**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Дніпропетровський державний університет  
внутрішніх справ**

Кафедра економічної та інформаційної безпеки

**КОНСПЕКТ ЛЕКЦІЙ**

**з дисципліни «ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ»**

Для здобувачів вищої освіти факультету соціально-психологічної освіти та управління,

спеціальності 073 "Менеджмент"

що навчаються на бакалаврському рівні вищої освіти

**Дніпро – 2019**

Укладач: Гавриш О.С, старший викладач кафедра економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ.

Конспект лекцій обговорений та схвалений на засіданні кафедри економічної та інформаційної безпеки 27.08.2019р., протокол No14

**ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**ПЛАН ЛЕКЦІЇ:**

1. Поняття “Інформаційна безпека“ (ІБ): проблема визначення, об’єкт, напрямки державної політики щодо забезпечення ІБ

2. Поняття “інформаційне право“ та загальні недоліки українського інформаційного законодавства

3. Інформаційний суверенітет: визначення, дискусії

4. Проблема доступу до інформації, що не становить державної таємниці.

5. Інформаційна відкритість влади: стан, проблеми та перспективи.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. –К.: ДУІКТ, 2006.–126с.

3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак;під ред. В.О. Хорошко.–Луганськ: Ноулідж, 2012.–480 с.

5. 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

6. 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

**МЕТА ЛЕКЦІЇ:**

Вивчити аспекти інформаційної безпеки пов’язані із входженням України в глобалізаційні процеси, в яких постійно зростає значення інформації.

**ВСТУП**

Актуальність вивчення різних аспектів інформаційної безпеки 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). Разом з тим, 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.

**1.Поняття “Інформаційна безпека“**

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 ВР 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 проекті Закону “Про інформаційний суверенітет та інформаційну безпеку України“. В ньому ІБ розглядається як «*захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовірність 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.

Існують інші визначення ІБ. За “Концепцією інформаційної безпеки України“, ІБ − це «*стан захищеності національних інтересів України в інформаційній сфері, за якою не допускається завдання шкоди особі, суспільству, державі*». , «*захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави*». В цих визначеннях ми можемо спостерігати зміну акцентів та пріоритетів: якщо проект Закону “Про інформаційний суверенітет та ІБ“ на перший план ставить інтереси суспільства та держави, то в останніх визначеннях на перший план виходять інтереси особи.

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.

Якою ж є політика держави у сфері ІБ? Україна − посттоталітарна країна, яка ніколи не розвивалася відповідно до західної демократичної моделі. Відтак, чимало проблем, що постають у сфері ІБ, вкорінюються у т.зв. “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. Так, Закон України “Про інформацію“ 1992 року, навіть з доповненнями до 2005 р., застарів і не відповідає цілому ряду демократичних засад. Єдиним законом, який регулює сферу ІзоД (інформації з обмеженим доступом), є чинний Закон “Про державну таємницю“ в редакції 1999 р. Тож 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 ін. 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 проводить 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*».

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

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 багатоманіття, інформація існувати не може.

**2.Поняття “Інформаційне право“ та загальні недоліки українського інформаційного законодавства**

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

− невідповідність більшості законів та нормативно-правових актів, ухвалених до 1996 року, Конституції України та міжнародним нормативно-правовим актам;

− надмірна декларативність українських законів, певні положення декларуються без вказівок на механізми їх реалізації;

− нерідко трапляються посилання на посилання, або посилання на такі норми, які неможливо застосувати;

− відсутність чіткої ієрархічної структури у нормативно-правовій базі (Конституція − закони − підзаконні акти та відомчі інструкції);

− велика кількість підзаконних актів ускладнює можливості їх застосування;

− випадки суперечностей між законами та відомчими інструкціями, міжнародними правовими актами та українськими законами, колізії між різними законами тощо;

− неузгодженість нових законів з попередніми, що спричиняє правовий хаос;

− перебування величезного масиву засекреченої інформації поза законодавчим полем;

− широкі можливості для посадових осіб безкарно і безпідставно засекречувати інформацію;

− незадовільна правова основа доступу громадян до інформації, що перебуває в руках державних органів;

− термінологічна неузгодженість (наприклад, в законодавстві відсутнє однозначне тлумачення таких підставових термінів як “документ“, “інформація“, “державні секрети“, “таємна інформація“, “таємниця“, “інформаційна безпека“, “інформаційний суверенітет“, “документована інформація“, є 5 різни визначень “конфіденційної інформації“, з визначення “захисту інформації“, 2 − “таємної інформації“ тощо).

