ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ КОМП"ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерної інженерії

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ З ДИСЦИПЛІНИ «Технології захисту інформації»

підготовки освітньо–кваліфікаційного рівня «бакалавр» напряму підготовки – 6.050101 Комп'ютерні науки

Укладач:
кандидат фізико–математичних наук,
доцент Касянчук М.М.

Тернопіль–2013

Тема 1. Вступ. Основні поняття та визначення. Законодавство України в галузі захисту інформації.

Структуру законодавства, що регулює відносини із захисту інформації утворюють Конституція України, загальні і спеціальні нормативно-правові акти.

До загальних нормативно-правових актів належать:

Закон України «Про державну таємницю». Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв, порядком доступу до державної таємниці та охороною державної таємниці з метою захисту національної безпеки України.

Закон України «Про інформацію». Він дає визначення інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Закон України «Про науково-технічну інформацію» визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни, регулює правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації.

Закони України «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації». Національна програма інформатизації, невід'ємною частиною якої є інфомаційна безпека, визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Закон України «Про електронні документи та електронний документообіг» встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Спеціальні нормативно-правові акти визначають конкретні методи та засоби захисту інформації, порядок розроблення та експлуатації захищених систем.

Закон України «Про захист інформації в автоматизованих системах». Метою цього Закону є 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.

Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Постанова Кабінету міністрів України від 29.03.2006 р. № 373 «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Ці правила визначають загальні вимоги і організаційні основи забезпечення захисту інформації, що є власністю держави або інформацією з обмеженим доступом.

Указ Президента України «Про Положення про технічний захист інформації в Україні». Це Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Постанова Кабінету міністрів України «Про затвердження Концепції технічного захисту інформації в Україні». Ця Концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами.

Указ Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних», метою якого є підвищення рівня захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення інформаційної безпеки держави.

Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні». Це Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі.

Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про внесення змін до Положення «Про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації» від 30.04.2004, № 30 (далі Наказ).

ДСТУ 4145–2002 Криптографічний захист інформації. Цифорвий підпис, що грунтується на еліптичних кривих. Формування та перевіряння».

Згідно зі ст. 1 Закону України «Про інформацію» інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Держава здійснює контроль за режимом доступу до інформації (ст. 28 Закону «Про інформацію»).

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов (ст. 30).

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

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

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

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист (ст. 30).

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою (ст. 1 Закону України «Про державну таємницю»).

Дамо визначення таким важливим поняттям, як допуск та доступ до секретної інфориації (ст. 1 того ж Закону):

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв (ст. 1).

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 (та ж стаття).

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації (та ж стаття).

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

– дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

– обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

– обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

– особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний та криптографічний захисти секретної інформації (ст. 18 того ж Закону).

Органи державної влади, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею (ст. 20).

Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як:

– розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю;

– порушення порядку зберігання інформації;

– навмисне знищення інформації;

– необгрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом;

– порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (ст. 47 Закону України «Про інформацію»).

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (ст.5 Закону України «Про електронні документи та електронний докумнтообіг»). Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису (ст. 12). Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу (ст. 6). Це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних. Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору

електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Де особистий ключ – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу, а відкритий ключ – це параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису (ст. 1 Закону України «Про електронний цифровий підпис»).

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

– електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

– під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

– особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті (ст. 3). Тобто у документі, що виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача (ст. 1).

Тема 2. Принципи криптографічного захисту інформації. Класичні симетричні криптосистеми.

Для позначення всієї оласті таємного зв'язку використовується термін криптологія, який походить від грецьких коренів «cryptos» – таємний та «logos» – повідомлення. Криптологія поділяється на дві області: криптографію та криптоаналіз. Завдання криптографа – забезпечити конфіденційність та аутентичність повідомлень, які передаються по каналах зв'язку. Завдання криптоаналітика – зламати систему захисту, розроблену криптографами без знання ключа. Ключ – це певний секретний стан деяких параметрів алгоритму криптографічного перетворення даних, які забезпечують вибір тільки одного варіанту із всіх можливих варіантів для даного алгоритму. На даний час розрізняється два класи криптосистем: симетричні одноключові криптосистеми (з секретним ключем) та асиметричні двохключові криптосистеми (з відкритим ключем). В симетричних криптосистемах один і той самий ключ використовується як для шифрування, так і для розшифровування даних. В асиметричних криптосистемах для шифрування і розшифровування використовуються різні, але взаємопов'язані, ключі, причому визначити один ключ, знаючи інший, практично неможливо.

До шифрів, які використовуються для криптографічного захисту інформації, представляється ряд певних вимог:

1. Достатня криптостійкість.
2. Простота шифрування та розшифровування.
3. Незначна надлишковість інформації в зв'язку з шифруванням.
4. Нечуттєвість до незначних помилок шифрування.

Криптологія є частиною такої науки, яка називається захистом інформації, яка охоплює, крім теоретичних основ, також технічні засоби, юридичні аспекти тощо. Тайнопис також є ширшим поняттям, оскільки охоплює також приховування самого факту існування повідомлень.

Будь–яка спроба зі сторони зловмисника розшифрувати шифртекст для отримання відкритого тексту або зашифрувати свій власний текст для отримання правдоподібного шифртексту, не знаючи істинного ключа, називається криптоаналітичною атакою. Фундаментальне правило криптоаналізу, вперше сформульоване у 19 ст. голандцем А.Керкхоффом полягає в тому, стійкість шифру або криптосистеми повинна визначатися тільки секретністю ключа. Іншими словами, це означає, що весь алгоритм шифрування, крім секретного ключа, відомий криптоаналітику зловмисника. Це пояснюється тим, що криптосистема, яка являє собою сукупність апаратних і програмних засобів, яку можна змінити тільки при значних затратах часу і засобів, тоді як ключ змінюється дуже легко.

Існують такі типи криптоаналітичних атак:

1. Криптоаналітична атака при наявності тільки відомого шифртексту.
2. Криптоаналітична атака при наявності відомого відкритого тексту.
3. Криптоаналітична атака при можливості вибору відкритого тексту.
4. Криптоаналітична атака з адаптивним вибором відкритого тексту.
5. Криптоаналітична атака з використанням вибраного шифртексту.
6. Криптоаналітична атака методом повного перебору всіх можливих ключів (брутальна атака).

При шифруванні перестановкою символи відкритого тексту переставляються за визначеним правилом в межах блоку цього тексту. Шифри перестановки є найпростішими та найдревнішими шифрами.

Найдревніший шифр – шифр скитала використовувався в 5 ст. до нашої ери правителями Спарти. На циліндричний стержень спіраллю намотувалась стрічка пергаменту і вздовж стержня писали повідомлення. Тді пергамент знімали і отримували хаотично розміщені букви. Ключем був діаметр валика.

Пізніше почали використовувати шифр частоколу. Наприклад:

р п о р ф я
к и т г а і

Отримується шифртекст: рпосфякитгаі. Ключем є висота частоколу. Зокрема, для частоколу висотою 3 маємо (ліворуч):

и г і и о а я
р п о р ф я р т р і
к т а к п г ф

Отримується шифртекст: ігірпорфякта. Це складний частокіл. При використанні простого частоколу отримуємо: иоаяртрікпгф. аналогічно можна використати частокіл і більшої висоти.

З кінця 14 ст. виникли шифруючі таблиці. Наприклад, відкритий текст записується в таблицю по стовбцях, а читається по рядках. Ключем є розмір таблиці. Їх удосконаленням стали шифруючі таблиці з ключовими словами, коли стовбці та рядки переставляються у відповідності до цих ключових слів.

		л	і	т	о
		2	1	4	3
з	2	п	р	и	л
и	3	і	т	а	ю
м	4	в	о	с	ь
а	1	м	о	г	о

		і	л	о	т
		1	2	3	4
з	2	р	п	л	и
и	3	т	і	ю	а
м	4	о	в	ь	с
а	1	о	м	о	г

1	о	м	о	г
2	р	п	л	и
3	т	і	ю	а
4	о	в	ь	с

В середні віки використовувалося також шифрування за допомогою магічних квадратів. Це квадратні таблиці з вписаними в клітинки послідовностями натуральних чисел, починаючи з 1, щоб їх сума по стовбцях, рядках та діагоналях дорівнювала одному і тому самому числу.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

о	и	р	м
і	о	с	ю
в	т	а	ь
л	г	о	п

Якщо не враховувати повороти, то існує тільки один квадрат розміром 3х3, 880 – розміром 4х4, біля 250000 – розміром 5х5.

Шифр Кардано являє квадрат з клітинками, частина яких вирізані. Цей квадрат накладають на такий самий суцільний квадрат і у вирізані клітинки вписують текст. Потім верхній квадрат повертають на 90 градусів і відкриваються нові клітинки. Таким чином заповнюється вся таблиця. Ключем у шифрі Кардано є розміщення вирізаних клітин. У кожному рядку і стовбці може бути вирізана тільки одна клітинка і кількість клітинок у рядку і стовбці має бути парною.

