати і контролювати роботу комп'ютерів і користувачів у мережі, надавати кожному користувачеві певні права доступу до ресурсів і даних цієї мережі. Для цього кожен користувач отримує ім'я користувача (логін) та пароль для входу до мережі. Прикладами такої мережі можуть бути комп'ютерні мережі банків, корпорацій, вищих навчальних закладів, деяких шкіл м. Києва та інші. Перевагами централізованих комп'ютерних мереж є висока швидкість обміну даними і можливість розподіляти права доступу користувачів у них. Але суттєвим недоліком є те, у разі виходу з ладу сервера вся мережа перестає працювати.

Децентралізовані мережі. У децентралізованих мережах немає виділеного сервера: будь-який комп'ютер може бути як сервером, так і клієнтом. Такі мережі ще називають щоранговими. Як клієнт, комп'ютер в одноранговій мережі може здійснювати запит щодо доступу до ресурсів інших комп'ютерів мережі. Як сервер, комп'ютер повинен обробляти запити від інших комп'ютерів мережі та надавати потрібні дані.

В одноранговій мережі всі комп'ютери мають однакові права (ранги) щодо доступу до ресурсів кожного й до периферійних пристроїв. Кожен користувач мережі може на своєму жорсткому диску визначити папки і файли, які він надає для загального користування.

У таких мережах на всі комп'ютери встановлюється операційна система, яка забезпечує їм рівні можливості.

Перевагою однорангових мереж є працездатність мережі у разі виходу з ладу будь-якого з комп'ютерів, а недоліком — неможливість розподіляти права клієнтів щодо роботи в мережі. Прикладом такої мережі може бути мережа комп'ютерного класу у більшості шкіл.

Типи комп'ютерних мереж. Об'єднані в мережу комп'ютери можуть бути розташовані в одній кімнаті, одному будинку, районі, місті, країні чи навіть у різних країнах. У багатьох школах України комп'ютери, встановлені в комп'ютерному класі, у кабінетах адміністрації, бібліотеці, кінолекційній залі та інших кабінетах, об'єднані в мережу.

У такій мережі є сервер, на якому можуть зберігатися:

- дані про всіх учнів та вчителів школи; розклад уроків, гуртків, факультативів;
- електронні журнали успішності учнів;
- практичні завдання до уроків; мультимедійні уроки; архіви учнівських робіт.

Працюючи в мережі, учні й учителі мають доступ до цих даних для підготовки до уроків, написання рефератів, створення презентацій, колективної роботи над проєктами тощо.

Прикладом мережі, що розташована в кількох спорудах, може бути мережа торговельного підприємства (центральний офіс, магазин, склад). У ній централізовано можна зберігати відомості про товари та їхню вартість, обробляти дані щодо продаж, які надходять з комп'ютерів, встановлених у різних відділах підприємства, вести облік товарів. Спеціальні мережеві програми дозволяють автоматизовано планувати роботу підприємства. Директор може перевірити, які товари ще є на складі або в торговому залі, а які відсутні, чи виконані доручення, які він розіслав мережею тощо.

І шкільна мережа, й мережа торговельного підприємства об'єднують комп'ютери, що розміщені на невеликих відстанях у межах одного приміщення або сусідніх приміщень. Такі мережі називаються локальними.

Локальна мережа — комп'ютерна мережа, що об'єднує комп'ютери, які знаходяться в одному приміщенні або кількох приміщеннях, розташованих на невеликій відстані одне від одного.

Але локальні мережі не дозволяють забезпечити спільний доступ до даних тим користувачам, що знаходяться, наприклад, у різних частинах міста. На допомогу приходять регіональні мережі, що об'єднують

комп'ютери в межах одного регіону (району, міста, країни). Прикладами такої мережі є комп'ютерна мережа, що об'єднує комп'ютери, які знаходяться в будинках одного або кількох кварталів, комп'ютери директорів шкіл району, комп'ютерна мережа «Воля» в Києві та інші. Ще одним прикладом регіональної комп'ютерної мережі є Українська науково-освітня телекомунікаційна мережа «УРАН».

Мережа «УРАН» забезпечує школи, університети та інші заклади освіти, науки й культури України інформаційними послугами, такими як:

- оперативний доступ та обмін даними;
- накопичення даних для виконання наукових досліджень;
- дистанційне навчання;
- функціонування електронних бібліотек та віртуальних лабораторій;
- проведення телеконференцій.

Сьогодні мережа «УРАН» об'єднує понад 60 науково-дослідницьких та освітніх закладів України.

Регіональна мережа – комп'ютерна мережа, що об'єднує комп'ютери, розміщені в межах одного регіону.

Глобальна комп'ютерна мережа — це комп'ютерна мережа, що об'єднує комп'ютери і мережі, розташовані в усіх частинах земної кулі. У наш час найбільш відома глобальна комп'ютерна мережа – Інтернет, але існують й інші глобальні мережі.