− невизначеність механізмів забезпечення відповідальності за порушення інформаційного законодавства;

− нерозробленість, точніше відсутність законодавчої бази для таких сфер як захист персональних даних, доступ до конфіденційної інформації, що є власністю держави, комерційна таємниця та ін.

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

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

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 та громадян.

**3. Інформаційний суверенітет: визначення, дискусії**

Важливе значення у контексті ІБ має поняття “інформаційний суверенітет“, для якого відсутнє однозначне тлумачення. Наприклад, Закон “Про національну програму інформатизації“ подає таке визначення: «*Інформаційний суверенітет − здатність держави контролювати й регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки*». Однак це визначення суперечить ст. 53 Закону “Про інформацію“ та ст. 23 Закону “Про науково-технічну інформацію“, згідно з якими, основою інформаційного суверенітету є національні інформаційні ресурси, а не “здатність держави контролювати“. Під “національними інформаційними ресурсами“ розуміють «*результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані на відповідних матеріальних носіях як окремі документи і масиви документів, бази і банки даних, усі види архівів, бібліотеки, музейні фонди та ін., що містять дані, відомості і знання, які є об’єктом права власності будь-якого суб’єкта України і мають споживчу цінність*».

Для розв’язання цієї проблеми підготовлено законопроект “Про інформаційний суверенітет та інформаційну безпеку України“, в якому інформаційний суверенітет визначено як «*право держави на формування і здійснення національної інформаційної політики відповідно до Конституції України і законодавства України, міжнародного права в національному інформаційному просторі України*». Фахівці вважають таке визначення незадовільним, оскільки воно не враховує глобального і динамічного характеру інформації, розвитку міжнародної інформаційної співпраці. Крім того, проблемним є саме поєднання термінів “інформація“ та “суверенітет“. Хіба інформація може бути суверенною? Адже цінність і продуктивність інформації зростає не в міру її консервування, а в міру її поширення, трансформації. Як показує досвід, втручання держави в інформаційну сферу, наприклад, у галузі наукового обміну, часто є некомпетентним і призводить до сумних наслідків.

**ВИСНОВКИ ДО ТРЕТЬОГО ПИТАННЯ**

Результатом надмірної опіки держави над інформацією може бути інформаційна ізоляція українських науковців від світової науки, що формує негативний образ України на міжнародній арені.

**4. Проблема доступу до інформації, що не становить державної таємниці**

Єдиною сферою ІзОД, яка має чітке законодавче оформлення, є державна таємниця (ДТ). Усі інші види інформації з обмеженим доступом регулюються не законами, а постановами органів виконавчої влади та відомчими інструкціями. З точки зору пріоритету права, така ситуація не є нормальною, бо таким чином різні грифи, які використовуються для службових документів (напр., “Службова таємниця“, “Не для друку“, “Для службового користування“ та ін.) є незаконними, а подекуди і самочинними. Для подібних грифів повинна існувати чітка, законодавчо виписана процедура їх надання, зняття, з критеріями обмеження доступу тощо. Для користування документами з грифом “ДСК“ (Для службового користування) існує урядова “Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави“ від 27 листопада 1998 року. Інструкція надзвичайно детальна, у ній беруться до уваги найменші подробиці користування документами. До речі, саме ця Інструкція тривалий час застосовувала відсутній у законодавстві термін “конфіденційна інформація, що є власністю держави“ (КІВД). Наприклад, у Законі України “Про інформацію“ говорилося, що «*конфіденційна інформація − це відомості, які знаходяться у володінні, користуванні, розпорядженні окремих фізичних чи юридичних осіб і поширюється за їхнім бажанням відповідно до передбачених ними умов*». Лише у 2004 році до Закону України “Про інформацію“ було внесено доповнення, за якими КІВД визначалася як інформація, що *«знаходиться в   
користуванні органів державної влади чи органів місцевого   
самоврядування, підприємств, установ та організацій усіх форм   
власності*», і якій з метою її збереження може бути надано статус конфіденційної. Характерно, що в законі не зазначаються критерії, за якими інформація може набути статусу КІВД. Навпаки, пропонується кілька негативних критеріїв, за якими інформація не може бути віднесена до КІВД. Це значно розширює інформаційний простір, який підлягає засекречуванню. Порядок обліку, зберігання та використання документів, що містять КІВД, закон не регламентує, вважаючи цю практику компетенцією Кабінету Міністрів України (КМУ).