До шифрів простої заміни відноситься шифр Цезаря, шифр Цезаря з ключовим словом, полібіанський квадрат, шифруючі таблиці Трисемуса.

Шифри складної заміни називають багатоалфавітними, оскільки для шифрування кожного символа вихідного повідомлення використовують свій шифр простої заміни.

Шифр Гронсфельда являє собою модифікацію шифра Цезаря з числовим ключем. Під буквами вихідного повідомлення записують цифри ключового слова. Якщо ключ коротший, то його запис циклічно повторюють. Шифртекст отримують аналогічно шифру зсуву, але кожен символ зсувають на ту кількість знаків, яка записана під символом. Потрібно відмітити, що шифр Гронсфельда зламується досить легко, але його можна вдосконалити, зокрема, подвійним шифруванням різними ключами.

Біграмний шифр Плейфейра, винайдений у 1854 році, використовує прямокутну таблицю з хаотично або з ключовим словом вписаними буквами алфавіту. Відкритий текст розбивається на біграми. Він повинен мати парну кількість символів і не містити біграм з однаковими буквами. В таблиці шукаються букви біграми і вважається, що вони є вершинами прямокутника. У двох інших вершинах будуть лежати дві букви шифртексту. Якщо букви відкритого тексту потрапляють в один рядок чи стовбець, то вибираються букви, що лежать під ними, або, відповідно, ліворуч.

Для усунення такого недоліку використовується подвійний квадрат Уїтстона, в якому використовується дві прямокутних таблиці з розміщеними буквами алфавіту. Букви відкритого тексту шукаються в різних таблицях і аналогічно утворюються прямокутники. Тепер букви відкритого тексту не потраплять в один стовбець, але можуть потрапити в один рядок. Для усунення цього недоліку використовується шифр чотирьох квадратів, розміщених в квадратах. Букви відкритого тексту шукаються в діагонально протилежних квадратах, в інших квадратах шукаються букви шифртексту. Тепер ні в один рядок, ні в один стовбець букви відкритого тексту не потраплять.

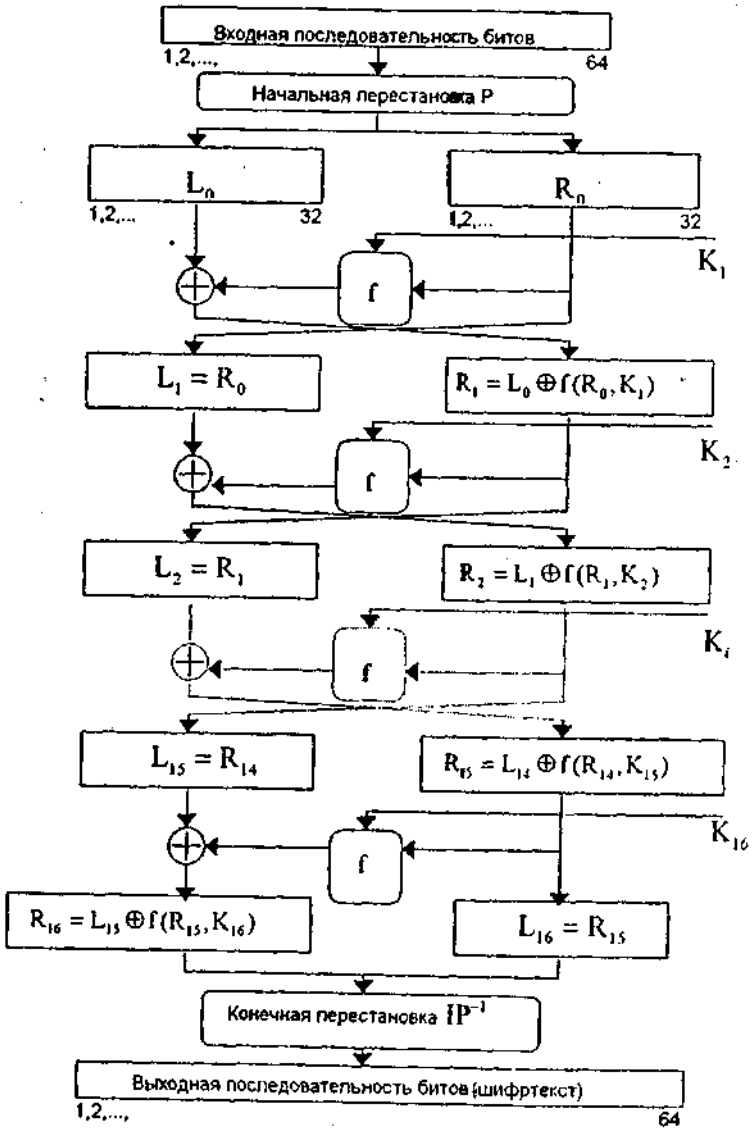
Узагальненням цих шифрів є шифр Віженера. він представляється квадратною таблицею Віженера, розмірність якої відповідає кількості букв в алфавіті. По горизонталі розміщуються букви відкритого тексту, по вертикалі – букви ключа. На їх перетині отримуємо букви шифртексту. Його удосконаленням є шифр Віженера з автоключем.

Для застосування шифру одноразового блокноту відкритий текст та ключ переводять у цифрову форму. Кожній букві відповідає її номер в алфавіті, нумерація починається з нуля. Потім це число переводять у двійкову форму. Для шифрування використовується додавання бітів по модулю 2. Операція позначається $\oplus$ і задається так: $0\oplus0=0$, $1\oplus0=1$, $0\oplus1=1$, $1\oplus1=1$. Ключем може служити довільне двійкове слово однакової довжини з відкритим текстом. Криптотекст отримують побітовим додаванням відкритого тексту та ключа за модулем 2. Дешифрування збігається із шифруванням. Щоб отримати відкритий текст, до криптотексту знову потрібно додати двійковий ключ. Шифр одноразового блокноту не є однозначним, оскільки той самий шифртекст можна отримати для деякого іншого відкритого тексту та іншого ключа.

Назва шифру походить від того, що агент, який здійснював шифрування вручну, отримував свої копії ключів, записаними в блокнот. Якщо ключ застосовувався, то сторінка з ним знищувалась.

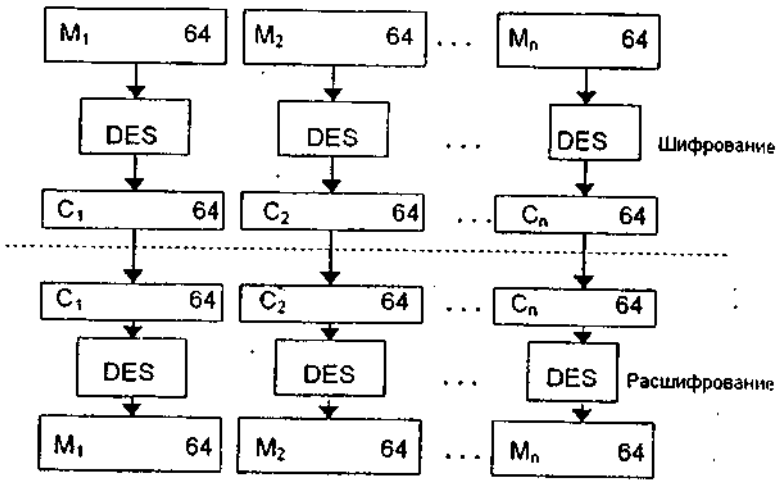
Тема 3. Сучасні симетичні криптосистеми. Алгоритм DES.

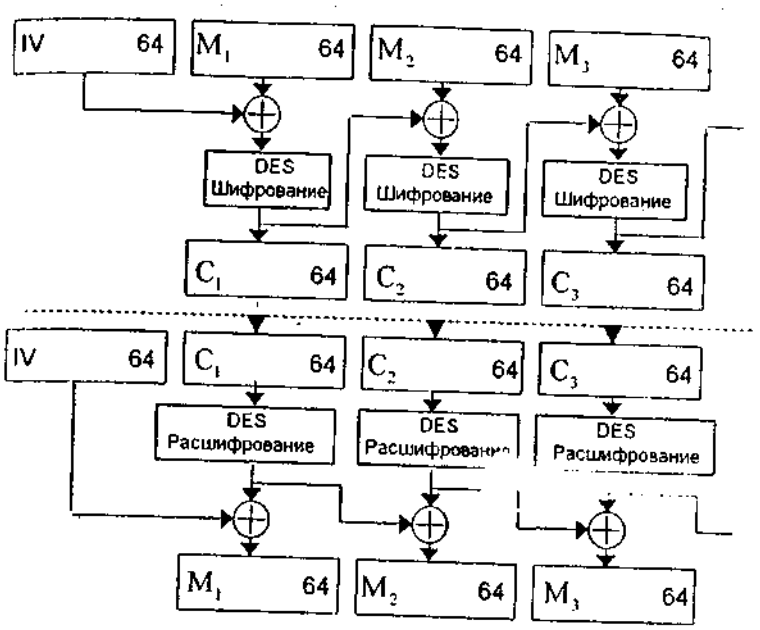
Стандарт шифрування даних DES (Data Encryption Standard) опублікований у 1977 році Національним бюро стандартів США і призначений для захисту від несанкціонованого доступу до важливої, але несекретної інформації в державних і комерційних установах США. При його використано такі позначення: L і R – ліва та права послідовності бітів; LR – конкатенація послідовностей; $\oplus$ – побітове додавання по модулю 2. Алгоритм використовує комбінацію підстановок і перестановок. Шифрування здійснюється 64–бітовими блоками за допомогою 64–бітового ключа, в якому значущими є 56 біт, решта 8 – перевірочні. На рис. зображено структуру алгоритму DES.

