КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кафедра інженерії програмного забезпечення та кібербезпеки

Захищено на кафедрі інженерії програмного забезпечення та кібербезпеки
«24»_листопада_____2021р.
з оцінкою _____96_____

Підпис членів комісії:
_____
_____
_____

КУРСОВА РОБОТА
з дисципліни
«БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»
НА ТЕМУ:

«Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper»

Виконала: студентка факультету
інформаційних технологій
3 курсу 12 групи
Войткевич Аліса Андріївна

Науковий керівник:
Тищенко Дмитро Олександрович

Київ 2021

Київський національний торговельно-економічний університет

Кафедра інженерії програмного забезпечення та кібербезпеки

Дисципліна Безпека інформаційних систем

Курс 3 Група 12 Семестр 5

ЗАВДАННЯ

на курсову роботу студента

Войткевич Аліси Андріївни

(прізвище, ім'я, по батькові)

1. Тема курсової роботи «Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper»

2. План курсової роботи

3. Перелік графічного матеріалу __зображень – 12, таблиць – 1._____

_____

4. Термін подання студентом завершеної курсової роботи (проекту) на кафедру _18.11.2021_____

5. Термін захисту курсової роботи (проекту)_24.11.2021__

6. Дата видачі завдання _15.09.2021_____

Студент_____
(підпис)

Науковий керівник _____ _____Тищенко Д.О._____
(підпис) (прізвище, ім'я, по батькові)

Завідувач кафедри _____ _____Криворучко О.В._____
(підпис) (прізвище, ім'я, по батькові)

Київський національний торговельно-економічний університет

Рецензія на курсову роботу (проект) і результат захисту

Студентки __ Войткевич Аліси Андріївни

(прізвище, ім'я та по батькові)

___3___ курсу __12____ групи _____ФІТ_____факультету

Курсова робота (проект) з дисципліни «Безпека інформаційних систем»

(назва навчальної дисципліни)

Тема «Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper»

Реєстраційний № 12-2, дата одержання 15.09.2021

Науковий керівник _____Тищенко Д. О._____

Зміст рецензії

У курсовій роботі студентки Войткевич А. А. на тему «Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper» зазначено актуальність дослідження, мету, об’єкт, предмет та задачі дослідження.

У теоретичній частині курсової роботи студентка розглянула питання цілісності та конфіденційності інформації. Автором детально описано та охарактеризовано основні загрози безпеки інформації. Також було розроблено моделі загроз і порушника. У третьому розділі для покращення роботи компанії автор розробив програмний модуль для шифрування за допомогою мови C# у середовищі Visual Studio. В цілому курсова робота студентки Войткевич А. А. на тему «Комплексний підхід до захисту конфіденційної інформації в компанії Golden Cooper» оформлена у відповідності до Вимог, може бути допущена до захисту та заслуговує на позитивну оцінку.

Допущено до захисту “18”_листопада____ 2021 р.

Захист планується о 09:00 “24” листопада_ 2021 р.

(час)

кафедра інженерії програмного забезпечення та кібербезпеки

(місце роботи комісії)

_____

(підпис наукового керівника)

Курсова робота захищена “24” листопада 2021 р.
з оцінкою « 96 » балів____«відмінно»_____

(за шкалою КНТЕУ, національною шкалою та шкалою ЄКТС)

Комісія:

1. _____ ___Тищенко Д.О.___

(підпис) (прізвище, ініціали)

2. _____ ___Савченко Т.В.___

(підпис) (прізвище, ініціали)

3. _____ ___Лукова-Чуйко Н.В.__

ЗМІСТ

АНОТАЦІЯ

Загальний обсяг роботи склав 44 сторінки, де знаходиться 12 рисунків, 1 таблиця. Розглянуто такі основні поняття як: інформаційна безпека, інформаційна загроза, комунікаційно-інформаційна система, порушник, пристрої, методи і системи захисту інформації.