Інструкція КМУ, на базі якої формуються інструкції в установах та підприємствах, далека від досконалості, викликаючи нарікання правників. Наприклад. У пункті 2 йдеться про те, що центральні і місцеві органи виконавчої влади і місцевого самоврядування повинні в 6-ти місячний термін розробити і ввести в дію переліки КІВД. Це породжує такі запитання: хто конкретно і за якими критеріями визначає, яка інформація зараховується до конфіденційної у власності держави? Чи будуть доступні ці переліки для широкого загалу, як це робиться в демократичних країнах шляхом опублікування спеціальних бюлетенів?

З точки зору інформаційного права доцільно опублікувати “Звід відомостей, які відносяться до конфіденційної інформації, що є власністю держави“, як це зроблено у випадку з державною таємницею. Згідно з пунктом 3 до переліку може потрапити не тільки інформація, створена органом державної влади, а й інформація, яка потрапила до державного органу з інших, наприклад, приватних джерел. При цьому власник інформації може й не здогадуватися про те, що його приватна інформація є службовою таємницею.

Особливе застереження викликає пункт 5, за яким державні документи, створені 1991 року і пізніше і не були опубліковані, не містили ніяких грифів обмеження доступу, відтепер отримують гриф ДСК. При цьому жодної експертизи змісту ці документи не проходять, а засекречуються за суто формальною ознакою.

Пункт 32 відносить справу з несекретними документами до документів з грифом ДСК, якщо у справі є хоч один документ з таким грифом. Відтак, це привід засекретити усю справу. До справ ДСК практично не мають доступу журналісти та громадяни. Керівник, згідно з Інструкцією, має право на власний розсуд вирішувати, надавати журналісту інформацію чи ні. Про це говориться в 29 пункті.

**ВИСНОВКИ ДО ЧЕТВЕРТОГО ПИТАННЯ**

Таким чином, доступ громадян до КІВД слід визнати незадовільним, а низку положень Інструкції − такими, що не відповідають принципам демократичної та правової держави.

**5. Інформаційна відкритість влади: стан, проблеми та перспективи**

З цього випливає проблема демократизації української політичної системи, важливим аспектом якої є інформаційна відкритість влади. Рівень відкритості влади є критерієм демократичності державної влади. Термін “інформаційна відкритість“ означає:

а) свободу доступу до інформаційних ресурсів держави на наявність ефективних процедур її забезпечення;

б) наявність механізмів обов’язкового інформування громадян про свою діяльність.

Міра відкритості влади обумовлена чинним політичним ладом. За тоталітаризму та авторитаризму громадяни одержують від держави не інформацію, а пропаганду; держава культивує секретність. Особливе значення інформаційна відкритість має за умов переходу від тоталітаризму до демократії. Ефективність інформування суспільства про дії влади визначаються такими вимогами до інформації: актуальність, достовірність, достатність, доступність, якісність. До принципів інформаційної відкритості влади відносять:

1. максимальне оприлюднення;

2. обов’язковість опублікування;

3. стимулювання відритого уряду;

4. обмеження сфери винятків і їх вмотивованість;

5. чітка процедура отримання доступу;

6. принцип безкоштовного надання інформації громадянам.

У демократичних країнах до найефективніших механізмів захисту права громадян отримувати доступ до державної інформації − це право звернення до суду в разі необґрунтованої відмови в наданні інформації. Громадяни навіть не зобов’язані обґрунтовувати свою правоту, такий обов’язок покладено на державні органи. До основних причин обмеження доступу громадян до інформації в західних країнах належать: обмеження в інтересах національної безпеки, з метою захисту економічних інтересів держави, дотримання правопорядку, захисту міжнародних відносин.

В Україні поки що не існує закону, який би гарантував інформаційну відкритість держави. Є лише проекти законів. Наприклад, «Про інформаційну відкритість органів державної влади та вищих посадових осіб України». Проект визначає перелік органів влади, які підпадають під дію закону, формулює поняття “інформаційна відкритість“, що полягає «*у створенні для громадян та юридичних осіб України можливості вільно отримувати інформацію про ці органи та їхніх посадових осіб в обсягах та порядку, встановлених законом*». Відкритість має забезпечуватися шляхом опублікування інформації, повідомлення по радіо та телебаченню, видання спеціальних бюлетенів, надання платних довідок.