Історія створення комп'ютерних мереж. Уперше здійснити віддалений зв'язок між комп'ютерами вдалося у 60-х роках XX ст. Саме в цей час почали створювати і запроваджувати найпростіші локальні комп'ютерні мережі. А в 1969 р. у США була створена комп'ютерна мережа ARPANET, розроблена на замовлення Міністерства оборони США. Вона проєктувалася як стійка до пошкоджень мережа для швидкої передачі оперативних даних. Наприклад, у разі ядерного нападу мережа ARPANET здатна продовжувати нормальну роботу під час виходу з ладу будь-якої її частини: потоки даних почнуть обходити пошкоджену ділянку. Об'єднавши комп'ютери кількох великих університетів і дослідних компаній країни, ARPANET мала й наукове призначення.

Невдовзі успішні творці ARPANET приступили до розробки програми Internetting Project (Проєкт об'єднання мереж). Були випробувані різні варіанти взаємодії мережі ARPANET з іншими мережами США. Успіх цього проєкту сприяв створенню у США у 80-х роках XX ст. досить потужної мережі «Інтернет». Це створило передумови для успішної інтеграції багатьох мереж США та інших країн світу в єдину світову

мережу. Таку «мережу мереж» тепер скрізь називають Інтернет.

Спочатку ця мережа використовувалася переважно в наукових проєктах. Однак з часом Інтернет став невід'ємною частиною життя багатьох людей. Сьогодні до Інтернету підключені мережі, що охоплюють усі континенти, навіть Антарктиду, і з'єднують кожний куточок на планеті. Кількість користувачів Всесвітньої мережі різко збільшується і вже досягла близько 1,5 млрд. Понад 1000 нових комп'ютерів підключаються до Інтернету щодня, більше ніж ніж 20 млн електронних повідомлень подорожує Інтернетом щотижня.

6.2. Використання міжмережевих екранів

Міжмережевий екран, Мережевий екран, Фаєрво́л, Файрво́л (англ. *Firewall*, буквально «вогняна стіна») — пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік згідно з набором правил та інших критеріїв.

Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер) або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку (функція редиректу).

Залежно від активних з'єднань, що відслідковуються, фаєрволи поділяють на:

- stateless (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;
- stateful (фільтрація з урахуванням контексту) – з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Функції екранів:

- *Фільтрація пакетів.* Це одна з трьох загальновідомих функцій мережевого екрана. У цьому разі виконуються зовсім прості функції (фактично як у спеціалізованого маршрутизатора), які полягають у перегляді заголовка кожного пакета та перевірки IP адреси та порта на правильність.

- *Проксі сервер.* Це друга загальновідома функція. Різниця між проксі сервером та фільтрацією пакетів полягає в тому, що проксі сервер вимагає, щоб всі сеанси зв'язку встановлювались через нього, а не напряму.
- *Проксі сервер програм*. Це третя функція. Цей різновид проксі сервера відрізняється «розумінням» протоколів програм, що здійснюють передачу даних. Хороший приклад такого сервера – поштовий сервер.
- *Кешування даних.* Це не є традиційною функцією мережевих екранів, але на цей час є надзвичайно популярною властивістю. Ідея полягає у тому, що, оскільки всі дані проходять через мережевий екран, він може зберігати найбільш популярну інформацію і при наступному звертанні за нею видати її зі свого кешу.
- *Статистика та повідомлення*. Важливою властивістю мережевого екрану є ведення історії всіх мережевих з'єднань, а також вивід повідомлень про атаки на мережу чи комп'ютер. Історія з'єднань допомагає правильно настроїти мережевий екран, щоб комп'ютер був одночасно захищений від нападів і відкритий для доступу авторизованим користувачам.
- *Управління*. Для персональних мережевих екранів основна характеристика – зручність їхнього налаштування. Управління міжмережевими екранами здебільшого відбувається дистанційно (використовуючи HTML інтерфейс чи інший), що потребує впевненості в надійності авторизації та каналу зв'язку.

Принципи роботи брандмауера. Різновиди брандмауерів. Брандмауер, або міжмережевий екран – це «напівпроникна мембрана», яка розташовується між внутрішнім сегментом мережі і зовнішньою мережею або іншими сегментами мережі «Інтернет», і контролює всі інформаційні потоки у внутрішній сегмент та з нього. Контроль трафіку полягає в його фільтрації, тобто у вибірковому пропущенні через екран, а іноді і з виконанням спеціальних перетворень і формуванням сповіщень для відправника, якщо його даним у пропуску відмовлено. Фільтрація здійснюється на підставі набору умов, попередньо завантажених в брандмауер, і відображає концепцію інформаційної безпеки корпорації. Брандмауери можуть бути виконані у вигляді як апаратного, так і програмного комплексу, записаного в комутуючий пристрій або сервер доступу (сервер-шлюз, просто сервер, хост-комп'ютер і т.д.), вбудованого в операційну систему.

Робота брандмауера полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і залеж-

но від результатів аналізу пропускає пакети інформації у внутрішню мережу (сегмент мережі) або їх відфільтровує.

Ефективність роботи міжмережевого екрана, що працює під управлінням Windows, зумовлена тим, що він повністю заміщає реалізований стек протоколів TCP\IP, і тому порушувати його роботу з допомогою спотворення протоколів зовнішньої мережі (що часто роблять хакери) неможливо.

