Центральноукраїнський національний технічний університет

Кафедра кібербезпеки та програмного забезпечення

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

з дисципліни

«Безпека інформації в інформаційно-комунікаційних системах»

для підготовки бакалаврів зі спеціальності 125 «Кібербезпека»

Складали: викл. Бісюк Віктор Анатолійович

Доц. Смірнов Сергій Анатолійович

ЦНТУ 2020

ЗМІСТ

Лабораторна робота №1

Тема: Вивчення правових засад захисту інформації в ІКС

Мета роботи: Придбання теоретичних знань з правових засад захисту інформації в ІКС України.

Короткі теоретичні відомості.

Діяльність в сфері безпеки інформації в ІТС визначає Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні: блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію; { Абзац четвертий статті 1 в редакції Закону N 1170-VII (1170-18) від 27.03.2014 }

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

володільці інформації;

власники системи;

користувачі;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи; { Абзац п'ятий частини першої статті 3 в редакції Закону N 879-VI (879-17) від 15.01.2009 }

{ Абзац шостий частини першої статті 3 виключено на підставі Закону N 767-VII (767-18) від 23.02.2014 }

{ Частину другу статті 3 виключено на підставі Закону N 1170-VII (1170-18) від 27.03.2014 }

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

{ Частина третя статті 4 із змінами, внесеними згідно із Законом N 1170-VII (1170-18) від 27.03.2014 }

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

{ Частина друга статті 8 із змінами, внесеними згідно із Законом N 1170-VII (1170-18) від 27.03.2014 }

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

{ Частина друга статті 9 із змінами, внесеними згідно із Законом N 1170-VII (1170-18) від 27.03.2014 }

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган. { Частина третя статті 9 із змінами, внесеними згідно із Законом N 879-VI (879-17) від 15.01.2009 }

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги (373-2006-п) до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

{ Частину другу статті 10 виключено на підставі Закону N 879-VI (879-17) від 15.01.2009 }

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації: { Абзац перший частини третьої статті 10 в редакції Закону N 879-VI (879-17) від 15.01.2009 }

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі. { Частину третю статті 10 доповнено абзацом згідно із Законом N 1180-VI (1180-17) від 19.03.2009 }

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

{ Частина четверта статті 10 із змінами, внесеними згідно із Законом N 879-VI (879-17) від 15.01.2009 }

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України Л.КУЧМА

м. Київ, 5 липня 1994 року N 80/94-ВР

Завдання: Ознайомитись з «Законом України Про захист інформації в інформаційно-телекомунікаційних системах». Вивчити термінинологію і дати відповіді на питання нижче.

Питання:

1. Скільки розділів містить Закон України Про захист інформації в інформаційно-телекомунікаційних системах? а) 4; б) 6; в) 8; г) немає правильної відповіді.

2. Яка мета Закону України Про захист інформації в інформаційно-телекомунікаційних системах?

а) забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації;

б) встановлення загальних правових основ одержання, використання, поширення та зберігання інформації, закріплення права особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначення статусу учасників інформаційних відносин, регулювання доступу до інформації та забезпечення її охорони, захист особи та суспільства від неправдивої інформації;

в) регулювання відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; г) встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

3. Згідно з Законом України Про захист інформації в інформаційнотелекомунікаційних системах під захистом інформації в системі розуміють…

а) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

б) діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

в) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

г) сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

4. Що не є суб'єктом відносин, пов'язаних із захистом інформації в системах?

а) інформація;

б) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

в) власники інформації;

г) користувачі.

5. Ким визначається порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації?

а) власником інформації;

б) законодавством;

в) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

г) власником системи.

6. Хто надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу?

а) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації;

б) законодавств;

в) користувач;

г) власник системи.

7. Відповідальність за забезпечення захисту інформації в системі покладається на…

а) власника інформації;

б)законодавство;

в) користувача;

г) власника системи.

8. Ким встановлюються особливості захисту інформації в системах, які забезпечують банківську діяльність?

а) Кабінетом Міністрів України;

б) законодавством;

в) Національним банком України;

г) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації.

9. Хто визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом?

а) Кабінет Міністрів України;

б) законодавство;

в) Національний банк України;

г) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації.

Лабораторна робота №2

Тема: Основні принципи розробки та використання антивірусного захисту ІКС

Мета роботи: Придбання практичних навичок роботи з антивірусними програмами.

Короткі теоретичні відомості:

Класифікація комп'ютерних вірусів

Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році).

Типи вірусів

Віруси - супутники. Найбільш примітивний тип вірусів. Для кожного файлу з розширенням. Exe створюють файл з тим же ім'ям, але з розширенням. Com. містить тіло вірусу. При запуску файлу операційна система спочатку шукає. Com файли, а потім. Exe файли. Тому спочатку управління отримує вірус, а потім вже він сам викликає необхідний exe файл.

Файлові віруси. Вражають файли з розширенням. Com,. Exe, рідше. Sys або оверлейні модулі. Exe файлів. Ці віруси дописують своє тіло на початок, середину або кінець файлу і змінюють його таким чином, щоб першими отримати управління. Деякі з цих вірусів не дбають про збереження заражає файли, в результаті чого він виявляється непрацездатним, і, що найсумніше, такий файл не можна відновити. Частина цих вірусів залишається в пам'яті резидентної.

Завантажувальні віруси. Вражають завантажувальні сектори дисків. Інфікування нових дисків відбувається в той момент, коли в заражений комп'ютер вставляють нову дискету і починають з нею працювати. Часто вірус не збожеволіє цілком у завантажувального запису, туди пишеться тільки його початок, а продовження тіла вірусу зберігається в іншому місці диска. Після запуску залишаються в пам'яті резидентної.

Віруси, що поєднують в собі властивості файлових і завантажувальних вірусів. Такі віруси можуть вражати як файли, так і завантажувальні сектори.

