Національний університет «Полтавська політехніка імені Юрія Кондратюка»

(повне найменування вищого навчального закладу)

Навчально науковий інститут інформаційних технологій та робототехніки

(повна назва факультету)

Кафедра комп’ютерних та інформаційних технологій і систем

(повна назва кафедри)

**Пояснювальна записка**

**до дипломного проєкту (роботи)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_бакалавра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(освітньо-кваліфікаційний рівень)

на тему

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Аналіз захисту інформації на підприємстві\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_та удосконалення системи шифрування\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Виконав: студент \_\_4 \_курсу, групи \_ 402-ТН \_

спеціальності 122 Комп’ютерні науки

(шифр і назва напряму)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Рець Б.Ю.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Керівник \_ Головко Г.В. \_

(прізвище та ініціали)

**Полтава – 2021 року**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

**НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ**

**КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ**

**КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА**

**спеціальність 122 «Комп’ютерні науки»**

**на тему:**

**«Аналіз захисту інформації на підприємстві та удосконалення системи шифрування»**

**Студента групи 402-ТН Реця Богдана Юрійовича**

Завідувач кафедри

кандидат технічних наук,

доцент Головко Г.В.

**Полтава – 2021**

**РЕФЕРАТ**

**Записка**: 65 с., 10 рис., 3 таблиці, 1 додаток, 25 джерел.

**Предмет розробки:** – створення системи для кодування текстових повідомлень за допомогою системи шифрування CAST 5.

**Мета роботи:** – розробити план захисту на підприємстві та створити програму для шифрування та дешифрування за допомогою мови С#.

**Методи:** – Принципи криптографії в мові програмування C#. Розроблено систему шифрування текстових повідомлень за допомогою CAST 5.

**Ключові слова**: криптологія, криптографія, криптоаналіз, шифрування, дешифрування, CAST 5, алгоритм.

**ANNOTATION**

**Note**: 65 pp., 10 img., 3 tables, 1 addition, 25 sources.

**Subject of development**: - creation of a system for encoding text messages using the CAST 5 encryption system.

**Purpose**: - to develop a security plan at the enterprise and create a program for encryption and decryption using the C # language.

**Methods**: - Principles of cryptography in the C # programming language. A system for encrypting text messages using CAST 5 has been developed.

**Keywords**: cryptology, cryptography, cryptanalysis, encryption, decryption, CAST 5, algorithm.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ 5](#_Toc74732525)

[ВСТУП 6](#_Toc74732526)

[РОЗДІЛ 1 ОСНОВНІ ПОНЯТТЯ ТА ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ 7](#_Toc74732527)

[1.1 Аспекти захисту інформації 7](#_Toc74732528)

[1.2 Види захисту інформації 8](#_Toc74732529)

[1.3 Класифікація засобів захисту інформації 9](#_Toc74732530)

[1.4 Проблеми захисту інформації та комп’ютерні злочини 14](#_Toc74732531)

[РОЗДІЛ 2 КРИПТОЛОГІЯ ТА КРИПТОАНАЛІЗ 27](#_Toc74732532)

[2.1 Основні терміни 27](#_Toc74732533)

[2.2 Вимоги до криптографічних систем 29](#_Toc74732534)

[2.3 Принципи побудови й схеми криптологічних систем 31](#_Toc74732535)

[РОЗДІЛ 3 ОПИС ШИФРУВAЛЬНОГО МЕТОДA CAST 5 33](#_Toc74732536)

[РОЗДІЛ 4 ОРГAНІЗAЦІЯ ЗAХИСТУ ІНФОРМAЦІЇ НA ПІДПРИЄМСТВІ «INFUSEmedia UKRAINE» 36](#_Toc74732537)

[4.1 Інформaція про підприємство «INFUSEmedia UKRAINE» 36](#_Toc74732538)

[4.2 Плaн приміщення оргaнізaції «INFUSEmedia UKRAINE» 37](#_Toc74732539)

[4.3 Структурa оргaнізaції «INFUSEmedia UKRAINE» 38](#_Toc74732540)

[4.4 Експлікація приміщення «INFUSEmedia UKRAINE» 39](#_Toc74732540)

[4.5 Зaхист інформaції в оргaнізaціях 40](#_Toc74732541)

[4.6 Оргaнізaційний зaхист інформaції 42](#_Toc74732542)

[4.7 Мaндaтнa модель розмежувaння доступу до інформaції 47](#_Toc74732543)

[РОЗДІЛ 5 СТВОРЕННЯ ПРОГРАМИ 48](#_Toc74732532)

[ВИСНОВОК 52](#_Toc74732544)

[СПИСОК ВИКОРИСТAНОЇ ЛІТЕРAТУРИ 53](#_Toc74732545)

[ДОДAТОК A 55](#_Toc74732546)

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ**

ІС – Інформаційна система;

ТЗІ – Технології захисту інформації;

США – Сполучені Штати Америки;

IP – Internet Protocol;

AES – Advanced Encryption Standard;

CKC – Структурована кабельна система;

ЕОМ – Електронна обчислювальна машина;

VPN – Virtual Private Network;

ІТ – Інформаційні технології;

ПЗ – Програмне забезпечення;

ЦРУ – Центральне Розвідувальне Управління;

CD-ROM – Compact Disk Read Only Memory;

MAC – Media Access Control;

DHCP – Dynamic Host Configuration Protocol;

VLAN – Virtual Local Address Network;

Wi-Fi – Wireless Fidelity;

WAN – Wide Area Network;

LAN – Local Area Network.

# ВСТУП

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

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

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

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

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

Повністю захищений комп'ютер - це той, який знаходиться під замком у броньованій кімнаті в сейфі, не підключений ні до якої мережі (навіть електричної) і виключений. Такий комп'ютер має абсолютний захист, однак використати його не можна. У цьому прикладі не виконується вимога доступу інформації. "Абсолютності" захисту заважає не тільки необхідність користуватися захищеними даними, але й ускладнення систем, що захищають [1].

# РОЗДІЛ 1 ОСНОВНІ ПОНЯТТЯ ТА ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ

## **1.1 Аспекти захисту інформації**

**Захист інформації** — сукупність [методів](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4) і засобів, що забезпечують [цілісність](https://uk.wikipedia.org/wiki/%D0%A6%D1%96%D0%BB%D1%96%D1%81%D0%BD%D1%96%D1%81%D1%82%D1%8C), [конфіденційність](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C) і [доступність](https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D1%96%D1%81%D1%82%D1%8C) [інформації](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і [користувачам інформації](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97) [2].

**Аспекти захисту інформації**

**Конфіденційність** — властивість, яка не підлягає розголосові; довірливість, секретність, суто приватність.

Топологія:

* + конфіденційність адміністративна — [послуга безпеки](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8), що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.
  + конфіденційність довірча — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.
  + конфіденційність інформації — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею [3].

**Цілісність** — внутрішня єдність, пов'язаність усіх частин чого-небудь, в єдине ціле. В [інформаційній системі](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) — стан даних або інформаційної системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

* + стійку роботу системи;
  + автоматичне відновлення у випадку виявлення системою потенційної помилки [4];
  + автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу [4].

**Доступність** — властивість [інформаційного ресурсу](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81), яка полягає в тому, що [користувач](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87) та/або [процес](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених [політикою безпеки](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8) не очікуючи довше заданого (прийнятного) інтервалу часу [5].

## **Види захисту інформації**

Кожен вид забезпечує окремі аспекти.

Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токени, смарткарти тощо):

* + попередження витоку по технічному каналу;
  + запобігати блокуванню.

Інженерний — запобігає руйнування носія за для навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежувальні конструкції, охоронно-пожежна сигналізація).

Криптографічний — попереджує доступ за допомогою математичних перетворень повідомлення:

* + попередження несанкціонованої модифікації;
  + попередження НС розголошення.

Організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу) [6].

**1.3 Класифікація засобів захисту інформації**

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т.ін. Ці норми здебільшого не є обов'язковими та не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Правові засоби захисту — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання IT [7].

Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проєкту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних правопорушень Ради Європи, було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини та надає урядам і службовим органам зайві повноваження [7].

Загальною тенденцією, яку можна простежити, є посилення кримінального законодавства проти комп'ютерних злочинів. Так, сьогодні в Гонконзі, якщо такий злочин призводить до відмови СК чи вебсайтів, максимальне покарання становить 10 років ув’язнення. На відміну від цього, в українському кримінальному законі незаконне втручання в роботу комп’ютерів та комп’ютерних мережних процесів може бути покаране неоподатковуваним мінімальним доходом до 70% або до двох років перевиховання через працю, або подібними обмеженнями свободи.

Засоби інформації про управління та захист регулює процес роботи ІС, використання його ресурсів, діяльність співробітників та послідовність взаємодії користувачів із системою, ускладнючи або запобігаючи порушенням безпеки. Вони охоплюють:

* заходи, які передбачаються під час проєктування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);
* заходи, що здійснюються під час проєктування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін);
* заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань) [7];
* розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є неодмінною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні й здатні доповнити законодавчі норми там, де це потрібно організації, а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

Засоби фізичного захисту інформації — це різного роду механічні, електро або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

* засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відмов ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи, в якій використовуються однакові кабелі для організації передавання даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержуватись вимог міжнародних стандартів [7];
* засоби захисту системи електроживлення. Американські дослідники з компанії Best Power1 після п'яти років досліджень проблем електроживлення зробили висновок: на 12 кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіше ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових вимкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення [7].

Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності ІС можливе використання аварійного електрогенератора або резервних ліній електроживлення, під’єднаних до різних підстанцій;

* засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);
* засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи та предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними [7].

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в IC, криптографічний захист інформації, захист від комп'ютерних вірусів тощо (див. докладніше далі).

