Харченко М.М.,
судентка 5 курсу фізико-математичного факультету
Науковий керівник: Вакалюк Т.А.
кандидат педагогічних наук, доцент,
доцент кафедри прикладної математики та інформатики
Житомирський державний університет імені Івана Франка

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні в інформаційному просторі, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Комп'ютерні системи активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. Внаслідок цього різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. В останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу (НСД) до конфіденційної інформації.

Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи.

Криптографія - наука про математичні методи забезпечення конфіденційності і автентичності інформації. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів.

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. [1]

Алгоритм DES (Data Encryption Standard) був стандартом симетричних блочних шифрів затверджених урядом США до 2001року (зараз використовується в режимі 3DES). Під словом «симетричний» розуміють те що для шифрування і дешифрування використовується один і той же ключ, а блоковий тому що шифрування даних відбувається поблоково. Тобто дані розбиваються на блоки фіксованої довжини (як правило для DES, довжина блоку дорівнює 64 біт), а потім шифруються. Даний алгоритм використовується для великих об’ємів даних. [24]

Алгоритм RSA є асиметричним шифром (або з відкритим ключем) в якому використовується ключ який складається з двох частин: відкритий (public key), що зашифровує дані, і відповідний йому закритий (private key), що їх розшифровує. Відкритий ключ поширюється по усьому світу, у той час як закритий тримається в таємниці. Хоча ключова пара математично зв'язана, обчислення закритого ключа з відкритого в практичному плані неможлива. Кожний, у кого є відкритий ключ, зможе зашифрувати дані, але не зможе їх розшифрувати. Тільки людина, яка володіє відповідним закритим ключем, може розшифрувати інформацію. [23]

Захист інформації (англ. Data protection) — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Те, що інформація має цінність, люди усвідомили дуже давно. Тоді-то і виникло завдання захисту від надмірно цікавих людей. Стародавні намагалися використовувати для вирішення цього завдання найрізноманітніші методи, і одним з них був тайнопис - уміння складати повідомлення так, щоб його сенс був недоступний нікому окрім присвячених в таємницю. Є свідоцтва тому, що мистецтво тайнопису зародилося ще в доантичні часи і проіснувало аж до зовсім недавнього часу. І лише декілька десятиліть тому все змінилося корінним чином -

інформація придбала самостійну комерційну цінність і стала широко поширеною, майже звичайним товаром. Її проводять, зберігають, транспортують, продають і купують, а значить - крадуть і підроблюють - і, отже, її необхідно захищати. Сучасне суспільство все більшою мірою стає інформаційно-обумовленим, успіх будь-якого виду діяльності все сильніше залежить від володіння певними відомостями і від відсутності їх у конкурентів. [25]

Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їх реалізації. В даний час особливо актуальною стала оцінка вже використовуваних криптоалгоритмів. Завдання визначення ефективності засобів захисту часто більш трудомістка, ніж їх розробка, вимагає наявності спеціальних знань і, як правило, вищої кваліфікації, ніж завдання розробки. Це обставини призводять до того, що на ринку з'являється безліч засобів криптографічного захисту інформації, про які ніхто нічого не знає. При цьому розробники тримають криптоалгоритм в секреті.

Шифрування — це спосіб зміни повідомлення або іншого документа, що забезпечує спотворення (захування) його вмісту. (Кодування – це перетворення звичайного, зрозумілого, тексту в код (виконується без ключа)). Шифрувати можна не тільки текст, але і різні комп'ютерні файли – від файлів баз даних і текстових процесорів до файлів зображень.

Ідея шифрування полягає в запобіганні прогляданню дійсного змісту повідомлення (тексту, файлу і т.п.) тими, у кого немає засобів його дешифровки. А прочитати файл зможе лише той, хто зможе його дешифрувати.

Шифрування з'явилося приблизно чотири тисячі років тому. Першим відомим застосуванням шифру (коду) вважається єгипетський текст,

датований приблизно 1900 р. до н. э., автор якого використовував замість звичайних (для єгиптян) ієрогліфів не співпадаючі з ними знаки.

Один з найвідоміших методів шифрування носить ім'я Цезаря, який якщо і не сам його винайшов, то активно їм користувався. Не довіряючи своїм посильним, він шифрував листи елементарною заміною A на D, B на E і так далі по всьому латинському алфавіту. При такому кодуванні комбінація XYZ була б записана як ABC (прямий код N+3). [4]

Інформація - це відомості про осіб, факти, предмети, події, явища і процеси, незалежно від форми їх уявлення.