Дослідники мають ряд зауважень до цього законопроекту. Наприклад, не витримує критики положення про “платну основу“ надання довідок, оскільки держава і так існує на кошти громадян; викликає сумніви стаття про те, що «*не підлягають оприлюдненню відомості, які можуть зашкодити безпеці особи, держави, суспільства*», оскільки до цих відомостей може потрапити будь-яка інформація (розклад робочого дня, кількість працівників і т.д.) Дія закону має поширюватися лише на вищі органи влади, але до переліку органів, які мають оприлюднювати інформацію про свою діяльність, не входять місцеві органи влади. Також викликає заперечення стаття про “обмеження щодо відомостей, які не можуть бути оприлюднені“. Список таких відомостей є недоцільним, бо ця сфера чітко визначена Законом “Про державну таємницю“ та “Переліком відомостей, що становлять державну таємницю“. Демократична держава не повинна діяти за принципом максимального засекречення, у тому числі, засекречення “про всяк випадок“.

**ВИСНОВКИ ДО П'ЯТОГО ПИТАННЯ**

Цей законопроект порушує ст. 10 “Європейської конвенції про захист прав людини та основних свобод“, не врегульовує баланс між потребою держави засекречувати інформацію про свою діяльність та інтересом суспільства до інформації про державні органи.

**ВИСНОВКИ З ТЕМИ**

В умовах сучасного розвитку технологій та різноманіття шляхів поширення інформації, питання проблематики захисту інформації від численних загроз займає найвищу позицію. Адже, з розвитком техніки та збільшенням способів передачі інформації відкривається усе більше можливостей для крадіжки інформації, несанкціонованого доступу, спотворення даних та інших типів інформаційного шахрайства. Тож, питання надійного та своєчасного захисту, запобігання та унеможливлення втручання можливих зловмисників до інформаційних систем є надзвичайно пріоритетним.

**ТЕМА 4. ПРОГРАМНІ ЗАСОБИ, ЩО МІСТЯТЬ НЕБЕЗПЕКУ**

**ПЛАН ЛЕКЦІЇ:**

1. Перехоплювачі паролів.

2. Принципи роботи троянських програм.

3. Комп’ютерні віруси і механізми боротьби з ними.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем.–М.: ГТУим. Н.Э. Баумана, 2016.–252с.

2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. –К.: ДУІКТ, 2006.–126с.

3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак;під ред. В.О. Хорошко.–Луганськ: Ноулідж, 2012.–480 с.

5. 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

6. 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

7.Eugene Н. Spafford.The Internet Worm Program: An Analysis // PurdueTechnical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

**МЕТА ЛЕКЦІЇ:**

Вивчити основні програмні засоби що містять небезпеку для користувача та методи протидії їм.

**ВСТУП**

Internet і інформаційна безпека несумісні по самій природі. У даний час за допомогою єдиного стека протоколів TCP/IP і єдиного адресного простору поєднуються не тільки корпоративні і відомчі мережі (освітні, державні, комерційні, військові і т.д.), що є, по визначенню, мережами з обмеженим доступом, але і рядових користувачів, що мають можливість одержати прямий доступ у Internet зі своїх домашніх комп'ютерів. Як відомо, чим простіше доступ у Мережу, тим гірше її інформаційна безпека, користувач може навіть і не довідатися, що в нього були скопійовані - файли і програми, не говорячи вже про можливість їхнього псування і коректування. Саме для повноцінного захисту даних існують програмні засоби захисту даних.

**1.Перехоплювачі паролів**

1.1 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.

1.2. Перехоплювачі паролів другого роду

Перехоплювачі паролів другого родуперехоплюють 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 паролів 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 C, 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.

1.3. 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 перехоплювача 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.

1. 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.
2. 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.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

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.

**2. Принципи роботи троянських програм**

# 2.1 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.

2.2. 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 запуску 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.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

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.

**3. Комп’ютерні віруси і механізми боротьби з ними**

3.1 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.