Віруси DIR -. Цікавий клас вірусів, що з'явився недавно. Ці віруси змінюють файлову систему диска дуже хитрим чином. У таблиці розміщення файлів (FAT) для всіх виконуваних файлів посилання на початок замінюються посиланнями на тіло вірусу. Адреси ж початку файлів в закодованому вигляді містяться в невикористовувані елементи директорії. У результаті, як тільки ви запускаєте будь-яку програму, управління автоматично отримує вірус. Він залишається в пам'яті резидентної і при роботі відновлює правильні посилання на початку файлів. Якщо диск, заражений вірусом DIR, потрапляє на чистий комп'ютер, рахувати з нього дані, природно, виявляється неможливим (читається тільки один кластер). При спробі протестувати файлову структуру - скажімо Norton Disk Doctor - на екран видається повідомлення про величезну кількість помилок, але варто запустити хоч одну програму з зараженого диска, як файлова система відразу ж "відновлюється". Насправді ж відбувається інфікування ще одного комп'ютера.

Макровіруси. Досить оригінальний клас вірусів (хоча вірусами в повному сенсі цього слова їх навіть не можна назвати), що заражає документи, в яких передбачено виконання макрокоманд. При відкритті таких документів спочатку виконуються дії (спеціальні програми високого рівня), що містяться в цьому

документі,-макровірус якраз іпредставляет собою таку макрокоманду. Таким чином, як тільки буде відкрито заражений документ, вірус отримає управління і зробить все шкідливий дії (зокрема, знайде і заразить ще не заражені документи).

За способом зараження віруси діляться на резидентні і нерезидентні. Резидентний вірус при зараженні (інфікуванні) комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення операційної системи до об'єктів зараження (файлам, завантажувальним секторам дисків і т.п.) і упроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до виключення або перезавантаження комп'ютера. Нерезидентні віруси не заражають пам'ять комп'ютера і є активними обмежений час.

По ступеню дії віруси можна розділити на наступні види:

· безпечні, такі, що не заважають роботі комп'ютера, але що зменшують об'єм вільної оперативної пам'яті і пам'яті на дисках, дії таких вірусів виявляються в яких-небудь графічних або звукових ефектах

· небезпечні віруси, які можуть привести до різних порушень в роботі комп'ютера

· дуже небезпечні, дія яких може привести до втрати програм, знищення даних, стирання інформації в системних областях диска.

По особливостях алгоритму віруси важко класифікувати із-за великої різноманітності. Прості віруси − паразитичні, вони змінюють вміст файлів і секторів диска і можуть бути достатньо легко виявлені і знищені. Можна відзначити віруси-реплікатори, звані черв'яками, які розповсюджуються по

комп'ютерних мережах, обчислюють адреси мережевих комп'ютерів і записують за цими адресами свої копії. Відомі віруси-невидимки, звані стелс-вірусами, які дуже важко виявити і знешкоджувати, оскільки вони перехоплюють звернення операційної системи до уражених файлів і секторів дисків і підставляють замість свого тіла незаражені ділянки диска. Найважче виявити віруси-мутанти, що містять алгоритми шифровки-розшифровки, завдяки яким копії одного і того ж вірусу не мають жодного ланцюжка байтів, що повторюється. Є і так звані квазівірусні або «троянські» програми, які хоч і не здібні до саморозповсюдження, але дуже небезпечні, оскільки, маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків.

Прийнято розділяти віруси за:

- об'єктами, які вражаються (файлові віруси, завантажувальні віруси, анти-антивірусні віруси, скриптові віруси, макро-віруси, мережеві черв'яки).
- способом зараження (перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси, віруси, що вражають вихідний код программ)
- операційними системами і платформами, які вражаються (Microsoft Windows, Unix, Linux, інші)
- активністю (резидентні віруси, нерезидентні віруси)
- технологіями, які використовуються вірусом (нешифровані віруси, шифровані віруси, поліморфні віруси, стелс-віруси (руткіт і буткіт))
- деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси)
- мовою, на якій написаний вірус (асемблер, високорівнева мова програмування, скриптова мова, інші).

До шкідливих програм, крім вірусів, відносяться також мережеві черв’яки, троянські коні (логічні бомби), intended-віруси, конструктори вірусів і поліморфні-генератори.

Мережеві черв’яки – програми, що розповсюджуються по мережі і не залишають своєї копії на магнітному носії або диску.

До троянських коней відносяться програми, що завдають будь-яку руйнівну дію, в залежності від яких-небудь умов або при кожному запуску знищують інформацію на дисках, зупиняють роботу операційної системи і т.д. Найпоширенішою різновидністю “троянських програм” є широко відомі програми масового використання (редактори, ігри, транслятори і т.п.), в які вбудовані, так звані “логічні бомби”, що спрацьовують у випадку виникнення деякої події. Різновидністю “логічної бомби” є “бомба з годинниковим механізмом”, яка запускається у визначенні моменти часу.

Потрібно зазначити, що “троянські програми” не можуть самостійно розмножуватися і розповсюджуватися по локальній обчислювальній мережі самими користувачами, зокрема, через загальнодоступні банки даних і програм. У порівнянні з вірусами “троянські коні“ не одержали широкого поширення внаслідок достатньо простих причин: вони або знищують себе разом з іншими даними на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

Серед шкідливих програм слід відмітити також «люті жарти» (hoax). До них відносяться програми, що не заподіюють комп’ютеру якоїсь прямої шкоди, проте виводять повідомлення про те, що така шкода вже заподіяна або буде заподіяною за яких-небудь умов, або попереджують користувача про неіснуючу небезпеку. До «лютих жартів» відносяться, наприклад, програми, що лякають користувача

повідомленнями про форматування диска (хоча ніякого форматування насправді не відбувається), виявляють віруси в неінфікованих файлах, виводять дивні вірусоподібні повідомлення у залежності від почуття гумору автора такої програми.

До intended-вірусів відносяться програми, що на перший погляд є стовідсотковими вірусами, але не спроможні розмножуватися через помилки. Наприклад, вірус, що при інфікації «забуває» передбачити активізацію вірусу, що розмножується тільки один раз – з «авторської» копії. Інфікувавши якийсь файл, вони втрачають спроможність до подальшого розмноження. Частіше всього intended-віруси з'являються при неякісній перекомпіляції якогось вже існуючого вірусу, або через недостатнє знання мови програмування, або через незнання технічних тонкощів операційної системи.

Конструктор вірусів − це програма, що призначена для виготовлення нових комп'ютерних вірусів. Відомі конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати вихідні тексти вірусів (ASM-файли), об'єктні модулі і (або) безпосередньо інфікувати файли.