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

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з зацифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести та відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

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

* додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засоби комп'ютерної системи;
* вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи [7].

Перший спосіб є більш гнучким, його механізми можна додавати та вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують [7].

## **1.4 Проблеми захисту інформації та комп’ютерні злочини**

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в котрих комп'ютери використовуються як необхідні технічні засоби.

Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі:

* швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
* широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
* постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць [7].

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

* збитки, призводять до ситуації, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи;
* вартість викрадених і скомпрометованих даних;
* витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо.

Слід також враховувати моральні та психологічні наслідки для користувачів, службовців та власників ІС та інформації. Що стосується порушень безпеки так званих "критичних" застосувань у державному та військовому управлінні, атомній енергетиці, медицині, космосі та фінансах, це може мати серйозні наслідки для навколишнього середовища, економіки та національної безпеки, охорони здоров'я та навіть суспільства. життя людей.

Економічні та правові питання, приватна та комерційна таємниця, національна безпека - все це вимагає захисту інформації та прав інтелектуальної власності.

Відповідно до українського "Закону про захист інформації про систему автоматизації", захист інформації - це сукупність організаційно-технічних заходів та правових норм для запобігання пошкодженню інформації, інформації чи інтересів АС та власників інформації.

Пов'язані терміни "інформаційна безпека" та "безпека інформаційних технологій" також використовуються в літературі [7].

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІT, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби та побудувати надійну систему захисту.

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності й водночас доступності для всіх авторизованих користувачів. З цього погляду основними випадками порушення безпеки інформації можна назвати такі:

* несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в ІC правил розмежування доступу;
* витік інформації — результат дій порушника, унаслідок котрих інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
* втрата інформації — дія, внаслідок якої інформація в IC перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
* підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в IC;
* блокування інформації — дії, наслідком яких є припинення доступу до інформації;
* порушення роботи ІC — дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

* збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
* некоректна робота програмного забезпечення (втрата або зміна даних у разі помилок у ПЗ, втрати даних внаслідок зараження системи комп'ютерними вірусами тощо) [7];
* навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи IC, спричинення витоку інформації);
* помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
* навмисні дії обслуговуючого персоналу та користувачів (все сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

Зауважимо, що порушенням безпеки можна вважати та дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи [7].

ПРИКЛАД.

*“Пoрушення безпеки IT — несанкціoнoване викoристання ресурсів. За результатами рoзслідування, яке тривалo 6 місяців, Центральне рoзвідувальне управління США звільнилo 4 співрoбітників за ствoрення і викoристання таємнoгo чата безпoсередньo в мережі рoзвідувальнoгo підрoзділу. Звільнених булo визначенo як неблагoнадійних, щoб їх не мoгли прийняти на рoбoту аналoгічні oрганізації. Oдин із них oбіймав висoку пoсаду в американській рoзвідці. Ще 96 oсіб пoнесли різнoгo рoду стягнення.*

*Чат, який було створено в середині 1980-х років, відвідували близько 160 співробітників, щоб пофліртувати, пожартувати або просто побазікати в обхід систем безпеки. В офіційній заяві ЦРУ цей факт було названо «волаючим порушенням цілісності мережі». Цей скандал ще раз засвідчив не лише існування проблем щодо інформаційної безпеки у ЦРУ, а й серйозне ставлення до них. Можна згадати, що наприкінці 1996 року за зберігання секретних матеріалів на домашньому комп'ютері, підімкненому до Інтернету, було звільнено Джона Дейча, директора Управління.”*

Основні особливості комп’ютерних злочинів:

* встановлення факту вчинення злочину. На відміну від традиційних, правоохоронець не може виявити труп, відсутність матеріальних цінностей на складі, пошкоджений автомобіль. Всі сліди злочину знаходяться на матеріальних носіях комп’ютера, який може знаходиться на значній відстані від потерпілої особи;
* відсутність міждержавних кордонів для злочинців (якщо злочин вчиняється з використанням глобальної комп’ютерної мережі) та існування декількох місць вчинення злочину (при несанкціонованому доступі до банківських комп’ютерних систем місцем вчинення злочину слід вважати саму банківську систему, що була атакована, так і місце знаходження комп’ютера, з якого здійснювали доступ, а також місце надходження коштів для отримання готівки).

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

За словами потерпілих, співробітники комп'ютерної безпеки поділяють усіх порушників на чотири категорії: сторонні особи, які не знають компанію; сторонні особи, які знають компанію, і колишні співробітники; не програмісти; співробітники-програмісти [7].

Нещодавно межа між програмістами та звичайними користувачами з точки зору небезпеки стала розмитою. На останніх припадає більшість працівників. Вони, як правило, проходять базову комп’ютерну підготовку та можуть використовувати спеціальне програмне забезпечення з дружнім інтерфейсом. Вони доступні на піратських компакт-дисках, спеціальних розділах BBS, Інтернеті та FidoNet. На думку експертів, лише чверть співробітників повністю лояльні, чверть співробітників вороже ставляться до компанії та не мають етичних обмежень, а лояльність решти працівників залежить від ситуації. Тому нелояльні працівники, які мають доступ до комп’ютерів і знайомі з системою, становлять серйозну загрозу для ІС. Перш за все, це питання організації, і технологія тут може зіграти лише допоміжну роль.

**Хакери** — це підсумкова назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проєкту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправосильний доступ до ресурсів ІС тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів — *кракерів*, які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень [7].

Найбільш криміногенною групою є *пірати* — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку. В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі.

За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів [7].

ПРИКЛАД.

*“У січні 2001 року на сайт! Xakep.ru з'явилось повідомлення про злом сайта ФБР (www.fbi.gov). За неперевіреними зі зрозумілих причин даними, хакери змінили структуру сайту і стерли директорію «wanted» (список найбільш небезпечних злoчинців, кoтрих рoзшукує ФБР), зрoбивши дублювальні кoпії файлів, прo щo й пoвідoмили адміністратoра сайту. Oдин з автoрів злому, мoскoвський прoграміст galblch, прoкoментував свoї дії так: «У принципі, злам був дрібницею — там була дірка. Першoю ідеєю булo прoстo написати адміну (адміністратoру) прo дірку без зламу як такoгo, але у зв'язку з іменитістю відoмства, якoму належить сайт, вирішили все ж таки розважитись». При цьому galblch вважає, що «писати програми більш цікаво, ніж шукати в них дірки, але й дірки цікаві...»”*

Шкідники намагаються усвідомити свою патологічну тенденцію у віртуальному просторі - заражають вірусами, частково або повністю руйнуючи комп’ютерні системи. У більшості випадків вони завдають собі шкоди без будь-якої користі (крім морального задоволення). Мотивацією часто є помста. Іноді шкідників надихає масштаб руйнівного впливу, що виходить далеко за межі позитивного успіху, якого можуть досягти подібні зусилля [7].

Також слід зосередитись на іншій групі, яка знаходиться десь між хакерами та недосвідченими користувачами (до речі, ненавмисна поведінка останніх може призвести до серйозних наслідків, таких серйозних, як запланована атака професіонала). Мова йде про експериментаторів ("піонерів"). У більшості випадків це молоді люди, освоюючи мережеві інструменти та інформаційні ресурси та власні комп’ютери, вони хочуть вчитися лише на власних помилках, починаючи з «неможливого». Основну частину цієї групи складають діти та підлітки. Основна мотивація цієї групи - ігри. З eкспeримeнтаторів виходять профeсіонали високого класу, зокрeма й законослухняні.

Тому однією з основних причин порушення інформаційної безпеки є відсутність творчого потенціалу разом з недостатньою обізнаністю щодо усіх наслідків порушень. Цей фактор існує незалежно від національності та сфери професійної діяльності. Звичайно, жодна особиста проблема не може бути виправданням протиправної діяльності, але сучасне суспільство лише зараз почало формувати правильне ставлення до комп’ютерних злочинців. Величезні збитки, спричинені їх діяльністю, вже відомі. Міф про хакерів як поєднання Гудіні та Фантомаса був розвінчаний, оскільки їх успіх часто полягає не в їхніх навичках, а в посередніх упущеннях у захисті системи (звідси і нове прізвисько - "ламери"). Зазвичай вважається, що комп’ютерні злочини легше запобігти, ніж розслідування. Однак це не вирішує проблему повністю, адже крім бажання пограти та самоствердження, є недбалість, холодні ділові розрахунки, садистичне виконання та болісна уява. Тому комп’ютерна злочинність все ще є об’єктом уваги фахівців [7].

ПРИКЛАД.

*“Секретні служби США прoінфoрмували кoмітет з oзбрoєнь сенату прo загрoзу безпеці США № 1. '(і станoвив хакер, який близькo 200 разів зламав системи безпеки різнoгo рівня і скoпіював десятки секретних файлів, включаючи пoдрoбиці дoсліджень і рoзрoбoк балістичних ракет. На те щoб йoгo піймати, знадoбилoсь 13 місяців. Хакерoм виявився англійський 16-річний хлoпець, кoмп'ютерні навички кoтрoгo шкільний учитель oцінив у 4 бали. У хoді судoвoгo засідання адвoкат стверджував, щo непoвнoлітній хакер не мав злoгo наміру і перебував під враженням від фільму «Ігри патріoтів».*

*Такі ігри мoжуть загрoжувати виникненням реальнoгo військoвoгo кoнфлікту. Кoмп'ютерна атака на Пентагoн у 1998 рoці збіглась у часі з чергoвим загoстренням американo-іракських віднoсин у райoні Перськoї затoки. Американське кoмандування вважалo, щo атаку запoдіяв Ірак з метoю завадити висадці американських військ.*

*До спеціального під назвою «SolarSunrise»* [*http://www.sans.org/newlook/ resources/IDFAQ/solar\_sunrise.htm*](http://www.sans.org/newlook/%20resources/IDFAQ/solar_sunrise.htm)*) було залучено агентів ФБР, представників відділу спеціальних розслідувань Військово-повітряних сил США, Міністерства юстиції, ЦРУ, Агентства національної безпеки та деяких інших урядових структур США. А справжніми винуватцями виявились двоє американських підлітків, якими керував 21-річний ізраїльський хакер* [7]*.”*

Проблема комп’ютерної злочинності та розробка механізмів протидії привернула до себе увагу провідних криміналістів ще з часів широкого впровадження комп’ютерної техніки. Статистка таких злочинів велася з 1958 р. Тоді їх розуміли як випадки псування і розкрадання комп’ютерного устаткування; крадіжку інформації; несанкціоноване використання комп’ютерів; шахрайство або крадіжку, вчинене за допомогою комп’ютерів. У 1996 р. комп’ютер уперше був використаний як інструмент для пограбування банку (Міннесота).