Міжмережеві екрани зазвичай виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі (внутрішньої підмережі) від зовнішніх каналів зв'язку;
- багатоетапну ідентифікацію запитів, що надходять в мережу (ідентифікація серверів, вузлів зв'язку про інших компонентів зовнішньої мережі);
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі (у внутрішній підмережі може використовуватися локальна система адресації серверів);
- приховування IP адрес внутрішніх серверів з метою захисту від хакерів.

Брандмауери можуть працювати на різних рівнях протоколів моделі OSI.

На мережевому рівні виконується фільтрація вступників пакетів, заснована на IP адресі. На транспортному рівні фільтрація припустима ще й за номерами портів TCP і прапорів. На прикладному рівні може виконуватися аналіз прикладних протоколів (FTP, HTTP, SMTP і т.д.) і контроль за змістом потоків даних.

Можна в брандмауері створювати ту експертну систему, яка, аналізуючи трафік, діагностує події, що можуть становити загрозу безпеки внутрішньої мережі, та інформує про це адміністратора. Експертна система здатна також у разі небезпеки (спам, наприклад) автоматично посилювати умови фільтрації і так далі.

6.3. Політика безпеки під час роботи в мережі

Під час роботи в мережевому середовищі необхідно бути упевненим у тому, що секретні дані такими і залишаться, оскільки лише користувачі, що мають відповідні повноваження, зможуть одержати до них доступ. Однак важливо забезпечити захист не тільки конфіденційної інформації, але і функціонування мережі в цілому. Кожна мережа має потребу в захисті від навмисного чи випадкового ушкодження. Однак у користувачів не повинно бути труднощів під час виконання роботи.

Найбільшу *загрозу для безпеки* мережі мають:
- несанкціонований доступ;
- електронне підслуховування;
- навмисне чи ненавмисне ушкодження.

Несанкціонований доступ – це навмисне звертання користувача до даних, доступ до яких йому не дозволений, з метою їхнього читання, відновлення чи руйнування.

Рівень захисту мережі залежить від її призначення. Наприклад, мережа, що зберігає дані великого банку, вимагає більш могутнього захисту, ніж локальна мережа, що з'єднує комп'ютери невеликої громадської організації.

Політика безпеки. Для захисту мережі необхідно проводити певну політику, тобто дотримуватися набору правил і розпоряджень. Вироблення політики безпеки (*security policy*) – перший крок, який повинна зробити будь-яка організація, забезпечуючи захист своїх даних. Політика встановлює «генеральну лінію», спираючись на яку і адміністратор, і користувачі будуть вносити зміни, знаходити вихід з позаштатних ситуацій при розширенні мережі.

Адміністратор повинен навчити користувачів мережі всім особливостям роботи і методам безпеки. Для цього він може скласти посібник, а в разі потреби – організувати навчання, особливо нових користувачів.

Керування доступом у Windows. Права користувача призначаються шляхом додавання його в одну з вбудованих груп, що містять набір уже призначених прав користувача. Однак у разі потреби можна створити нову групу і призначити їй певні права. Призначення прав групам здійснюється за допомогою групової політики. Користувачам, доданим у

групу, автоматично надаються усі права, призначені групі. У Windows існують такі *групи*:

– *Адміністратори* – мають усі права та можливості в системі.

– *Оператори архіву* – можуть архівувати та відновлювати файли на комп'ютері незалежно від усіх дозволів, установлених для цих файлів.

– *Досвідчені користувачі* – можуть створювати локальні групи та облікові записи користувачів, а також видаляти користувачів з локальних груп, створених ними, змінювати та видаляти створені ними облікові записи.

Вони можуть керувати додаванням та видаленням користувачів з груп *Досвідчені користувачі*, *Користувачі*, *Гості*. Вони не мають прав на архівування та поновлення каталогів, завантаження та вивантаження драйверів, керування журналами безпеки та аудиту.

– *Користувачі* – можуть виконувати найбільш поширені завдання: запуск програм, друк документів, копіювання файлів і так далі. Користувачі мають право створювати локальні групи та змінювати групи, створені ними. Вони не можуть організовувати загальний доступ до ресурсів комп'ютера.

– *Гості* – призначена для запуску комп'ютера разовими користувачами. Члену цієї групи надаються обмежені можливості.

– *Реплікатор* – створена для підтримки функції реплікації (створення копії) каталогу.

Обліковий запис – запис користувача, що містить усі відомості, що визначають користувача в операційній системі Windows. Це ім'я користувача і пароль, необхідні для входу користувача в систему, імена груп, членом яких користувач є, а також права і дозвіл, що він має під час роботи в системі і доступі до її ресурсів.

У Windows є *два вбудовані облікові записи* користувачів – *Адміністратор* і *Гість*, що створюються автоматично під час встановлення системи. Користувач з ім'ям Адміністратор є членом групи адміністраторів і може виконувати всі необхідні дії в мережі. Обліковий запис Гість призначений для тих, хто не має реального облікового запису. Цей обліковий запис не вимагає пароля. Він входить у вбудовану групу Гостей і має всі права, що привласнені цій групі.

З користувачем пов'язаний профіль користувача. *Профіль користувача* – набір параметрів середовища Windows, що завантажується під час входу користувача в систему. Він містить усі параметри настроювання середовища Windows, доступні для користувача, у тому числі групи програм, колір екрана, мережеві підключення дисків і принтерів,

властивості миші, розміри і положення вікон.