Поліморфік-генератори, як і конструктори вірусів, не є вірусами в буквальному значенні цього слова, оскільки в їхній алгоритм не закладаються функції розмноження, тобто відкриття, закриття і запису у файли, читання і запису секторів і т.д. Головною функцією подібного роду програм є шифрування тіла вірусу і генерація відповідного розшифровувача. Звичайні поліморфні генератори поширюються їхніми авторами без обмежень у вигляді файла-архіву. Основним файлом в архіві будь-якого генератора є об'єктний модуль, що містить цей генератор. В усіх генераторах, що зустрічалися, цей модуль містить зовнішню (external) функцію - виклик програми генератора. У такий спосіб автору вірусу, якщо він бажає створити справжній поліморфік-вірус, не потрібно розробляти

власний за- чи розшифровувач. За бажанням він може підключити до свого вірусу будь-який відомий поліморфік-генератор.

Ознаки зараження вірусом

- Зменшення вільної пам'яті
- Уповільнення роботи комп'ютера
- Затримки при виконанні програм
- Незрозумілі зміни в файлах
- Зміна дати модифікації файлів без причини
- Незрозумілі помилки Write-protection
- Помилки при інсталяції і запуску Windows
- Відключення 32-розрядного допуску до диску
- Неспроможність зберігати документи Word в інші каталоги, крім Template
- Погана робота дисків
- Файли невідомого походження
- Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни:
- Зникнення файлів
- Форматування HDD
- Неспроможність завантажити комп'ютер
- Неспроможність завантажити файли
- Незрозумілі системні повідомлення, звукові ефекти і т. д.

Віруси можуть проникати в обчислювальну систему двома шляхами:

по-перше, з інфікованого комп'ютера при копіюванні з нього файлу, що містить вірус;

по-друге, при запуску програми, розділеної між кількома комп'ютерами, в тому числі і при завантаженні операційної системи.

Зазвичай віруси розміщуються у файлах, які здебільшого керують роботою. Це файли ОС, системних і прикладних програм, драйверів пристроїв, файли об'єктних модулів і бібліотек, дисковий і системний завантажувачі, початкові тексти програм мовами високого рівня.

Здебільшого, все це в минулому. Зараз основні ознаки — самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус.

Засоби захисту від комп'ютерних вірусів та їх особливості

Для захисту від різноманітних вірусів існує декілька видів антивірусів, які за своїм призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини. Розглянемо їх характеристики більш докладно.

Детектори (сканери) – перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм. Якщо детектор – резидентний, то програма перевіряється і тільки в разі відсутності вірусів вона активується. Детекторами є, наприклад, програма MS AntiVirus.

Фаги (поліфаги) – виявляють та знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть проводити евристичний аналіз файлу, досліджуючи його на наявність коду, характерного для вірусу (додання частини однієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Дуже часто функції детектора та фага суміщені в одній програмі, а вибір режиму роботи здійснюється завданням відповідних параметрів (опцій, ключів). На початку вірусної ери кожний новий вірус визначався та лікувався окремою програмою. При цьому для деяких з вірусів (наприклад, VIENNA) цих програм було не менше десятка. Згодом окремі програми почали виявляти та лікувати декілька типів вірусів, тому їх стали звати полідетекторами та поліфагами відповідно.

Сучасні антивірусні програми знаходять і знешкоджують багато тисяч різновидів вірусів і заради простоти їх звуть коротко детекторами та фагами. Серед детекторів та фагів найбільш відомими та популярними є програми Aidstest, DrWeb (фірма «ДиалогНаука», Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США). Ці програми періодично поновлюються, даючи користувачеві змогу боротися з новими вірусами.

Ревізори – програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів. При створенні будь-яких змін користувачеві видається повідомлення (навіть у разі відсутності вірусів, але наявності змін).

При першому запуску ревізор утворює таблиці, куди заносить інформацію про вільну пам'ять, Partition Table, Boot-сектор, директорії, файли, що містяться у них, погані кластери тощо. При повторному запуску ревізор сканує пам'ять та диски і видає повідомлення про всі зміни, що відбулися у них з часу останнього сеансу ревізії. Нескладний аналіз цих змін дозволяє надійно визначити факт зараження комп'ютера вірусами. Серед ревізорів найбільш популярною є програма ADinf (фірма «ДиалогНаука», Росія).

Свого часу, коли не було надійних засобів боротьби з вірусами, широкого поширення набули так звані фільтри. Ці антивірусні програми блокують операцію записування на диск і виконують її тільки при вашому дозволі. При цьому легко визначити, чи то ви санкціонували команду на запис, чи то вірус намагається щось заразити. До числа широко відомих свого часу фільтрів можна віднести програми VirBlk, FluShot та ін.

Зараз фільтри майже не використовують, оскільки вони, по-перше, дуже незручні, бо відволікають час на зайвий діалог, по-друге, деякі віруси можуть обманювати їх.

Сторожі – резидентні програми, які постійно зберігаються у пам'яті комп'ютера й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера, файли, BOOT-сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP.

Вакцини – це програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів.

Існують три рубежі захисту від комп'ютерних вірусів:

1. Запобігання надходженню вірусів.

2. Запобігання вірусній атаці, якщо вірус усе-таки потрапив у комп'ютер.

3. Запобігання руйнівним наслідкам, якщо атака відбулася.

Є три методи реалізації рубіжної оборони:

- «Програмні методи захисту».

- Апаратні методи захисту.

- Організаційні методи захисту.

Основним засобом захисту інформації є резервне копіювання найцінніших даних. У разі втрати інформації внаслідок будь-якої з названих вище причин,

жорсткий диск треба відформатувати й підготувати до нової експлуатації. На «чистий» диск установлюють операційну систему з дистрибутивного компакт-диска, потім під її керуванням треба встановити все необхідне програмне забезпечення, яке теж беруть з дистрибутивних носіїв. Відновлення комп’ютера завершують відновленням даних, які беруть з резервних носіїв.

Створюючи план заходів з резервного копіювання інформації, необхідно враховувати, що резервні копії повинні зберігатися окремо від комп’ютера. Тобто, наприклад, резервне копіювання інформації на окремому жорсткому дискові того самого комп'ютера лише створює ілюзію безпеки. Відносно новим і досить надійним методом зберігання даних є зберігання їх на віддалених серверах в Інтернеті. Є служби, які безплатно надають простір для зберігання даних користувача.