Проведено детальний огляд та аналіз системи захисту інформації від несанкціонованого доступу, сформоване технічне завдання, здійснено детальний аналіз загроз інформаційній безпеці об'єкта захисту та розроблено моделі загроз і порушника з описом системи захисту інформації, інженерно-технічних, апаратних та програмних засобів, підготовлено об’єкт дослідження та необхідні програмні засоби.

ВСТУП

Всі процеси, пов’язані з обробкою інформації, можуть піддаватися комп’ютерним атакам, що націлені на порушення властивостей безпеки. Основну загрозу для інформаційної безпеки компанії становлять викрадення даних, використання неперевіреного програмного забезпечення, хакерські атаки, отримання спаму, безвідповідальність працівників. Така діяльність може за секунду знищити репутацію компанії, що створювалась роками. Клієнти втратять довіру до компанії, адже вона допустила витік конфіденційної інформації, що має фінансову цінність. А шахраї навіть можуть залишитися непоміченими.

Ефективне забезпечення інформаційної безпеки на будь-якому рівні, чи то персональний комп’ютер, локальна мережа, підприємство, регіон або держава, можливе лише на шляху реалізації комплексного підходу. Саме такий підхід може забезпечити дієвий захист, що дозволить організації відновити контроль, знизити ризики. Система захисту інформації повинна бути гнучкою, адаптивною та використовувати не тільки технічні засоби захисту, а й організаційні, правові. Механізм протидії повинен створюватися після проведення оцінки ризиків і загроз інформаційній безпеці, враховуючи доцільність.

У курсовій роботі «Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper» розглянуто питання потенційних загроз безпеці інформації і даних, що підлягають захисту та визначено основні напрямки інформаційної безпеки компанії.

Тема курсової є дуже важливою і актуальною у наш час. Адже частота та складність інцидентів значно збільшилися. Навіть державні організації страждають від зловмисників, що ставить під загрозу людські життя.

Об’єктом дослідження визначено комплекс систем та заходів безпеки Golden Cooper. А для більш чіткої та дієвої роботи системи пропонується

розробити додатковий технічний засіб для шифрування інформації за допомогою Microsoft Visual Studio.

Предметом дослідження визначено систему захисту інформації, а саме системи захисту від несанкціонованого доступу.

Завданням являється дослідження внутрішньої системи доступу працівників та покращення умов захисту.

Ціль дослідження – покращення системи захисту інформації, тому було прийнято рішення розробити засіб для шифрування цінної інформації, так як до компанії постійно надходять особисті дані під час роботи.

Практичне значення засобу полягає в тому, що прочитати певну інформацію, документ зможе лише та людина, яка розшифрує цю інформацію.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОМПАНІЇ «GOLDEN COOPER»

1.1. Сфера діяльності підприємства

Будівельна компанія «Golden Cooper» займає провідні позиції на ринку приватного та комерційного будівництва в Україні. Вона є постачальником фасадних і покрівельних матеріалів провідних світових брендів. Також компанія надає послуги з архітектурного проектування, будівництва та реалізації проектів з урахуванням всіх побажань і особливостей клієнта.

Головне завдання компанії – підтримувати високий сервіс обслуговування на всіх етапах управління будівництвом, починаючи від першого дзвінка, закінчуючи врученням ключів від житла, а також цінувати час клієнта і мінімально залучати його в будівельний процес. Команда (директор з будівництва, інженер ПТО, керівник проєкту, інженер-кошторисник) самостійно займається усіма питаннями (адміністративними, технічними, фінансовими, господарськими), пов'язаними з проєктом.

Послуги «Golden Cooper»:

- будівництво, генпідряд і комплексне управління будівельними проектами;
- ремонт квартир, офісів, будинків і шоу-румів;
- виробництво та монтаж фальцевої покрівлі та фасаду;
- імпорт матеріалів для покрівлі та фасаду;
- імпорт паркету.

1.2. Характеристика інформації, що підлягає захисту

Компанія займається не лише будівництвом, а й комплексним управлінням проєктами, тому кожного дня працівники отримують велику кількість конфіденційної інформації. Основні, оперативні та транзакційні дані, які

використовує підприємство, мають високу вартість, а їх втрата, видалення чи викрадення можуть призвести до серйозних фінансових проблем.