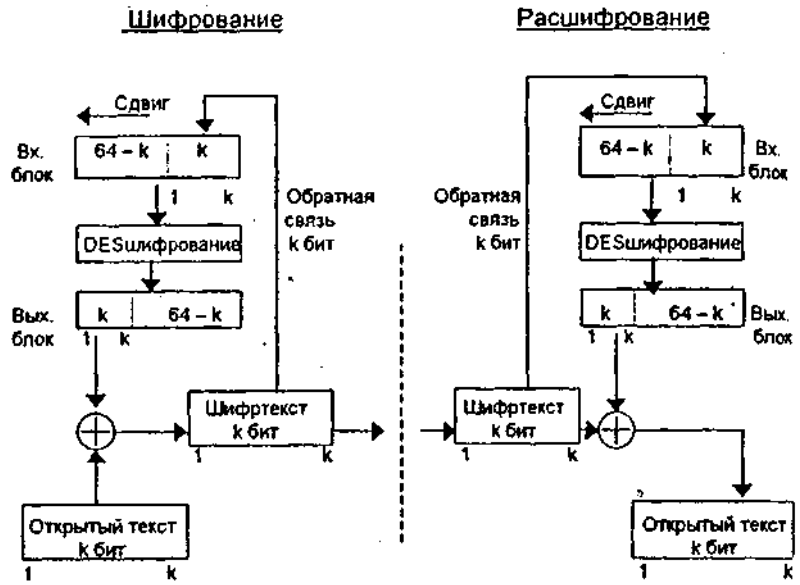


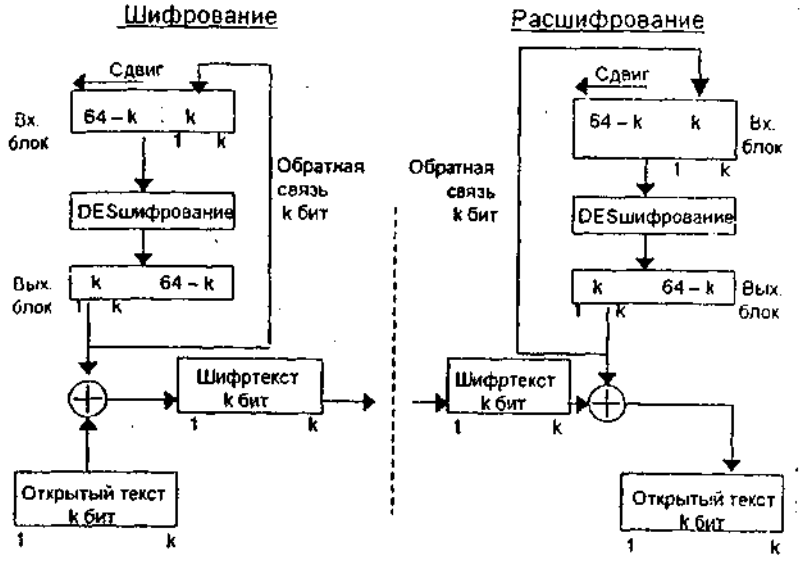
Початковий 64–бітовий блок перетворюється за допомогою матриці початкової перестановки. Потім виконується ітеративний процес шифрування, що складається з 16 циклів. Після них виконується кінцева перестановки у відповідності з матрицею кінцевої перестановки. Для виконання алгоритму потрібно 16 ключів, які генеруються з 56–бітового ключа.

Існує 4 режими роботи алгоритму DES: електронна кодова книга (ECB), зчеплення блоків шифру (CBC), зворотній зв'язок по шифртексту (CFB), зворотній зв'язок по виходу (OFB). Їх схеми відповідно зображені на рисунках.




IV 64
M1 64
M2 64
M3 64
DES Шифрование
C1 64
C2 64
C3 64
DES Расшифрование
M1 64
M2 64
M3 64


Шифрование
Расшифрование
Сдвиг
Вх. блок
64 – k
k
Обратная связь k бит
DESшифрование
Вых. блок
Шифртекст k бит
Открытый текст k бит
1
k


Шифрование
Расшифрование
Сдвиг
Вх. блок
64 – k
k
Обратная связь k бит
DESшифрование
Вых. блок
Шифртекст k бит
Открытый текст k бит
1
k

Тема 4. Сучасні симетичні криптосистеми. Алгоритм IDEA, стандарт шифрування ГОСТ 28147–89. Сімейство алгоритмів RC.

Алгоритм IDEA (International Data Encryption Algorithm) є блоковим шифром. Він оперує 64–бітовими блоками відкритого тексту. Його ключ має 128 біт. Один і той же алгоритм використовується і для шифрування, і для розшифровування. В алгоритмі використовуються такі математичні операції: побітове додавання по модулю 2; додавання беззнакових цілих по модулю 2^{16}; множення цілих по модулю (2^{16} +1). Всі операції виконуються над 16–бітовими підблоками. Ці три операції несумісні в тому, що ніяка пара з цих трьох операцій не задовольняє асоціативному та дистрибутивному законам. Всього виконується 8 циклів.

Комбінування цих трьох операцій забезпечує комплексне перетворення входу, істотно затрудняючи криптоаналіз IDEA в порівнянні з DES, який базується тільки на побітовому додаванні по модулю 2.

Алгоритм IDEA використовує 52 підключі (по шість для кожного з 8 циклів і чотири для перетворення виходу). Розшифрування здійскнюється в зворотньому порядку.

Алгоритм IDEA може працювати в тих же режимах, що і DES, однак має ряд переваг. Він значно безпечніший DES, оскільки має вдвічі більший ключ. Його внутрішня структура забезпечує кращу стійкість до криптоаналізу. Програмні реалізації IDEA приблизно вдвічі швидші, ніж DES.

Стандарт шифрування ГОСТ 28147–89 являє собою 64–бітовий блочний алгоритм з 256–бітовим ключем. Використовуються такі операції: побітове додавання по модулю 2; операція додавання по модулю 2^{32} двох 32–розрядних двійкових чисел; операція додавання двох 32–розрядних чисел за модулем 2^{32}-1.

Алгоритм передбачає чотири режими роботи:

1. Шифрування даних в режимі простої заміни.
2. Шифрування даних в режимі гамування.
3. Шифрування даних в режимі гамування із зворотним зв’язком.
4. Вироблення імітовставки.

RC–4 являє собою потоковий шифр із змінною довжиною ключа. Алгоритм працює в режимі зворотнього зв’язку по виходу (OFB). Ключова послідовність не залежить від вихідного тексту. Структура алгоритму включає блок заміни розмірністю 8x8, який являє собою залежну від ключа перестановку чисел 0, ..., 255 змінної довжини. Є два лічильники i та j, початкове значення яких дорівнює 0. На початку генерується псевдовипадковий байт, який потім додається по модулю 2 з байтом вихідного тексту для отримання шифртексту. Ініціалізація блоку заміни виконується за допомогою ключа. За програмною реалізацією алгоритм RC–4 приблизно в 10 разів швидший від DES. Можливі узагальнення алгоритму на більшу довжину слів і розмір блоку заміни. Можна побудувати шифр з блоком заміни розмірністю 16x16 (потрібно 128 Кбайт пам’яті) і довжиною слова 16 біт. Етап ініціалізації буде відбуватися значно повільніше, але в результаті алгоритм все одно буде швидшим.

В алгоритмі RC–6 передбачено використання чотирьох робочих регістрів, а також введена операція цілочисельного множення, яка дозволяє збільшити збурення, створене кожним циклом шифрування, що приводить до збільшення стійкості та можливості зменшити число циклів.

RC–6 є повністю параметризованим алгоритмом шифрування. Конкретна версія RC–6 позначається як RC–6–w/r/b, w позначає довжину слова в бітах, r – ненульова кількість ітераційних циклів шифрування, b – довжина ключа в байтах. У всіх варіантах RC–6–w/r/b працює з чотирма w – бітовими словами, використовуючи шість базових операцій, які позначаються таким чином:

a+b – цілочисельне додавання по модулю 2^w;

a-b – цілочисельне віднімання по модулю 2^w;

a⊕b – побітове виключаюче або w–бітових слів;

a×b – цілочисельне множення по модулю 2^w;

a<<b – циклічний зсув w–бітового слова ліворуч на величину, задану $\log_2 w$ молодшими бітами b;

a>>b – циклічний зсув w–бітового слова праворуч на величину, задану $\log_2 w$ молодшими бітами b.