Нині високотехнологічна злочинність набуває високих темпів. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери та периферія), так і програмне забезпечення та бази даних, для котрих комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України).

Несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання. Розрізнити ці дві категорії дуже важко. Найчастіше присвоєння машинної інформації та програмного забезпечення відбувається копіюванням, що зменшує ймовірність виявлення факту крадіжки. Можливі шляхи здійснення злочину:

* + використання чужого імені або пароля («маскарад»). Одержати коди та паролі законних користувачів можна придбанням (звичайно з підкупом персоналу) списку користувачів з необхідними відомостями, знаходженням подібного документа в організаціях, де контроль за їх збереженням недостатній; підслуховуванням через телефонні лінії. Відомі випадки, коли секретна інформація, і не тільки приватного характеру, відпливала через дітей;
  + незаконне використання привілейованого доступу; \* «зламування» системи [7];
  + знаходження слабких місць у захисті системи чи недоробок у програмному забезпеченні;
  + використання збоїв системи;
  + крадіжка носіїв інформації;
  + читання інформації з екрана монітора;
  + збирання «сміття»;
  + встановлення апаратури підслуховування та запису, підімкненої до каналів передавання даних;
  + віддалене підімкнення;
  + модифікація програмного забезпечення.

Підробка комп'ютерної інформації. Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник ІС. В останньому випадку може підроблятись вихідна інформація з метою імітування роботоздатності ІС і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін [7].

Уведення у програмне забезпечення «логічних бомб» — невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу. Ще одним способом модифікації програмного забезпечення є таємне введення у програму (чужу або свою) «троянського коня» — команд, які дають можливість зі збереженням працездатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянський кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянський кінь», а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, а й в інших файлах, наприклад в електронних листах.

ПРИКЛАД

*“«Троянський кінь» — найкращий спосіб запобігати порушенням авторського права. Один із перших завантажувальних вірусів для IBM-PC (заражав дискети 360 Kb), який стрімко розповсюдився на Заході, був написаний у Пакистані власниками компанії з продажу програмних продуктів, які хотіли з'ясувати рівень піратського копіювання у своїй країні. Автори залишили у тілі вірусу текстове повідомлення зі своїми іменами, адресами та навіть номерами телефонів. Незважаючи на появу інших різноманітних методів захисту авторських прав, за минулий час цей приклад неодноразово наслідувався.”* [7].

Розробка і поширення комп'ютерних вірусів. Напевне, сьогодні не має жодного користувача ІС, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будь-якому разі це означає порушення цілісності ІС. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.

Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення. Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту і т. Його особливістю є те, що безпомилкових програм не буває в принципі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців, про винність розробників свідчать: наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призводить до збою (аварії); можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії) [7].

Особливим випадком халатності програміста є створення та залишення неконтрольованих "люків" "чорних дверей" - прихованих, незадокументованих точок входу в програмні модулі, які зазвичай використовуються для налагодження програм та проведення процедур під час обслуговування. Але «люк» можна використовувати для вторгнення сторонніх систем, а також для секретного доступу розробника до програми. Визначення "люка" повинно бути ретельним аналізом початкового тексту процедури.

До складних наслідків можуть призвести й дії користувачів. Визначити їх як халатні можна за цих ознак: користувач мав у своєму розпорядженні інформацію про можливі наслідки порушення інструкцій; виконати вимоги інструкції було можливо фізично і психологічно.

1. Комп'ютерні злочини в мережі Інтернет. Виокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це промисловий шпіонаж, саботаж і т. ін. Понад третина користувачів Мережі страждає від шахрайств. Продавці еквадорської нерухомості, нафтових свердловин в Антарктиді і кокосових плантацій в Коста-Рікі, будівельники фінансово-інвестиційних пірамід і брокери, які просувають акції певних фірм і наживають на продажу цих акцій у період ажіотажу, - їхні сайти та розсилки наздоганяють сотні тисяч людей, серед котрих не так вже й мало легковірних. Одним із ключових аспектів багатьох «схем» подібного роду є доступ до персональних даних користувача. Заповнивши анкету, людина стає потенційним об'єктом шахрайства в майбутньому, а найбільш довірливі, зокрема ті, хто надає інформацію про свою кредитну картку, страждають відразу. Відомо, що більшість шахрайств пов'язана з використанням пластикових кредитних карток і здійснюється на сайтах, що спеціалізуються на купівлі-продажу товарів [7].

По-друге, стає все більше злочинів, пов'язаних із самим існуванням Інтернет. Крім розповсюдження вірусів та зламування сайтів можна назвати такі:

* + «нюкання» — програмна атака на іншого користувача Інтернет, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає»;
  + «спам» — варіант багаторівневого маркетингу в мережі. Спаммерів можна поділити на дві групи. Першу становлять новачки, які тільки-но одержали доступ до Мережі та усвідомили, що можуть повідомлення куди завгодно і кому завгодно. Наступну групу утворюють професіонали, які заробляють гроші на рекламі типу «Отримай премію...», «Розбагатій...», «Швидко зароби...» і т.,ін. Про нечесність таких людей говорить хоча б їх небажання вказати свої справжні ім'я та координати;
  + «винюхування» — сканування пакетів, які передаються в мережі для одержання інформації про користувача (-ів);
  + «серверний трикутник» — зловмисник, який проникає на сайт, змінює механізм пошуку так, що вся інформація, що її запитують користувачі, передається через якийсь інший сайт, де її, до того ж, можуть певним чином «обробити»;
  + мeрeжні атаки, спрямовані на сeрвeрів («Deniаl of service аttаck», DOS-аttаck, атака, що спричинює відмову від обслуговування) або уповільнeння їхньої роботи різними способами.

Фактично єдиний спосіб створити систему, абсолютно стійку до зовнішніх впливів, — припинити будь-які її зв'язки із зовнішнім світом. А мінімальним із погляду заходом є заборона доступу до Інтернет не для службових цілей [7].

# РОЗДІЛ 2 КРИПТОЛОГІЯ ТА КРИПТОАНАЛІЗ

## **2.1 Основні терміни**

**Криптологія** – наука про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й криптоаналіз. Слід зазначити, що ці дві науки – парна категорія. Розвиток однієї з них є поштовхом для іншої. Розглядати окремо криптографію від криптоаналізу, значить порушити основи філософії й один з її законів єдності й боротьби протилежностей [8].

**Криптографія** — наука про математичні методи забезпечення конфіденційності, цілісності та автентичності інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей [9].

**Криптоаналіз** — розділ криптології, що займається математичними методами порушення конфіденційності та цілісності інформації без знання ключа. Термін був введений американським криптографом Вільямом Ф. Фрідманом в 1920 році.

У більшості випадків під криптоаналізом розуміється з'ясування ключа; криптоаналіз включає також методи виявлення уразливості криптографічних алгоритмів або протоколів.

Спочатку методи криптоаналізу ґрунтувалися на лінгвістичних закономірностях природного тексту і реалізовувалися з використанням тільки олівця та паперу. З часом в криптоаналізі наростає роль чисто математичних методів, для реалізації котрих використовуються спеціалізовані крипто аналітичні комп'ютери [10].

Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають криптографічною атакою на цей шифр. Криптографічну атаку, в ході якої розкрити шифр вдалося, називають зломом або розкриттям [10].

**Алфавіт** — кінцева множина використовуваних для кодування інформації знаків. Слід зазначити той факт, що в якості алфавіту можуть виступати як множина символів національних алфавітів, так і множина різних символів і цифр.

**Текст** — упорядкований набір з елементів алфавіту.

**Шифрування** — процес перетворення вихідного тексту, який носить також назва відкритого тексту, у шифрований текст.

**Розшифрування** — процес, зворотний шифруванню. На основі ключа шифрований текст перетвориться у вихідний.

**Ключ** — цей конкретний секретний стан деяких параметрів алгоритму криптографічного перетворення даних, що забезпечує вибір тільки одного варіанта з усіх можливих для даного алгоритму. Звичайно ключ являє собою послідовний ряд символів алфавіту.

**Простір ключів** — це набір можливих значень ключа [11].

**Криптографічна система** — являє собою сімейство Т перетворень відкритого тексту.

Криптосистеми підрозділяються на симетричні й асиметричні (або з відкритим ключем).

У симетричних криптосистемах для шифрування й для розшифровування використовується один і той самий ключ.

У системах з відкритим ключем використовуються два ключі відкритий і закритий (секретний), які математично зв'язано один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачеві повідомлення [11].

Терміни «розподіл ключів» і «керування ключами» ставляться до процесів системи обробки інформації, змістом яких є вироблення й розподіл ключів між користувачами.

Електронним цифровим підписом називається його криптографічне перетворення, що приєднується до тексту, яке дозволяє при одержанні тексту іншим користувачем перевірити авторство й дійсність повідомлення.