Перелік паперової інформації, що підлягає захисту:

- рахунки;
- накладні;
- контракти;
- акти виконаних робіт;
- кошториси.

Перелік електронної інформації, що підлягає захисту:

- рахунки;
- накладні;
- контракти;
- акти виконаних робіт;
- кошториси;
- скани документів;
- корпоративні пошти;
- архів з відеонагляду.

В ході дослідження було виявлену головну проблему компанії – відсутність конфіденційності інформації. Будь-який співробітник може підійти до робочого столу колеги і подивитися документи, що його цікавлять. Так само будь-який співробітник може вільно отримати доступ до архівних відеозаписів чи комп'ютеру колеги.

1.3. Можливі заходи щодо захисту інформації

По-перше, працівники мають зберігати документи в паперовому вигляді не просто на робочій поверхні, а у спеціально відведених під це шухлядах на замках або сейфах. Адже викрадення паперової документації – це найпростіший спосіб для

недобросовісного працівника/шахрая дізнатися інформацію і скористатися нею в особистих цілях.

По-друге, необхідно підвищити безпеку комп'ютерних систем. Для цього треба встановити паролі до облікового запису кожного працівника і змінювати їх кожного місяця. Таким чином буде забезпечена надійність та якісніша робота системи підрозділу захисту інформації.

Ключовим моментом є забезпечення конфіденційності інформації, що зберігається на комп'ютерах чи надсилається електронною поштою. Так як працівники компанії активно спілкуються з клієнтами і мають необхідність знати особисті дані для роботи, потрібно краще стежити де й у якому вигляді зберігається інформація. Тому дані можна зашифрувати. Адже зловмисники можуть перехопити лист або скористатися обліковим записом працівника і дізнатися особисті дані клієнтів та компанії. А це може спричинити погані наслідки.

1.4. Висновки до розділу

В даному розділі було проаналізовано і описано напрями діяльності компанії, виявлено можливі проблеми із захисту інформації у процесі використання сучасних технологій під час роботи. Також запропоновано деякі заходи для захисту інформації і сформовано технічне завдання. Обрана тема для програмного забезпечення є дуже корисною та актуальною.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОМПАНІЇ «GOLDEN COOPER»

2.1. Побудова моделі загроз

Щоб визначити методи захисту інформації, потрібно спочатку проаналізувати загрози інформаційній безпеці від несанкціонованого доступу.

Більшість користувачів не знають, що основними загрозами кібербезпеки для організації є загрози безпеці електронної пошти. Кіберзлочинці використовують різні атаки на основі електронної пошти, щоб доставити шкідливе програмне забезпечення, залучити жертв на шкідливі веб-сайти та вкрасти конфіденційні дані.

Зловмисник може реалізувати наступні види загроз електронної пошти, які в залежності від цілі атаки можна розділити на:

1. Напади на файлову систему клієнта електронної пошти:
   - витік секретної інформації;
   - крадіжка баз даних електронної пошти;
   - крадіжка каталогів адрес електронної пошти.
2. Атаки на оперативну пам'ять поштового клієнта:
   - витік секретної інформації;
   - перехоплення електронної пошти в оперативній пам'яті.
3. Атаки на локальну мережу, що з'єднує комп'ютер клієнта електронної пошти з сервером електронної пошти:
   - перехоплення деталей доступу до системи електронної пошти;
   - перехоплення електронної пошти;
   - підробка електронної пошти;

- придушення захисту електронної пошти;

- розповсюдження шкідливого програмного забезпечення;

- поширення небажаної кореспонденції.

4. Атаки на зону оперативної пам'яті сервера:

- перехоплення електронної пошти в оперативній пам'яті;

- обхід фільтрів електронної пошти;

- маршрутизація електронної пошти.

5. Атаки на файлову систему сервера електронної пошти:

- перехоплення електронної пошти в черзі на відправку;

- нав'язування електронної пошти в чергу для відправки.