Алгоритм обчислення ключів виглядає таким чином. Користувач задає ключ довжиною b байтів. Достатня кількість ненульових байтів дописується в кінець, щоб отримати ціле число слів. Потім ці байти записуються, починаючи з молодшого, в масив з c слів.

Структура шифру RC–6 є узагальненням мережі Фейстела. Блок тексту розбивається не на 2, а на 4 підблоки і на кожній ітерації змінюються два підблоки з чотирьох. При цьому в кінці ітерації шифрування відбувається циклічний зсув підблоків ліворуч (при розшифруванні відповідно праворуч). Це узагальнення привело до того, що була втрачена властивість інваріантності блоків шифрування і розшифровки, хоча це не є визначальним в оцінці даного алгоритму.

Тема 5. Принципи асиметричних криптосистем.

Для будь-якого цілого a і натурального b однозначно визначені цілі числа *q* і r такі, що a = *bq* + *r* і *0* < *r* < *b*. Число q називається *часткою,* а r – *остачею* від ділення a на b Наприклад, рівність –20= (–1)·67 + 47 означає, що –20 при діленні на 67 дає частку –1 і остачу 47. Для остачі будемо вживати таке позначення r = a mod *b*. Число r будемо також називати *(зведеним) лишком* числа a за модулем b. Числа *a* і b називаються *взаємно простими,* якщо НСД (a, b) = 1. *Алгоритм Евкліда* (3 ст. до н.е.) для знаходження НСД двох натуральних чисел a і *b* грунтується на співвідношеннях

НСД (a, b*)* = НСД (a, a mod b*)* для a > b

НСД(a,0) = a

Продемонструємо ідею цього алгоритму на прикладі.

ПРИКЛАД. Щоб знайти НСД (211, 79), застосовуємо алгоритм Евкліда. Робота алгоритму зводиться до кількаразового ділення з остачею:

$$211 = 79\cdot 2 + 53$$
$$79 = 53\cdot 1 + 26$$
$$53 = 26\cdot 2 + 1$$
$$26 = 1\cdot 26 + 0$$

Маємо НСД (211, 79) = НСД (79, 53) = НСД (53, 26) = НСД (26,1) = НСД(1,0) = 1.

Алгоритм Евкліда дає такий наслідок.

ТВЕРДЖЕННЯ 2.2. *Для кожної пари взаємно простих чисел a і b можна знайти такі цілі u і v, що ua + vb* = 1.

ПРИКЛАД. Нехай a = 211, *b* = 79. Протокол роботи алгоритму Евкліда виписаний у попередньому прикладі. Рухаючись знизу вверх, отримуємо

$$1 = 1 \cdot 53 + (-2) \cdot 26 = 1 \cdot 53 + (-2) \cdot (79 - 1 \cdot 53) = (-2) \cdot 79 + 3 \cdot 53 = (-2) \cdot 79 + 3 \cdot (211 - 2 \cdot 79) = 3 \cdot 211 + (-8) \cdot 79.$$

Отже, *u* = 3 і *v*= – 8.

Елемент, обернений до x за модулем n відносно множення, будемо позначати через x^{-1} mod n або просто x^{-1}. Це означає, що $x\cdot x^{-1} \bmod n = 1$.

ПРИКЛАД. Нехай ми хочемо знайти елемент, обернений до 79 за модулем 211. Вище була отримана рівність 1 = 3·211 + (– 8·79. З неї випливає, що (–8)·79 = 1(mod211). Отже, 79^{-1} mod 211 = (-5) mod 211 = 203.

Функцією Ейлера від числа n є кількість натуральних чисел, взаємно простих з n і позначається $\phi(n)$.

ТЕОРЕМА ЕЙЛЕРА (1763). *Для взаємно простих цілого x і натурального n справедлива конгруенція* $x^{\phi(n)} = 1 \pmod n$.

МАЛА ТЕОРЕМА ФЕРМА (1640). *Якщо ціле x не ділиться на просте p, то* $x^{p-1} = 1 \pmod p$.

КИТАЙСЬКА ТЕОРЕМА ПРО ОСТАЧІ (І СТ. ДО Н.Е.). *Для будь-якої пари взаємно простих натуральних чисел n_1 і n_2 та для будь-якої пари цілих чисел x_1* і x_2, *можна знайти таке ціле x, що* $x = x_1 \pmod{n_1}$ і $x = x_2 \pmod{n_2}$.

ПРИКЛАД. Нехай ми хочемо знайти ціле *x,* яке при діленні на 211 давало б остачу 100, а при діленні на 79 остачу 10. Вище була отримана рівність $1 = 3\cdot211 + (-8)\cdot79$. Отже, в якості *x* можна взяти: $10\cdot3\cdot211 + 100\cdot(-8)\cdot79 = -56870$. Зрозуміло, що це число можна замінити його остачею від ділення на $211\cdot79 = 16669$. В результаті отримуємо 9806.

Тема 6. Криптосистема RSA.

Запропонована 1977 року система RSA є чи не найполулярнішою криптосистемою з відкритим ключем. Назва системи утворена з перших літер імен її винахідників — Рональда Райвеста, Алі Шаміра та Леонарда Адлемана.

Генерування ключів. Вибирають два досить великі прості числа *p* і q. Для їх добутку $n = pq$ значення функції Ейлера дорівнює $\varphi(n) = (p-1)(q-1) = n-p-q+1$. Далі випадковим чином вибирають елемент e, що не перевищує значення $\phi(n)$ і взаємно простий з ним. Для e за алгоритмом Евкліда знаходять елемент *d,* обернений до e за модулем $\phi(n)$, тобто $ed = 1 \pmod{\phi(n)}$.

Як результат покладають:

Відкритий ключ: e, n.

Таємний ключ: d.

Шифрування відбувається блоками. Для цього повідомлення записують у цифровій формі і розбивають на блоки так, що кожен блок позначав число, яке не перевищує *n.* Алгоритм шифрування *E* у системі RSA полягає у піднесенні *M* до степеня e. Записуємо це так: $E(M) = M^e \bmod n$. В результаті отримується блок криптотексту $C = E(M)$.

Дешифрування. Алгоритм дешифрування *D* блоку криптотексту *C* полягає у піднесенні *C* до степеня *d,* тобто

$$D(C) = C^d \bmod n.$$

ПРИКЛАД 2.1. Нехай p = 53 і $q = 67$. Тоді $n = 3551$ і $\varphi(n) = 3432$. Візьмемо e = 1021 — за допомогою розширеного алгоритму Евкліда легко перевірити, що НСД (1021,3432) = 1. Одночасно обчислюємо $d = 1021^{-1} \bmod 3432 = 1237$. Ключі вибрано.

Відкритий ключ e = 1021 і n = 3551 оприлюднюємо. Тепер будь-хто може послати нам зашифроване повідомлення. Припустимо, один із ділових партнерів вирішив послати нам вказівку ПРОДАЙ. Спочатку він перетворює своє повідомлення у цифрову форму, замінюючи кожну літеру її двоцифровим десятковим номером в алфавіті: 1920 1805 0013. Видно, що з нашим модулем *n* цифрове повідомлення варто розбивати на блоки по 4 цифри, як це і зроблено. При шифруванні перший блок 1920 перетворюється у $1920^{1021} \bmod 3551 = 2393$. Таким же чином шифруються наступні два блоки, і в результаті виходить криптотекст 2393 17S8 2188.

Отримавши цей криптотекст, проводимо дешифрування піднесенням кожного блоку до степеня $d = 1237$ за модулем $n = 3551$. Можна переконатись, що $2393^{1237} \bmod 3551 = 1920$ і т.д.

Тема 7. Криптосистема Ель–Гамаля.

Генерування ключів. Вибирають велике просте p, а також просте число g, $1 < g < p - 1$. Ці числа не є таємницею і перебувають в загальному користуванні. Кожен абонент вибирає собі випадкове число a у проміжку від 1 до p–1, і обчислює $h = g^a \bmod p$.

Відкритий ключ: p, g, h.

Таємний ключ: a.

Шифрування відбувається блоками. Кожен блок *M* не повинен перевищувати p.

- Вибирають випадкове число r таке, що $1 < r < p - 1$.

• Обчислюють $C = (c_1, c_2)$, де

$$c_1 = g^r \bmod p, \quad c_2 = Mh^r \bmod p.$$

Дешифрування. Маючи таємний ключ a і криптотекст $C = (c_1, c_2)$, обчислюють:

$$M = c_2 \cdot (c_1^{-1})^a \bmod p$$

Приклад. Нехай p=23, g=5, a=6. Обчислюємо $h=5^6 \bmod 23=8$. Відкритий і таємний ключ сформовано.