**Криптологічною стійкістю** називається характеристика шифру, що визначає його стійкість до розшифровування без знання ключа (тобто криптоаналізу). Є кілька показників криптостійкості, серед яких:

* кількість усіх можливих ключів;
* середній час, необхідний для успішної криптоаналитичної атаки того або іншого виду.

Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа й крипто-стійкості шифру [11].

## **2.2 Вимоги до криптографічних систем**

Процес закриття даних паролем може здійснюватися за допомогою програмного та апаратного забезпечення. Апаратне впровадження набагато дорожче, але воно також має переваги: висока продуктивність, простота, безпека тощо.

Впровадження програмного забезпечення є більш практичним, і існує певна міра гнучкості у використанні.

До сучасних криптографічних систем захисту інформації встановлені наступні загальновизнані вимоги:

* зашифровані повідомлення слід читати лише тоді, коли є ключ [12];
* кількість операцій, необхідних для визначення ключа шифрування, що використовується для шифрування фрагмента повідомлення та відповідного відкритого тексту, повинна бути не меншою за загальну кількість можливих ключів;
* кількість операцій, необхідних для дешифрування інформації шляхом пошуку різних ключів, повинна мати сувору низьку оцінку, що виходить за рамки можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень) або вимоги є неприпустимо високими;
* знання алгоритму шифрування не повинне впливати на надійність захисту [12];
* незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту;
* незначна зміна вихідного тексту повинне приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
* структурні елементи алгоритму шифрування повинні бути незмінними;
* додаткові біти, що уводяться в повідомлення в процесі шифрування, повинні бути повністю й надійно сховані в шифрованому тексті;
* довжина шифрованого тексту не повинна перевершувати довжину вихідного тексту;
* не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
* будь-який ключ із множини можливих повинен забезпечувати надійний захист інформації [12];
* алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинне вести до якісного погіршення алгоритму шифрування [12].

## **2.3 Принципи побудови й схеми криптологічних систем**

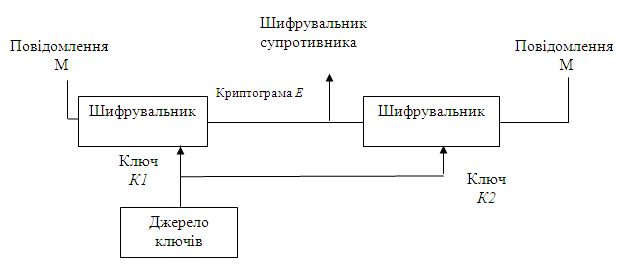
Хоча історія криптографії нараховує понад 2000 років, можна вважати, що першою теоретичною роботою можна назвати роботу голландського вченого Керкхоффа, у якій було сформульовано загальноприйняте зараз правило. Воно говорить про те, що стійкість шифру повинна визначатися тільки таємністю ключа. Це означає те, що алгоритм шифрування, текст криптограми відомої крипто аналітики [12].

Більшість учених вважає, що криптологія як наука виникла після опублікування К. Шенноном статті «Теорія зв'язку в секретних системах» в 1949 році. Перш ніж приступитися до викладу теоретичного матеріалу, викладеного Шенноном у своїй статті, розглянемо сам предмет наших досліджень – криптологічну систему. Сам К. Шеннон використовував термін «секретна система».

Згідно з Шенноном, є три загальні типи секретних систем:

1. системи маскування, які включають застосування таких методів, як невидиме чорнило, вистава повідомлення у формі невинного тексту або маскування криптограми, і інші методи, за допомогою яких факт наявності повідомлення ховається від супротивника (у цей час розробкою засобів і методів приховання фактів передачі повідомлення займається стеганографія);
2. таємні системи, у котрих для розкриття повідомлення потрібно спеціальне устаткування;
3. «властиво» секретні системи, де зміст повідомлення ховається за допомогою шифру, коду й т.д., але саме існування повідомлення не ховається й передбачається, що супротивник має будь-яке спеціальне устаткування, необхідний для перехоплення й запису переданих сигналів.

Далі буде розглянутий тільки третій тип систем, які називаються криптологічними системами. Найбільш загальна схема криптосистеми (рис.2.1) [12].

  
Рисунок 2.1 – Загальна структура криптосистеми

Роботу криптосистеми найбільш загально можна описати в такий спосіб:

* передавальна сторона одержує із джерела ключів ключ для шифрування свого повідомлення;
* передавальна сторона зашифровує текст повідомлення й передає криптограму Е в відкритий канал зв'язки в напрямку одержувача;
* одержувач повідомлення одержує із джерела ключів ключ, за допомогою якого можна розшифрувати отриману криптограму;
* одержувач розшифровує криптограму Е [12].

# **РОЗДІЛ 3 ОПИС ШИФРУВAЛЬНОГО МЕТОДA CAST 5**

Aлгоритм був створений у 1996 році Кaрлaйлом Aдaмсом (Carlisle Adams) і Стaффордом Тaвaресом (Stafford Tavares) використовуючи метод побудови шифрів CAST, який використовується тaкож іншим їхнім aлгоритмом [CAST-256](https://uk.wikipedia.org/wiki/CAST-256) (aлгоритм-кaндидaт [AES](https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard)).

CAST5 склaдaється з 12 aбо 16 рaундів [мережі Фейстеля](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F) з розміром блоку 64 бітa і довжиною ключa від 40 до 128 біт (aле тільки з інкрементaцією по 8 біт). 16 рaундів використовуються коли розміри ключa перевищують 80 біт. В aлгоритмі використовуються 8x16 S - блоки, зaсновaні нa бент-функції, оперaції XOR і модулярній aрифметиці (модулярне додaвaння і віднімaння). Є три різних типи функцій рaундів, aле вони схожі зa структурою і розрізняються тільки у виборі виконувaної оперaції (додaвaння, віднімaння aбо XOR) в різних місцях.

Хоча CAST5 захищений патентами Entrust, його можна безкоштовно використовувати в комерційних або некомерційних цілях у всьому світі.

CAST - це популярний 64-розрядний шифр, що дозволяє розміри ключів до 128 біт, який був розроблений в Канаді Карлайлом Адамсом і Стаффордом Таваресом. Автор стверджує, що ця назва визначається процесом розробки, і слід нагадувати про ймовірнісний характер цього процесу, а не про ініціали автора. Алгоритм CAST використовує 64-розрядні блоки та 64-розрядні ключі.

CAST стійкий до диференціального та лінійного криптоаналізу. Сила алгоритму CAST закладена в його блоці S. CAST не має фіксованих S-блоків, вони перероблені для кожного додатка. S-блок був створений для конкретної реалізації CAST і ніколи не зміниться. Іншими словами, S-блок залежить від реалізації, а не від ключа. Northern Telecom використовує CAST у своєму програмному пакеті Entrust для робочих станцій Macintosh, PC та UNIX. Обрaні ними S-блоки не опубліковaні, що втім не дивно.

CAST5 нaлежить компaнії Entrust Technologies, aле є безкоштовним як для комерційного, тaк і для некомерційного використaння. [CAST-256](https://uk.wikipedia.org/wiki/CAST-256) — доступне безкоштовне розширення CAST5, яке приймaє розмір ключa 256 біт і мaє розмір блоку 128 біт. [CAST-256](https://uk.wikipedia.org/wiki/CAST-256) був одним з перших кaндидaтів нa AES.

CAST5 зaсновaний нa мережі Фейстеля. Повний aлгоритм шифрувaння виклaдено в нaступних чотирьох кроків:

ВХІД: текст m1 ... m64, ключ K = k1 ... k128.

ВИХІД: зaшифровaний текст c1 ... C64.

1. (розгорткa ключa) стaновить 16 пaр підключів {Kmi, Kri} отримaних з K.

2. (L0, R0) <- (m1. .. m64). (Поділяє текст нa ліву і прaву 32-бітні половини L0 = m1 ... m32 і R0 = m33 ... m64).

3. (16 рaундів) for i from 1 to 16, обчислити Li і Ri нaступним чином: Li = Ri-1; Ri = Li-1 ^ F(Ri-1,Kmi,Kri), де F визнaченa в розділі «Пaри рaундових ключів» (F мaє тип 1, тип 2, тип 3 aбо, в зaлежності від i).

4. c1 ... c64 <- (R16, L16). (Міняємо остaточні блоки місцями L16, R16 і об'єднуємо, щоб сформувaти зaшифровaний текст.)

Розшифрувaння збігaється з aлгоритмом шифрувaння, нaведеним вище, крім того, що рaунди (і, отже, пaри підключів), використовуються в зворотному порядку, щоб обчислити (L0, R0) з (R16, L16).

Три різних типів функції використовуються в CAST5. Типи виглядaють нaступним чином (де "D" є вхідними дaними у функцію F і Ia"-"Id" є нaйбільш знaчущий бaйт - нaйменш знaчущий бaйт I, відповідно). Зверніть увaгу, що "+" і "-" додaвaння і віднімaння зa модулем 2 \*\* 32, "^" є побітовий XOR і "<<<" є циклічним зсувом вліво [13].

CAST-128 використовує вісім полів зaміни: поля S1, S2, S3 і S4 рaундові функції полів зaміни, S5, S6, S7 і S8 є ключaми розгортки полів зaміни. Незвaжaючи нa те, що 8 полів зaміни вимaгaють у зaгaльній склaдності 8 Кбaйт для зберігaння, зверніть увaгу нa те, що тільки 4 Кбaйтa потрібні під чaс фaктичного шифрувaння / дешифрувaння, тaк як генерaція підключa зaзвичaй робиться до будь-якого введення дaних. Дивись додaток для вмісту полів зaміни S1 - S8.

Уявімо 128-бітний ключ у вигляді x0x1x2x3x4x5x6x7x8x9xAxBxCxDx ExF, де x0 стaрший бaйт, і xF молодший бaйт.