6. Атаки на локальну мережу, що з'єднує два сервери електронної пошти:

- зміна архітектури системи електронної пошти;

- змодельовані помилки сеансу електронних повідомлень;

- відсторонення абонентів електронної пошти;

- заміна, перехоплення чи блокування повідомлень електронної пошти.

7. Атаки на зону оперативної пам'яті клієнта одержувача:

- впровадження шкідливого програмного забезпечення;

- заміна повідомлення електронної пошти в оперативній пам'яті;

- нав'язування повідомлення електронної пошти в оперативній пам'яті.

8. Атаки на локальну мережу, що з'єднує клієнт, сервер електронної пошти та сервер резервного копіювання:

- перехоплення електронної пошти;

- перехоплення реквізитів доступу до поштової скриньки;

- розповсюдження шкідливого програмного забезпечення;

- поширення небажаної кореспонденції;

- помилковий сервер;

- помилковий клієнт. [1]

Іншими загрозами інформаційній безпеці є порушення або повне припинення роботи комп’ютерної інформаційної системи, отримання доступу до керування роботою комп’ютерної інформаційної системи, знищення або спотворення даних.

2.2. Побудова моделі порушника

Модель порушника інформаційної безпеки – абстрактний (формалізований чи неформалізований) опис потенціального порушника інформаційної безпеки, його кваліфікації, технічних та матеріальних засобів.

Якщо модель порушника розроблена коректно, то і система забезпечення інформаційної безпеки буде побудована правильно.

Модель порушника визначає:

- категорії порушників, які можуть впливати на об’єкт;
- цілі, які можуть переслідувати порушники кожної категорії;
- типові сценарії можливих дій порушників. [2]

Порушник – це особа або група осіб, які в результаті умисних або ненавмисних дій забезпечують реалізацію загроз інформаційній безпеці.

Зовнішні порушники - особи, які не мають права перебувати на території контрольованої зони, в межах якої розташоване обладнання комп'ютерної (інформаційної) системи. Зовнішніми порушниками можуть виступати:

- конкуренти;

- недобросовісні партнери;
- клієнти;
- звільнені працівники компанії;
- співробітники органів відомчого нагляду і управління.

Внутрішні порушники - фізичні особи, які мають право перебувати на території контрольованої зони, в межах якої розташовано обладнання комп'ютерної (інформаційної) системи. Внутрішніми порушниками можуть виступати:

• співробітники служби безпеки;

• програмісти;

• співробітники компанії, від прибиральниці до інженера-кошторисника;

• технічний персонал і тимчасові працівники.

Можна припустити, що порушник може знати деталі конкретної інформаційної системи. А саме:

- загальну інформацію – інформацію про призначення системи, загальні характеристики;
- експлуатаційну інформацію – інформацію, отриману з експлуатаційної документації;
- чуттєву інформацію – інформацію, що доповнює експлуатаційну інформацію про систему.

Порушник може мати:

- дані про організацію роботи, структуру та технічні, програмні засоби, що використовуються в системі;
- дані про інформаційні ресурси системи: порядок та правила створення, зберігання та передачу інформації;
- дані про уразливі місця системи;

- вихідні тексти програмного забезпечення системи;
- дані про способи реалізації загроз.

Передбачається, що порушник має:

- апаратні компоненти засобів захисту інформаційної системи;
- технічні засоби та програмне забезпечення, що є у вільному продажу;
- спеціально розроблені технічні засоби та програмне забезпечення.

Внутрішній порушник може використовувати штатні засоби.

Можна виділити наступні мотиви, що спонукають співробітників до неправомірних дій:

- некомпетентність і халатність;
- помилки користувачів та адміністраторів;
- перевищення повноважень;
- самоствердження;
- «спортивний інтерес»;
- незаконні операції в корисливих цілях;
- помста за нанесену образу;
- цікавість;
- зговір зі сторонніми особами.

2.3. Оцінювання ризику реалізації загроз у комунікаційних системах

Комунікаційний процес - це послідовність передачі та отримання інформації від відправника користувачеві і навпаки.