Захист інформації - комплекс заходів, проведених із метою запобігання (зниження до безпечного рівня) можливостей витікання, розкрадання, втрати, поширення, знищення, перекручування, підробки або блокування інформації. [25]

Види дій над інформацією:

1. Блокування інформації (користувач не може дістати доступ до інформації; за відсутності доступу сама інформація не втрачається).

2. Порушення цілісності (втрата, вихід з ладу носія; спотворення, тобто порушення смислової значущості; порушення логічної зв'язаності; втрата достовірності (наявна інформація не відповідає реальному стану)).

3. Порушення конфіденційності (з інформацією ознайомлюються суб'єкти, на яких це не покладено). Рівень допуску до інформації визначає її власник. Порушення конфіденційності може відбутися із-за неправильної роботи системи обмеження доступу або наявності побічного каналу доступу.

Автоматизована система (АС) - це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. [26]

Захист інформації в АС (information security, computer system security) - діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому і дозволяє запобігти або ускладнити можливість

реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Загроза - потенційно можлива подія, дія, процес або явище, яке може привести до нанесення збитку інтересам певної фізичної чи юридичної особи. Реалізацією загрози є порушення роботи системи. Загрози поділяються на природні та штучні.

Природні загрози - загрози, викликані дією на АС об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини. До них відносяться: стихійні лиха, магнітні бурі, радіоактивне випромінювання, опади тощо, а також загрози опосередковано технічного характеру, пов'язані з надійністю технічних засобів обробки інформації і підсистем забезпечення АС.

Штучні загрози - такі, що викликані діяльністю людини. Вони поділяються на:

•ненавмисні - загрози, пов'язані з випадковими діями людей, через незнання, халатність, цікавість, але без злого наміру.

•навмисні - дії людини, що здійснюються умисне для дезорганізації роботи системи, виведення її з ладу, для незаконного проникнення в систему і несанкціонованого доступу до інформації.

Сучасні засоби перехоплення інформації дозволяють на відстані в десятки і сотні, а іноді і більше метрів реєструвати різної природи побічні інформативні сигнали, що виникають при роботі технічних засобів, і за результатами цієї реєстрації відновлювати оброблювану, передану, прийняту, копійовану інформацію. [26]

Інформацію можна одержувати не тільки шляхом перехоплення побічних інформативних сигналів, але й за результатами прямої реєстрації сигналів, що циркулюють в інформаційних ланцюгах технічних систем

(насамперед, у лініях зв'язку). Реалізувати засоби перехоплення тут, як правило, легше, ніж у випадку побічних випромінювань і наведень.

Фізичні заходи захисту інформації базуються на застосуванні всілякого роду механічних, електро- або електронно-механічних пристроїв, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи і інформації, а також технічних засобів візуального нагляду, зв'язку та охоронної сигналізації.

Ідентифікація - привласнення суб'єктам або об'єктам доступу ідентифікатора або порівняння пред'явленого ідентифікатора з переліком привласнених ідентифікаторів. Ідентифікація об'єкта - це його впізнання, ототожнення із чим-небудь. Якщо ж говорити про області інформаційних технологій, то даний термін звичайно означає встановлення особистості користувача. Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу до закритої інформації тощо. Таким чином, ідентифікація є одним з основних понять в інформаційній безпеці.

Аутентифікацією - називається процедура верифікації належності ідентифікатора суб'єкту. Аутентифікація здійснюється на основі того чи іншого секретного елемента (аутентифікатора), який є у розпорядженні як суб'єкта, так і інформаційної системи. Звичайно, інформаційна система має в розпорядженні не сам секретний елемент, а деяку інформацію про нього, на основі якої приймається рішення про адекватність суб'єкта ідентифікатору. Наприклад, перед початком інтерактивного сеансу роботи більшість операційних систем запитують у користувача його ім'я та пароль. Введене ім'я є ідентифікатором користувача, а його пароль - аутентифікатором. Операційна система зазвичай зберігає не сам пароль, а його хеш-суму, що забезпечує складність відновлення пароля.

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ

розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами. Під НСД мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розуміються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін. [25]

Захист від НСД може здійснюватися в різних складових інформаційної системи:

1. Прикладне й системне ПЗ.

2. Апаратна частина серверів і робочих станцій.

