МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Факультет менеджменту

Кафедра економічної кібернетики, комп'ютерних наук та інформаційних технологій

КІБЕРБЕЗПЕКА ТА КІБЕРЗАХИСТ

методичні рекомендації для практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності F3 (122) «Комп'ютерні науки» денної форми здобуття вищої освіти

МИКОЛАЇВ
2025

УДК 004.056.5
К38

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного аграрного університету від 27 березня 2025 року, протокол № 7

Укладачі:

О. В. Шебаніна — д-р екон. наук, професор, декан факультету менеджменту Миколаївського національного аграрного університету;

С. І. Тищенко — к.п.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Ю. Пархоменко — к.ф.-м.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. О. Жебко — асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївського національного аграрного університету;

А. М. Коломієць — асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївського національного аграрного університету;

Рецензенти:

О. С. Садовий - канд. техн. наук, доцент, завідувач кафедри агроінженерії Миколаївського національного аграрного університету

Ю. В. Грицук - канд. техн. наук, доцент кафедри загальної інженерної підготовки Донбаської національної академії будівництва і архітектури

ЗМІСТ

МЕТА, ЗАВДАННЯ КУРСУ, ВИМОГИ ДО ОСНОВНИХ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Дисципліна «Кібербезпека та кіберзахист» вивчається здобувачами вищої освіти спеціальності 122 «Комп'ютерні науки» на четвертому курсі і є обов'язковою компонентою.

Покликана сформувати у здобувачів необхідний обсяг теоретичних знань та практичних навичок з кібербезпека, навчити їх визначати джерела, об'єкти небезпек інформації, засоби протистояння небезпекам та технології і алгоритми шифрування інформації, ознайомити з використанням сучасної обчислювальної техніки і пакетів для роботи криптографічними алгоритмами.

В процесі проходження курсу здобувачі навчаться визначати джерела загроз кібербезпеці, моделі захисту та порушника в комп'ютерних системах, визначати методи та створювати криптографічний захист інформації як самостійно, так і за допомогою пакетів.

Мета дисципліни: сформувати у здобувачів вищої освіти необхідний обсяг теоретичних і практичних знань для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Завдання дисципліни: оволодіння здобувачами вищої освіти знаннями і навичками для визначення джерел небезпеки кіберпростору, розуміння моделі порушника та побудови криптографічних алгоритмів.

Предмет дисципліни: кібербезпека та кіберзахист.

Кожна лабораторна робота містить методичні поради та хід порядку її виконання.

ЛАБОРАТОРНА РОБОТА 1

Тема: Атаки на КС.

Завдання:

1) виділити Рамкою ВЛАСНОГО кольору у нижченаведеному тексті терміни, які є відповідями на запропоновані питання (терміни наведені у називному відмінку);
2) написати відповіді ПЕРЕД кожним запитанням у Таблиці.

Підказка: Відповіді на запитання є термінами, що розташовані в алфавітному порядку (англійською мовою). В КОЖНОМУ рядку міститься ОДИН термін, що порушує вміст оригінального тексту!

IWalkAlongTheAvenueINeverThoughtI'dMeetATrojanLikeYouMeetAGirlLikeYou WithAuburnHairAndTawnyEyesTheKindOfBugThatHypnotizeMeThroughYouHypn otizeMeThroughAndIRanIRanSoFarAwayIJustRanIRanAllNightAndDayICouldn'tFl ameAwayACloudAppearsAboveYourHeadABeamOfLightComesPharmingDownOn YouShiningDownOnYouTheCloudIsMovingNearerStillAuroraBorealisComesInVie wSpoofingComesInViewAndIRaniRanSoFarAwayIJustRaniRanAllSmurfSuiteAndD ayICouldn'tGetAwayReachedOutAHandToTouchYourFaceYou'reSlowlySocialEngin eeringFromMyViewDisappearingFromMyViewReachedOutAHandToTryAgainHack erFloatingInABeamOfLightWithManInTheMiddleABeamOfLightWithYouAndIRani RanSoFarAwayIJustRaniRanAllNightAndDayAndIExploitIRanSoFarAwayIJustRani RanAllNightAndDayLastNightALittleDancerCameDancin'ToMyDoorLastNightALit tleVishingCamePumpingOnTheFloorSheSaid,ComeOnBaby,IGotALicenseForAutho rizationAndIfItExpires,PrayHelpFromAboveBecauseInTheMidnightHourSheCried,D enialOfService,More,MoreWithARebelYellSheCried,More,More,MoreInTheSniffer Hour,Babe,More,More,MoreWithARebelYell,More,More,MoreMore,More,MoreShe Don'tLikeSlavery,SheWon'tSitAndFloodBut,WhenI'mTiredAndSMShingSheSeesMe ToBedWhatSetYouFreeAndBroughtYouToMe,BabeWhatSetsYouFree,INeedYouHe arByMeBecauseInTheEtherealHourSheCried,More,More,MoreWithARebelYellSheS PicedhAM,More,More,MoreInTheMidnightHour,Babe,More,More,MoreWithARebel Yell,More,More,MoreHeAttackInHisOwnHeavenCollectsItToGoFromTheSevenElev enWellHe'sOutAllNightToMailbombingAFareJustSoLong,JustSoLong,ItDon'tMessU pHisAuthenticationiWalkedTheWardWithYou,BabeAThousandMilesWithYouIDried YourTearsOfPain,BabeAMillionTimesForYouI'dSellMySoulForBotnet,BabeForMon eyToBurnForYouI'dGiveYouAll,AndHaveIdentification,BabeJusta,Justa,Justa,JustaT oHaveYouHereByMeBecauseInTheMidnightHourSheCried,More,More,MoreWithA RebelYellSheCried,More,More,MoreInTheInjectionHour,Babe,More,More,MoreWit hARebelYellSheCried,More,More,MoreMore,More,MoreOhYeahLittleBabySheWan tMoreMore,More,More,More,MoreOhYeahLittleAngelSheWantMoreMore,More,Mo re,More,More

1.	Замах на систему ІБ, спрямований проти ІТС для отримання НСД до комп'ютера
2.	Процедура встановлення належності користувачеві інформації, яку він пред'являє автоматизованій системі (АС). Передує Авторизації.

3.	Процес перевірки прав на доступ і надання доступу Користувача до ІТС. Після того, як об'єкт / користувач / комп'ютер / сервіс був ідентифікований або аутентифікований, він може запросити доступ до будь-яких ресурсів ІТС
4.	Жаргонізм, що означає помилку, ваду або дефект в програмі або системі, що викликає в ній неправильний або неочікуваний результат або неочікувану поведінку.
5.	Комп'ютерна мережа, що складається з деякої кількості хостів із запущеними програмами, які скрито встановлюються на комп'ютері жертви і дозволяють зловмисникові виконувати якісь дії з використанням ресурсів зараженого комп'ютера (***два слова***, *з яких утворений термін*)
6.	Будь-яка дія або послідовність дій, яка призводить до виходу з ладу будь-якої частини системи, яку атакують, при чому така система перестає виконувати свої функції Одна з найрозповсюдніших атак, яка також називається "Відмова сервісу" (повна назва).
7.	Медичний термін – вид наркозу, прикметник – Попередня назва програми "WireShark" (аналізатора мережевих протоколів у режимі реального часу) – ПЗ для створення пакетних фільтрів як для файлів перехоплених пакетів (фільтри відображення), так і для «живого» перехоплення (фільтри перехоплення).
8.	Комп'ютерна програма або частина коду, яка шукає уразливі місця в програмному забезпеченні і в разі знаходження таких отримує контроль над системою або порушує її роботу. Використовується для подальшого впровадження вірусів за допомогою отримання НСД до комп'ютера і обходу його захисту.
9.	Лайка в Мережі в чию-небудь адресу або занадто жваве обговорення якої-небудь теми, у т. ч. спеціально організоване, наприклад, з використанням "ботів", при здійсненні DDoS-атаки
10.	Потік безглуздої інформації, що заповнює (заливає, затоплює!) комунікаційний простір форумів, блогів, чатів, конференцій при здійсненні DDoS-атаки
11.	Спеціаліст в області комп'ютерних технологій, діяльність якого пов'язана з намаганням одержати НСД до систем із ІзОД, комп'ютерний злочинець
12.	Процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені або іншої апріорної інформації про нього, яка сприймається ІТС
13.	Впровадження сторонніх команд або даних в працюючу систему з метою зміни ходу роботи системи, а в результаті - одержання НСД до закритих функцій та інформації або дестабілізації роботи системи в цілому.
14.	Найстаріший метод атак, за яким велика кількість листів унеможливлюють роботу з поштовими скриньками, а іноді і з цілими поштовими серверами.
15.	Атака, при якій атакуючий здатний читати і видозмінювати повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про присутність атакуючого в каналі (Скорочена+Повна назва атаки+Архетип).
16.	Процедура таємного перенаправлення жертви на помилкову IP-адресу (веб-сайт), щоб обманом змусити Користувача ввести Ім'я користувача та Пароль в БД на фальшивому сервері. Для цього може використовуватися навігаційна структура – файл hosts, система доменних імен (DNS).
17.	Різновид Інтернет-шахрайства з масовою розсилкою на мобільні телефони фальшивих повідомлень, що заманюють користувача на інфікований веб-сайт
18.	Набір секретних методів перехоплення, які використовуються організацією GCHQ і були оприлюднені Сноуденом, названий на честь синіх істот (придуманих і намальованих бельгійським художником П'єром Кюлліфор), що використовується для Вкл./Викл. смартфона без відома Власника (Dreamy), відстеження Власника смартфона з більшою точністю за допомогою механізму геолокації (Tracker), управління мікрофоном смартфона для підслуховування того, що відбувається навколо смартфона (Curious)
19.	Прикладна програма, що перехоплює імена та паролі користувачів та інші мережеві пакети. Використовується для діагностики несправностей, аналізу трафіку, та виявлення присутності працівників на роботі.
20.	Використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання НСД до інформації.