Для того, щоб процес зв'язку був максимально ефективним, необхідно мати в компанії інформаційно-комунікаційну систему у вигляді автоматизованої системи або на основі наявних на підприємстві інформаційних технологій створити банк даних та службу інформації.

В інформаційно-комунікаційній системі використовуються практично всі джерела, методи передачі та обробки інформації. Особливе значення в останні роки надають електронним засобам.

У сучасних умовах загальної інформатизації та розвитку інформаційних технологій велика увага повинна надаватися забезпеченню інформаційної безпеки в інформаційно-комунікаційній системі, де постійно зростають можливості проведення кіберзлочинів. Ефективність забезпечення інформаційної безпеки в інформаційно-комунікаційних системах залежить від реалізації комплексного підходу до побудови мережевої структури на основі коректного моделювання загроз, вибору засобів захисту її елементів, методів моніторингу.

У кіберпросторі на програмно-апаратні засоби елементів ІКС постійно напрямлені деструктивні дії, що носять як випадковий, так і навмисний характер.

Таблиця 2.1. Класифікація загроз ІБ в розподілених ІКС

№	Ознаки класифікації	Значення ознаки
1	По характеру дії	1.1 Пасивні 1.2 Активні
2	По меті впливу	2.1 Порушення конфіденційності інформації чи ресурсів 2.2 Порушення цілісності інформації 2.3 Порушення працездатності системи (доступності)
3	По умові початку реалізації впливу	3.1 Атака по запиту від об’єкта, що атакується 3.2 Атака по наступу очікуваної події на об’єкті, що атакується 3.3 Безумовна атака

4	По наявності зворотного зв’язку з об’єктом, що атакується	4.1 Зі зворотнім зв’язком 4.2 Без зворотного зв’язку
5	По місцезнаходженню суб’єкта атаки відносно об’єкта, що атакується	5.1 Внутрішньосегментне 5.2 Міжсегментне
6	По рівню еталонної моделі, на яку реалізується вплив	6.1 Фізичний 6.2 Канальний 6.3 Мережевий 6.4 Транспортний 6.5 Сеансовий 6.6 Представницький 6.7 Прикладний

Отже, враховуючи атаки на систему, можна виділити такі види загроз інформаційній безпеці ІКС:

- загроза аналізу мережевого трафіку;
- загроза віддаленого адміністрування;
- загроза підміни довіреного об’єкта чи суб’єкта системи;
- загроза несанкціонованого доступу;
- загроза відмови в обслуговуванні;
- загроза порушення цілісності;
- загроза від інсайдерів;
- загроза впровадження в систему неправдивого об’єкта шляхом нав’язування неправдивого маршруту;
- загроза впровадження в систему неправдивого об’єкта шляхом використання недоліків алгоритмів віддаленого пошуку.

Модель порушника ІКС визначає:

• категорії осіб, у числі яких може бути правопорушник;

• можливі цілі правопорушника та їх градація за ступенем важливості та небезпеки;

• припущення щодо його кваліфікації;

• оцінка його технічного озброєння;

• обмеження і припущення щоо характеру його дій.

2.4. Інженерно-технічні, апаратні та програмні засоби захисту інформації в компанії «Golden Cooper»

2.4.1. Опис фізичних об'єктів захисту в компанії

Інженерно-технічний захист (ІТЗ) - це сукупність спеціальних органів, технічних засобів та заходів щодо їх використання на користь захисту конфіденційної інформації. ІТЗ характеризується:

1) за об'єктами впливу;

2) за характером заходів;

3) за способом реалізації;

4) за масштабом охоплення;

5) за класом технічних засобів захисту;

6) за класом засобів зловмисника.

Фізичні засоби - це пристрої, інженерні споруди та організаційні заходи, що ускладнюють або виключають проникнення зловмисників до конфіденційної інформації. До них відносяться механічні, електромеханічні, електронні, електронно-оптичні та радіотехнічні пристрої для заборони несанкціонованого доступу пронесення коштів та матеріалів та інших можливих видів злочинних дій.

Системи контролю і управління доступу (СКУД) виконують функцію захисту від несанкціонованого проникнення сторонніх осіб на територію і розмежування доступу співробітників усередині підприємства.