Припустимо, що шифрується числова інформація, і потрібно зашифрувати повідомлення $M = 7$. Нехай вибрано r = 10. Тоді $c_1 = 5^{10} \bmod 23 = 9$ і $c_2 = (7 \cdot 8^{10}) \bmod 23 = 21$. Отримуємо криптотекст $C = (9,21)$. Що стосується дешифрування, то легко перевірити, що справді $D(9,21) = 21 \cdot (9^6)^{-1} \bmod 23 = 7$.

Тема 8. Криптосистема Рабіна.

Генерування ключів. Вибирають два великі прості числа *p* і *q*. Обчислюють їх добуток *n = pq*. Покладають

Відкритий ключ: n .

Таємний ключ: p, q.

Шифрування відбувається блоками подібно до системи RSA, згідно з формулою

$$E(M) = M^2 \bmod л.$$

Алгоритм дешифрування складніший, тому розглянемо його на прикладі.

Нехай таємний ключ вибрано так: $p = 53$ і q = 67. Тоді відкритим ключем буде $n = 3551$.

Розглянемо шифрування повідомлення ПРОДАЙ. Спочатку повідомлення записується у цифровій формі і розбивається на блоки по чотири цифри: 1920 1805 0013. Поший блок 1920 перетворюється у $1920^2 \bmod 3551 = 0462$. Подібно шифруються наступні два блоки, і в результаті виходить криптотекст: 0462 1758 0169.

Припустимо тепер, що ми отримали криптотекст 1497. Для шифрування слід з нього добути квадратні корені за модулем 3551. З цією метою добуваємо корені за простими модулями 53 і 67 із лишків $1497 \bmod 53 = 13$ і $1497 \bmod 67 = 23$, відповідно. Знаходимо $\sqrt{13} \bmod 53 = 15, 38$ і $\sqrt{23} \bmod 67 = 31, 36$. За допомогою алгоритму з Китайської теореми про остачі визначаємо чотири корені з 1497 за модулем 3551: (15,31) = 0969, (15,36) = 1711, (38,31) = 1840, (38,36) = 2582. Як зразу видно, лише другий корінь є числовим еквівалентом тексту в українській абетці, а саме повідомлення НІ.

Тема 9. Криптографічні протоколи .

Обмін ключем.

Нехай абоненти А і Б, які, спілкуючись через канал, що ймовірно прослуховується, хочуть домовитися про спільний таємний ключ. Тоді:

- абонент А вибирає велике просте число p та просте $1<g<p-1$ і відкрито, не роблячи з цього жодної таємниці, посилає p і g абонентові Б;
- абонент А вибирає випадкове число *a* в межах від 1 до p – 1, а абонент Б –випадкове число *b* в тих же межах;
- абонент А обчислює $g^a \bmod p$ і посилає це значення абонентові Б, який обчислює $g^b \bmod p$ і теж посилає абоненту А;
- обидва абоненти обчислюють одне і теж число

$$(g^b)^a \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p,$$

яке і приймають в якості ключа.

ПРИКЛАД. Нехай p = 97, а g = 5. Припустимо, що абонент А вибрав число a = 12, а абонент Б вибрав b = 63. Тоді абонент А посилає абоненту Б $5^{12} \bmod 97 = 42$, абонент Б абоненту А $5^{63} \bmod 97 = 75$, і обоє обчислюють $75^{12} \bmod 97 = 42^{63} \bmod 97 = 21$.

Жереб по телефону

• абонент А вибирає своє число *a* і пару ключів *(K,K')*. Після цього зашифровує *a* і

результат $c = E_K(a)$ разом з ключем К посилає абоненту Б;

- абонент Б вибирає число b і посилає його абоненту А;
- абонент А посилає абоненту Б дешифруючий ключ К';
- абонент Б перевіряє, що (K,K') справді є парою шифруючого та дешифруючого ключів, і обчислює $a = D_{K'}(c)$.
- Обоє обчислюють $R = a \oplus b$.

Гра в карти заочно:

- абоненти А і Б досягають згоди про кодування карт словами $M_1,..., M_{52}$, і домовляються, яка саме комутативна криптосистема буде використовуватись;
- Обоє таємно один від другого вибирають собі шифруючий та дешифруючий ключі;
- абонент А зашифровує повідомлення $M_1,..., M_{52}$, перемішує випадковим чином крнптотексти $E_A(M_1), ..., E_A\{M_{52}\}$ і посилає їх абоненту Б;
- абонент Б вибирає випадкові п'ять криптотекстів, і посилає їх назад абоненту А. Це карти, якими буде грати абонент А;
- із карт, що залишилися, абонент Б вибирає ще п'ять для себе;
- абонент Б зашифровує відібрані карти за допомогою власного ключа і отримані криптотексти посилає абоненту А;
- абонент А дешифрує отримані криптотексти і повертає абоненту Б результат;
- абонент Б дешифрує надіслані абонентом А криптотексти і отримує свою п'ятірку карт;
- в кінці гри абоненти обмінюються ключами і перевіряють, чи ніхто з них не хитрував.

Розподіл таємниці.

Нехай натуральне число s є цінною секретною інформацією (номер рахунку у швейцарському банку, код команди на запуск балістичної ракети тощо). Завданням протоколу є так подрібнити секрет s на частини, по одній для кожного із n учасників, щоб будь-які k учасників могли відновити s, поєднавши свої частинки, але щоб ніяка група з $k - 1$ учасника цього зробити не могла.

Вибирають досить велике просте число p, більше за s. Покладають $a_0 = s$, і вибирають випадковим чином числа $a_1,...., a_{k-1}$. Нехай $f(x) = \Sigma_{0\le i<k} a_i x^i$ – многочлен від змінної x. і-ий учасник протоколу, де $1 \le i \le n$, отримує значення $s_i = f(i)$.

Якщо відомі довільні k значень $f(i_1), \ldots, f(i_k)$, то многочлен f можна реконструювати за інтерполяційною формулою Лагранжа:

$$f(x) = \sum_{i=1}^{k} f(i_1) \prod_{j \neq 1} \frac{x - i_j}{i_i - i_j}.$$

Після цього легко знаходиться секрет $s = a_0 = f(0)$.

Знання лише k - 1 значення функцій f не дає *жодної* інформації про секрет.

Тема 10. Проблема ідентифікації та аутентифікації користувача. Електронний цифровий підпис.

В системі RSA кожен абонент має пару ключів – загальновідомий відкритий і таємний, який знає лише абонент і ніхто інший. Таким чином, будь-хто може скористатися алгоритмом шифрування E_x абонента X, але тільки він сам володіє алгоритмом дешифрування D_x. Важливим є виконання таких співвідношень для довільного повідомлення M: $D_x(E_x(M)) = E_x(D_x(M)) = M$.

Ці співвідношення зводяться до рівностей $(M^{ex})^{dx} = (M^{dx})^{cx} = M$ і виражають той факт, що шифруюче відображення Ex та дешифруюче Dx є взаємно оберненими.

Припустимо тепер, що абонент А хоче послати абонентові Б повідомлення M таким чином, щоб той був певен, що повідомлення справді послане абонентом А. Для цього пропонується такий протокол, в якому (E_A, D_A) та (E_B, A_B) — алгоритми шифрування та дешифрування абонентів А та Б.

- Абонент А обчислює $C = E_B(D_A(M))$ і посилає C абонентові Б.

- Абонент Б, отримавши С, обчислює $M = E_A(D_B(C))$.

Коректність протоколу зводиться до рівності $E_A(D_B(E_B(D_A(M)))) = M$.

Підпис у системі Ель–Гамаля.

Для генерування ключів *в*ибирають велике просте p, а також просте число g, $1 < g < p–1$. Числа *p* і g не є таємницею і перебувають в загальному користуванні. Кожен абонент вибирає собі випадкове число *a* у проміжку від 1 до *p*–1, і обчислює $h = g^a \bmod p$.

Відкритий клюй: p, g, h. Таємний клюй: a.

Підписування. Абонент А виробляє свій підпис *S* на повідомленні *M* таким чином:

- вибирає випадкове число 1<r<p-1;
- обчислює $s_1 = g^r \bmod p$;
- обчислює $r' = r^{-1} \bmod (p - 1)$;
- обчислює $s_2 = (M — as_1)r' \bmod (p — 1)$;
- покладає $S = (s_1, s_2)$.

Підтвердження підпису.

- Абонент Б перевіряє, чи $g^M = h^{S1}s_1^{S2} (\bmod p)$.

DSA.

Запропонований у 1991 році.

Генерування ключів. Вибирають велике просте число p таке, що p – 1 має досить великий простий дільник *q*. Стандарт вимагає, щоб $2^{512} < p < 2^{1024}$ і $q > 2^{160}$. Далі вибирають довільний елемент *h* порядку *q*. Параметри *p, q, h* не становлять таємниці і є спільними для всіх абонентів мережі.