21.	Умисне масове розповсюдження повідомлень, здійснене без попередньої згоди адресатів (***<u>два слова</u>***, *з яких утворений термін*)
22.	Атака, при якій зловмисник видає себе за санкціонованого користувача для отримання від АС важливого файлу або для зміни таблиці маршрутизації та направлення трафіку на помилкову IP-адресу.
23.	Різновид шкідливих програм, які всіляко маскуються під корисні програми, вводячи в оману користувача, і виконують шкідливі дії, наприклад, крадуть особисту інформацію або перехоплюють контроль над комп'ютером. На відміну від вірусів не мають здатності до розмноження.
24.	Різновид «рибалки», при якому до користувача звертаються з проханням подзвонити на телефонний номер, де до нього звернуться з проханням повідомити конфіденційні дані.

ЛАБОРАТОРНА РОБОТА 2-4

Тема: Розробка та оформлення моделі загроз для інформації об’єкту інформаційної діяльності (ОІД).

Завдання:

1) вивчити умовні скорочення та терміни;
2) побудувати ситуаційний план ОІД;
3) побудувати генеральний план ОІД;
4) визначити та описати умовні позначення до кожного плану;
5) зробити висновки.

Приклад виконання роботи:

АС – автоматизована система

ДТЗС – допоміжні технічні засоби

ІзОД – інформація з обмеженим доступом

КСЗІ – комплексна система захисту інформації

ОІД – об’єкт інформаційної діяльності

ОТЗ – основні технічні засоби

ПЕМВН – побічні електромагнітні випромінювання випромінювання і наводки

ТЗІ – технічний захист інформації

ТКВІ – технічний канал витоку інформації

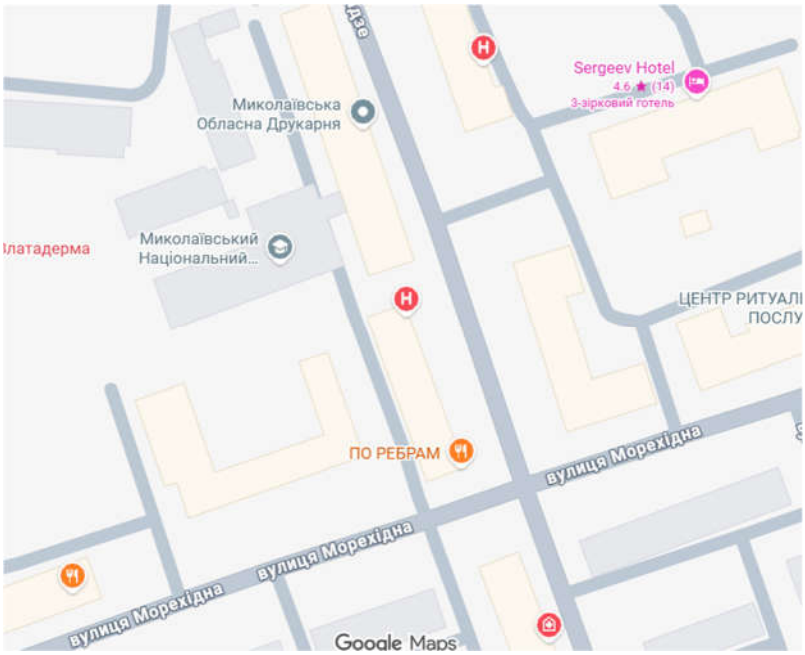


Рисунок 1 – Ситуаційний план ОІД

Точкою відмічено положення аудиторії. З огляду на червоний контур, можна побачити, що джерелом небезпеки є неконтрольована територія з боку вулиці 1 Воєнної, де може бути розміщено АЗ для витоку інформації.

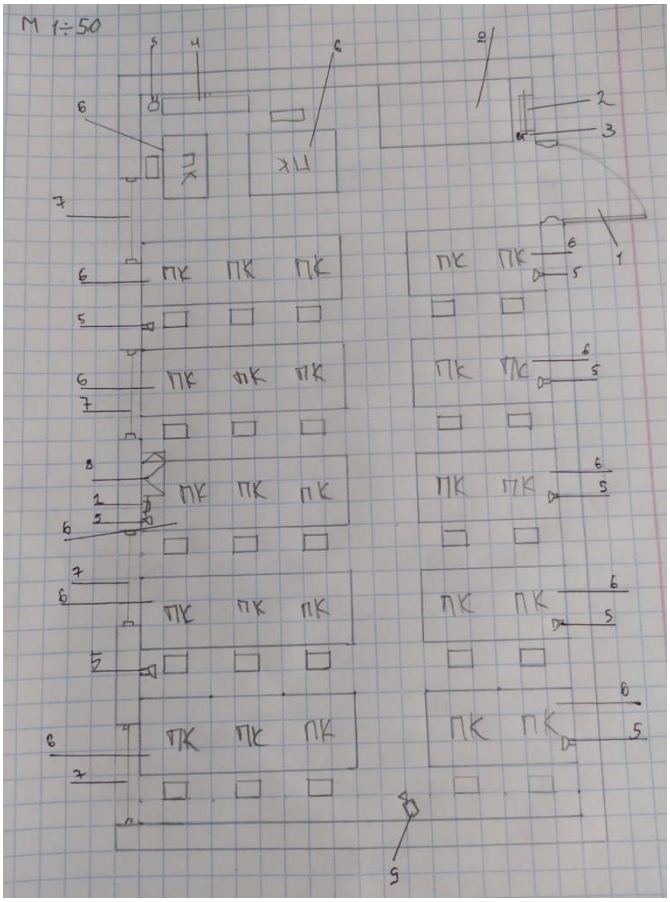


Рисунок 2 – Генеральний план ОІД

Умовні позначення:

1 – двері;

2 – щит електричний з 3 автоматами;

3 – вогнегасник вуглекислотний (ВВК-2);

4 – телевізор;

5 – розетка(и);

6 – стіл(столи) з ПК;

7 – вікно з вертикальними шторами;

8 – кондиціонер;

9 – система відеоспостереження;

10 – шафа.

Згідно з вказаним планом, автомат на вході мережі є безпечним засобом від витоку інформації через розетки, хоча таку ймовірність відкидати неможливо. У аудиторії відсутня вентиляція, що унеможливлює встановлення засобів стеження у важкодоступних місцях, хоча, в той же час, відсутність вентиляції ставить під загрозу життя відвідувачів у спекотну пору року. З протипожежних засобів є тільки вогнегасник, що також знижує можливість витоку інформації. Вікна мають непогану звукоізоляцію, а от двері та стіни з цією задачею впоратися на прийнятному рівні не можуть. Також, шафа є потенційним місцем положення апаратних засобів для стеження.

Рисунок 3 – Приклад висновків

ЛАБОРАТОРНА РОБОТА 5

Тема: Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет.

Приклад виконання роботи:

Таблиця 1 – Таблиця для заповнення

Тип/назва реусурсу, url-адреса	Доступ до електронного каталогу або пошук по сайту	Доступ до повних текстів електронних документів	Посилання на інші інформаційні ресурси мережі Інтернет
https://allo.ua/	+ 	+	+ 

Загальні відомості

Подання органами державної влади інформації у мережі Інтернет є одним найбільш дієвих способів взаємодії влади і суспільства.

Сайт органу державної влади є відкритим і загальнодоступним інформаційним ресурсом, використання якого здійснюється безоплатно, однак, сайт може містити також інформацію обмеженого доступу.

До сайта органу державної влади висуваються певні вимоги:

— представлення інформації про орган влади, його місцезнаходження, наявність контактної інформації, визначення умов і форм використання матеріалів сайта;

— забезпечення цілодобового контролю за працездатністю сайта;

— з метою запобігання створенню нерівних умов для різних користувачів для доступу до сайта не повинні пред’являтись завищені вимоги до апаратного і програмного забезпечення;

— дотримання принципу поваги до практики інформаційного обміну у мережі Інтернет (відсутність відповідей на звертання громадян і організацій є неприйнятною практикою);

— обмеження на сайті органу державної влади інформації, джерелом якої виступають треті особи (у випадку, якщо така інформація наявна, орган влади повинен визначити межі своєї відповідальності за її повноту і достовірність);

— кожен електронний документ повинен мати власну унікальну адресу, має публікуватись інформація про дату його розміщення, а також забезпечуватись довготривале зберігання оновлюваної інформації;

— розміщення інформації про умови використання сайта.