Додатковими завданнями СКУД є:

- ідентифікація осіб, що мають право доступу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об’єкті;
- обробка інформації та ведення статистики.

Основні переваги систем контролю і управління доступом (СКУД):

- система контролю відповідає на питання «хто?», «де?» і «коли?»;
- система контролю доступу визначає хто допускається до входу або виходу, куди і звідки дозволено заходити і виходити, коли можна знаходитися в тих або інших приміщеннях;
- на відміну від звичайних замків системи контролю доступу можуть обмежити доступ власникові ключа по певних датах або часу;
- звичайні замки не здатні надати повний звіт про того, хто і коли відкривав певні двері;
- ключ від звичайного замку дуже просто скопіювати і передати сторонній особі. При втраті ключа або звільненні співробітника для повної упевненості часом необхідно поміняти замки. Система контролю доступу дозволяє заборонити доступ звільненому працівникові по карті, ключу та відбиткам пальців;
- СКУД стежить за дверима і сигналізує у тому випадку, якщо двері залишаться відкритими занадто довго після того, як були розблоковані;
- Система контролю дозволяє доступ на основі облікових користувачів, що надаються їй. Якщо доступ дозволений, то двері будуть відкриті, а операція

– записана. У разі відмови – двері залишаться закритими, а спроба доступу також буде зафіксована.

Системи контролю і управління доступом часто інтегровані з системами охоронної сигналізації, відеоспостереження і пожежної сигналізації, що дозволяє найефективніше вирішити завдання забезпечення безпеки підприємства.

Призначення системи охоронної сигналізації полягає у виявленні несанкціонованого проникнення на об'єкт, що охороняється, і формуванні відповідного сповіщення. Повідомлення про спрацювання системи охоронної сигналізації бувають:

- звукові;
- світлові.

До складу системи входять:

- сповіщувачі різного принципу дії;
- приймально-контрольні прилади (ПКП) та панелі;
- блоки живлення;
- обладнання для передачі інформації на пульт охорони або телефон власника об'єкта.

Система відеоспостереження дозволяє централізовано спостерігати за подіями як на самому об'єкті, що охороняється, так і в його околицях. Це дає можливість своєчасно виявити наближення підозрілих осіб чи спробу проникнення на територію.

З чого складається система відеоспостереження:

- камери;
- відеореєстратори;
- блок живлення;
- розгалужувач живлення;

- BNC-power кабель.

Апаратура для відеоспостереження поділяється на дві основні категорії: внутрішні та зовнішні. Хоча обидва вони забезпечують одну й ту саму функцію - щоб можна було бачити, що відбувається у певній галузі, вони мають схожі функції, між ними є певні відмінності. Основна відмінність між внутрішніми та зовнішніми полягає в тому для якого завдання вони призначені. Зовнішня камера відеоспостереження для вулиці має бути водонепроникною та захищеною від атмосферних впливів, зазвичай він виготовляється з міцніших матеріалів. З іншого боку, внутрішні камери не повинні працювати у суворих погодних умовах. У цих категоріях є багато моделей, які виконують різні функції. Внутрішні камери відеоспостереження встановлені власноруч, зосереджують увагу на інтер'єрі вашого будинку.

Пожежна сигналізація – система, що складається з обладнання спрямованого на захист, добірка якого проводиться в залежності від ризику, площі та обсягів зони, що охороняється, а також від кількості приміщень всередині об'єкта. Забезпечення безпеки будівель та територій – це головна умова його експлуатації. Одним із найнебезпечніших факторів, що загрожують життю та матеріальним цінностям, є пожежа. Його найважчі загрози – це відкрите полум'я та сильне задимлення приміщення. Сучасні засоби захисту від вогню, оповіщення та пожежогасіння можуть з великою ефективністю попередити та мінімізувати важкі наслідки займання.