3. Комунікаційне устаткування й канали зв'язку.

4. Периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

· системи розмежування доступу до інформації;

· системи ідентифікації й аутентифікації;

· системи аудиту й моніторингу;

· системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

· апаратні ключі;

· системи сигналізації;

· засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

· міжмережеві екрани (Firewall);

· системи виявлення вторгнень (IDS - Intrusion Detection System;

· засоби створення віртуальних приватних мереж (VPN - Virtual Private Network;

· засоби аналізу захищеності.

Для захисту периметра інформаційної системи створюються:

· системи охоронної й пожежної сигналізації;

· системи цифрового відеоспостереження;

· системи контролю й керування доступом (СККД). При створенні програмно-апаратних засобів захисту від несанкціонованого доступу керуються наступними принципами:

1) принцип обґрунтованості доступу (виконавець повинен мати достатню «форму допуску» до закритої інформації, відомості про яку потрібні йому для повноцінного виконання професійних обов'язків);

2) принцип достатньої глибини контролю доступу (СЗІ повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів);

3) принцип розмежування потоків інформації (не дозволяє переписувати закриту інформацію на незакриті носії; здійснюється мічення на носії інформації і ідентифікація цих носіїв);

4) принцип чистоти повторно використовуваних ресурсів (звільнення від закритої інформації ресурсів при їх видаленні);

5) принцип персональної відповідальності (виконавець повинен нести персональну відповідальність за свою діяльність в системі, включаючи всі дії із закритою інформацією);

6) принцип цілісності засобів захисту (засоби захисту повинні точно виконувати свої функції і бути ізольовані від користувача). [26]

Не слід недооцінювати можливості непрофесіоналів щодо здійснення комп'ютерних злочинів. Нелояльні співробітники, що мають доступ до комп'ютерів, грають головну роль в більшості фінансових злочинів. Це швидше організаційна, ніж технічна проблема.

Процедури безпеки можуть забезпечувати перевірку паролів і строгий контроль доступу до цінних загальних даних, але зловмисника, обізнаного у внутрішньому устрої системи, практично неможливо зупинити.

Для побудови надійного захисту необхідно виявити можливі погрози безпеці інформації, оцінити їх наслідки, визначити необхідні заходи і засоби захисту і оцінити їх ефективність. [25]

Криптографічний захист інформації — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. [1]

Криптографія (від грецького kryptos — прихований і graphein — писати) — наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри. [20].

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття» (тобто, шифротекст). Дешифрування — це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, та і в кожному випадку ключем. [12]

Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключей алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування, без виконання додаткових процедур, таких як аутенифікація або перевірка цілісності.

В англійській мові слова криптографія та криптологія інколи мають однакове значення, в той час, як деколи під криптографією може

розумітись використання та дослідження технологій шифрування, а під криптологією — дослідження криптографії та криптології.

Дослідження характеристик мов, що мають будь-яке відношення до криптології, таких як частоти появи певних літер, комбінацій літер, загальні шаблони, тощо, називається криптолінгвістикою.

Криптоаналіз — розділ криптології, що займається математичними методами порушення конфіденційності і цілісності інформації без знання ключа.

Криптологія — розділ науки, що включає криптографію та криптоаналіз.

Криптографія займається розробкою методів шифрування даних, у той час як криптоаналіз займається оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів, які дозволяють зламувати криптосистеми. [20]

До нашого часу, криптографія займалася виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) — перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотнє відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного знання (а саме ключа, необхідного для дешифровки повідомлення). В останні десятиліття сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування, тощо. [25]

Найперші форми тайнопису вимагали не більше ніж аналог олівця та паперу, оскільки в ті часи більшість людей не могли читати. Поширення писемності, або писемності серед ворогів, викликало потребу саме в криптографії. Основними типами класичних шифрів є перестановочні шифри, які змінюють порядок літер в повідомленні, та підстановочні

шифри, які систематично замінюють літери або групи літер іншими літерами або групами літер. Прості варіанти обох типів пропонували слабкий захист від досвідчених супротивників. Одним із ранніх підстановочних шифрів був шифр Цезаря, в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував, зі зсувом в 3 позиції, для спілкування з генералами під час військових кампаній, подібно до коду EXCESS-3 в булевій алгебрі.