Абонент А вибирає випадкове число *a* в діапазоні від 0 до *q* – 1 і обчислює число $b = h^a \bmod p$. Його ключі формуються так.

Відкритий КЛЮЧ: b таке, що $b = h^a \bmod p$.

Таємний ключ: a.

Підписування. Алгоритм підписування використовує вкорочуючу функцію f з довжиною вкорочення 160 бітів. Щоб виробити свій підпис *S* для повідомлення M, абонент А:

- вибирає випадкове число r в діапазоні від 0 до q-1;
- обчислює $r' = r^{-1} \bmod q$;
- обчислює $s_1 = (h^r \bmod p) \bmod q$;
- обчислює $s_2 = (r'(f(M) + as_1)) \bmod q$;
- формує підпис $S = (s_1, s_2)$.

Підтвердження підпису. Отримавши повідомлення *M* із підписом $S = (s_1,.s_2)$, абонент Б:

- обчислює $s' = S_2^{-1} \bmod q$;
- обчислює $u_1 = (f(M)s') \bmod q$;
- обчислює $u_2 = (s_1 \cdot s') \bmod q$;
- обчислює $t = (h^{U1} \cdot b^{U2} \bmod p) \bmod q$;
- перевіряє рівність $t = s_1$.

Тема 11. Парольна та біометрична ідентифікація

Захист інформації за допомогою пароля є одним з найпростіших з точки зору реалізації типів захисту.

Принцип роботи парольного захисту полягає в наступному: при запуску ПП з реалізованим парольним захистом, користувачу пропонується ввести з клавіатури пароль (код, секретне слово, комбінація секретних символів). Після введення пароля відбувається процедура його порівняння з певним еталоном та надання або відхилення доступу до програмного продукту.

Основною проблемою при парольному захисті є проблема зберігання паролів. У більшості випадків паролі зберігаються у коді програми або в окремому файлі в відкритому чи зашифрованому вигляді. Необхідно відмітити що пароль, який знаходиться в відкомпільованій програмі змінити не можливо, тоді як пароль у файлі можна змінювати.

В більшості випадків парольний захист програмний продуктів реалізовується одноманітно і для його зламу необхідно 10-15 хвилин.

Для запобігання такого швидкого зламу при реалізації захисту ПП необхідно дотримуватись таких принципів:

1. Не застосовуйте стандартні функції, особливо API-функції і компоненти VCL, оскільки сучасні дисасемблери вміють розпізнавати стандартні процедури високорівневих мов програмування.
2. Застосовуйте нестандартний спосіб введення пароля. Найпростішим прикладом може служити розробка власного візуального компоненту для введення пароля.
3. Не зберігайте пароль в одному місці, оскільки при цьому досить легко встановити точку зупинки на зону пам'яті, в якій розміщено введений пароль.
4. Не зберігайте пароль у вигляді відкритого тексту. Для правильної реалізації цього принципу можна оголосити в програмі 5-10 змінний типу STRING і після введення пароля переписати його у ці змінні при цьому ці змінні можна розкидати по різних частинах програмного коду. При такому підході пошук пароля дасть багато адрес по яким буде знаходитись введений пароль.
5. Ні в якому разі не можна аналізувати пароль зразу після його введення. Найкраще буде після введення пароля подякувати користувачеві за співробітництво і повідомити його що з йде перевірка пароля. А сам аналіз пароля провести вже після виконання цієї процедури.
6. Не перевіряйте пароль тільки в одному місці і не пишіть для його перевірки окрему функцію, оскільки для зламу такого захисту достатньо буде тільки знайти дану функцію та відключити її. Якщо перевірок правильності пароля декілька і вони знаходяться в різних місцях програмного коду то злам такого програмного продукту затрудняється.
7. Не перевіряйте пароль одним алгоритмом. Рекомендується розробити 2-3 алгоритми перевірки, наприклад 1-2 цифри повинні ділитись на 3, а 3-7 розміщені по якомусь алгоритму на ім'я користувача повинні дати в сумі 4. При цьому ці дві перевірки мають відбуватись в різних місцях з достатньо широким часовим розмежуванням.
8. Ні в якому разі не можна виконувати ніяких дій після перевірки пароля. По невідомій причині більшість програмний продуктів має приблизно такий вигляд:

   ```
   IF NOT(SuperRegCodeCheck) then
    Begin
    ShowMessage('Невірний пароль, подальша робота з програмою не    можлива');
   halt;
   end;
   ```
9. Відволікаючі маневри. Крім реальний функцій перевірки пароля інколи вводять додаткові (бутафорські) процедури, які імітують перевірку пароля.
10. Будь-який файл можна захистити контрольною сумою (CRC), яку потім можна розрахувати і порівняти з еталоном. Це дозволяє не тільки захистити ПП від зламу але і захистити його від вірусу чи трояну.

Тема 12. Особливості фізичного, технічного та програмного захисту інформації.

В обчислювальних машинах є велике число лазівок для несанкціонованого доступу до інформації. Ніякий окремо взятий спосіб захисту не може забезпечити адекватну безпеку. Надійний захист може бути гарантований лише при створенні механізму комплексного забезпечення безпеки як засобів опрацювання інформації, так і каналів зв'язку [10].

Технічні засоби являють собою електричні, механічні, електромеханічні або електронні пристрої.

Вся сукупність технічних засобів ділиться на фізичні й апаратні.

Фізичні засоби реалізуються у виді автономних пристроїв і систем і виконують функції загального захисту об'єктів, на яких опрацьовується інформація. До них ставляться, наприклад, устрої захисту територій і будинків, замки на дверях, де розміщені апаратура, грати на вікнах, електронно-механічне устаткування охоронної сигналізації.

Під апаратними технічними засобами прийнято розуміти пристрої, що вбудовуються безпосередньо в обчислювальну техніку, у телекомунікаційну апаратуру, або пристрої, що працюють з подібною апаратурою по стандартному інтерфейсу. З найбільше відомих апаратних засобів можна відзначити схеми контролю інформації з парності, схеми захисту масивів пам'яті по ключу та ін.

Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Організаційні засоби захисту подають собою організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їхнього життєвого циклу (будівництво помешкань, проектування системи, монтаж і наладка устаткування, іспити й експлуатація).

Морально-етичні засоби захисту реалізуються у вигляді всіляких норм, що склалися традиційно в даній країні або товаристві. Ці норми здебільшого не є обов'язковими, як законодавчі міри, проте їхнє недотримання веде звичайно до втрати авторитету і престижу співробітника.

Законодавчі засоби захисту визначаються законодавчими актами країни, який регламентуються правила використання, опрацювання і передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил.

Необхідно також відзначити, що всі розглянуті засоби захисту діляться на формальні, що виконують захисні функції строго по заздалегідь передбаченій процедурі без особистої участі людини, і неформальні, обумовлені цілеспрямованою діяльністю людини або регламентуючої цієї діяльності.

Необхідність забезпечення безпеки і вимоги сумісності різноманітних служб існуючих і розроблювальних інформаційно-обчислювальних мереж визначили напрямок у діяльності Міжнародної організації по стандартизації і Міжнародній спілці електрозв'язку. Концепція архітектури безпеки орієнтується на застосуванні в мережах, що використовують міжнародні стандарти і цілком відповідає еталонній моделі взаємозв'язку відкритих систем. Забезпечення безпеки інформації при її передачі здійснюється спеціальним підрозділом, що включає в себе ряд служб, кожна з яких вирішує задачу захисту інформації від визначеної погрози (сукупності погроз).

У загальному випадку в систему забезпечення безпеки інформації можуть бути включені:

1) Служба таємності даних – може бути використана для захисту переданих даних від скресання інформації, що утримується в них, і від можливості проведення аналізу інтенсивності потоків даних між користувачами

2) Служба аутентифікації – призначена для підтвердження того, що в даний момент зв'язку користувач є дійсно тим користувачем, за якого він себе видає;

3) Служба цілісності даних – забезпечує доказ цілісності даних у процесі їхньої передачі, тобто забезпечує захист переданих повідомлень від випадкових і навмисних впливів, спрямованих на зміну переданих повідомлень, затримку і знищення повідомлень або переупорядочення повідомлень;

4) Служба керування доступом – забезпечує захист від несанкціонованого доступу до інформації, що утримується в віддалених банках даних, або від несанкціонованого використання мережі;

5) Служба цілосності інформації – забезпечує доказ цілісності повідомлення, прийнятого від відповідного джерела і знаходиться на збереженні, наприклад, у терміналі-приймачі, і яке може бути перевірене в будь-який момент часу арбітром (третьою стороною);

6) Служба доставки – забезпечує захист від спроб зловмисника порушити зв'язок або затримати передачу повідомлення на час, що перевищує час цінності переданої в повідомленні інформації; ця служба безпосередньо пов'язана з процесами передачі інформації в мережах зв'язку.