Допоміжним засобом захисту інформації є антивірусні програми та засоби апаратного захисту. Так, наприклад, просте відключення перемички на материнській платі не дозволить здійснити стирання перепрограмовуваної мікросхеми ПЗП (флеш-BIOS), незалежно від того, хто буде намагатися зробити це: комп’ютерний вірус чи неакуратний користувач.

Існує досить багато програмних засобів антивірусного захисту, їхні можливості такі:

1. Створення образу жорсткогодиска на зовнішніх носіях. У разі виходу з ладу інформації в системних ділянках жорсткого диска, збережений «образ диска» може дозволити відновитиякщо не всю інформацію, то принаймні її більшу частину. Цей засіб можезахистити від утрати інформації під час апаратних збоїв та неакуратного форматування жорсткого диска.

2. Регулярне сканування жорсткого диска в пошуках комп'ютернихвірусів. Сканування звичайно виконують автоматично під час кожного ввімкнення комп'ютера або при розміщенні зовнішнього диска у зчитувальному пристрої. Під час сканування треба мати на увазі, що антивірусна програма шукає вірус шляхом порівняння коду програми з кодами відомих їй вірусів, що зберігаються в базі даних. Якщо база даних застаріла, а вірус є новим, то програма сканування його не виявить. Для надійної роботи варто регулярно оновлювати антивірусну програму. Так, наприклад, руйнівні наслідки атаки вірусу W95.CIM.1075 («Чорнобиль»), який знищив інформацію на сотнях тисяч комп'ютерів ... 26 квітня 1999 року, були пов'язані не з відсутністю засобів захисту від нього, а з тривалою затримкою (більше року) в оновленні цих засобів.

3.Контроль за змінами розмірів та інших атрибутів файлів. Оскільки на етапі розмноження деякі комп'ютерні віруси змінюють параметри зараженихфайлів, програма контролю можевиявити їх діяльність і попередити користувача.

4. Контроль за зверненням до жорсткого диска. Оскільки найнебезпечніші операції, пов'язані з діяльністю комп'ютер-них вірусів, так чи інакше спрямовані на модифікацію даних, записаних на жорсткому дискові, антивірусні програми можуть контролювати звернення до нього та попереджати користувача щодо підозрілої активності.

Завдання: Обрати 3 або більше різні антивірусні пакети і протестувати їх. У звіті проаналізувати і описати їх функціональні можливості, ступінь захисту та зручність використання.

Лабораторна робота №3

Тема: Програмні методи та засоби захисту в ІКС

Мета роботи: Освоєння практичних навичок з встановлення, модифікації та роботи з програмними засобами захисту інформації в ІКС.

Короткі теоретичні відомості

Програмні засоби захисту даних – це складові програмного забезпечення, що реалізують функції захисту даних самостійно або в комплексі з іншими засобами захисту.

Класифікацію програмних засобів захисту за функціональним призначенням наведено на рис. 3.1.

Рисунок 3.1 – Класифікація програмних засобів захисту

До програмних засобів зовнішнього захисту належать програмні засоби забезпечення функціонування фізичних засобів, захисту території, приміщень, окремих каналів зв'язку й пристроїв ІС. У цей час випускається безліч систем охоронної сигналізації, що містять мікропроцесори та комп'ютери. Програмні засоби використовуються також у пристроях біометричного розпізнавання особистості.

Основним методом захисту даних, що передаються по каналах зв'язку, є криптографічне закриття даних, яке реалізується програмними, апаратними і програмно-апаратними засобами.

Крім цього використовуються такі програмні засоби:

- розпізнавання користувачів;
- перевірка рівня таємності каналу;
- перевірка адрес користувачів;
- перевірка ідентифікаторів користувачів під час обміну великими обсягами даних і т.д.

Ідентифікація – це процедура однозначного розпізнавання унікального імені суб'єкта інформаційної системи.

Автентифікація – це процедура підтвердження того, що пред'явлене ім'я відповідає даному суб'єктові (підтвердження дійсності суб'єкта).

Програмні засоби внутрішнього захисту охоплюють сукупність засобів і механізмів захисту даних, що знаходяться в апаратурі ІС. Їхнім основним призначенням є регулювання і контроль використання даних та ресурсів системи відповідно до встановлених прав доступу.

Типова схема функціонування цих програмних засобів складається з таких основних етапів:

- установлення дійсності суб'єкта, що звертається до ресурсів системи;
- перевірка відповідності характеру запиту наданим повноваженням даного суб'єкта;
- ухвалення рішення відповідно до результату перевірки повноважень.

Регулювання використання технічних засобів звичайно здійснюється за такими параметрами, як час доступу і запитувана дія при доступі.

Захист програмного забезпечення здійснюється такими методами, як, наприклад, контрольне підсумовування і шифрування.

Програмні засоби керування захистом призначені для виконання таких завдань:

- керування користувачами мережі (реєстрація користувачів, генерування службової інформації для користувачів, розсилання службової інформації користувачам);
- керування базами даних (розподіл ресурсів захисту, координація роботи підсистем системи керування базами даних (СКБД);
- завдання прийняття рішень у позаштатних ситуаціях (система підтримки ухвалення рішення адміністратором СКБД, вироблення керувальних впливів для усунення порушення функціонування СКБД).

Програмні засоби забезпечення захисту функціонування СКБД виконують функції контролю, реєстрації, знищення, сигналізації та імітації.

Засоби контролю здійснюють тестування елементів СУБД, а також постійний збір інформації про функціонування елементів СКБД. Ця інформація служить вихідними даними для засобів підтримки ухвалення рішення і вироблення керуючих впливів.

Засоби реєстрації забезпечують збирання, зберігання, оброблення і видачу даних про стан СКБД.

Засоби знищення призначені для знищення залишкових даних і можуть передбачати аварійне знищення даних у випадку прямої загрози несанкціонованого доступу, яке не може бути блоковано системою.

Засоби сигналізації призначені для попередження користувачів при їхньому звертанні до захищених даних і для попередження адміністратора СКБД при виявленні факту несанкціонованого доступу до даних, спотворення програмних засобів захисту, виході з ладу апаратних засобів захисту тощо.