Пошук урядових ресурсів України доцільно починати з урядового порталу України (https://www.kmu.gov.ua/).

Повний список адрес серверів парламентів світу представлений на сайті Міжпарламентського союзу (http://archive.ipu.org/english/parlweb.htm).

Пошук парламентської інформації України - з сайту Верховної Ради України (https://www.rada.gov.ua/).

Інформаційні ресурси архівів у мережі Інтернет

Архіви зберігають найрізноманітніші види документів з усіх сфер суспільної і особистої діяльності: управлінську документацію, документи особового походження, картографічні документи, науково-технічну документацію, кіно-, фото-, фоно-, відеодокументи, документи церковних конфесій тощо.

Метою функціонування сайтів архівних установ є популяризація архівної справи, розширення доступу громадян і організацій до архівних матеріалів, надання інтерактивних послуг, висвітлення діяльності архівних установ, висвітлення змісту періодичних видань з архівної справи.

Сайти архівів виконують такі функції: надання для широкого кола користувачів науково-довідкового апарату архівів, інформування про діяльність архівних закладів, надання інформації про склад і зміст архівних документів,

подання законодавчої, нормативної та методичної бази функціонування архівних установ, висвітлення змісту публікацій (з повними текстами) з архівної справи.

Пошук інформації, яка надається архівами України, можна починати з порталу “Архіви України” (https://archives.gov.ua/ua/).

Бібліотечно-бібліографічні ресурси мережі Інтернет

У мережі Інтернет представлено значну кількість бібліотечнобібліографічних інформаційних ресурсів як у вигляді бібліотечної реклами, так і з власне бібліографічною інформацією, яка міститься у електронних каталогах. Крім цього, бібліографічна інформація розташовується на серверах наукових і освітніх закладів, які представляють доступ до своєї наукової продукції – періодичним виданням у електронній формі, при чому як на бібліографічному рівні, так і на повнотекстовому.

Бібліографічна інформація може надаватись також серверами видавництв та книготорговельних організацій, спеціальними службами, які забезпечують рефератами або анотаціями журнальних статей та інших друкованих матеріалів та ін.

Сайт найбільшої бібліотеки України – Національної бібліотеки України ім. В.В. Вернадського (http://www.nbuv.gov.ua/), який містить гіперпосилання на провідні бібліотеки світу і України.

ЛАБОРАТОРНА РОБОТА 6

Тема: Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем.

Завдання:

1) Охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки (NIST, CRAMM та OCTAVE) та здійснивши аналіз основних їх властивостей, необхідно визначити основні їх переваги та недоліки і заповнити таблицю.

Приклад виконання роботи:

Таблиця 1 – Таблиця для заповнення

Методика	Переваги	Недоліки
NIST	Стандартизований підхід до безпеки	Складність та ресурсоємність
CRAMM	Широкий охоплення аспектів безпеки	Часові затрати
OCTAVE	Глибока аналітика ризиків	Залежність від експертів

Загальні відомості

У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність системи (надалі розглядатимемо бізнес-процес компанії) ефективно функціонувати за умови впливу чинників дестабілізації (ЧД): збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу. Згідно з цим визначенням невід’ємною складовою властивості живучості бізнес-процесу компанії є неперервність його виконання. Міжнародний стандарт ISO 27001, який визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ),

тлумачить неперервність функціонування як один із рекомендованих контролів у життєвому циклі СМІБ. Отже, неперервність функціонування є не лише запорукою ефективного розроблення та впровадження СМІБ, але й дієвим способом та невід'ємною складовою процесу забезпечення властивості живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації корпоративні мережі зв'язку (КМЗ) є основним методом збору, оброблення, зберігання та передавання інформації. Водночас, відмітимо важливість такого складового компонента КМЗ, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних активів компанії. Тому наголошуємо не просто на властивості живучості організації загалом, а на забезпеченні неперервності функціонування СЗІ в КМЗ як невід'ємній та критично важливій частині ефективного та безпечного функціонування компанії, виконання її основних бізнес-процесів.

Розрізнятимемо такі основні категорії чинників дестабілізації нормальної роботи СЗІ як складової КМЗ в контексті забезпечення їхнього неперервного функціонування:

− Стихійні лиха. Порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині.

− Соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства (наприклад, акти вандалізму, терористичні акти, війни тощо).

− Фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на СЗІ або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил, корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації).

− Порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування КМЗ (наприклад, відмова мережі електроживлення, системи кондиціонування повітря, системи водопостачання).

− Технічний збій. Порушення ІБ, спричинене відмовами СЗІ або пов'язаними з нею нетехнічними можливостями. До такого типу ризиків зараховуємо апаратний, програмний збій, перевантаження, порушення ремонтоздатності.

− Технічні атаки. Порушення ІБ, що зумовлене атакуванням КМЗ та використанням її уразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS / DDoS).

У роботі розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як невід'ємної складової ефективної та безпечної роботи компанії.

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ, зокрема підсистеми СЗІ:

1. Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності уразливостей, величини завданого збитку.

3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування СЗІ.

4. Оцінка уразливостей та контролів. Аналіз основних властивостей КМЗ та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Представимо графічне зображення життєвого циклу процесу управління ризиками ІБ в контексті забезпечення неперервності функціонування (рис. 1).

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30, методика CRAMM та методика OCTAVE.

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози.

Рисунок 1 – Життєвий цикл процесу управління ризиками ІБ

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Використання такої методики передбачає такі етапи:

− опис характеристик системи;

− ідентифікація загроз;

− ідентифікація уразливостей; аналіз наявних засобів/заходів захисту;

− визначення значення ймовірності;

− аналіз впливу;

− визначення значення ризику;

− вибір засобів/заходів захисту;

− документування отриманих результатів. Алгоритм цієї методики зображено на рис. 2.

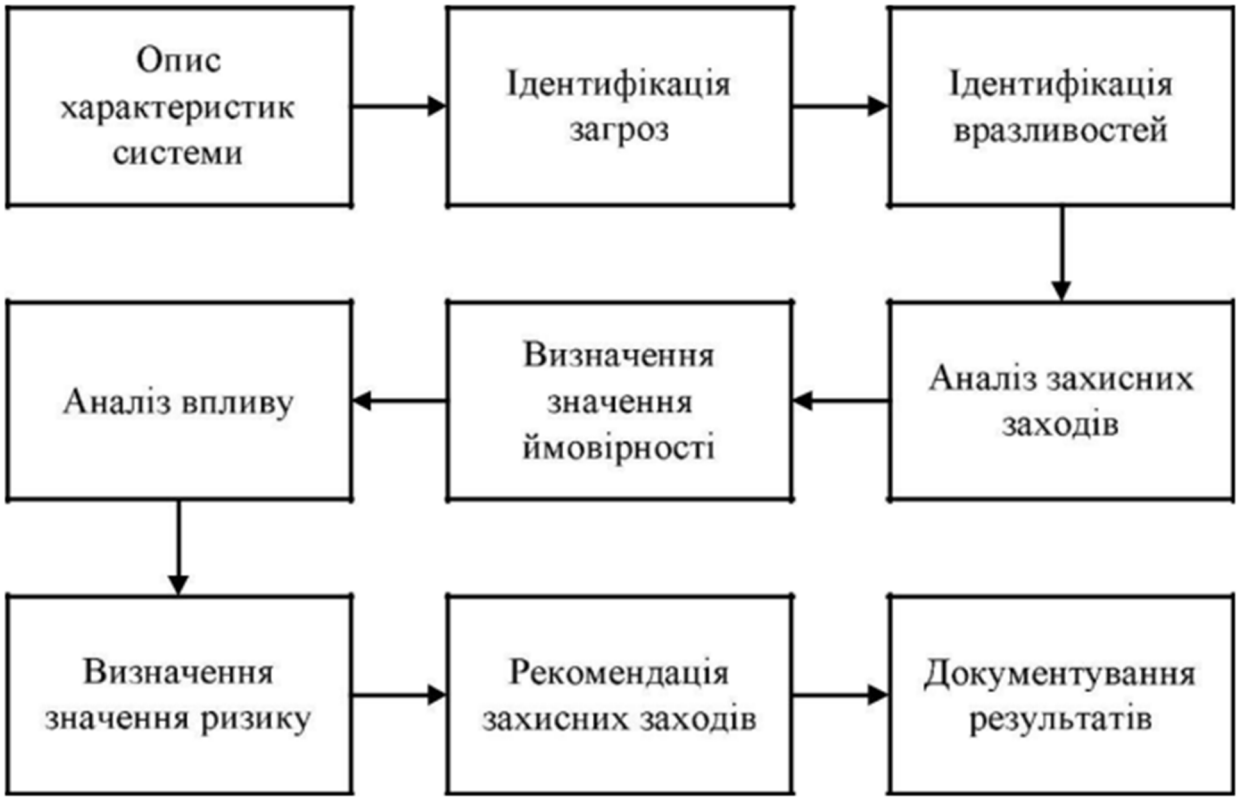


Рисунок 2 – Алгоритм методики управління ризиками NIST 800-30

Наступною методикою, яку потрібно проаналізувати є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM.