Безпека інформації в системах телекомунікації забезпечується застосуванням комплексу прийомів, що можна класифікувати в такий спосіб:

- організація охорони помешкань у тому числі з застосуванням систем радіосигналізації; забезпечення безпеки комп'ютерних систем програмними й апаратними засобами;
- періодичне тестування помешкань методами нелінійної радіолокації;
- забезпечення захищеності від прослуховування засобів мобільного радіозв'язку;
- забезпечення акустичної безпеки помешкань і персоналу;
- криптографічні заходи.

Нижче зупинимося на аналізі організаційно-технічних прийомів.

Організаційні заходи включають активне вивчення і використання нормативно-законодавчої бази по забезпеченню безпеки в інформаційних і телекомунікаційних системах, добір персоналу, що допускається до обробки конфіденційної інформації, організацію збереження і доступу до документів, організацію контрольно-пропускного й охоронного режиму, виключення впливу стихійних лих на безпеку збереженої й опрацьовуваної інформації і т.п.

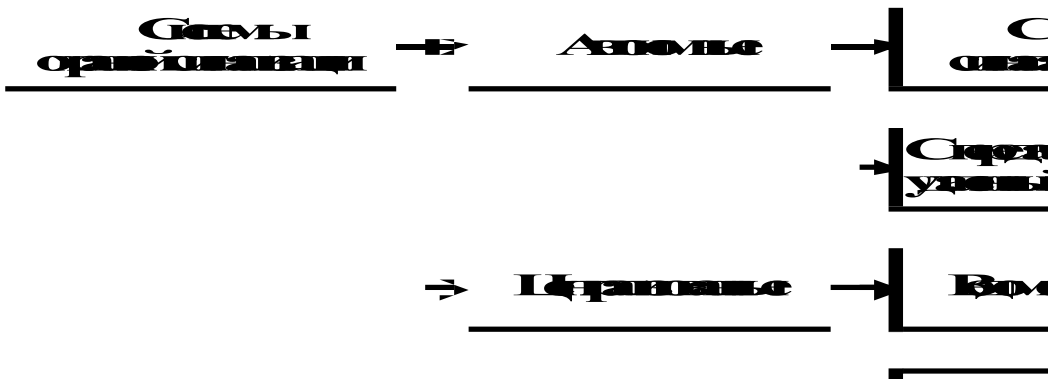
На початковій стадії організації робіт:

- встановлюється наявність конфіденційної інформації в системі, оцінюється рівень її конфіденціальності й обсяг;
- оцінюється можливість використання наявних на ринку сертифікаційних засобів захисту, виходячи з режиму обробки і передачі інформації в системі, типу системи, складу основних технічних засобів техніки і т.п.;
- визначається ступінь участі персоналу, функціональних і виробничих служб у процесі опрацювання і передачі інформації, характер їхньої взаємодії між собою і зі службою забезпечення безпеки;
- визначається план заходів щодо забезпечення безпеки.

Серед організаційних заходів щодо забезпечення безпеки інформації важливе місце займає охорона об'єкта, на якому розміщена захищаєма система (територія, будинки, помешкання, сховища інформаційних носіїв і т.д.), шляхом установлення відповідних постів технічних засобів охорони, що запобігають розкрадання інформаційних носіїв, а також несанкціонований доступ до апаратури і каналів зв'язку.

Системи охоронної сигналізації можна умовно віднести до одного з двох основних видів: автономні і централізовані. В свою чергу, автономні системи охоронної сигналізації можуть подавати сигнал тривоги на місці установки або передавати повідомлення на віддалений пульт. Централізовані системи охоронної сигналізації звичайно припускають наявність пульта, на якому відображається стан об'єктів що охороняються, і чергового персоналу.

Найбільше поширення серед відомчих систем охоронної сигналізації раніше одержали системи, у яких апаратура аналізу стану об'єктів що охороняються зосереджена на центральному пульті, а зв'язок із розташованими в охоронних помешканнях датчиками здійснюється по виділених провідних лініях. У загальногромадянських системах сигналізації (позавідомча охорона) апаратура аналізу стану об'єкта знаходиться в помешканні що



охороняється, а зв'язок її з апаратурою центрального пульта здійснюється по лініях телефонного зв'язку.

Цим системам охоронної сигналізації властиві такі недоліки:

1. Наявність провідного зв'язку між помешканням що охороняється і центральним пультом, а також досить прості сигнали в лініях зв'язку лишають можливість підключення до цих ліній із метою злочинного порушення правильного функціонування системи.

2. Обмеження по числу абонентів у зв'язку концепцією апаратного рішення.

3. Якість телефонних і виділених ліній зв'язку недостатньо високе для забезпечення високої надійності роботи системи. Підтримка їх у робочому стані пов'язана з додатковими поточними витратами.

4. Підключення нових об'єктів потребує наявності телефонної або прокладки виділеної лінії зв'язку, що збільшує розмір початкових витрат і обмежує можливість розширення системи.

5. У рамках, існуючих систем неможливо без істотних капітальних вкладень підключення віддалених окремо розташованих об'єктів.

Для надійного захисту території об'єктів сучасний комплекс повинен містити в собі такі основні компоненти:

- механічну систему захисту;
- пристрій оповіщення про спроби вторгнення;
- оптичну (телевізійну) систему впізнання порушників;
- центральний пост охорони, що здійснює збір, аналіз, реєстрацію й представлення повідомлень, що надходять, а також керування периферійними пристроями (брамою, загородженнями й ін);
- персонал охорони (патрулі, чергові на центральному посту).

У якості механічних засобів захисту використовуються: цегельні або кам'яні стіни, рови, огорожі, спеціальні дротові огородження, штахети й ін. Ці перешкоди можуть мати багаторядну систему для збільшення часу опору порушнику.

Сповіщення про вторгнення на територію що охороняється здійснюється за допомогою різноманітних датчиків. У системах захисту периметру території без огорожі використовують мікрохвильові, інфрачервоні, ємнісні й електричні датчики.

Мікрохвильові системи грунтуються на контролю інтенсивності СВЧ спрямованого випромінювання передавача, що сприймається приймачем. Спрацьовування сигналізації відбувається при перериванні цього спрямованого випромінювання. Помилкові вмикання сигналізації (помилкова тривога) можуть бути обумовлені переміщенням у контрольованій зоні тварини, впливом рослинності, атмосферних опадів, пересуванням транспортних засобів, а також впливом сторонніх передавачів.

У інфрачервоних системах між передавачем і приймачем контролюється інтенсивність монохроматичного світлового випромінювання в невидимій ІЧ області. Спрацьовування сигналізації відбувається при перериванні одного або декількох світлових променів. Помилкові вмикання сигналізації можуть бути обумовлені переміщенням у контрольованій зоні тварин, сильним туманом або снігопадом.

Принцип дії ємнісної системи оповіщення грунтується на формуванні електростатичного поля між паралельно розташованими передаючими і сприймаючими дротовими елементами спеціального огородження. Спрацьовування сигналізації відбувається при реєстрації визначеної зміни електростатичного поля, що має місце при наближенні людини до елементів огородження. Помилкові вмикання сигналізації обумовлені переміщенням тварини, впливом рослинності, зледенінням елементів огородження, атмосферними впливами або забрудненням ізоляторів.

Електричні системи оповіщення базуються на використанні спеціального огородження з дротового матеріалу, що проводить струм. Критерієм спрацьовування сигналізації є реєстрація змін електричного опору елементів, що проводять струм при дотику до них. Помилкові вмикання сигналізації можуть бути викликані тваринними, рослинністю або забрудненням ізоляторів.

Системи об'ємного контролю помешкань і територій. Вони засновані на тому, що фіксується об'ємне поле, утворене датчиком-генератором (СВЧ, ІЧ, ультразвук і ін). При появі стороннього об'єкта конфігурація поля змінюється, що і фіксується приймачем.

Системи, що реагують на зміну якихось фізичних параметрів оптичних кабелів при торканні й ін.

У механічних системах захисту території (огорожа, будинки, стіни, вікна і т.д.) використовуються різноманітні датчики: вібраційні, акустичні, електричні перемикачі (з контактами), електричні дротові елементи (спрацьовування відбувається при деформації їх). Широке поширення знайшли телевізійні системи спостереження й оповіщення.

Для запобігання вторгнення на територію, що охороняється, використовується система, у якій знаходять застосування освітлювальні або звукові сигнальні установки. У обох випадках порушник, що намагається проникнути на територію що охороняється, інформується про те, що він виявлений охороною, що робить цілеспрямований психологічний вплив. Крім того, використання освітлювальних установок забезпечує сприятливі умови для дій охорони.

Складні комплекси захисту територій що охороняються, які складаються, як правило, із декількох систем, можуть ефективно функціонувати за умови, що робота всіх технічних установок постійно контролюється й управляється центральним пристроєм.