Засоби імітації імітують роботу з порушниками при виявленні спроби несанкціонованого доступу до даних, що захищають. Імітація дозволяє збільшити час на визначення місця і характеру несанкціонованого доступу, що особливо важливо в територіально розподілених мережах, і “відвести” порушника вбік від даних, що захищаються.

Перевагами програмних засобів захисту інформації є:

- простота тиражування;
- гнучкість (можливість настроювання на різні умови застосування, що враховують специфіку загроз інформаційній безпеці конкретних ІС);
- простота застосування – одні програмні засоби, наприклад шифрування, працюють у “прозорому” (непомітному для користувача) режимі, а інші не вимагають від користувача ніяких нових (порівняно з іншими програмами) навичок;
- практично необмежені можливості їхнього розвитку шляхом внесення змін для врахування нових загроз безпеці інформації.

До недоліків програмних засобів захисту інформації належать:

- зниження ефективності ІС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;
- більш низька продуктивність виконання аналогічних функцій порівняно з апаратними засобами захисту;
- приєднання багатьох програмних засобів захисту, а не їхня вбудованість у програмне забезпечення, створює для порушника принципову можливість їхнього обходу;
- можливість злочинної зміни програмних засобів захисту в процесі експлуатації ІС

TCPView - це утиліта, призначена для ОС Windows, яка виводить на екран списки кінцевих вузлів всіх установлених у системі з'єднань за протоколами *TCP* і *UDP* з докладними даними, у тому числі із вказівкою локальних і вилучених адрес і стану TCP-з*′єднань*, повідомляє ім'я процесу, якому належить кінцевий

вузол. При запуску утиліта *TCPView* перераховує всі з'єднання *TCP* і *UDP*, конвертує всі IP-адреси в доменні назви.

XSpider – це засіб мережного аудита, призначений для пошуку уразливостей на серверах і робочих станціях. *XSpider* дозволяє виявляти уразливості на комп'ютерах, що працюють під керуванням різних операційних систем: AIX, Solaris, Unix-Системи, Windows і ін. Програма працює під керуванням MS Windows.

Ключові питання

1. Поясніть призначення утиліт *TCPView* і *XSpider*. У чому полягає принципова відмінність даних утиліт?

2. При яких факторах можливе перевантаження каналу утиліти *XSpider*? Яким чином можна боротися з даним перевантаженням?

3. Призначивши для кожного завдання певний розклад роботи, які переваги ви одержуєте?

4. Для чого бажано задати інтервал, протягом якого створюваний автоматичний розклад буде активним?

5. Які типи уразливостей можна виявити за допомогою утиліти *XSpider*?

6. За портами яких мережних служб ведеться спостереження за допомогою сканера безпеки *XSpider*?

7. Поясніть призначення сервісу «*Перевизначення уразливості*».

8. Де зберігається, за замовчуванням, файл портів утиліти *XSpider* і яким чином ви можете настроїти сканування тільки за певними портами?

9. Поясніть поняття евристичних методів пошуку уразливостей. У чому перевага даного методу?

10. Яким чином можна автоматизувати роботу утиліти XSpider?

Завдання до лабораторної роботи

1. Відкрийте утиліту *TCPView*. При запуску ви побачите список всіх активних кінцевих вузлів з'єднань за протоколами *TCP* і *UDP*. Ознайомтеся з основними пунктами меню. Змініть період відновлення інформації, за допомогою

пункту «*Період відновлення» (Refresh Rate»* у меню «*Параметри» Options)*. Якщо в період між відновленнями стан кінцевих вузлів мережі змінився, вони виділяються жовтим кольором, якщо вузол не знайдено, то червоним кольором, нові вузли мережі відображаються зеленим кольором.

2. Занесіть до протоколу результати сканування відкритих з'єднань.

3. Закрийте встановлені підключення за протоколами *TCP/IP,* з станом «*Установлене» (ESTABLISHED)*, за допомогою пункту «*Закрити підключення» (Close Connections)* у меню «*Файл» (File).* Закрийте утиліту *TCPView.*

4. Відкрийте утиліту *XSpider*. Вивчіть основні пункти меню, скориставшись документацією з меню «*Довідка*».

5. Сформуйте завдання для сканування, для цього створіть нове робоче вікно *XSpider* і додайте список робочих станцій. Для цього виберіть команду меню «*Виправлення/Додати*». У вікні, що з’явилося, *задайте IP-адресу*, імена або діапазон комп'ютерів, згідно завданню. Обмежте одночасне сканування, тільки для двох робочих станцій.

6. Створіть свій профіль сканування, для цього виберіть пункти «*Профіль*», «*Створення нового профілю*». Визначте набір настроювань для сканування, виходячи з завдання. Для цього в діалозі, що з'явився, у дереві настроювань виберіть пункт *«Сканер уразливостей/Визначення уразливостей*». Збережіть створені вами завдання.

7. Запустіть сканування. Для цього виберіть відповідну команду з меню «*Сканування*».

8. Перескануйте окремі сервіси. Це може знадобитися в деяких особливих ситуаціях, наприклад, для підтвердження наявності DoS-уразливості. Іноді, при поганій якості зв'язку перевіряється можливе помилкове визначення DoS уразливості, коли зв'язок з вузлом перервався випадково, а *XSpider* зробив висновок, що пройшла DoS-атака. У цьому випадку можна провести повторне сканування відповідного сервісу й при повторному виявленні уразливості більш упевнено зробити висновок про її наявність.

9. Заплануйте запуск вашого завдання за допомогою планувальника. Для цього викличте з меню «*Розклад/Створити*» майстер створення розкладу. Виберіть ваше завдання для автоматизації зі списку збережених завдань у директорії *Tasks* або натисніть «*Огляд*», якщо потрібне завдання перебуває не в директорії *Tasks*. Виберіть інтервал періодичності перевірок, інтервал, протягом якого створюваний розклад буде активним. Задайте автоматичну генерацію й параметри звіту після кожного автоматичного виконання завдання.

10. За результатами кожного сканування згенеруйте звіт про поточне сканування. Для цього виберіть команду з меню «*Сервіс/Створити звіт*», у вікні «*Майстер створення звіту*». Виберіть формат звіту. *RTF*, потім виберіть варіант звіту.