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами

знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC (“Помаранчева книга”).

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв’ю, списки перевірки і набір звітних документів.

Алгоритм методики CRAMM подано на рис. 3.

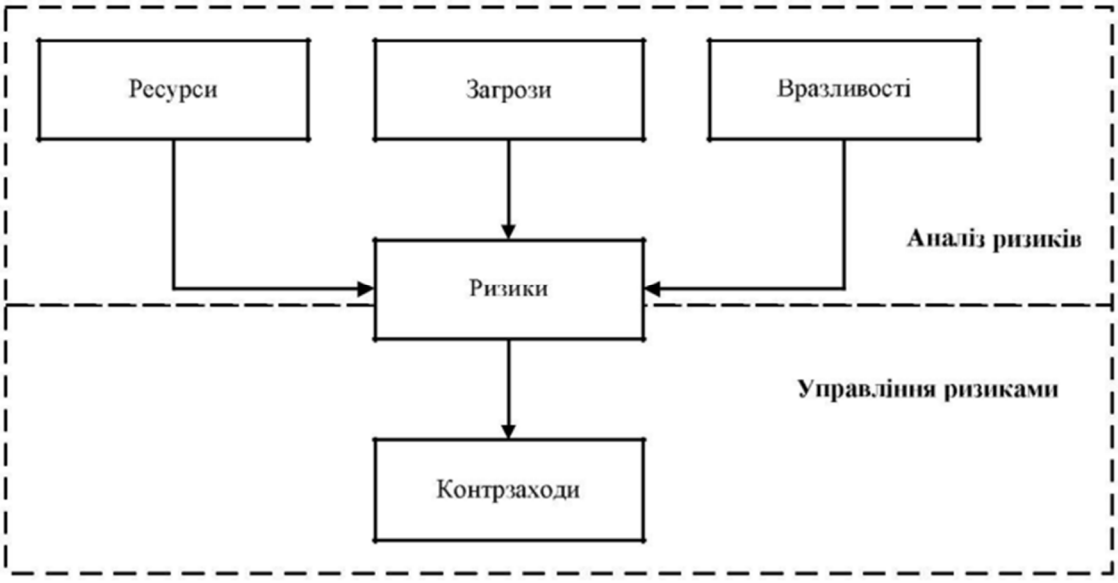


Рисунок 3 – Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності.

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз уразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних уразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням уразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 4

Рисунок 4 – Алгоритм методики управління ризиками OCTAVE

ЛАБОРАТОРНА РОБОТА 7

Тема: Шифр Цезаря.

Завдання:

1) Створити програму, що реалізую шифр Цезаря та зашифрувати і розшифрувати текст відповідно до варіанту;

2) у звіт додати скріншоти виконання роботи та повну версію коду;

3) **ДОДАТКОВЕ ЗАВДАННЯ**: додати можливість шифрування разом з числами або знаками пунктуації.

Приклад виконання роботи:

```
public static String decryptData(String inputStr, int shiftKey)
{
    inputStr = inputStr.toLowerCase();
    String decryptStr = "";
    for (int i = 0; i < inputStr.length(); i++)
    {
        int pos = ALPHABET.indexOf(inputStr.charAt(i));
        int decryptPos = (pos - shiftKey) % 26;
        if (decryptPos < 0){
            decryptPos = ALPHABET.length() + decryptPos;
        }
        char decryptChar = ALPHABET.charAt(decryptPos);
        decryptStr += decryptChar;
    }
    return decryptStr;
}
```

Рисунок 1 – Приклад коду для дешифрування

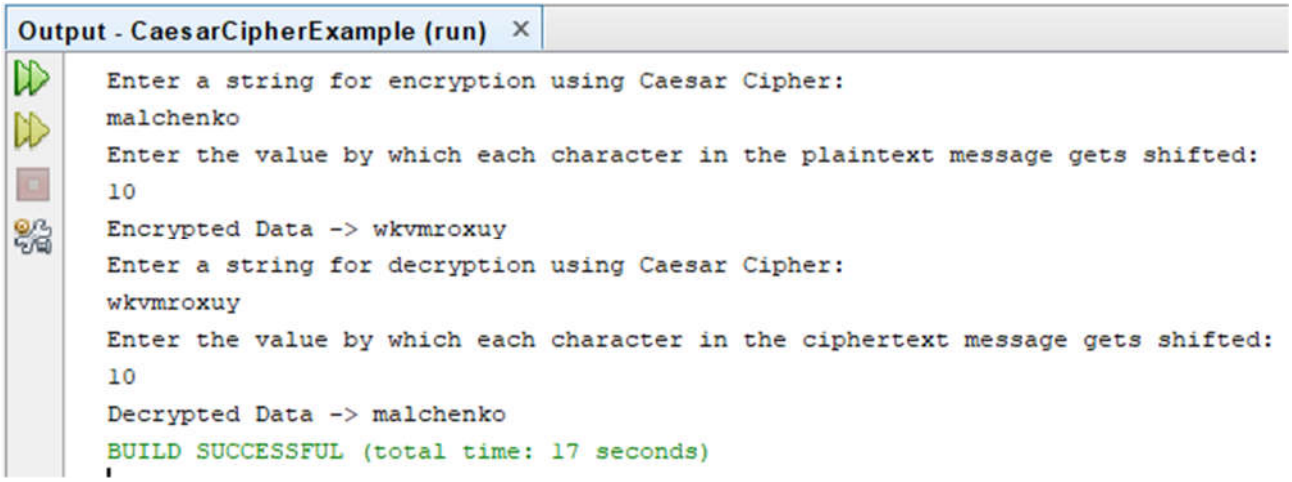


Рисунок 2 – Приклад результату роботи програми

Загальні відомості

Для шифрування заданого тексту потрібно ціле число. Це ціле значення називається зсувом, який вказує на кількість позицій, на які кожна буква тексту була зміщена вниз.

Ми можемо математично представити шифрування літери за допомогою зсуву n наступним чином:

Фаза шифрування зі зсувом n = En (x) = (x+n)mod 26

Фаза розшифрування зі зсувом n = Dn (x) = (x-n)mod 26

Реалізація програми для шифру Цезаря відбувається за допомогою наступних кроків:

- Отримати вхідний рядок від користувача і зашифрувати його за допомогою методу шифру Цезаря.
- Отримати від користувача ціле число для зсуву символів. Вхідне число повинно знаходитись у діапазоні 0-25.
- Пройдіть вхідний рядок по одному символу за раз.
- В залежності від способу шифрування та розшифрування, кожен символ перетворюється згідно з правилом.
- Повертає новий згенерований рядок.

ЛАБОРАТОРНА РОБОТА 8-9

Тема: Обчислення дайджесту повідомлення. Формування та перевірка електронного підпису.

Завдання:

1) Створити програму, що реалізує алгоритм обчислення дайджесту повідомлення SHA-1, реалізує та перевіряє алгоритм DSA знаходження та перевірки електронного підпису.

Приклад виконання роботи:

Для виконання обох частин завдання було обрано мову програмування Java і середовище розробки NetBeans. Спочатку було реалізовано алгоритм обчислення дайджесту повідомлення (рис. 1).

```
39
40      static String sha1(String input) throws NoSuchAlgorithmException {
41          MessageDigest mDigest = MessageDigest.getInstance("SHA1");
42          byte[] result = mDigest.digest(input.getBytes());
            StringBuffer sb = new StringBuffer();
44          for (int i = 0; i < result.length; i++) {
45              sb.append(Integer.toString((result[i] & 0xff) + 0x100, 16).substring(1));
46          }
47          return sb.toString();
48      }
49
```

Рисунок 1 – Алгоритм обчислення дайджесту повідомлення

Реалізація за допомогою стандартних бібліотек. Наступним кроком стала генерація пар ключей з використанням інтерфейсів java.security.interfaces.DSAPrivateKey та java.security.interfaces.DSAPublicKey (рис. 2).

```
13
14      public static KeyPair buildKeyPair() throws NoSuchAlgorithmException {
15          KeyPairGenerator keyGenerator = KeyPairGenerator.getInstance("DSA");
16          keyGenerator.initialize(1024);
17          return keyGenerator.genKeyPair();
18      }
19
```

Рисунок 2 – Генерація пар ключей довжиною 1024 біта

Генерція електронного підпису за допомогою закритого ключа стала наступним кроком (рис. 3) та його перевірка (рис. 4).

```
19
20      public static byte[] sign(PrivateKey privateKey, byte[] message)
21          throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
22          Signature signAlgorithm = Signature.getInstance("DSA");
23
24          signAlgorithm.initSign(privateKey);
25          signAlgorithm.update(message);
26
27          return signAlgorithm.sign();
28      }
```

Рисунок 3 – Підпис повідомлення за допомогою закритого ключа

```
30  public static boolean verify(PublicKey publicKey, byte[] message, byte[] signature)
31      throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
32      Signature verifyAlgorithm = Signature.getInstance("DSA");
33
34      verifyAlgorithm.initVerify(publicKey);
35      verifyAlgorithm.update(message);
36
37      return verifyAlgorithm.verify(signature);
38  }
```