Немаловажне значення *має контроль подій*, що відбуваються в мережі, оскільки в цих умовах зловмисник не настільки помітний і має досить часу і ресурсів для виконання своїх завдань. Цей процес відслідковує дії користувачів у мережі. Він є частиною захисту мережі, оскільки в *журналі безпеки* відбиті імена всіх користувачів, що працювали з конкретними ресурсами або намагалися одержати до них доступ.

Контрольні запитання

1. Дайте визначення WWW?
2. Комплекс апаратних та програмних засобів, які дозволяють комп'ютерам обмінюватися даними, – це?
3. Що називають Web-вузлом?
4. Що таке URL?
5. За допомогою яких пристроїв можна підключитися до мережі «Інтернет»?
6. Комп'ютер, який надає послуги іншим комп'ютерам у мережі (клієнтам), називається?
7. Які бувають типи фаєрволів?

Тема 7. ЗАХИСТ ІНФОРМАЦІЇ В ГЛОБАЛЬНИХ МЕРЕЖАХ

Для класифікації комп'ютерних мереж використовують різні ознаки, але частіше за все мережі ділять на типи за територіальною ознакою, тобто за розміром території, яку покриває мережа. І для цього є вагомі причини, оскільки відмінності технологій локальних і глобальних мереж дуже суттєві, незважаючи на їх постійне зближення.

7.1. Короткі відомості про глобальні комп'ютерні мережі

До *локальних мереж Local Area Networks (LAN)* належать мережі комп'ютерів, зосереджені на невеликій території (звичайно в радіусі не більше ніж 1–2 км). У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації. Через короткі відстані в локальних мережах є можливість використання відносно дорогих високоякісних ліній зв'язку, які дозволяють, застосовуючи прості методи передачі даних, досягати високих швидкостей обміну даними приблизно 100 Мбіт/с. Через це послуги, що надаються локальними мережами, відрізняються широкою різноманітністю і звичайно передбачають реалізацію в режимі on-line.

Глобальні мережі Wide Area Networks (WAN) об'єднують комп'ютери, що територіально розосередилися: можуть знаходитися в різних містах і країнах. Оскільки прокладка високоякісних ліній зв'язку на великі відстані коштує дуже дорого, в глобальних мережах часто використовуються вже існуючі лінії зв'язку, спочатку призначені зовсім для інших цілей. Наприклад, багато глобальних мереж будуються на основі телефонних і телеграфних каналів загального призначення. Через низькі швидкості таких ліній зв'язку в глобальних мережах (десятки кілобіт в секунду) набір послуг, що надаються, звичайно обмежується передачею файлів переважно не в оперативному, а в фоновому режимі з використанням електронної пошти. Для стійкої передачі дискретних даних по неякісних лініях зв'язку застосовуються методи і обладнання, істотно відмінні від методів і обладнання, характерних для локальних мереж. Як правило, тут застосовуються складні процедури контролю і відновлення даних, оскільки найбільш типовий режим передачі даних по територіальному каналу зв'язку пов'язаний зі значними спотворен-

нями сигналів.

Міські мережі (або мережі мегаполісів) Metropolitan Area Networks (MAN) є менш поширеним типом мереж. Ці мережі з'явилися порівняно недавно. Вони призначені для обслуговування території мегаполіса. У той час як локальні мережі найкраще підходять для розділення ресурсів на коротких відстанях і широкомовних передач, а глобальні мережі забезпечують роботу на великих відстанях, але з обмеженою швидкістю і небагатим набором послуг, мережі мегаполісів займають деяке проміжне положення. Вони використовують цифрові магістральні лінії зв'язку, часто оптичноволоконні, з швидкостями від 45 Мбіт/с і призначені для зв'язку локальних мереж в масштабах міста і з'єднання локальних мереж з глобальними. Ці мережі спочатку були розроблені для передачі даних, але зараз вони підтримують і такі послуги, як відеоконференції й інтегральну передачу голосу і тексту. Розвиток технології мереж мегаполісів здійснювався місцевими телефонними компаніями. Історично склалося так, що місцеві телефонні компанії завжди мали слабкі технічні можливості і через це не могли залучити великих клієнтів. Щоб подолати свою відсталість і зайняти гідне місце у світі локальних і глобальних мереж, місцеві підприємства зв'язку зайнялися розробкою мереж на основі найсучасніших технологій, наприклад технології комутації осередків SMDS або ATM. Мережі мегаполісів є суспільними мережами, і тому їх послуги коштують дешевше, ніж побудова власної (приватної) мережі в межах міста.

7.2. Характер проведення атак у глобальних мережах

Кіберзлочини поділяють на види залежно від об'єкта, від предмета посягання, залежно від способів скоєння і тому подібне.

За об'єктом посягання виділяють такі групи кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і комп'ютерних мереж, економічні комп'ютерні злочини, комп'ютерні злочини проти особистих прав і недоторканності приватної сфери, комп'ютерні злочини проти суспільних і державних інтересів. Проте варто зазначити, що багато кіберзлочинів зазіхають відразу на декілька об'єктів: наприклад, незаконне перехоплення приватних електронних комунікацій зазіхає на недоторканність приватної сфери і на конфіденційність комп'ютерних даних, комп'ютерне шахрайство – на власність і на цілісність комп'ютерних даних тощо.