Теми 13, 14. Віруси. Захист інформації від вірусів. Антивірусні програми.

Найбільш поширеним засобом нейтралізації вірусів є антивірусні програми (антивіруси). Антивіруси, виходячи з реалізованого в них підходу до виявлення і нейтралізації вірусів, прийнято ділити на наступні групи:

- детектори;
- фаги;
- вакцини;
- щеплення;
- ревізори;
- монітори.

Детектори забезпечують виявлення вірусів за допомогою проглядання виконуваних файлів і пошуку так званих сигнатур - стійких послідовностей байтів, наявних в тілах відомих вірусів. Наявність сигнатури в якому-небудь файлі свідчить про його зараження відповідним вірусом. Антивірус, що забезпечує можливість пошуку різних сигнатур, називають полідетектором.

Фаги виконують функції, властиві детекторам, але, крім того, «виліковують» інфіковані програми за допомогою «вирізування» вірусів з їх тіл. По аналогії з полідетекторамі, фаги, орієнтовані на нейтралізацію різних вірусів мають назву поліфагамі.

На відміну від детекторів і фагів, вакцини за своїм принципом дії подібні до вірусів. Вакцина імплантується в програму, що захищається, і запам'ятовує ряд кількісних і структурних характеристик програми. Якщо вакцинована програма не була до моменту вакцинації інфікованою, то при першому ж після зараження запуску відбудеться наступне. Активізація носія віруса приведе до отримання вірусом керування, який, виконавши свої цільові функції, передасть керування вакцинованій програмі. У останній, в свою чергу, спочатку керування отримає вакцина, яка виконає перевірку відповідності запам’ятованих нею характеристик аналогічним характеристикам, отриманим у певний момент. Якщо вказані набори характеристик не співпадають, то робиться висновок про зміну тексту вакцинованої програми вірусом. Характеристиками, використовуваними вакцинами, можуть бути довжина програми, її контрольна сума і т.д. Принцип дії щеплень базується на обліку тієї обставини, що будь-який вірус, як правило, позначає програми, що інфікуються, якою-небудь ознакою з тим, щоб не виконувати їх повторне зараження. У іншому випадку мало б місце багатократне інфікування, супроводжується істотним і тому таким, що легко виявляється збільшенням об'єму заражених програм. Щеплення, не вносячи ніяких інших змін в текст програми, що захищається, позначає її тією ж ознакою, що і вірус, який, таким чином, після активізації і перевірки наявності вказаної ознаки, вважає її інфікованою і «залишає у спокої».

Ревізори забезпечують стеження за станом файлової системи, використовуючи для цього підхід, аналогічний реалізованому у вакцинах. Програма-ревізор в процесі свого функціонування виконує до кожного виконуваного файлу порівняння його поточних характеристик з аналогічними характеристиками, отриманими в ході попереднього перегляду файлів. Якщо при цьому виявляється, що, згідно наявної системної інформації, файл з моменту попереднього перегляду не оновлювався користувачем, а порівнювані набори характеристик не

співпадають, то файл вважається інфікованим. Характеристики виконуваних файлів, отримувані в ході чергового перегляду, запам’ятовуються в окремому файлі (файлах), у зв'язку з чим збільшення довжин виконуваних файлів, що має місце при вакцинації, в даному випадку не відбувається. Інша відмінність ревізорів від вакцин полягає в тому, що кожен перегляд виконуваних файлів ревізором вимагає його повторного завантаження.

Монітор є резидентною програмою, що забезпечує перехоплення потенційно небезпечних переривань, характерних для вірусів, і що вимагає у користувачів підтвердження на виконання операцій, наступних за перериванням. У разі заборони або відсутності підтвердження монітор блокує виконання призначеної для користувача програми.

Антивіруси розглянутих типів істотно підвищують вірусозахищеність окремих ПК і обчислювальних мереж в цілому. Відомо ряд недоліків при використанні антивірусів. У зв'язку з цим необхідна реалізація альтернативних підходів до нейтралізації вірусів: створення операційних систем, що володіють високою вірусозахищеністю в порівнянні з найбільш «дружньою до вірусів» MS DOS, розробка апаратних засобів захисту від вірусів і дотримання технології захисту від вірусів.

Теми 15, 16. Безпека сучасних мережевих технологій, методи і засоби захисту від віддалених атак через Інтернет. Захист інформації в електронних платіжних системах.

Міжмережний екран - це набір пов’язаних між собою програм, що встановлюються на комп’ютері, який містить ресурси власників та захищає їх від користувачів із зовнішньої мережі, наприклад Internet. Власник комп’ютера, що має вихід в Internet, встановлює міжмережний екран, щоб запобігти одержанню сторонніми конфіденційних даних, котрі зберігаються на комп’ютері, а також для контролю за зовнішніми ресурсами, до яких мають доступ інші користувачі даної комп’ютерної системи.

Ряд завдань стосовно захисту від найбільш імовірних атак для внутрішніх мереж здатні вирішувати тільки міжмережні екрани. У вітчизняній літературі частіше зустрічаються терміни іноземного походження: брандмауер і firewall. Поза комп’ютерною сферою брандмауером (чи firewall) називають протипожежну стіну, зроблену з вогнестійких матеріалів, щоб перешкодити поширенню пожежі. У сфері використання комп’ютерних технологій міжмережний екран становить собою бар’єр, що захищає від умовної пожежі - спроб зловмисників несанкціоновано вторгнутися у внутрішню мережу для вчинення протиправних дій. Міжмережний екран покликаний створити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Вибір оптимальних міжмережних екранів (firewalls) – це, головним чином, питання правильного співвідношення між вимогами користувачів стосовно доступу та вірогідності несанкціонованого доступу. В ідеалі система має запобігати будь-якому несанкціонованому вторгненню. Однак, враховуючи широкий спектр Web-сервісів, необхідних користувачам, ftp, telnet, SNMP, Network File System, IP телефонія, електронна пошта тощо, досягнути певного рівня запобігання несанкціонованому втручанню дуже важко.

Основна мета firewall - не допустити несанкціонованого доступу в локальну мережу через Internet шляхом перегляду пакетів даних і використання спеціальних засобів підтвердження повноважень для додатків. Перегляд пакетів проводиться з метою блокування підозрілих видів трафіка. Функції підтвердження повноважень, які орієнтовані на прикладні програми, здійснюють повний контроль і перевірку на допустимість усіх вхідних і вихідних даних. Усе більше фахівців у галузі захисту інформації приходить до розуміння, що використання firewall для захисту локальної мережі значно зменшує ризик несанкціонованого втручання через Internet.

Ряд firewall дозволяють також організовувати віртуальні корпоративні мережі Virtual Private Network (VPN), що об’єднують декілька локальних мереж, включених у Internet в одну віртуальну мережу. Така система дозволяє організувати прозоре для користувачів з’єднання локальних мереж, зберігаючи секретність і цілісність інформації, що передається за допомогою шифрування. При цьому під час передачі даних по Internet шифрується не лише інформація, призначена для користувача, але і мережна - мережні адреси, номери портів тощо. VPN створює захищене з’єднання через Internet. Зараз подібне використовується в багатьох технологіях.

Наведемо перелік та коротку характеристику найбільш розповсюджених засобів стеганографічного захисту:

1. Steganos v.1.4. – програма, яка може приховувати інформацію, використовуючи стеганографічні методи, і шифрувати її за допомогою технології криптографії. Призначена для роботи в середовищі DOS. Дає можливість приховувати всі види файлів у графічних файлах формату BMP, у звукових файлах формату WAV і VOC, текстових ASCII. Може не вилучати файл "повідомлення" і створювати резервну копію файла "контейнера". Отриманий в результаті цього перетворення файл формату BMP можна перевести в інші графічні формати, не руйнуючи структуру зображення, наприклад, GIF, і зворотно без втрати закодованої інформації.
2. Hideseek – програма може приховувати файл "повідомлення" лише у графічних файлах GIF, а найбільше розширення екрану, з яким вона може працювати, – 320*480 пікселів.
3. Hide 4PGP v.1.0 – програма, призначена для роботи в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату BMP (256-кольорове або 24-бітне зображення не повинно бути стиснутим) і звукових файлах формату WAV і VOC.
4. PGE v.1.0 – програма, що також працює в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату GIF (87,89) і JPG (JFIF).
5. S-Tools v.4 for Windows – програмний засіб, що дає можливість приховувати всі види файлів у графічних файлах формату BMP і GIF і звукових файлах формату WAV. При роботі створює новий файл з закодованою інформацією. Має багатовіконний режим роботи і може одночасно кодувати кілька файлів. Використовує кілька стеганографічних алгоритмів, і користувач може вибрати найбільш придатний.
6. White Noise StormTM – призначений для роботи в середовищі DOS. Може приховувати всі види файлів у графічних файлах формату BMP і GIF і звукових файлах формату VOC. У ході тестування найпереконливіші результати продемонстрували Steganos for Windows 95 і S-Tools v.4.