3.2. 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 можуть бути класифіковані за такими ознаками :

* 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 небезпечнимислід 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» (companion);*
* *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 .ЕХЕ. Копії привласнюється те ж ім’я, що і виконуваному файлу, але розширення змінюється на .СОМ. При запуску файлу із загальним ім’ям операційна система першим завантажує на виконання файл з розширенням .СОМ, який є програмою-вірусом. Файл-вірус запускає потім і файл з розширенням .ЕХЕ.

*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 (ВАТ), завантажувальні драйвери (SYS), програми в машинних (двійкових) кодах (ЕХЕ, СОМ), 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

Вірус

Файл

Вірус

Файл

Файл

Вірус

Файл

Заголовок віруса

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 інше.

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 використання 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.

Сектор 1

Тіло вірусу

Boot – сектор або MBR

Або MBR

Заголовок віруса

Сектор 2

…

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.

3.3 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 застосовують 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 сторожи. 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 інформації 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.

3.4. 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 отримає 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.

**ВИСНОВКИ ДО ТРЕТЬОГО ПИТАННЯ**

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.

**ВИСНОВКИ З ТЕМИ**

Платою за користування Internet є загальне зниження інформаційної безпеки, тому для запобігання несанкціонованого доступу до своїх комп'ютерів усі корпоративні і відомчі мережі, а також підприємства, що використовують технологію intranet, ставлять фільтри (fire-wall) між внутрішньою мережею і Internet, що фактично означає вихід з єдиного адресного простору. Ще велику безпеку дасть відхід від протоколу TCP/IP і доступ у Internet через шлюзи.

Цей перехід можна здійснювати одночасно з процесом побудови всесвітньої інформаційної мережі загального користування, на базі використання мережних комп'ютерів, що за допомогою мережної карти 10Base-T і кабельного модему забезпечують високошвидкісний доступ (10 Мбіт/с) до локального Web-сервера через мережу кабельного телебачення.

Для рішення цих і інших питань при переході до нової архітектури Internet потрібно передбачити наступне:

По-перше, ліквідувати фізичний зв'язок між майбутньої Internet (який перетвориться у Всесвітню інформаційну мережу загального користування) і корпоративними і відомчими мережами, зберігши між ними лише інформаційний зв'язок через систему World Wide Web.

По-друге, замінити маршрутизатори на комутатори, виключивши обробку у вузлах IP-протоколу і замінивши його на режим трансляції кадрів Ethernet, при якому процес комутації зводиться до простої операції порівняння MAC-адрес.

По-третє, перейти в новий єдиний адресний простір на базі фізичних адрес доступу до середовища передачі (MAC-рівень), прив'язане до географічного розташування мережі, і 48-бітний створити адрес, що дозволяє в рамках, для більш ніж 64 трильйонів незалежних вузлів.

**ТЕМА 5. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**

**ПЛАН ЛЕКЦІЇ:**

1. Криптографічні методи захисту

2. Основи криптоаналізу

3. Стеганографія

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА:**

1.Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.

2.Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації -Харків: ХНУРЕ, 2004 -368 с.

3.Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. –Львів : Видавництво Львівської політехніки, 2013. –96 с

**МЕТА ЛЕКЦІЇ:**

Познайомити студентів з основними поняттями криптології, сформувати в студентів представлення про сучасні методи криптології.

**ВСТУП**

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.

**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.

Біометричні системи ідентифікації

Фізичні

Особливості поведінки

Відбитки пальців

Підпис

Геометрія руки

Геометрія обличчя

Структура ДНК

Форма вушної раковини

Рисунок райдужної оболонки ока

Форма вушної раковини

Форма вушної раковини

Форма вушної раковини

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 повідомлення – 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.

010101100010001

Шифрування

Привіт

Розшифровка

Привіт

Ключ

Канал зв'язку

Шифроване повідомлення

Повідомлення

Повідомлення

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.

01100010001

Привіт

Привіт

Шифрування

Розшифровка

Відкритий ключ

Канал зв'язку

Шифроване повідомлення

Повідомлення

Повідомлення

11110101

Закритий ключ

Рис. 5.3. Несиметричне 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.

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.

**ВИСНОВКИ ДО ПЕРШОГО ПИТАННЯ**

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 методи, 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.

**ВИСНОВКИ ДО ДРУГОГО ПИТАННЯ**

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 Даґером 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 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.

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.

**ВИСНОВКИ ДО ТРЕТЬОГО ПИТАННЯ**

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.

**ВИСНОВКИ З ТЕМИ**

Криптографічний захист секретної інформації-вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових Даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.