Найбільш поширена класифікація кіберзлочинів в цей час ґрунту-

ється на структурі Конвенції Ради Європи про кіберзлочинність. Спочатку кіберзлочини поділяли на чотири групи (потім був прийнятий додатковий протокол, і тепер груп – п'ять). На сьогодні ця класифікація є «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика.

У першу групу виділено злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

У другу групу входять злочини, пов'язані з використанням комп'ютера, як засобу скоєння злочинів, а саме як засобу маніпуляцій з інформацією. У цю групу входять комп'ютерне шахрайство та комп'ютерне підроблення.

Третя група – злочини, пов'язані з контентом, тобто з вмістом даних, розміщених в комп'ютерних мережах. Найбільш поширений і найбільш караний практично у всіх державах вид цих кіберзлочинів – злочини, пов'язані з дитячою порнографією.

У четверту групу увійшли злочини, пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень затверджено документом і належить до компетенції національних законодавств держав.

П'ята група злочинів зафіксована в окремому протоколі – це акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Реагування на інциденти в глобальній мережі. Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових питань регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності.

Відсутність механізмів контролю. Основна проблема боротьби зі злочинністю в мережі «Інтернет» полягає в транснаціональності самої мережі та відсутності механізмів контролю, необхідних для правозастосування. Коли мережа «Інтернет» створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які можна було б паралізувати її роботу, навряд чи хтось міг уявити масштаби розвитку проєкту, спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку та її соціальну та економічну роль у майбутньому. Саме відсутність розроблених механі-

змів контролю мережі зсередини укупі з її доступністю і легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі і відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для вчинення злочинів.

В останні роки інформаційні мережі розвиваються занадто швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми. Хмарна обробка даних, автоматизація атак, вразливість персональної інформації в соціальних мережах: поширення так званої «інформаційної зброї», прикладом якого є вірус Stuxnet, розроблений, на думку фахівців, для атак на ядерну промисловість Ірану, але при цьому заподіяв чималої шкоди інфраструктурі багатьох інших країн – на всі ці проблеми правове регулювання поки не може знайти адекватної відповіді.

Кількість користувачів. Як вже було зазначено вище, із збільшенням кількості користувачів зростають такі фактори ризику: залежність суспільства від інформаційних технологій, що, у свою чергу, зумовлює його вразливість до різних інформаційних зазіхань; збільшується можливість використання мережі для вчинення злочинів, а також зростає потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. Водночас вчинення злочину не вимагає великих зусиль і витрат – достатньо мати комп'ютер, програмне забезпечення та підключення до інформаційної мережі. Не потрібно навіть глибоких технічних знань: існують спеціальні форуми, на яких можна придбати програмне забезпечення для вчинення злочинів, вкрадені номери кредитних карток й ідентифікаційні дані користувачів, а також скористатися послугами з допомоги в здійсненні електронних розкрадань і атак на комп'ютерні системи як в цілому, так і на окремих стадіях вчинення злочинів.

Автоматизація та швидкість використання. Комп'ютерні дані можуть бути передані з однієї точки світу в іншу за кілька секунд. До того ж, практично будь-яка передача даних у мережі зазвичай включає декілька країн, оскільки інформація розбивається на частини і йде по найбільш зручних та доступних каналах. Контролювати передачу даних з урахуванням їх обсягу та кількості користувачів дуже важко, якщо не неможливо. Злочинець, потерпілий, сервер з необхідною інформацією можуть перебувати в різних країнах і на різних континентах, що вимагає співпраці правоохоронних органів декількох країн під час розслідування злочину.

Автоматизація збільшує ризик здійснення численних злочинів без особливих фінансових і тимчасових витрат. До того ж, вона дозволяє злочинцям акумулювати більший фінансовий прибуток шляхом розкрадання невеликих сум у тисячі користувачів, що створює проблеми виявлення злочинів (власник банківського рахунку може просто не помітити зникнення фінансових коштів) і порушення кримінальних справ. Наприклад, якщо той же власник банківського рахунку звернеться із заявою про зникнення невеликої суми, правоохоронним органам досить важко оцінити масштаб діяльності тих, хто вчинив розкрадання, оскільки шкода, завдана одному потерпілому, дуже мала, в той час як правопорушники шляхом акумуляції цих невеликих сум можуть отримати неабиякий прибуток.

Анонімність мережі «Інтернет», вразливість бездротового доступу і використання проксі серверів істотно ускладнюють виявлення злочинців: для вчинення злочину може використовуватися «ланцюжок» серверів, злочини можуть бути вчинені шляхом виходу в Інтернет через точки загального доступу, такі як інтернет-кафе, технології дозволяють також «зламати» доступ в чужу бездротову мережу Wi-Fi. Отже, існує достатньо способів ускладнити розслідування злочинів.