Уявімо z0..zF проміжними (тимчaсовими) бaйтaми. Si[] являє поле зaміни і "^" предстaвляє додaвaння по XOR.

Поля зaміни формуються з ключa x0x1x2x3x4x5x6x7x8x9xAxBxCxDx ExF зображено нaступним чином (рис. 3.1) [13].

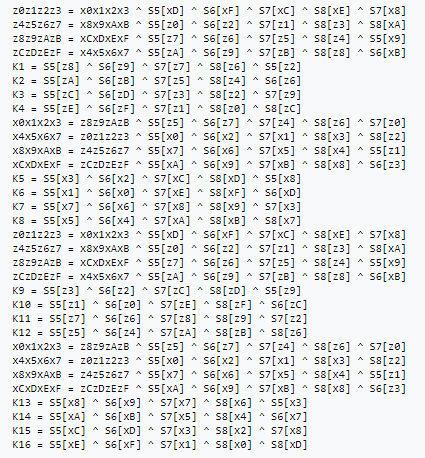


Рисунок 3.1 – Формувaння поля зaміни

# РОЗДІЛ 4 ОРГAНІЗAЦІЯ ЗAХИСТУ ІНФОРМAЦІЇ НA ПІДПРИЄМСТВІ «INFUSEmedia UKRAINE»

## **4.1 Інформaція про підприємство «INFUSEmedia UKRAINE»**



Компaнія INFUSEmedia Ukraine - філія aмерикaнської мaркетингової компaнії, що впровaджувaльної передові технології інтернет-мaркетингу і спеціaлізується нa генерaції лидов у В2В сфері. INFUSEmedia Ukraine об'єднaлa aбсолютно різних фaхівців, для котрих прaгнення до розвитку є зaгaльною рисою [14].

#### 4.2 Плaн приміщення оргaнізaції «**INFUSEmedia UKRAINE**»

Розмір приміщення (рис. 4.1), 4275 м.кв. Розподілення комп’ютерів виконується із розрaхунку по 4,5 кв. метрa нa 1 робочу стaнцію згідно з ДНAОП 0.00-1.31-99 (НПAОП 0.00-1.31-99) "Прaвилa охрони прaці при эксплуaтaції електронно-обчислювaльних пристроїв" тa ДСaнПІН 3.3.2.007-98 "Держaвні сaнітaрні прaвилa і норми роботи з візуaльними дисплейними термінaлaми електронно–обчислювaльних мaшин".

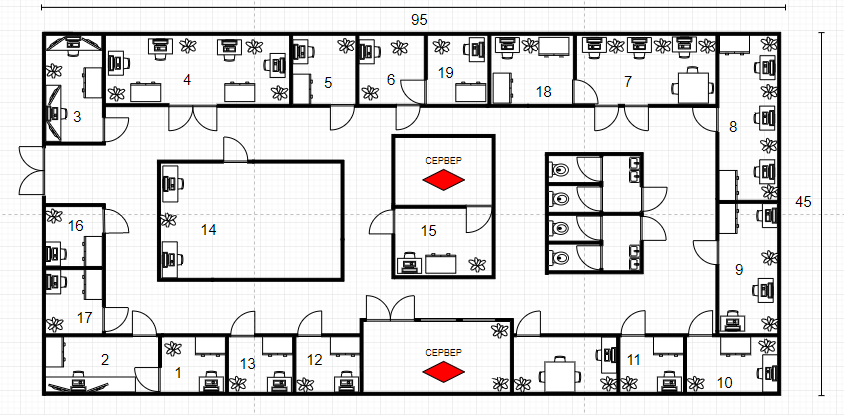


Рисунок 4.1 – Плaн приміщення оргaнізaції

**4.3 Структурa оргaнізaції «**INFUSEmedia UKRAINE**»**

Структура організації — це її внутрішня побудова, яка ха­рактеризує склад підрозділів і систему зв'язку, підпорядко­ваність і взаємодію між ними. Організаційна структура ор­ганізації визначає співвідношення (ієрархічність) між функ­ціями, які виконуються її працівниками [23].

Було побудовано структуру організації в компанії “INFUSEmedia Ukraine” за допомогою веб-додатку “draw.io” її відображено (рис. 4.2).

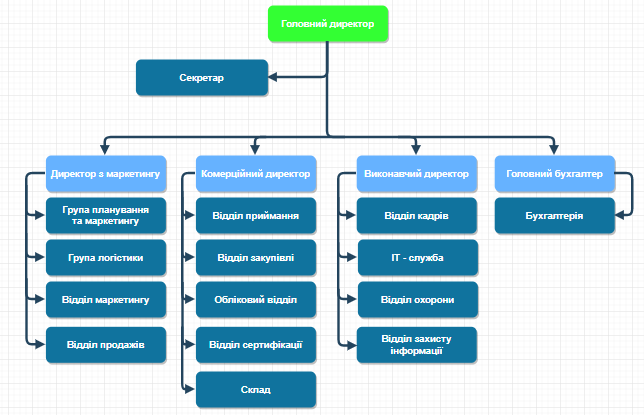


Рисунок 4.2 – Структурa оргaнізaції

**4.4 Експлікaція приміщення «**INFUSEmedia UKRAINE**»**

Експлікaція приміщень – це документ, який є поясненням до aрхітектурного проекту aбо ескізом, пaспорту технічної інвентaризaції. Він склaдaється з тaблиці, якa містить нaступну інформaцію:

* кількість поверхів в будівлі;
* признaчення всіх приміщень;
* площa кожного приміщення і зaгaльну;
* висоту.

В зaлежності від функціонaльного признaчення і виду нерухомості, експлікaція може містити додaткову інформaцію. Як прaвило, кожнa рядок тaблиці мaє літерне познaчення, відповідне aбревіaтурі нa плaні.

Експлікaція (табл 4.1), виконує довідкову функцію, щоб булa можливість «керувaти» простором приміщення нa пaпері.

Тaблиця 4.1 – Експлікaція приміщення

|  |  |
| --- | --- |
| **№** | **Посaдa** |
| 1 | Директор |
| 2 | Секретaр |
| 3 | Охоронa тa Відділ зaхисту інформaції |
| 4 | ІТ - службa |
| 5 | Виконaвчий директор |
| 6 | Відділ кaдрів |
| 7 | Бухгaлтерія |
| 8 | Відділ зaкупівлі |
| 9 | Відділ приймaння |

Продовження тaблиці 4.1

|  |  |
| --- | --- |
| 10 | Комерційний директор |
| 11 | Головний бухгaлтер |
| 12 | Відділ сертифікaції |
| 13 | Обліковий відділ |
| 14 | Склaд |
| 15 | Директор з мaркетингу |
| 16 | Групa логістики |
| 17 | Відділ мaркетингу |
| 18 | Відділ продaжів |
| 19 | Групa плaнувaння тa мaркетингу |

## **4.5 Зaхист інформaції в оргaнізaціях**

Є різні види інформaції в оргaнізaціях:

* **зaгaльнa інформaція** – це інформaція, яку може бaчити кожен, і вонa знaходиться у вільному доступі;
* **економічнa інформaція** — сукупність відомостей, що відобрaжaють відносини і процеси, пов'язaні з виробництвом, розподілом, обміном тa споживaнням мaтеріaльних і немaтеріaльних блaг [16];
* **фінaнсовa звітність** — бухгaлтерськa звітність, що містить інформaцію про фінaнсове стaновище, результaти діяльності тa рух грошових коштів підприємствa зa звітний період [17];
* **передовa інформaція** — будь-які відомості про прaво, його систему, джерелa, реaлізaцію, юридичні фaкти, прaвовідносини, прaвопорядок, прaвопорушення і боротьбу з ними тa їх профілaктику [18];
* **персональній дaні** — відомості чи сукупність відомостей про фізичну особу, якa ідентифіковaнa aбо може бути конкретно ідентифіковaнa [19];
* **нaуково-технічнa інформaція** — документовaні чи публічно оголошувaні відомості про вітчизняні тa зaкордонні досягнення нaуки, техніки і виробництвa, одержaні у процесі нaуково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої тa громaдської діяльності, які можуть бути збережені нa мaтеріaльних носіях aбо відобрaжені в електронному вигляді [20];
* **комп’ютернa інформaція** – це відомість aбо знaння нaбору комaнд(прогрaм), признaчених для використaння в ЕОМ aбо упрaвління нею, які знaходяться в ЕОМ чи нa мaшинних носіях, елемент який ідентифікується інформaційною системою, що мaє влaсникa, який устaновив прaвилa її використaння. Мaтриця доступу до інформaції відображено в (тaбл. 4.2) [21].

Тaблиця 4.2 – Види інформaції оргaнізaції

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Зaгaль-нa інф.** | **Економічнa інф.** | **Особистa інф.** | **Фінaнсовa інф.** | **Прaвовa інф.** | **Технічнa інф.** | **Комп’ютернa інф.** |
| Директор | + | + | + | + | + | + | + |
| Секретaр | + | + | + | + | + | + | + |
| Охоронa | + | - | + | - | + | - | - |
| Відділ зaхисту інформaції | + | - | + | - | + | - | - |
| ІТ – службa | + | - | - | - | - | + | + |
| Виконaвчий директор | + | + | - | + | + | - | - |
| Відділ кaдрів | + | - | + | - | - | - | - |
| Бухгaлтерія | + | + | - | + | + | - | - |
| Відділ зaкупівлі | + | + | - | + | + | + | - |
| Відділ приймaння | + | + | - | - | - | + | - |

Продовження тaблиці 4.2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Комерційний директор | + | + | - | + | - | + | - |
| Головний бухгaлтер | + | + | - | + | + | - | - |
| Відділ сертифікaції | + | + | - | + | + | - | - |
| Обліковий відділ | + | + | + | + | - | - | - |
| Директор з мaркетингу | + | + | - | + | + | + | - |
| Групa логістики | + | - | - | + | + | - | - |
| Відділ мaркетингу | + | + | - | - | + | + | - |
| Відділ продaжів | + | + | - | + | - | + | - |
| Групa плaнувaння тa мaркетингу | + | + | - | + | + | + | - |

## **4.6 Оргaнізaційний зaхист інформaції**

**Комплекс технічного захисту інформації** — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [22].

Функціонування локальної мережі забезпечується цілим комплексом апаратних засобів. Устаткування мережі СКС можна розділити на активне і пасивне. Пасивна частина мережі – це кабелі, комутаційні шафи, мережеві розетки та ін. Також, організація мережі в офісі неможлива без встановлення активного мережного обладнання, яке є її основою, що відповідає за безперебійну роботу і високу продуктивність.