Рисунок 4 – Перевірка електронного підпису

Після створення алгоритмів, залишилося використати їх. Викликаємо функції у main(), але перед цим створимо відповідні змінні для повідомлення, що буде шифруватися, для закритого і відкритого ключів (рис. 5).

```
    public static void main(String[] args) throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
56      String input = "Pavlo_Malchenko";
        byte[] signature = {'s'};
58      KeyPair kp = buildKeyPair();
59      PrivateKey pr = kp.getPrivate();
60      PublicKey pub = kp.getPublic();
        boolean ver = false;
62      System.out.println("SHA1:    " + sha1(input));
63      MessageDigest mDigest = MessageDigest.getInstance("SHA1");
64      byte[] message = mDigest.digest(sha1(input).getBytes());
65      signature = sign(pr, message);
66      if(signature.length != 0)
67      {
68          System.out.println("\nText successfully signed!");
69      }
70      else System.out.println("Signing ERORR");
71      ver = verify(pub, message, signature);
72      if (ver == true)
73      {
74          System.out.println("\nVerification completed successfully!");
75      }
76      else System.out.println("Verification ERROR");
77  }
```

Рисунок 5 – Функція main() з викликом усіх функцій

В результаті виконання програми можна побачити зашифроване повідомлення SHA-1, результати електронного підпису та його перевірки (рис. 6).

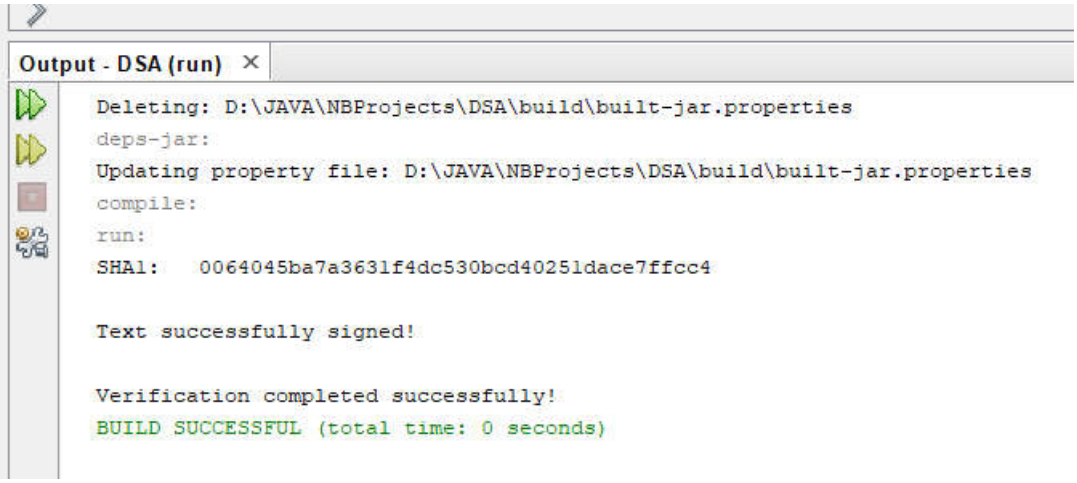


Рисунок 6 – Результат виконання програми

ЛАБОРАТОРНА РОБОТА 10-11

Тема: Шифрування методом поліалфавітної заміни. Криптографічний алгоритм з відкритим ключем.

Завдання:

1) Створити програму, що реалізує алгоритм шифрування методом поліалфавітної заміни та оцінку криптостійкості рішення. Реалізація та перевірка роботи алгоритму RSA.

Приклад виконання роботи:

Для виконання обох частин завдання було обрано мову програмування Java і середовище розробки NetBeans. Спочатку було реалізовано алгоритм шифру Віженера (рис. 1). Алфавітом став звичайний англійський.

Якщо пронумерувати літери алфавіту від 0 до 26 (a → 0, b → 1, c → 2, …), то шифрування Віженера є можливим представити формулою:

$C_i = (P_i + K_j) \bmod 33$, де K_j — j-та літера ключового слова, P_i — i-а літера вихідного слова.

Ключове слово повторюється, поки не отримано гаму, рівну довжині повідомлення.

Дешифрування відбувається за наступною формулою:

$$C_i = (P_i + 33 - K_j) \bmod 33$$

```
public String encrypt(final String text, final String key) {
    String encrypt = "";
    final int keyLen = key.length();
    for (int i = 0, len = text.length(); i < len; i++) {
        encrypt += (char) (((text.charAt(i) + key.charAt(i % keyLen) - 2 * this.bias) % this.letters) + this.bias);
    }
    return encrypt;
}

public String decrypt(final String cipher, final String key) {
    String decrypt = "";
    final int keyLen = key.length();
    for (int i = 0, len = cipher.length(); i < len; i++) {
        decrypt += (char) (((cipher.charAt(i) - key.charAt(i % keyLen) + this.letters) % this.letters) + this.bias);
    }
    return decrypt;
}
```

Рисунок 1 – Алгоритм шифру Віженера

Криптостійкість визначено за формулою $T = \frac{S^L}{V * t}$, де S – потужність ключа (2), L –довжина ключа, V – швидкість перебору, t – коефіцієнт переводу часу, T – час повного перебору в роках. Результат шифрування повідомлення, його дешифрування, та час, що може бути витрачений на злам ключа наведені на рисунку 2.

```
Encrypted string:   iepddirlk
Decrypted string:   malchenko
For 16 bit key: 0,000082 years, or 43.03486365205385 minutes
```

Рисунок 2 – Результат шифрування повідомлення, його дешифрування, та час, що може бути витрачений на злам ключа

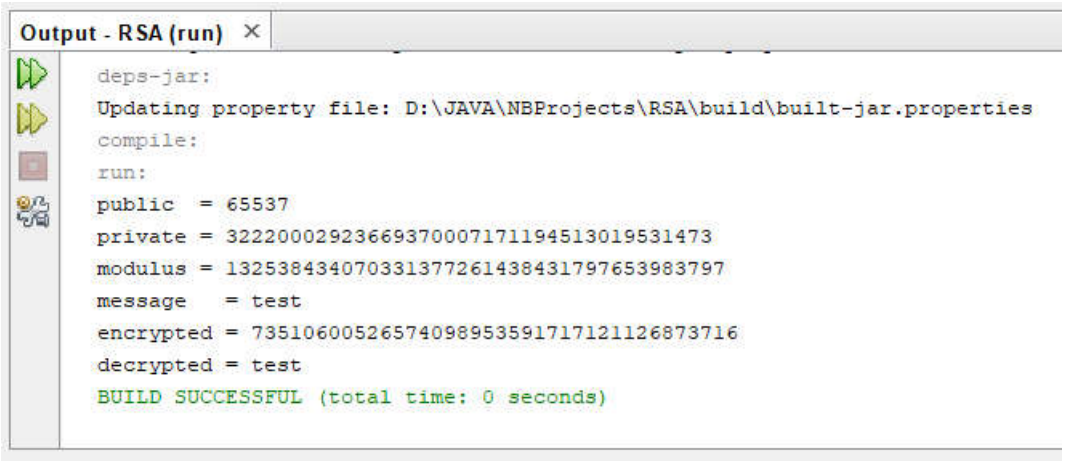
В наступній частині реалізовано RSA алгоритм (рис. 3), та його використання, в залежності від бітності ключа (рис. 4).

```
RSA(int N) {
    BigInteger p = BigInteger.probablePrime(N/2, random);
    BigInteger q = BigInteger.probablePrime(N/2, random);
    BigInteger phi = (p.subtract(one)).multiply(q.subtract(one));

    modulus    = p.multiply(q);
    publicKey  = new BigInteger("65537");
    privateKey = publicKey.modInverse(phi);
}


BigInteger encrypt(BigInteger message) {
    return message.modPow(publicKey, modulus);
}

BigInteger decrypt(BigInteger encrypted) {
    return encrypted.modPow(privateKey, modulus);
```

Рисунок 3 – RSA алгоритм

```
public static void main(String[] args) {
   int N = 128;
   RSA key = new RSA(N);
    System.out.println(""+key);
    String s = "test";
    byte[] bytes = s.getBytes();
    BigInteger message = new BigInteger(bytes);

   BigInteger encrypt = key.encrypt(message);
   BigInteger decrypt = key.decrypt(encrypt);
   System.out.println("message   = " + new String(message.toByteArray()));
   System.out.println("encrypted = " + encrypt);
   System.out.println("decrypted = " + new String(decrypt.toByteArray()));
}
```

Рисунок 4 – Використання RSA алгоритму для 128-бітного ключа



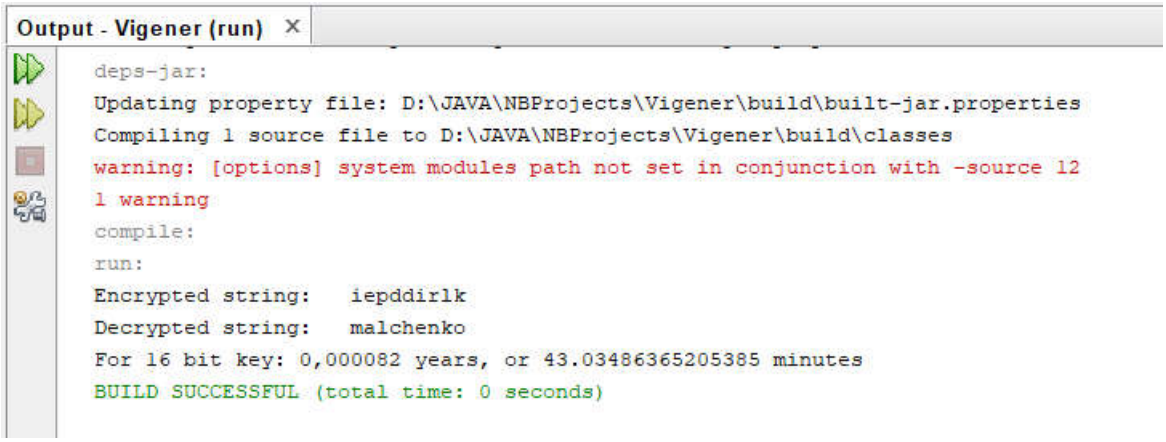


Рисунок 5-6 – Результат виконання програм

Розрахунок криптостійкісті шифру до атаки brute force (методом грубої сили) з урахуванням вимог до безпеки трафіку різних типів (див. табл. 1).