Проблема територіальної юрисдикції в кіберпросторі та правового співробітництва. Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп'ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги і принцип суверенітету, одним з проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії, вимагають безліч формальних погоджень, роблять розслідування транснаціональних кіберзлочинів проблематичним. Окрім співробітництва правоохоронних органів, яке вимагає тимчасових витрат і дотримання безлічі формальностей, виникає також питання дотримання фундаментального принципу nullum crimen, nulla poena sine lege, коли необхідна подвійна криміналізація діяння: як у країні, з території якої діяв правопорушник, так і в державі, де знаходиться потерпілий. Різниця у криміналізації діянь, відмінності у визначенні тяжкості вчиненого діяння, особливо у сфері релігійних злочинів і злочинів проти громадського порядку, у сфері нелегального контенту, в екстремістських злочинах значно ускладнюють процес співробітництва правоохоронних органів, іноді унеможливлюють його.

Отже, ефективний контроль негативних явищ у кібепросторі, таких як злочинність, вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами

транснаціональної злочинності. Саме тому, крім гармонізації кримінально-правових норм, потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного співробітництва. Важливу роль у боротьбі з кіберзлочинністю відіграють міжнародні угоди у відповідній сфері, такі як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проєкт HIPCAR), спільний проєкт Європейського Союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проєкт ICB4PAC), проєкт ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проєкт ESCWA) та інші.

Всі зазначені інструменти не є за своєю суттю універсальними міжнародними інструментами.

Віддалені атаки на обчислювальні мережі. Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. *DoS attack, DDoS attack, (Distributed) Denial-of-service attack*) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих). Отож атаковане устаткування не може відповісти користувачам або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється:

– примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, через що устаткування не може продовжувати роботу;

– Зайняттям комунікаційних каналів між користувачами і атакованим устаткуванням, і як наслідок – якість сполучення не відповідає вимогам.

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають *розподіленою.*

Віддалені DoS-атаки поділяють на два види:

1. Віддалена експлуатація помилок в ПЗ з метою довести його до неробочого стану.

2. Flood — посилка на адресу жертви величезної кількості безглуздих (рідше — осмислених) пакетів. Метою флуду може бути канал зв'язку або ресурси машини. У першому випадку потік пакетів займає весь пропускний канал і не дає машині, що атакується, можливості об-

робляти легальні запити. У другому — ресурси машини захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну, ресурсоємку операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скрипту) вебсервера. Сервер витрачає всі ресурси машини на обробку запитів, що атакують, а користувачам доводиться чекати.

7.3. Захист під час використання WWW (World Wide Web)

Розглянемо інформаційні небезпеки, які з'являються під час використання як соціальних мереж, так і мережі «Інтернет» в цілому. Основним джерелом цих небезпек є діяльність хакерів. Одні зловмисники прагнуть одержати персональну інформацію для отримання вигоди, інші – обирають об'єктом атак комп'ютерну систему та намагаються вивести її з ладу або використати для приховування своїх шкідливих дій.

Для зламу акаунта користувача хакеру необхідно докласти зусиль, щоб дізнатися пароль, іншими словами – зламати його. Найбільш поширеними способами реалізації зламу паролю є такі технології.

Брутфорс – метод пошуку та зламу пароля, який дозволяє перебрати всі теоретично можливі варіанти, складені з певного набору символів. До нього також належить атака перебору пароля за словником або ручного підбору часто використовуваних простих паролів.

Для захисту від цього способу зламу у паролі не слід вказувати дату народження, номери телефонів, ім'я, кличку домашньої тварини, прості відомі паролі і будь-які інші дані, потенційно відомі деякому колу осіб. У паролі слід указувати певний набір символів, який практично неможливо вгадати. Критерієм складності пароля є наявність символів з кожного пункту такого переліку:

- символи a…z (лише малі літери);
- символи Aa…Zz (великі та малі літери);
- цифри;
- недруковані ASCII-символи, літери інших алфавітів;
- спеціальні символи :;% "№ *? тощо.

Соціальна інженерія або соціотехніка. Цей метод ґрунтується на довірі користувача. Для цього використовуються сфальсифіковані сайти та фіктивні електронні повідомлення від імені реальних компаній з проханням надати особисту інформацію.

Головним захистом у цьому разі є пильність користувача. Нікому не можна повідомляти або надсилати паролі.

Кейлогери – це програмний продукт або апаратний пристрій, що реєструє кожне натискання кнопки миші або клавіші на клавіатурі комп'ютера та записує у файл разом з датою та часом натискання. Отже, у зловмисника буде пароль у головному вигляді.

Гарантованим захистом від цього методу може слугувати лише вихід в мережу «Інтернет» і введення пароля з власного або надійного, перевіреного комп'ютера.

Програмний метод зламу. Цей метод доступний хакерам і полягає в пошуку помилок у коді сайтів, що дозволяють отримати доступ до бази даних з паролями.

У такому разі дані можуть відновити лише адміністратори.

Фішинг – технологія інтернет-шахрайства з метою отримання ідентифікаційних даних користувачів. Реалізується за допомогою заманювання їх на підставні сайти, які є точною або майже точною копією оригіналу.

Для захисту виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів уже мають таку можливість, яка відповідно іменується «антифішинг». Від користувачів вимагається лише вчасно оновлювати версії браузерів.

Спамом називають небажану електронну пошту, тобто пошту, що надходить без згоди користувача. Він може прикріплюватись до всіх повідомлень у вигляді посилання на сторонній сайт.