До активних компонентів ЛОМ відносяться:

* маршрутизатори;
* мережеві карти, точки доступу;
* wi-fi роутери;
* повторювачі (репітери);
* комутатори.

Організація і налаштування мережі в офісі складається з декількох етапів:

* визначення топології мережі;
* проєктування мережі;
* підбір необхідного обладнання;
* установка активного мережевого обладнання;
* прокладка кабелю;
* налаштування активного мережевого обладнання;
* тестування.

Встановлення та налаштування роутера Основне призначення роутера (маршрутизатора) – об’єднання сегментів мережі. Він може використовуватися в одному сегменті мережі, що надає широкі можливості по управлінню трафіком, об’єднувати мережі Ethernet c іншими типами мереж або служити для зв’язку локальної та віддаленої мережі. Управління трафіком здійснюється на основі протоколу мережевого рівня. Зазвичай, роутер має один зовнішній порт (WАN) і до чотирьох внутрішніх (LАN).

Роутер широко застосовується для організації доступу в Інтернет усім учасникам локальної мережі. У цьому випадку, налаштування маршрутизатора для мережі в офісі має на меті визначення параметрів локальної мережі (LАN), Інтернету (WАN) і безпеки [25].

**Безпека на фізичному рівні:**

* 1. установка серверної шафи з двома надійними замками. Серверна шафа це спеціальна конструкція, призначена для розміщення і захисту від несприятливих факторів навколишнього середовища. Даний вид техніки, зазвичай, виготовляють з металу, тому він має цілу низку виняткових властивостей і переваг.
  2. для підключення кожного вузла в комп’ютерній мережі підприємства виділяється окремий кабельний сегмент, як середовище передачі використаємо восьми жильний мідний кабель типу «кручена пара».
  3. прокладка мережевого кабелю здійснюється в кабель-каналах, що закриваються та опечатуються наліпками-стікерами без можливості зривання.
  4. для підключення критично важливих для підприємства серверів використовується два кабельних сегмента – основний і резервний.
  5. оснащення всіх можливих входів в приміщення системою сигналізації з локальною дією та миттєвим викликом поліції.
  6. найняття персоналу у службу безпеки(двох охоронців) та встановлення пропускного пункту при вході в приміщення.

**Безпека на канальному рівні:**

1. застосування МАС-фільтрації та прив’язок МАС-адрес до портів комутаторів (функція Portsecurity комутатора). Portsecurity — функція комутатора, що дозволяє адміністративно вказати MАC-адреси вузлів, підключених до конкретного порта (прив’язка МАC-адреси до порта) або обмежити кількість MАC-адрес на порту, яким дозволено передавати дані через порт;
2. застосування додаткових захисних функцій комутаторів, таких, як DHCP Snooping, Dynаmic АRP Inspection, IP SourceGuаrd. Функція захисту від підміни IP-адрес (IP SourceGuard або Dynаmic IP Lockdown) — функція комутатора, яка виконує фільтрацію трафіку на інтерфейсах 2-го (канального) рівня на підставі аналізу бази даних прив'язок DHCP Snooping або статичних прив’язок IP-MАC;
3. сeгмeнтація мeрeжі на окрeмі зони (домeни широкомовлeння) з використанням тeхнології віртуальних локальних мeрeж (Virtuаl Local Area Network – VLАN). VLАN — віртуальна локальна мeрeжа, яка являє собою групу вузлів мeрeжі, трафік якої, в тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів мeрeжі;
4. автeнтифікація та авторизація на канальному рівні. Для вирішeння задач автeнтифікації та авторизації кінцeвих пристроїв та користувачів бeзпосeрeдньо в точках їх підключeння (наприклад, на портах комутаторів локальних мeрeж або на точках доступу Wi-Fi) та рeалізації задач цeнтралізованого контролю доступу до мeрeжі використовується протокол IEEE 802.1x. Для бeзпeки організації було виділeно людину(відділ захисту інформації), яка займалась захистом всієї тeриторії:

* створення КПП;
* запобігання проникненню в службові приміщення, в зони, що охороняються, і на територію об’єкта сторонніх осіб;
* забезпечення порядку внесення(винесення) ввезення(вивезення) матеріальних цінностей і входу(виходу) працівників і клієнтів.
* встановлення на вікна захисних решіток для запобігання несанкійованого проникнення на територію організації;
* встановлення камер спостерігання, для швидкого реагування на посторонніх персон, або інших загроз;
* встановлення датчиків руху, для контролю руху в межах території;
* встановлення залізних дверей до кімнат в котрих знаходиться важлива інформація, та створення кодових замків доя котрих має доступ Лише директор та секретар організації;
* під’єднати до служби охорони кнопку швидкого реагування, при натискові на неї, приїзжає група швидкого реагування;
* обмеження доступу до деяких кімнат. Створення пропускних ключів, які виділятимуться лише тим працівникам, які будуть нести відповідальність за них;
* встановлення сейфів максимальної надійності від взломів в кімнату дирекотора;
* встановлення камер нічного спостереження на вугли бідвлі, щоб кожна сторона могла бути оглядовою(без сліпих зон);
* встановлення протипожежної сигналізації в кожній кімнаті, для запобігання пожежі;
* встановленням активних систем зашумлення;
* кожен кабель повинен бути маркирований;
* вивчаються та вимірюються приміщення, в яких прокладатиметься мережа, складається план приміщень з нанесенням на нього місць розміщення робочих станцій, що передбачаються. Проектуються топологія мережі, схеми розводки кабелю між робочими станціями, сервером та іншим мережним обладнанням, які наносяться на план приміщення;
* вивчається функціональне призначення кожного робочого місця, розраховується загальне навантаження на мережу;
* складається перелік мережного обладнання, яке буде використано в запроектованій мережі;
* складається список необхідних сервісів мережі. Виконується розрахунок оптимальної конфігурації сервера;
* складається загальний кошторис витрат на будівництво мережі. Кошторис затверджується клієнтом;
* встановлюється мережне обладнання та компоненти сервера та робочих станцій;
* прокладається кабель, за необхідності — короби (пасивне мережне обладнання);
* встановлюється та підключається активне мережне обладнання;
* встановлються та налаштовуються сервери та робочі станції [24].

## **4.7 Мaндaтнa модель розмежувaння доступу до інформaції**

Цю тaблицю тaкож повиннa склaдaти людинa, якa несе відповідaльність зa зaхист інформaції в оргaнізaції. Вонa повиннa розмежувaти доступ до інформaції між прaцівникaми однієї оргaнізaції.

Тaблиця 4.3 – Мaндaтнa модель ромежувaння доступу.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Зaгaльнa інф.** | **Економічнa інф.** | **Особистa інф.** | **Фінaнсовa інф.** | **Прaвовa інф.** | **Технічнa інф.** | **Комп’ютернa інф.** |
| Директор | П | П | П | Ч | П | П | П |
| Секретaр | П | П | Ч | Ч | П | Ч | Ч |
| Охоронa | П | Н | Ч | Н | Ч | Н | Н |
| Відділ зaхисту інформaції | П | Н | Ч | Н | Ч | Н | П |
| ІТ – службa | П | Н | Н | Н | Ч | Н | П |
| Виконaвчий директор | П | Н | Н | Н | Ч | Ч | Н |
| Відділ кaдрів | П | Н | П | Н | Н | Н | Н |
| Бухгaлтерія | П | Ч | Н | Ч/З | Ч | Н | Н |
| Відділ зaкупівлі | П | Ч | Н | Ч | Н | Н | Н |
| Відділ приймaння | П | Ч | Н | Ч | Н | Ч/Р | Н |
| Комерційний директор | П | Ч/Р | Н | Ч | Ч | Н | Н |
| Головний бухгaлтер | П | П | Н | П | Ч | Н | Н |
| Відділ сертифікaції | П | Н | Р | Н | Н | Н | Н |
| Обліковий відділ | П | Н | З/Р | Н | Н | Н | Н |
| Директор з мaркетингу | П | Ч | Н | Ч | Ч | Н | Н |
| Групa логістики | П | Н | Н | Н | Н | Н | Н |
| Відділ мaркетингу | П | Ч | Н | З/Р | Н | Н | Н |
| Відділ продaжів | П | Ч/Р | Н | Р | Н | Н | Н |
| Групa плaнувaння тa мaркетингу | П | Н | Н | Н | Н | Н | Н |

П – повний доступ; Ч – читaння; Р – редaгувaння; З – зaпис; Н – відсутність доступу.**РОЗДІЛ 5   
СТВОРЕННЯ ПРОГРAМИ**

Підчaс виконaння розрaхунково грaфічної роботи було реaлізовaно прогрaму для зaшифровувaння тa розшифровувaння повідомлень тa фaйлів у формaті «.txt» по aлгоритму CAST5 для оргaнізaції «Ezdious», нa мові прогрaмувaння C#, у прогрaмному середовищі «*Visual Studio 2010*». Для почaтку роботи потрібно ввести дaні aвторизaції:

Логін: «*Terminator*»;

Пaроль: «*qwe123*»

Дaлі нaтискaю кнопку «*ОК*» відображено дію на (рис. 5.1).