11. Проаналізуйте результати сканування вашого завдання. Занесіть до протоколу результат сканування.

12. Занесіть до протоколу порівняльну характеристику отриманих вами результатів за допомогою утиліт *TCPView* і *XSpider*.

Варіанти завдань для виконання лабораторної роботи:

1. Вам необхідно перевірити мережу на уразливість в «*безпечному*» режимі, без DoS-атак, у мережі немає сервера баз даних.

2. Вам необхідно перевірити мережу на уразливість нових DoS-атак, за допомогою евристичного методу.

3. Вам необхідно перевірити мережу на уразливість за допомогою аналізатора скриптів, включивши складну перевірку всіх скриптів.

4. Вам необхідно перевірити мережу на уразливість протоколів, для передачі/прийому пошти, використовуючи розширені словники логинів і паролів.

5. Вам необхідно перевірити мережу на уразливість, збільшивши час пошуку одного вузла до 5 секунд.

6. Вам необхідно перевірити мережу на уразливість, використовуючи весь діапазон портів, з 1 по 65535.

7. Вам необхідно перевірити мережу на уразливість, визначаючи операційну систему вузлів, за допомогою *Nmap*.

8. Вам необхідно перевірити мережу на уразливість у полях запиту Cookie.

9. Вам необхідно перевірити мережу на уразливість, збільшивши кількість директорій, що перевіряються, на підбір пароля до 10.

10. Вам необхідно перевірити мережу на уразливість, якщо у вашій мережі немає поштового й ftp сервера, немає СУБД. Для прискорення роботи утиліти, відключіть невикористовувані параметри.

11. Вам необхідно перевірити мережу на уразливість, збільшивши кількість потоків для пошуку до 100.

12. Вам необхідно перевірити мережу на уразливість, збільшивши час очікування сканування портів.

Зміст звіту

До звіту внести докладну інформацію про всі робочі станції, сервіси, уразливості, які було скановано. Також потрібен звіт про статистику і перелік виявлених уразливостей, звіт про перелік виявлених портів і сервісів для кожного вузла, звіт про угруповання вузлів, із сортуванням за убування небезпек, звіт про угруповання за уразливостей, із сортуванням за убування небезпеки. Діаграму за історії сканування завдання.

Зробіть висновок про продуктивність розглянутих вами утиліт, з погляду забезпечення безпеки в локальних комп'ютерних мережах.

Лабораторна робота №4

Тема: Криптографічні методи захисту інформації

Мета роботи: Отримати практичні навички роботи з криптографічними засобами захисту.

Короткі теоретичні відомості

Використання криптографічного захисту інформації під час побудови політики безпеки інформаційно-телекомунікаційної on-line-системи значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

Криптографічні методи захисту інформації - це методи захисту даних із використанням шифрування

Головна мета шифрування (кодування) інформації - її захист від несанкціонованого читання. Системи криптографічного захисту (системи шифрування інформації) для банківських on-line -сисгем можна поділити за різними ознаками:

• за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

• за способом реалізації (апаратний, програмний, програмно-аларатний);

• за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

• за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачи);

• за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Вбудовані механізми криптографічного захисту входять до складу системи, їх створюють одночасно з розробленням банківської on-line-системи. Такі механізми можуть бути окремими компонентами системи або бути розподіленими між іншими компонентами системи.

Додаткові механізми криптозахисту - це додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту - найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передачі в апаратуру може бути виконана за допомогою спеціально розроблених програм типу "вірус".

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від "вірусних" атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм "збирання сміття".

Крім того, можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні

засоби для зберігання криптографічних ключів, треба пам'ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм - це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв язаного (шифрованого) тексту.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, а загальні криптоалгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхня висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його "злому". Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою відповідно до збільшення довжини ключа.

Є дві великі групи загальних криптоалгоритмів: симетричні і асиметричні. До симетричних криптографічних алгоритмів належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник, і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість обробки як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов'язані з

дотриманням безпечного розподілу ключів між абонентами системи. Для асиметричних криптоалгоритмів шифрування і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостій-кості алгоритму і не дає можливості відновлення парного йому ключа.

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

• для шифрування інформації, тобто приховування змісту повідомлень і даних;

• для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування DES (Data Encryption Standart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування.

Алгоритм Потрійний DES був запропонований як альтернатива DES і призначений для триразового шифрування даних трьома різними закритими ключами для підвищення ступеня захисту.

RC2, RC4, RC5 - шифри зі змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (International Data Encryption Algoritm) призначений для швидкої роботи в програмній реалізації.

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

Алгоритм RSA дозволяє виконувати шифрування в різних режимах:

• за допомогою таємного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;

• за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;

• за допомогою таємного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Другою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підробки. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена. Для симетричних алгоритмів шифрування така додаткова інформація - це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву електронний цифровий підпис. Формуючи електронний цифровий підпис, виконують такі операції:

• за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;

• отримане значення хеш-функції шифрується: а) таємним або відкритим; б) таємним і відкритим ключами відправника і отримувача повідомлення - для алгоритму RSA

• використовуючи значення хеш-функції і таємного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису, - наприклад, для російського стандарту Р.31-10.

Для того, щоб перевірити цифровий підпис, потрібно:

• виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;

• обчислити хеш-функцію з тексту повідомлення;

• порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і відправлене саме цим відправником.

Останнім часом використання електронного цифрового підпису значно поширюється, у тому числі для регулювання доступу до конфіденційної банківської інформації та ресурсів системи, особливо для on-line -систем реального часу.

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1. Метод базових/сеансових ключів. Такий метод описаний у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто

сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.

2. Метод відкритих ключів. Такий метод описаний у стандарті ISO 11166 і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує "абсолютного" захисту інформації, але гарантує, що вартість "злому" у кілька разів перевищує вартість зашифрованої інформації.

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів - через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат - це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

Шифри перестановки

При шифруванні перестановкою символи вихідного тексту переставляються за визначеним правилом у межах блоку всього тексту. Шифри перестановки є найпростішими і, ймовірно, самими стародавніми шифрами.

Як приклад шифру перестановки розглянемо таблиці шифрування, що застосовувалися з початку епохи Відродження. Таблиці шифрування задають правила перестановки букв у тексті. Застосування таблиць шифрування для шифрування і розшифрування тексту продемонструємо на прикладах.