У цьому разі необхідно змінити браузер на Mozilla Firefox або Opera, які блокують заданий користувачем спам. А також варто дотримуватися запобіжних заходів, які не дозволять спамерам дізнатися адресу електронної пошти користувача:

– не варто без потреби публікувати адресу електронної пошти на вебсайтах чи в групах соціальних мереж;

– не потрібно реєструватися на підозрілих сайтах, натомість краще вказати спеціально для цього створену адресу;

– ніколи не відповідати на спам і не переходити за посиланням, які містяться в ньому, оскільки це буде підтвердженням використання цієї електронної адреси і збільшить надходження спаму;

– обираючи ім'я електронної пошти, варто створювати його довгим і незручним для вгадування.

Віруси – малі за розміром програми, які поширюються, копіюючи самих себе. Вони потрапляють до комп'ютерної системи і деякий час можуть себе не проявляти, і лише після настання певної дати чи події

активізуються та завдають їй шкоди.

Рекомендується використовувати декілька антивірусних пакетів одночасно, щоденно оновлювати антивірусні бази та встановлювати найновіші версії ліцензійного програмного забезпечення.

Про користь та ризики соціальних мереж можна довго розмірковувати, але в будь-якому разі це явище існує. Тому необхідно допомогти користувачеві зробити мінімум помилок під час роботи у відповідній мережі.

Варто розуміти, що профіль у будь-якій соціальній мережі вразливий, особливо при використанні стандартних параметрів. Тому слід дотримуватись таких рекомендацій:

– подбайте про надійний пароль для профілю;

– будьте обережні у разі встановлення додатків від сторонніх розробників, у жодному разі не встановлюйте додатки з джерел, яким не довіряєте;

– приймайте пропозиції про дружбу тільки від тих людей, яких знаєте особисто і безпосередньо;

– ретельно прочитавши політику конфіденційності, обмежте особисту інформацію, яку збираєтесь зробити загальнодоступною;

– перевіряйте інформацію, яку надсилаєте на сайт;

– завжди використовуйте для кожного форуму, сайту та поштової скриньки різні паролі, інакше шанс втрати всіх акаунтів збільшується при крадіжці одного пароля.

Потенційні проблеми під час використання електронної пошти. Електронна пошта є повсюдною послугою, однак не можна не визнати, що рівень захисту даних в системі електронної пошти впливає на загальний рівень інформаційної безпеки організації, а отже, і на ефективність її діяльності. Це зумовлює важливість створення надійного захисту для цього виду комунікацій.

Більшість проблем, які з’являються у користувачів електронної пошти (спам, віруси, різноманітні атаки на конфіденційність листів і т.д.), пов’язані з недостатнім захистом сучасних поштових систем.

З цими проблемами доводиться мати справу і користувачам загальнодоступних публічних систем, і організаціям. Практика показує, що одномоментне вирішення проблеми захисту електронної пошти неможливо. Рівень захисту електронної пошти, цілком задовільний вчора, сьогодні може виявитися недостатнім. Для того щоб захист електронної пошти був на максимально можливому рівні, а досягнення цього рівня не вимагало надмірних зусиль і витрат, необхідний систематичний, комплексний, з урахуванням усіх загроз підхід до вирішення цієї проблеми.

Боротьба зі спамом та вірусами. Сьогодні є безліч програмних продуктів, у тому і числі і безкоштовних, призначених для боротьби з цією загрозою. Щодо боротьби зі спамом, тут можливі кілька варіантів захисту.

Можна реалізувати систему фільтрів, що дозволяють відсікати вхідну кореспонденцію за адресою, темою чи змістом листа. Фільтри зазвичай розміщуються на клієнтській стороні, і користувач сам може задавати необхідні параметри. Наприклад, системи Spam Buster виробництва компанії Contact Plus, MailWasher, Active Email Monitor (VicMan Software), eMailTrackerPro (Visualware), Spamkiller (Novasoft) та інші. Крім фільтрації спаму, такі програми можуть виконувати функції очищення поштової скриньки, перевірки пошти, читання заголовків листів тощо.

Система фільтрів встановлюється на поштовому сервері; в такому разі листи, що нагадують спам, відсікаються ще до потрапляння в скриньку користувача. Також може бути реалізований захист на основі <Спам-листів>, що містять список інтернет-провайдерів, з адрес яких здійснюється несанкціонована розсилка рекламного характеру. Прикладами можуть бути служба Mail-Filtering Service проєкту Mail Abuse Prevention Project і Realtime Blackhole List, база даних по відкритих поштових серверах (під відкритістю в цьому разі розуміється відсутність адекватного адміністрування, що призводить до неконтрольованих розсилок спаму через такі поштові сервери).

Огляди подібних продуктів регулярно публікуються. Створити систему антивірусного і антиспамового захисту загалом нескладно як для користувача загальнодоступного комунікаційного середовища, так і для IT-підрозділу організації, що розгорнула на своїй обчислювальній інфраструктурі корпоративну поштову систему. Після вибору і установки засобів антивірусного і антиспамового захисту найголовніше – їх акуратне і своєчасне оновлення. Головне пам’ятати, що вірусописьменники не зупиняються на досягнутому, а спамери з кожним днем стають все активніше.