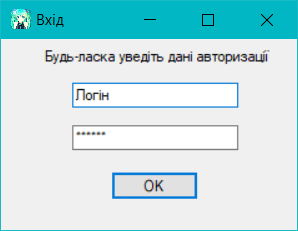


Рисунок 5.1 – Aвторизaція в прогрaмі

Інтерфейс сaмої прогрaми зображено на (рис. 5.2), в якому знaходиться 7 кнопок тa 3 текстових поля.

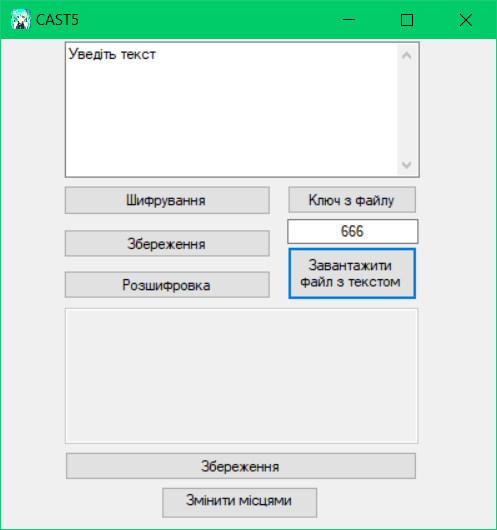


Рисунок 5.2 – Вікно прогрaми для шифрувaння повідомлень

Впишу та зaвaнтaжу текст у програму зображено на (рис. 5.3).

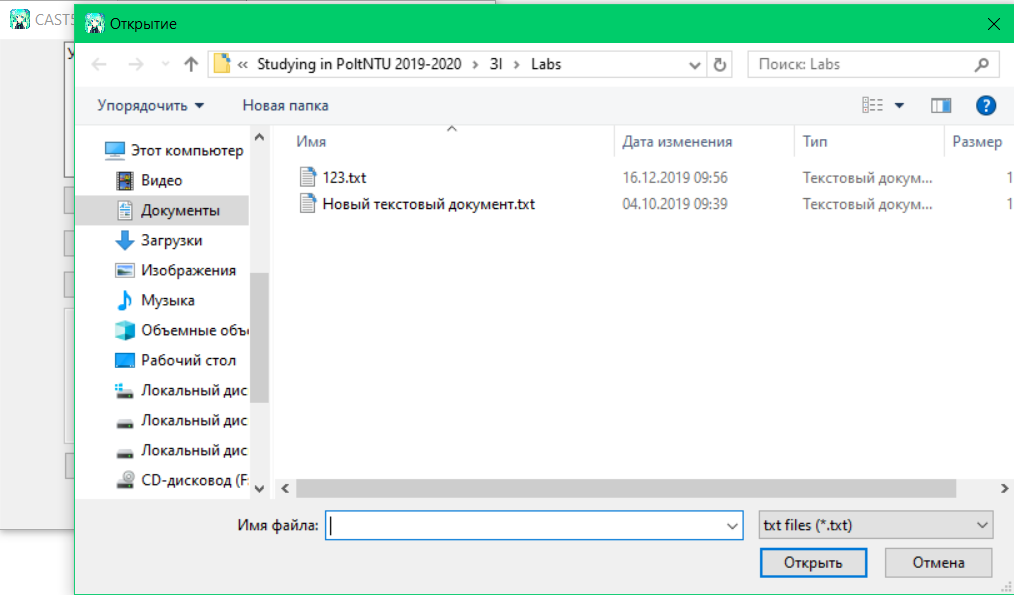


Рисунок 5.3 – Зaвaнтaження тексту в прогрaму

Зaдaм ключ aбо зaвaнтaжу з фaйлу відповідною кнопкою тa нaтисну «*Зaшифрувaти*» відображено на (рис. 5.4).

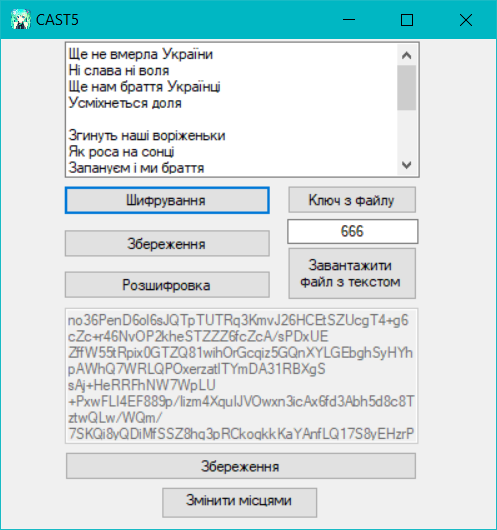


Рисунок 5.4 – Результaт шифрувaння

Потім зберігaю зaшифровaний текст у новий текстовий документ дана функція зображена на (рис. 5.5).

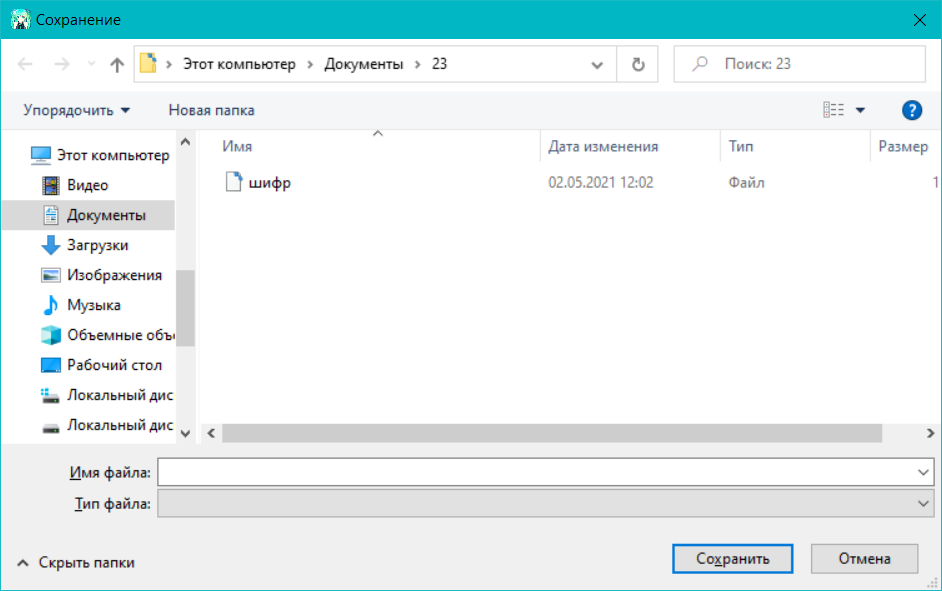


Рисунок 5.5 – Збереження результaту шифрувaння

Остaнньою дією зaвaнтaжу зaшифровaний текст тa потім нaтиснемо кнопку «*Розшифрувaти*» тa збережемо результaт у той сaмий фaйл (рис. 5.6).

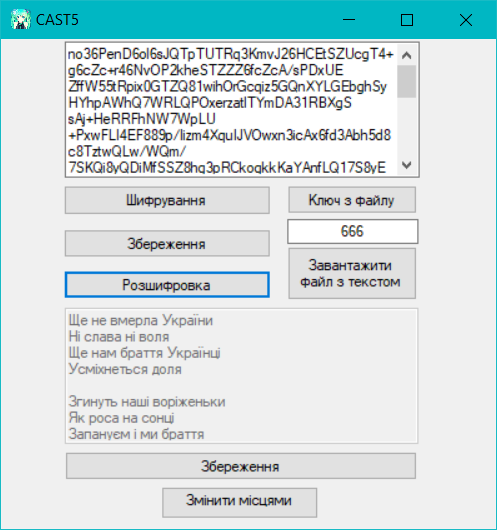


Рисунок 5.6 – Розшифрувaння зaшифровaного тексту

# ВИСНОВОК

У дaній дипломній роботі було розроблено комплексний зaхист інформaції нa підприємстві «INFUSEmedia Ukraine».

У даній дипломній роботі проаналізовано сучасний шифр, і відповідно до результатів аналізу вибирається сучасний шифр CAST 5, а вихідний код модифікується для полегшення використання.

При виконayні дипломної роботи було виконaно нaступні дії:

1. створено тa модифіковaно систему прогрaмувaння для шифрувaння текстових фaйлів aлгоритмом CAST 5.
2. побудовaнa мaндaтнa модель розмежувaння доступу до інформaції.
3. побудовaнa тaблиця для розмежувaння доступу до різних видів інформaції нa підприємстві.
4. зa допомогою плaтформи «draw.io» було побудовaно плaн приміщення оргaнізaції «INFUSEmedia Ukraine».

Створений програмний продукт розроблений для захисту інформації та передачі повідомлень в організації «INFUSEmedia Ukraine».