Шляхом застосування шифрування намагаються зберегти зміст спілкування в таємниці, подібно до шпигунів, військових лідерів, та дипломатів. Збереглися також відомості про деякі з ранніх єврейських шифрів. Застосування криптографії радиться в Камасутрі як спосіб спілкування закоханих без ризику незручного викриття. Стеганографія (тобто, приховування факту наявності повідомлення взагалі) також була розроблена в давні часи. Зокрема, Геродот приховав повідомлення — татуювання на поголеній голові раба — під новим волоссям. До сучасних прикладів стеганографії належать невидимі чорнила, мікрокрапки, цифрові водяні знаки, що застосовуються для приховування інформації [3].

Список використаних джерел та літератури:

1. Указ Президента України від 22 травня 1998 року N 505/98«Про Положення про порядок здійснення криптографічного захисту інформації в Україні». Перевірено 2009-06-12.

2. Соболева Т.А. Введение // История шифровального дела в России. — М.: ОЛМА-ПРЕСС Образование, 2002. — 512 с. — (Досье). — 5 000 экз. — ISBN 5-224-03634-8

3. Павел Исаев. Некоторые алгоритмы ручного шифрования (рус.) // КомпьютерПресс. — 2003. — В. 3.

4. Жельников В. Появление шифров // Криптография от папируса до компьютера. — М.: ABF, 1996. — 335 с. — ISBN 5-87484-054-0

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы,

исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4 (http://www.ssl.stu.neva.ru/psw/crypto/appl_ rus/appl_cryp.htm)

6. Саломаа А. Криптография с открытым ключом.

7. PGP. Распределение ключей. (http://www.re.mipt.ru/infsec/2004/essay/2004_PGP_Keys_Web_of_Trust_Lukjanchenko.htm)

8. Принцип достаточной защиты. (http://pmi.ulstu.ru/new_project/telecommunication/redar.htm)

9. Баричев С. Криптографія без секретов. с. 20

10. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин Основы криптографии.

11. Семенов Ю.А. Алгоритм DES. (http://book.itep.ru/6/des_641.htm)

12. Венбо Мао Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. — М.: Вильямс, 2005. — 768 с. — 2 000 экз. — ISBN 5-8459-0847-7, ISBN 0-13-066943-1

13. Нильс Фергюсон, Брюс Шнайер Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: «Диалектика», 2004. — 432 с. — 3 000 экз. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3

14. Хорст Файстель. Криптография и компьютерная безопасность. Перевод Андрея Винокурова

15. А. Винокуров. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86

16. ДИСКРЕТНАЯ МАТЕМАТИКА: АЛГОРИТМЫ. Симметричные системы и блочные шифры

17. Журнал Byte. № 8 (60), август 2003. Современные алгоритмы шифрования, Сергей Панасенко

18. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с. —

(Специальность. Для высших учебных заведений). — 3000 экз. — ISBN 5-93517-075-2

19. Коркішко Т., Мельник А. Алгоримти та процесори симетричного блокового шифрування. – Львів, БаК, 2003.-163 с.

20. http://uk.wikipedia.org/wiki/Криптографія

21. http://uk.wikipedia.org/wiki/Симетричні_алгоритми_шифрування

22. http://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом

23. http://ru.wikipedia.org/wiki/RSA

24. http://ru.wikipedia.org/wiki/DES

25. Міністерство освіти і науки України, Одеський національний політехнічний університет, лекцій до дисципліни «Захист інформації», Укладач Ю.С.Ямпольський,Одеса, ОНПУ, 2002 р.

26. Вакалюк Т. А. Основні поняття захисту інформаційних ресурсів у комп'ютерних системах / Т. А. Вакалюк // Науковий пошук молодих дослідників: збірник наукових праць / за ред. канд. пед. наук Королюк О.М. – Випуск 6. – Житомир: Вид-во ЖДУ ім. І.Франка, 2013. – С. 230-233.

27. Вакалюк Т. А. Загрози безпеки інформаційних ресурсів у комп'ютерних системах / Т. А. Вакалюк // Сучасні інформаційні технології: теорія, практика, досвід та перспективи розвитку : матеріали міжрегіонального семінару (17 квітня 2013 р.). – Житомир : Вид-во ЖДУ ім. Івана Франка, 2013. – С. 16-20.

28. Вакалюк Т. А. Захист інформації в комп'ютерних системах: навчально-методичний посібник для студентів фізико-математичного факультету / Тетяна Анатоліївна Вакалюк. – Житомир: Вид-во ЖДУ, 2013. – 136 с.