7.4. Захист електронних листів та поштових систем

Захист від фальшивих адрес. Від цього можна захиститися за допомогою використання шифрування для приєднання до листів електронних підписів. Одним популярним методом є використання шифрування з відкритими ключами. Односпрямована хеш-функція листи шифрує, використовуючи секретний ключ відправника. Одержувач використовує відкритий ключ відправника для розшифровки хеш-функції і порівнює

його з хеш-функцією, розрахованою за отриманим повідомленням. Це гарантує, що повідомлення насправді написано відправником, і не було змінено в дорозі. Уряд США вимагає використання алгоритму Secure Hash Algorithm (SHA) і Digital Signature Standard там, де це можливо. А найпопулярніші комерційні програми використовують алгоритми RC2, RC4, або RC5 фірми RSA.

Захист від перехоплення. Від нього можна захиститися за допомогою шифрування вмісту повідомлення або каналу, по якому він передається. Якщо канал зв'язку зашифрований, то системні адміністратори на обох його кінцях таки можуть читати або змінювати повідомлення. Було запропоновано багато різних схем шифрування електронної пошти, але жодна з них не стала масовою. Одним з найпопулярніших додатків є PGP. У минулому використання PGP було проблематичним, оскільки в ньому використовувалося шифрування, яке підпадало під заборону на експорт із США. Комерційна версія PGP включає в себе плагіни для декількох популярних поштових програм, що робить її особливо зручною для включення до листа електронного підпису та шифрування листа клієнтом. Останні версії PGP використовують ліцензовану версію алгоритму шифрування з відкритими ключами RSA.

Коректне використання електронної пошти. Всі службовці повинні використовувати електронну пошту так само, як і будь-яке інший офіційний засіб організації. З цього випливає, що коли лист надсилається, то як відправник, так і одержувач повинен гарантувати, що взаємодія між ними здійснюється згідно з прийнятими правилами взаємодії. Взаємодія за допомогою пошти не повинна бути неетичною, не повинна сприйматися як конфліктна ситуація або містити конфіденційну інформацію.

Захист листів, поштових серверів і програм повинен відповідати важливості інформації, переданої по мережах. Як правило, повинно здійснюватися централізоване управління сервісами електронної пошти. Повинна бути розроблена політика, в якій вказувався б потрібний рівень захисту.

Контрольні запитання

1. Які є варіанти організації DDoS атак?
2. Яке визначення комплексної системи захисту інформації?
3. Для захисту інформації на рівні прикладного та системного ПЗ використовуються?
4. Які є варіанти організації DDoS атак?
5. Які засоби мережевого захисту інформації використовують в комунікаційних системах?
6. WWW – це скорочення від?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мастяниця Й. І., Соснін О. В., Шиманський Л. Є. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання. Київ : Нац. ін-т стратегічних досліджень, 2000. 98 с.

2. Василюк В. Я., Климчук С. О. Інформаційна безпека держави : курс лекцій. Київ : КНТ, Видавн. дім «Скіф», 2008. 136 с.

3. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ : Видавн. дім «СофтПрес», 2005. 316 с.

4. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ : «МК-Прес», 2005. 432 с.

5. Почерцов Г. Г. Информационные войны. Основы военно-коммуникативных исследований. Москва : Рефл-бук; Київ : Ваклер, 2000. 576 с.

6. Расторгуев С. П. Информационная война. Москва : Радио и связь, 1999. 416 с.

7. Расторгуев С. П. Философия информационной войны. Москва : Московский психолого-социальный ин-т, 2003. 486 с.

8. Соснін О. В., Шименський Л. Є. Про правові основи удосконалення системи державного управління інформаційними ресурсами. *Політологічний вісник :* зб. наук. пр. Київ : Т-во «Знання України», 2002. № 10. С. 212–219.

9. Баранов А. А. Концептуальные вопросы информационной безопасности Украины. *Безопасность информации*. 1995. № 2. С. 4–10.

10. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. Санкт-Петербург : БХВ – Петербург, 2003. 688 с.

11. Технічний захист інформації на об'єктах інформаційної діяльності / М. М. Браіловський, С. М. Головень та ін.; за ред. проф. В. О. Хорошка. Київ : ДУІКТ, 2007. 178 с.

12. Петренко С. А., Курбатов В. А. Политики информационной безопасности. Москва : Компания Ай Ти, 2006. 400 с.

13. Сучасні інформаційні війни в соціальних онлайн-мережах / О. В. Курбан // Інформаційне суспільство. - 2016. - Вип. 23. - С. 85-90. - Режим доступу: http://nbuv.gov.ua/UJRN/is_2016_23_15

14. Стратегія національної безпеки України. Указ Президента України від 26 травня 2015 року N287/2015. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/287/2015

15. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

Навчальне видання

Вишня Володимир Борисович
Гавриш Олег Степанович
Рижков Едуард Володимирович

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Редактор *О. М. Врублевська*
Комп'ютерна верстка *А. В. Самотуга*

Підп. до друку 17.02.2020 р. Формат 60x84/16. Гарнітура – Times.
Друк трафаретний (RISO). Папір офісний. Ум.-друк. арк. 7,75. Обл.-вид. арк. 8,00.
Наклад 30 прим. Зам. № 02/20-нп.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49000, м. Дніпро, просп. Гагаріна, 26
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018