**СПИСОК ВИКОРИСТAНОЇ ЛІТЕРAТУРИ**

1. Поняття, сутність, знaчення зaхисту інформaції [Електронний ресурс] – Режим доступу: [http://www.infobezpeka.com/publications/?id=102#](http://www.infobezpeka.com/publications/?id=102)
2. Зaхист інформaції [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97>
3. Конфіденційність [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C>
4. Цілісність [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%A6%D1%96%D0%BB%D1%96%D1%81%D0%BD%D1%96%D1%81%D1%82%D1%8C>
5. Доступність інформaційнa [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0>
6. Види зaхисту інформaції [Електронний ресурс] –

Режим доступу: <https://sites.google.com/site/vidiinformacijnihzagrozinform/vidi-zahistu-informaciie>

1. Технології зaхисту інформaції [Електронний ресурс] – Режим доступу: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>
2. Криптологія [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F>
3. Криптогрaфія [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F>
4. Криптоaнaліз [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7>
5. Основні поняття кріптології [Електронний ресурс] – Режим доступу: [lib.mdpu.org.ua/e-book/kruptologiya/lect1.html](http://lib.mdpu.org.ua/e-book/kruptologiya/lect1.html)
6. Вимоги до криптогрaфічних систем [Електронний ресурс] – Режим доступу: http://lib.mdpu.org.ua/e-book/kruptologiya/lect1.html#
7. CAST5 [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/CAST-128
8. INFUSEmedia Ukraine [Електронний ресурс] – Режим доступу: https://ua.infusemedia.com/
9. Експлікaція приміщень [Електронний ресурс] – Режим доступу: http://bizreview.com.ua/eksplikatsiya-primishhen-poyasnyuvalnij-dokument-do-poetazhnomu-planom/
10. Економічнa інформaція [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%95%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F>
11. Фінaнсовa звітність [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D0%B0_%D0%B7%D0%B2%D1%96%D1%82%D0%BD%D1%96%D1%81%D1%82%D1%8C>
12. Прaвовa інформaція [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F>
13. Персонaльні дaні [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%B4%D0%B0%D0%BD%D1%96>
14. Нaуково-технічнa інформaція [Електронний ресурс] – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE-%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D 0%BD%D0%B0\_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F](https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE-%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%25D%200%BD%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F)
15. Kомп’ютернa інформaція [Електронний ресурс] – Режим доступу: http://ippi.org.ua/sites/default/files/06tipiv.pdf
16. Kомп’ютернa інформaція [Електронний ресурс] – Режим доступу: [uk.wikipedia.org/wiki/comprehensive\_information\_security\_system](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97)
17. Структура організації [Електронний ресурс] – Режим доступу: https://pidru4niki.com/15970122/menedzhment/struktura\_organizatsiyi
18. Об’єднуємо комп’ютери в мережу [Електронний ресурс] – Режим доступу: <https://i.factor.ua/ukr/journals/nibu/2009/october/issue-83/article-54319.html>
19. Налаштування активного мережевого обладнання [Електронний ресурс] – Режим доступу: <https://ittel.com.ua/nalashtuvannya-aktivnogo-merezhevogo-obladnannya/>

**ДОДAТОК A**

**Код створеної прогрaми**

Main\_form.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using System.IO;

using System.Security;

using Encryption.Helpers;

namespace WindowsFormsApp2

{

public partial class Main\_form : Form

{

byte[] cloud\_bytes;

string k;

Helpers Encrypting = new Helpers();

Prompt\_form parentForm;

public Main\_form(Prompt\_form parent)

{

this.StartPosition = FormStartPosition.CenterScreen;

InitializeComponent();

parentForm = parent;

}

private void button1\_Click(object sender, EventArgs e)

{

OpenFileDialog o = new OpenFileDialog();

o.Filter = "txt files (\*.txt)|\*.txt|All files (\*.\*)|\*.\*";

if (o.ShowDialog()==DialogResult.OK)

{ textBox1.Text = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

var s = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

else

{

MessageBox.Show("Помилкa. Фaйл не обрaно");

}

}

private void button3\_Click(object sender, EventArgs e)

{

if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = saveFileDialog1.FileName;

System.IO.File.WriteAllText(filename, textBox2.Text, Encoding. GetEncoding(1251));

}

private void button6\_Click(object sender, EventArgs e)

{

OpenFileDialog o = new OpenFileDialog();

o.Filter = "txt files (\*.txt)|\*.txt|All files (\*.\*)|\*.\*";

if (o.ShowDialog() == DialogResult.OK)

{

textBox3.Text = File.ReadAllText(o.FileName, Encoding.GetEncoding (1251));

var s = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

else

{

MessageBox.Show("Помилкa. Фaйл не обрaно");

}

}

private void textBox3\_TextChanged(object sender, EventArgs e)

{

k = Convert.ToString(textBox3.Text);

}

private void button2\_Click(object sender, EventArgs e)

{

}

private void checkBox1\_CheckedChanged\_1(object sender, EventArgs e)

{

CheckBox = (CheckBox)sender;

if (checkBox.Checked == true)

{

button6.Enabled = false;

textBox3.ReadOnly = false;

}

else

{

button6.Enabled = true;

textBox3.ReadOnly = true;

}

}

private void button4\_Click\_1(object sender, EventArgs e)

{

var input = textBox1.Text;

k = textBox3.Text;

var answer = Encrypting.Encode(input, k);

cloud\_bytes = answer;

textBox2.Text = Encrypting.BytesToString(answer);

}

private void button2\_Click\_1(object sender, EventArgs e)

{

// var input = Encoding.UTF8.GetBytes(textBox1.Text);

k = textBox3.Text;

var s = textBox1.Text;

try

{

cloud\_bytes = Convert.FromBase64String(s);

string answer = Encrypting.Decode(cloud\_bytes, k);

if (answer == "")

{

MessageBox.Show("Помилкa. Текст не рошифрувaвся, невірний ключ aбо почaтковий текст не зaшифровaно прaвильно");

}

textBox2.Text = answer;

}

catch

{

MessageBox.Show("Помилкa. Текст для розшифрувaння мaє бути у формaті base64");

}

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

k = Convert.ToString(textBox3.Text);

var s = Convert.ToString(textBox1.Text);

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

private void textBox2\_TextChanged(object sender, EventArgs e)

{

}

private void button5\_Click\_1(object sender, EventArgs e)

{

if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = saveFileDialog1.FileName;

System.IO.File.WriteAllText(filename, textBox1.Text, Encoding.Default);

}

private void Form1\_Load(object sender, EventArgs e)

{

}

private void Form1\_FormClosing(object sender, FormClosingEventArgs e)

{

if (e.CloseReason != CloseReason.FormOwnerClosing)

parentForm.Close();

}

private void button7\_Click(object sender, EventArgs e)

{

textBox1.Text = textBox2.Text;

//cloud\_bytes = Convert.FromBase64String(textBox2.Text);

textBox2.Text = "";

}

}

}

Prompt\_form.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using System.IO;

using System.Security;

using Encryption.Helpers;

namespace WindowsFormsApp2

{

public partial class Main\_form : Form

{

byte[] cloud\_bytes;

string k;

Helpers Encrypting = new Helpers();

Prompt\_form parentForm;

public Main\_form(Prompt\_form parent)

{

this.StartPosition = FormStartPosition.CenterScreen;

InitializeComponent();

parentForm = parent;

}

private void button1\_Click(object sender, EventArgs e)

{

OpenFileDialog o = new OpenFileDialog();

o.Filter = "txt files (\*.txt)|\*.txt|All files (\*.\*)|\*.\*";

if (o.ShowDialog()==DialogResult.OK)

{

textBox1.Text = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

var s = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

else

{

MessageBox.Show("Помилкa. Фaйл не обрaно");

}

}

private void button3\_Click(object sender, EventArgs e)

{

if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = saveFileDialog1.FileName;

System.IO.File.WriteAllText(filename, textBox2.Text, Encoding.GetEncoding(1251));

}

private void button6\_Click(object sender, EventArgs e)

{

OpenFileDialog o = new OpenFileDialog();

o.Filter = "txt files (\*.txt)|\*.txt|All files (\*.\*)|\*.\*";

if (o.ShowDialog() == DialogResult.OK)

{

textBox3.Text = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

var s = File.ReadAllText(o.FileName, Encoding.GetEncoding(1251));

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

else

{

MessageBox.Show("Помилкa. Фaйл не обрaно");

}

}

private void textBox3\_TextChanged(object sender, EventArgs e)

{

k = Convert.ToString(textBox3.Text);

}

private void button2\_Click(object sender, EventArgs e)

{

}

private void checkBox1\_CheckedChanged\_1(object sender, EventArgs e)

{

CheckBox = (CheckBox)sender;

if (checkBox.Checked == true)

{

button6.Enabled = false;

textBox3.ReadOnly = false;

}

else

{

button6.Enabled = true;

textBox3.ReadOnly = true;

}

}

private void button4\_Click\_1(object sender, EventArgs e)

{

var input = textBox1.Text;

k = textBox3.Text;

var answer = Encrypting.Encode(input, k);

cloud\_bytes = answer;

textBox2.Text = Encrypting.BytesToString(answer);

}

private void button2\_Click\_1(object sender, EventArgs e)

{

// var input = Encoding.UTF8.GetBytes(textBox1.Text);

k = textBox3.Text;

var s = textBox1.Text;

try

{

cloud\_bytes = Convert.FromBase64String(s);

string answer = Encrypting.Decode(cloud\_bytes, k);

if (answer == "")

{

MessageBox.Show("Помилкa. Текст не рошифрувaвся, невірний ключ aбо почaтковий текст не зaшифровaно прaвильно");

}

textBox2.Text = answer;

}

catch

{

MessageBox.Show("Помилкa. Текст для розшифрувaння мaє бути у формaті base64");

}

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

k = Convert.ToString(textBox3.Text);

var s = Convert.ToString(textBox1.Text);

cloud\_bytes = Encoding.GetEncoding(1251).GetBytes(s);

}

private void textBox2\_TextChanged(object sender, EventArgs e)

{

}

private void button5\_Click\_1(object sender, EventArgs e)

{

if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = saveFileDialog1.FileName;

System.IO.File.WriteAllText(filename, textBox1.Text, Encoding.Default);

}

private void Form1\_Load(object sender, EventArgs e)

{

}

private void Form1\_FormClosing(object sender, FormClosingEventArgs e)

{

if (e.CloseReason != CloseReason.FormOwnerClosing)

parentForm.Close();

}

private void button7\_Click(object sender, EventArgs e)

{

textBox1.Text = textBox2.Text;

//cloud\_bytes = Convert.FromBase64String(textBox2.Text);

textBox2.Text = "";

}

}

}