Для шифрування фрази **I_WANT_TO_KNOW_MORE** будемо використовувати таблицю з 5 рядків і 4-х стовпців. Ключем у цьому випадку служить розмір таблиці. Запишемо в цю таблицю вихідний текст по рядках, а зчитаємо по стовпцях (рис. 1.1). Шифрований текст (шифр-текст) буде таким: **INOOO_T_WRW_K_EATNM_ .**

I _ W A
N T _ T
O _ K N
O W _ M
O R E _

Рис. 4.1.

Для розшифрування шифртекста треба в таку ж таблицю вписати шифр-текст по стовпцях, а зчитати по рядках.

Шифри простої заміни

При шифруванні заміною (підстановкою) символи вихідного (відкритого) тексту заміняються символами того ж, чи іншого алфавіту за заздалегідь установленим правилом заміни. У шифрі простої заміни кожен символ вихідного тексту заміняється символами того ж алфавіту однаково в усьому тексту. Часто шифри простої заміни називають шифрами одноалфавітної підстановки.

Прикладом шифра простої заміни є система шифрування Цезаря. Свою назву цей шифр одержав від імені римського імператора Гая Юлія Цезаря, який використовував цей шифр при листуванні з Цицероном.

Для шифрування вихідного тексту кожна буква замінюється на іншу букву за наступним правилом. Буква заміни визначається шляхом зсуву за алфавітом від вихідної букви на k букв. При досягненні кінця алфавіту виконується циклічний перехід до його початку. Цезар використовував шифр заміни при зсуві k = 3. Такий шифр заміни можна задати таблицею підстановок, що містить відповідні пари букв відкритого тексту і шифртекста. Сукупність можливих підстановок при k=3 для англійського алфавіту показана на рис. 4.2.

A → D G → J M → P S → V Y → A
B → E H → K N → Q T → W Z → C
C → F I → L O → R U → X
D → G J → M P → S V → Y
E → H K → N Q → T W → Z
F → I L → O R → U X → A

Рис. 4.2.

Тепер слово **ROYAL** у шифрованому вигляді буде таким:**URADO.**

Шифри складної заміни

Шифри складної заміни називають багатоалфавітними, бо для шифрування кожного символу вихідного повідомлення застосовують свій шифр простої заміни. Багатоалфавітна підстановка послідовно і циклічно змінює використовувані алфавіти.

При N-алфавітній підстановці символ x_0 вихідного повідомлення заміняється символом y_0 з алфавіту B_0, символ x_1 – символом y_1 з алфавіту B_1, символ x_{N-1} заміняється символом y_{N-1} з алфавіту B_{N-1}, символ x_N заміняється символом y_0 знову з алфавіту B_0, і т.д.

Ефект використання багатоалфавітної підстановки забезпечує маскування природної статистики вихідної мови, тому що конкретний символ з вихідного алфавіту **A** може бути перетворений у кілька різних символів шифрувальних алфавітів B_j. Ступінь захисту теоретично пропорційний довжині періоду N у послідовності використовуваних алфавітів B_j.

Завдання: Розробити програму для шифрування-дешифрування англомовного тексту не менше 15 символів методами простої заміни та перестановки. Можна використовувати будь-яку мову програмування. Віконний або консольний інтерфейс.

Лабораторна робота №5

На тему: Стеганографічні методи захисту інформації

Мета роботи: Ознайомитись з алгоритмами стеганографічного шифрування.

Короткі теоретичні відомості

Основні принципи комп'ютерної стеганографії

У сучасній КС існує два основних типи файлів: повідомлення - файл, що призначений для приховування, і контейнер - файл, що може бути використаний для приховування в ньому повідомлення. При цьому контейнери бувають двох типів. Контейнер-оригінал (або "порожній" контейнер) - це контейнер, що не містить схованої інформації. Контейнер-результат (або "заповнений" контейнер) - це контейнер, що містить сховану інформацію.

Під ключем розуміється секретний елемент, що визначає порядок занесення повідомлення в контейнер. Класичним є наступний принцип вбудовування даних. Нехай сигнал контейнера представлений послідовністю з N біт. Процес приховання інформації починається з визначення біт контейнера, які можна змінювати без внесення помітних спотворень — стеганошляху. Далі серед цих біт, зазвичай у відповідності до ключа, обираються біти, що замінюються бітами приховуваного повідомлення.

Базовими положеннями сучасної КС є:

1. Забезпечення автентичність і цілісність файлу.

2. Обізнаність супротивника з можливостями КС.

3. Безпека ґрунтується на збереженні стеганографічним перетворенням основних властивостей переданого файлу при внесенні в нього секретного повідомлення і деякої невідомої супротивникові інформації - ключа.

4. Витяг секретного повідомлення має становити складну обчислювальну задачу.

Огляд стеганографічних методів і їх класифікація

Сучасні методи КС розвиваються у двох основних напрямках:

1) методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;

2) методи, засновані на надмірності аудіо і візуальної інформації.

Більшість методів КС базується на двох принципах:

1) файли, які не вимагають абсолютної точності (наприклад, файли з зображенням, звуковою інформацією тощо), можуть бути видозмінені (до певного ступеня) без втрати своєї функціональності;

2) органи чуття людини не здатні надійно розрізняти незначні зміни у модифікованих таким чином файлах та/або відсутній спеціальний інструментарій, який був би спроможним виконати дану задачу.
Існуючі методи КС можна класифікувати (рис.1), спираючись на відомі публікації та вибираючи той чи інший класифікаційний критерій.