Типи трафіку	Час життя	Мінімальна довжина ключа (у бітах)
Тактична військова інформація	хвилини/години	56-64
Оголошення про продукти, злиття компаній, процентні ставки	дні/тижні	64
Довготривалі бізнес-плани	Роки	64
Торгові секрети (наприклад, рецепт кока-коли)	Десятиліття	112
Секрети водневої бомби	➢ 40 років	128
Особистості шпигунів	➢ 50 років	128
Особисті справи	➢ 50 років	128
Дипломатичні конфлікти	➢ 65 років	128

Таблиця 1 – Вимоги до безпеки різної інформації. Брюс Шнайер, Прикладна криптографія, розділ 7, п.7.1 (табл.7-10), 1996 р.

Формула для розрахунку має вигляд:

$T = \frac{S^L}{V * t}$ (1), де S – потужність алфавіту ключа. Алфавіт системи числення – це множина цифр, використовуваних в ній. Основа системи числення дорівнює потужності алфавіту (числу цифр). Тобто, S=2 (0 або 1) по формулі Р. Хартли.

L – довжина ключа (кількість двійкових розрядів символу алфавіту * к-ть символів ключа);

V – швидкість перебору (операцій в секунду АБО флопс);

t – коефіцієнт переводу секунд у роки (t = 60 * 60 * 24 * 365 = 31536000);

T – час повного перебору (в роках).

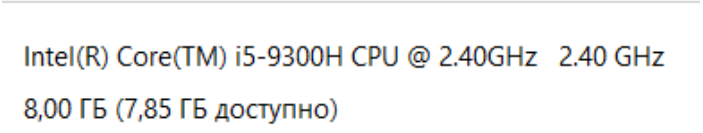


Рисунок 12 – Комп’ютерні характеристики

Intel(R) Core(TM) i5-7500 CPU @ 2.40GHz

V = 2400 МГц * 4 яяр * 4 * 10^6 = 38,4 Гфлопс

Відповідно до Закону Мура кожні 5 років потужність обчислювальної техніки збільшується у 10 разів (2 рази на рік).

Тобто, треба перетворити формулу (1) з урахуванням закону Мура; отримаємо

$$\sum_{1}^{T} x(t) = \frac{S^l}{t}, \text{ де } x(t) = V * 10^{T/5} \quad (2)$$

Далі, перетворюємо отриману геометричну прогресію ($q=10^{1/5}$), знайдемо суму та отримаємо T

$$T = 5 * \lg\left(\frac{S^l * (10^{1/5} - 1)}{10^{1/5} * V * t} + 1\right) \quad (3)$$

Таким чином 50% ключів знаходяться при переборі половини комбінацій; тоді:

$$Tc = 5*\lg(\frac{S^l * (10^{1/5} - 1)}{2*10^{1/5} * V * t} + 1) \quad (4)$$

Таким чином, час криптоаналізу скорочується більш ніж на порядок.

Таблиця 2 – Оцінка середнього часу для вскриття шифру методом грубої сили (повного перебору всіх ключів). Брюс Шнайер, Прикладна криптографія (глава 7, 1996г.) – 608 с. дані змінені з урахуванням закону Мура.

Час крипто аналізу	30 біт	40 біт	56 біт	64 біт	80 біт	112 біт	128 біт
Без урахування закону Мура	0,02 секунд	20,206 секунд	1324198,656 секунд	10,749 років	704476,372 років	3025702978941740 років	1,98292470427925 87e+20 років
З урахуванням закону Мура	0,008 секунд	8,096 секунд	528538,911 секунд	2,374 років	25,57 років	73,734 років	97,816 років

ЛАБОРАТОРНА РОБОТА 12-13

Тема: Стеганографія.

Завдання:

1) Створити програму, що реалізує стенографію;

2) **ДОДАТКОВЕ ЗАВДАННЯ**: знайти та використати онлайн-засоби стенографії.

Приклад виконання роботи:

Стеганогра́фія — (з грец. στεγανός — прихований + γράφω — пишу)

— тайнопис, при якому повідомлення, закодоване таким чином, що не виглядає як повідомлення — на відміну від криптографії. Таким чином непосвячена людина принципово не може розшифрувати повідомлення — бо не знає про факт його існування.

Якщо криптографія приховує зміст повідомлення, то стеганографія приховує сам факт існування повідомлення.

GIF (англ. Graphics Interchange Format - формат для обміну зображеннями) - формат зберігання графічних зображень, здатний зберігати стислі дані без втрати якості у форматі до 256 кольорів. Даний формат був розроблений в 1987 році (GIF87a) фірмою CompuServe для передачі растрових зображень по мережах. У 1989-му формат був модифікований (GIF89a), були додані підтримка прозорості і анімації.

Файли формату GIF мають блочну структуру. Дані блоки завжди мають фіксовану довжину (або вона залежить від деяких прапорів), так що помилитися в тому, де який блок знаходиться, практично неможливо.

Методи шифрування

В якості методів шифрування повідомлень в файлах зображень будуть використовуватися:

Метод **LSB** (Least Significant Bit, найменший значущий біт)

Метод доповнення палітри

Метод LSB - поширений метод стеганографії. Він полягає в заміні останніх значущих біт в контейнері (в нашому випадку байти глобальної палітри) на біти приховуваного повідомлення.

У програмі будуть використовуватися в рамках цього методу два останніх біта в байтах глобальної палітри. Це означає, що для 24-бітного зображення, де колір палітри є три байта для червоного, синього, і зеленого кольорів, після впровадження повідомлення в нього, кожна складова кольору зміниться максимум на 3/255 градації. Така зміна, по-перше, буде непомітно або

труднозаметно для людського ока, а по-друге, не буде помітно на низькоякісних пристроях виведення інформації.

Кількість інформації буде прямо залежати від розміру палітри зображення. Оскільки максимальний розмір палітри 256 кольорів і, якщо записувати по два біта повідомлення в складову кожного кольору, то максимальна довжина повідомлення (при максимальній палітрі в зображенні) становить 192 байта. Після впровадження повідомлення в зображення, розмір файлу не змінюється.

Метод **розширення палітри**, що працює тільки для структури GIF. Він буде найбільш ефективний в зображеннях з палітрою невеликих розмірів. Суть його полягає в тому, що він збільшує розмір палітри, тим самим давши додатковий простір для запису необхідних байт на місці байт квітів. Якщо врахувати що мінімальний розмір палітри становить 2 кольори (6 байт), то максимальний розмір впроваджуваного повідомлення може бути 256 × 3-6 = 762 байт. Недолік - низька криптозахищені, прочитати запроваджене повідомлення можна за допомогою будь-якого текстового редактора, якщо повідомлення не піддавалося додатковому шифрування.

Для виконання роботи було використано мову програмування Java у середовищі розробки NetBeans.

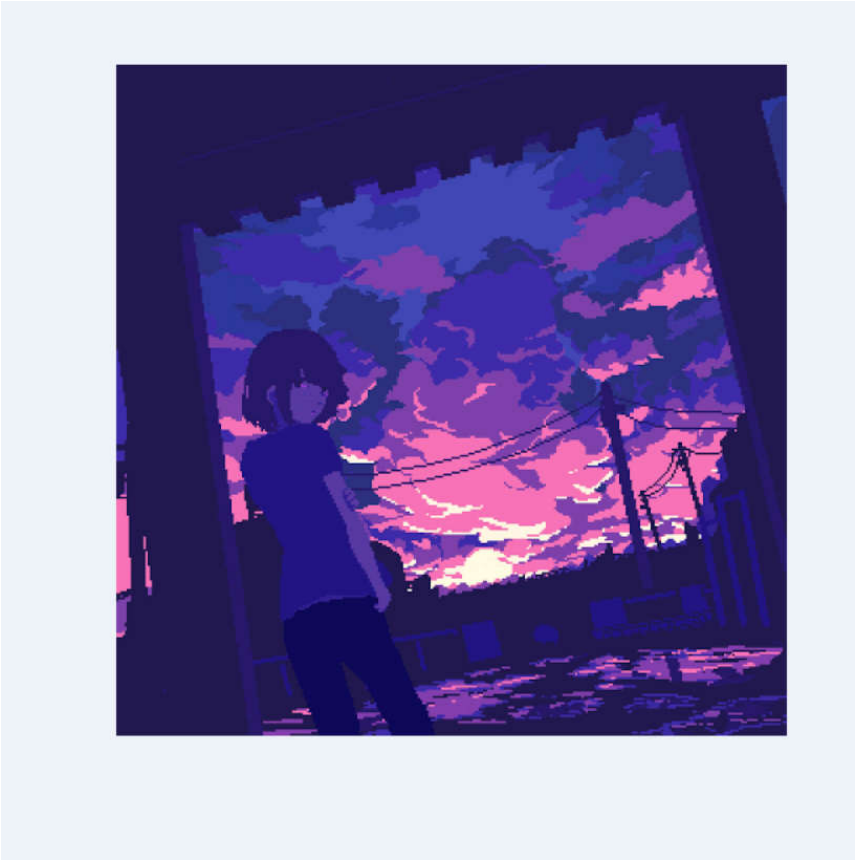


Рисунок 1 –Зображення для кодування (GIF)