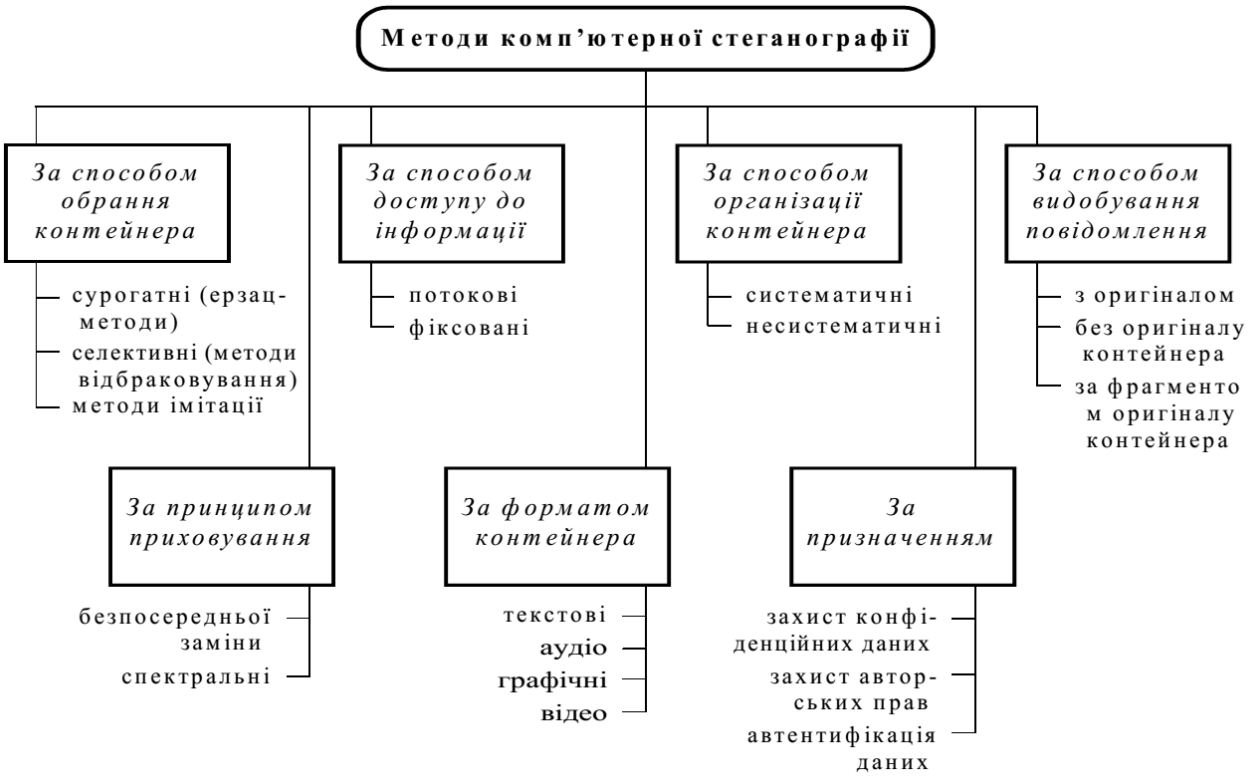

Рисунок 5.1 - Класифікація методів комп'ютерної стеганографії

За способом доступу до приховуваної інформації розрізняють методи потокових (безперервних) і фіксованих (обмеженої довжини) контейнерів.

За способом організації контейнери, подібно завадозахищеним кодам, можуть бути систематичними і несистематичними. У перших можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти власне контейнера, а де шумові біти, призначені для приховування інформації (як, наприклад, у широко поширеному методі найменшого значущого біту). У випадку несистематичної організації контейнера такий поділ не можливий. У цьому разі для виділення прихованої інформації необхідно обробляти вміст усієї стеганограми.

За використовуваним принципом приховування методи комп'ютерної стеганографії поділяють на два основних класи: методи безпосередньої заміни і спектральні методи. Якщо перші, використовуючи надлишковість інформаційного середовища в просторовій (для зображення) або часовій (для звуку) області, полягають в заміні малозначимої частини контейнера бітами секретного

повідомлення, то другі для приховування даних використовують спектральне представлення елементів середовища, куди вбудовуються приховувані дані (наприклад, до різних коефіцієнтів дикретно-косинусних перетворень, перетворень Фур'є, Карунена - Лоева, Адамара, Хаара тощо).

Основним напрямком КС є використання властивостей саме надлишковості контейнера-оригінала. Але при цьому треба зважати на те, що при приховуванні інформації відбувається спотворення деяких статистичних властивостей контейнера або ж порушення його структури. В особливу групу можна виділити методи, що використовують спеціальні властивості форматів представлення файлів:

— зарезервовані для розширення поля файлів, які зазвичай заповнюються нулями і зазвичай не враховуються програмою;

— спеціальне форматування даних (зсування слів, речень, абзаців або обирання визначених позицій літер);

— використання незадіяних ділянок на магнітних та оптичних носіях;

— видалення файлових заголовків-ідентифікаторів тощо.

Для таких методів характерні низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

За призначенням розрізнюють стеганометоди власне для прихованого передавання (прихованого збереження) даних і методи для приховування даних у цифрових об'єктах з метою захисту авторських прав на них.

За типами контейнера виділяють стеганографічні методи із контейнерами у вигляді тексту, аудіофайлу, зображення та відео.

Завдання: Розробити програму для стеганографічного шифрування-дешифрування англомовного тексту не менше 20 символів. В якості файлу контейнера можна використовувати відео, аудіо або графічні файли. Можна використовувати будь-яку мову програмування. Віконний або консольний інтерфейс.

Література

1. Конституція України // Урядовий кур'єр, 13 липня 1996 р.

2. Закон України "Про основи національної безпеки України"// Урядовий кур'єр, 30 липня 2003 р.

3. Закон України "Про державну таємницю" від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

4. Закон України "Про інформацію" // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

6. Закон України "Про телекомунікації" від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.

7. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко – К.: МК–Пресс", 2006. – 283 с.

8. С. Синх. Книга кодов. Тайная история кодов и их "взлома" / С. Синх. – М.: ООО "Издательство Астель", 2007. – 447 с.

9. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ "ПоліграфКонсалтинг", 2004. – 216 с.

4. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов.– К.: "МК–Пресс", 2005. – 288 с.

10. Ленков С.В. Методы и средства защиты информации. В 2–х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.– Под ред. В.А. Хорошко.–К.: Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.

11 Ленков С.В. Методы и средства защиты информации. В 2–х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 2. Информационная безопасность. – 344 с.

12. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

13. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.

14. Коваленко М.М. Комп’ютерні віруси і захист інформації. Навчальний посібник / М.М. Коваленко. – К.: Наукова думка, 1999. – 268 с.

15. Каторин О.Ф. Большая энциклопедия промышленного шпионажа / О.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – С.Пб.: ООО "Издательство Полигон", 2000. – 896 с.