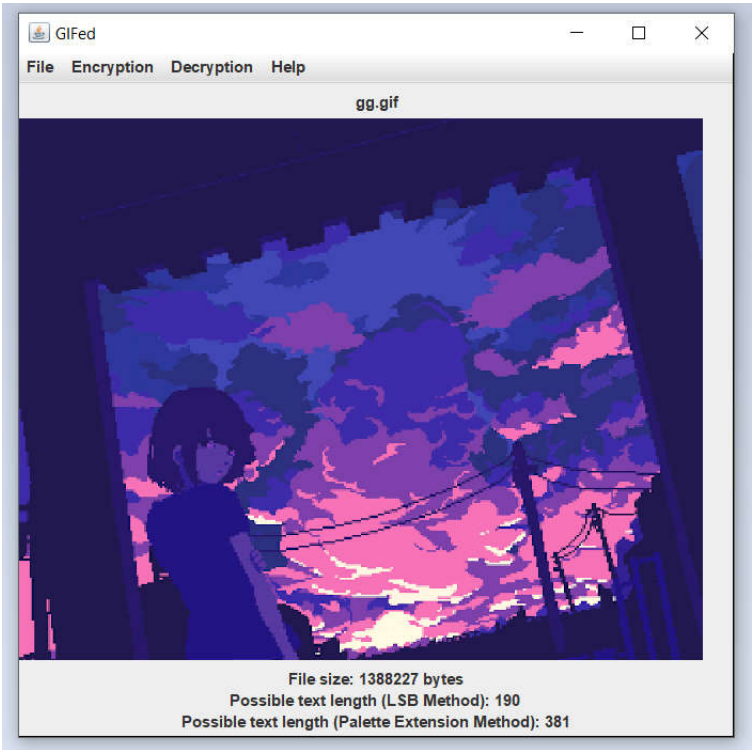


Рисунок 2 – Вікно програми з підготовленим зображенням

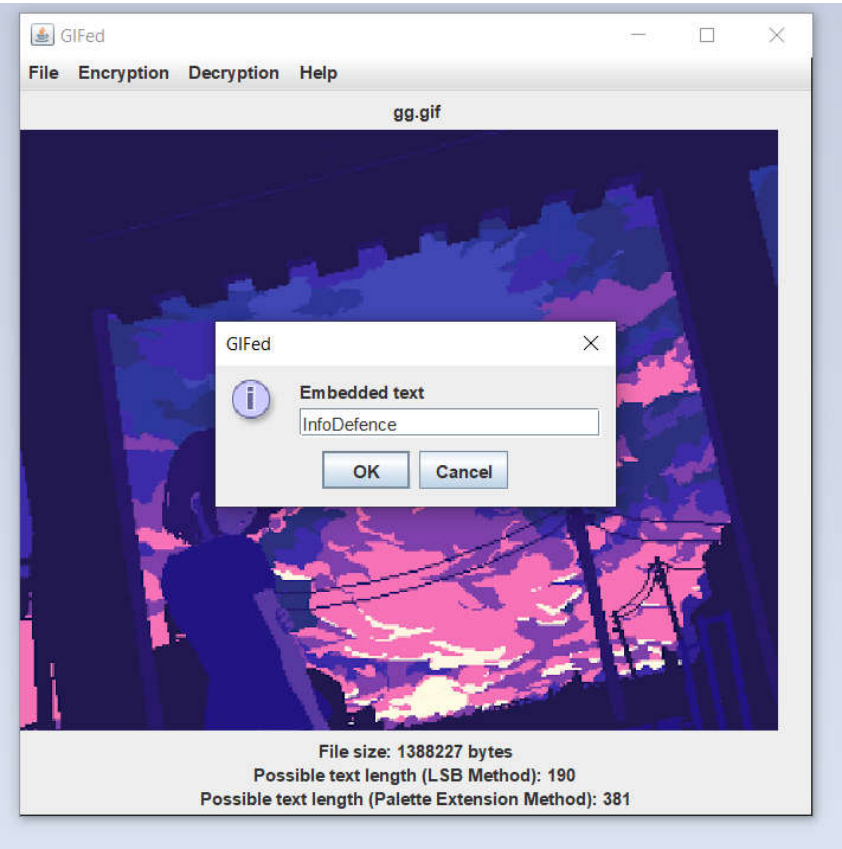


Рисунок 3 –Текст для кодування

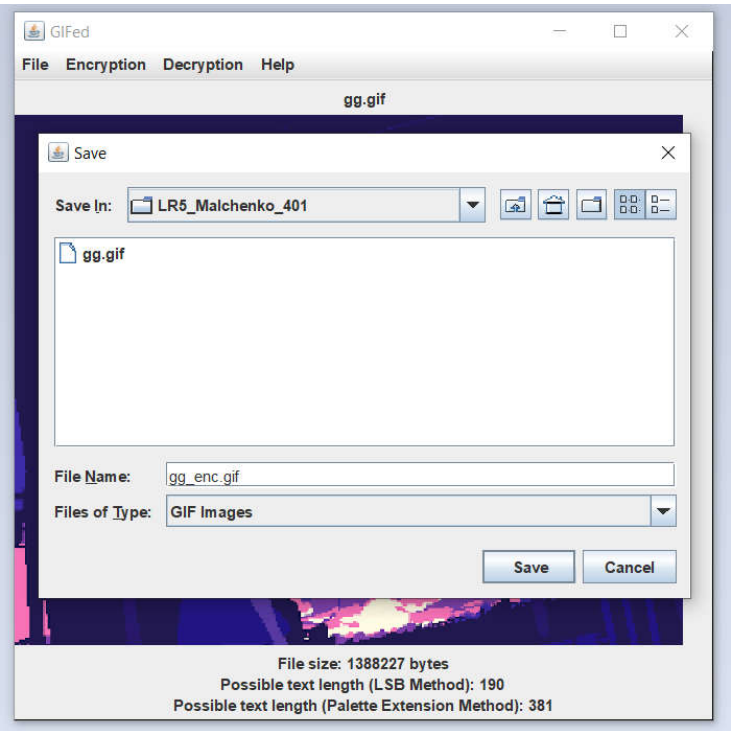


Рисунок 4 – Збереження закодованого тексту у новому файлі

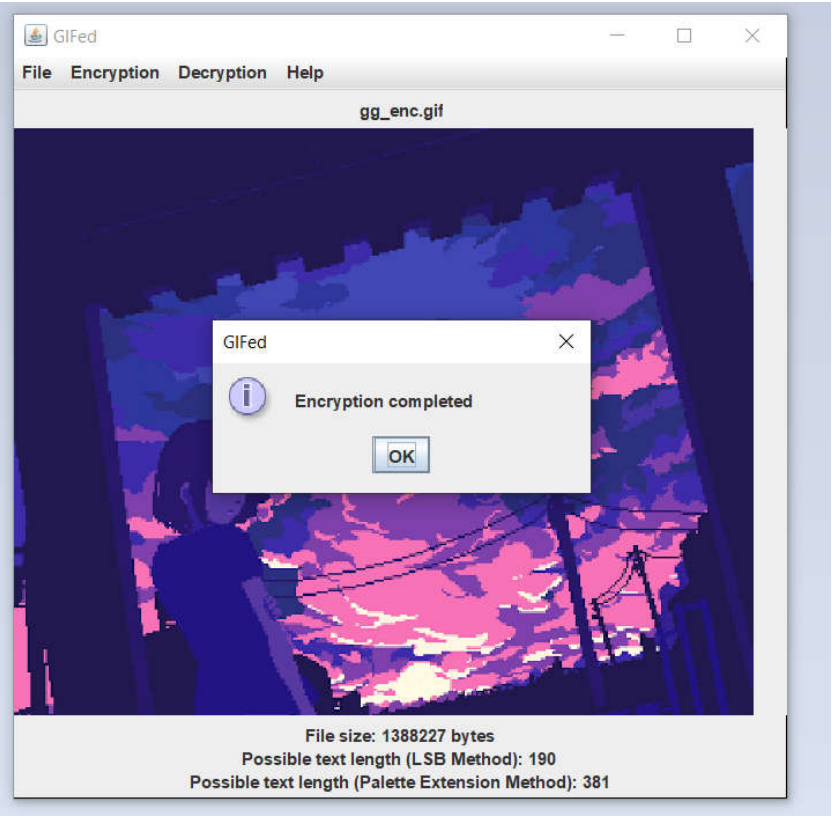


Рисунок 5 – Результат

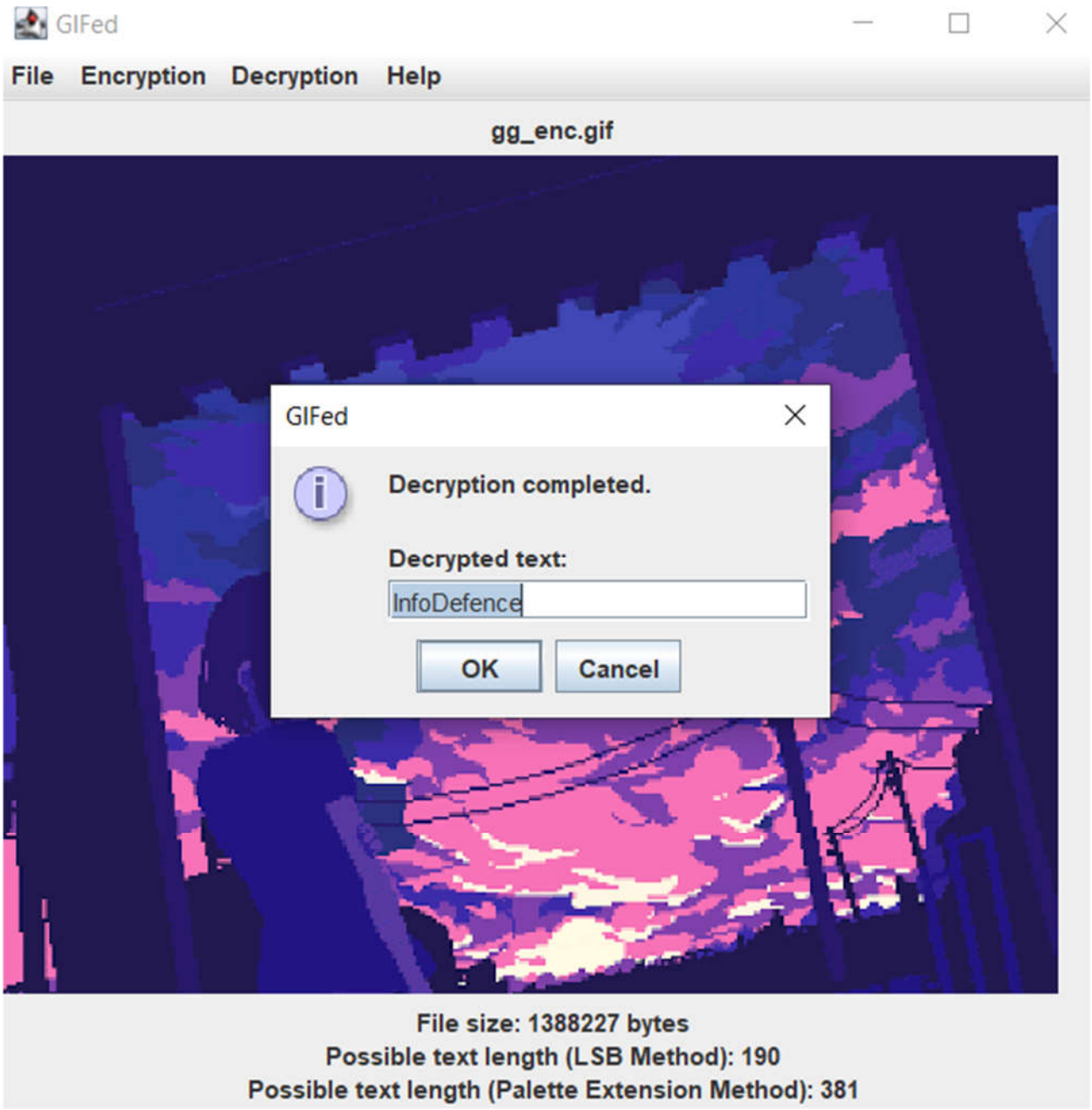


Рисунок 6 – Декодування тексту з зображення

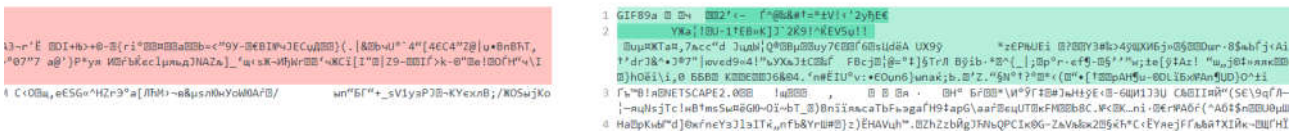


Рисунок 7 – Перевірка на різницю між файлами до кодування та після

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. *Офіційний вісник Президента України*. 2017. № 5. С. 15. – Ст. 102
2. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».
3. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)"
4. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. (ISO/IEC 27002:2013; Cor 1:2014, IDT).
5. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
6. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
7. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення
8. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
9. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. С. 69. Ст. 899
10. Стратегія національної безпеки України : Указ Президента України від 06.05.2015 р. № 287/2015. *Офіційний вісник України.* 2015. № 43. С. 14. Ст. 1353
11. Управління інформаційною безпекою. Конспект лекцій : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
12. Атаки на системи штучного інтелекту : навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н. Л. Чернова ; за заг. ред. С. П. Євсеєва. Львів : «Новий Світ-2000», 2025. 108 с. (Серія «Кібербезпека та штучний інтелект»).
13. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посіб. Київ : Юрінком Інтер, 2025. 236 с.
14. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навчальний посібник. Запоріжжя : ЗНУ, 2025. 151 с. https://dspace.znu.edu.ua/jspui/bitstream/12345/25701/3/0061692m.pdf
15. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ : Видавництво НА СБ України, 2020. 256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf

16. Дорогий Я. Ю., Нікітенко А. О. Методи та засоби технічного захисту інформації : практикум.Луцьк : ДонНТУ, 2024. 242 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/6c78d848-37f7-41f1-b139-c933fddedab6/content
17. Етичний хакінг : навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. Львів : «Новий Світ-2000», 2025. 100 с. (Серія «Кібербезпека та штучний інтелект»).
18. Кібербезпека : WEB-технології : навчально-довідковий посібник / С. П. Євсеєв, А. М. Ткачов, В. О. Алексієв, Ю. М. Рябуха. Львів : «Новий Світ-2000», 2026. 390 с.
19. Кібербезпека : глосарій / Т. Пазковскі, В. Собчук, О. Лаптєв. Львів : «Новий Світ-2000», 2025. 244 с.
20. Кібербезпека та новітні технології захисту інформації : навчальний посібник / В. Ю. Ковтун, С. П. Євсеєв, І. В. Аксьонова ; за заг. ред. С. П. Євсеєва. Львів : «Новий Світ-2000», 2025. 285 с. (Серія «Кібербезпека та штучний інтелект»).
21. Кібербезпека: WEB-технології: навчально-довідковий посібник / уклад. С. П. Євсеєв, А. М. Ткачов, В. О. Алексієв, Ю. М. Рябуха. Харків : ХНЕУ ім. С. Кузнеця. Львів: Новий Світ-2000, 2024. 390 с.
22. Кібербезпека: основи кодування та криптографії : навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Львів : “Новий Світ-2000”, 2025. – 658 с.
23. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.
24. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін ; під. ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2020. 554 с.
25. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту : навчальний посібник для студентів вищих навчальних закладів. Львів : Новий Світ- 2000, 2020. 678 с.
26. Сілін Є. С., Кадубовський О. А. Основи кібербезпеки : навчальний посібник. Дніпро, 2023. 200 с. URL: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
27. Якименко Ю. М., Савченко В. А., Легомінова С. В. Системний аналіз інформаційної безпеки: сучасні методи управління : підручник. Київ : Державний університет телекомунікацій, 2022. 308 с. https://duikt.edu.ua/uploads/l_2230_88161692.pdf

Навчальне видання

КІБЕРБЕЗПЕКА ТА КІБЕРЗАХИСТ

Методичні рекомендації

Укладачі:

Шебаніна Олена В’ячеславівна

Тищенко Світлана Іванівна

Пархоменко Олександр Юрійович

Жебко Олександр Олегович

Коломієць Андрій Миколайович

Формат 60х84 1/16. Ум. друк. арк. 2.94.

Наклад 50 прим. Зам. № _____

Надруковано у видавничому відділі

Миколаївського національного аграрного університету

54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб’єкта видавничої справи ДК № 4490 від 20.02.2013