Пожежна сигналізація є слаботочною електричною установкою. Базова схема включає три рівні з погляду технічної класифікації обладнання:

- датчики (сповіщувачі): кожен з цих модулів є детектором високої чутливості, який спрацьовує на певні фактори пожежі, що впливають. Це може бути дим або пряма дія вогню (температура). Цей периферійний пристрій здійснює моментальний аналіз ситуації, і відразу відправляє сигнал на ПКУ;

- приймально-контрольні пристрої або ПКУ (контролери): завдання цих приладів – швидкий прийом отриманої від датчиків інформації, її обробка рамках закладеного алгоритму;
- виконавчі пристрої: до них належать контрольні реле, спеціальні оповіщувачі та диспетчерські пульти управління.

На сьогоднішній день існують такі види пожежної сигналізації:

- пороговий (аналоговий): побудова ліній комутувальних кабелів тут відбувається за радіальною топологією. Кожен робочий шлейф, з'єднаний з ЦП (центральною панеллю) контролює щонайменше 20 сповіщувачів. Якщо відбудеться спрацювання будь-якого з них, ЦП відразу передасть інформацію, що містить номер шлейфу, на робочу панель або підключений монітор;
- адресно-опитувальний тип: відрізняється від попереднього принципу зв'язку між сповіщувачем та ЦП. Центральна панель тут запрограмована таким чином, щоб через встановлені проміжки часу може проводити чергове опитування всіх підключених сповіщувачів з метою швидкої оцінки стану;
- адресно-аналоговий тип: один із найбільш затребуваних видів ПС на сьогоднішній день. Ця система автоматичної пожежної сигналізації набула широкого поширення за рахунок своєї функціональності та надійності. Остаточне рішення про тривожне сповіщення приймає контрольна панель, яка попередньо проводить аналіз отриманих значень від сповіщувачів, з актуальними параметрами кімнат. Цей варіант особливо ефективний на ранніх стадіях пожежі.

- Нормою вважається 1 кг. гасячої речовини на 25 м² площі об'єкта.
- Наявність плану евакуації обов’язкова.
- Евакуаційні виходи повинні бути відчинені.

2.4.2. Опис апаратних пристроїв у компанії

Апаратні засоби – це механічні, електричні, електронні пристрої, призначені для захисту інформації від витоку та розголошення та протидії технічним засобам шпигунства.

- до основних апаратних засобів захисту інформації відносяться: пристрої для введення ідентифікаційної користувачем інформації (магнітні і пластикові картки, відбитки пальців і т.д.);
- пристрої для шифрування інформації;
- пристрої для запобігання несанкціонованого включення робочих станцій і серверів (електронних замків і блокаторів).

Отже, системи контролю доступу складаються з наступних основних елементів:

1. Зчитувачів**.** Вони зчитують кодований сигнал (код) з карток, транспондерів, пультів, смарфонів (за допомогою бездротових з'єднань WI-FI, BLUETOOTH, NFC, тощо). А також зчитують біометричні данні (відбиток пальця, долоні, сітківку ока). Є ще кодові панелі, на яких користувач вводить відповідний код.

2. Керуючих елементів. Ними виступають контролери. Вони ідентифікують сигнал, який надходить від зчитувачів, порівнюють надісланий код з тими, що занесені в базу контролера. І, в разі їх співпадіння, подають сигнал на відкриття замикаючих пристроїв.
   До керуючих елементів також відносяться кнопки виходу.

3. Виконавчих елементів, якими зазвичай виступають: електрозаскочки, електроригелі, електрозамки та електромагніти.

4. Системи безперебійного електроживлення. Вони можуть опціонально додаватись до СКД.

Ідентифікатори СКУД:

- картка з магнітною смужкою;
- безконтактна картка;
- спеціальний брелок;
- цифровий код, що безпосередньо вводиться на клавіатурі;
- унікальні особисті ознаки людини: відбитки пальця / долоні, малюнок сітківки ока тощо.

Найпоширенішим типом ідентифікатора, який в даний час використовується в СКУД, є безконтактні Proximity картки. Картки доступу СКУД (або безконтактні радіочастотні ідентифікаційні картки) є електронними носіями унікального коду. Код зчитується спеціальним приймальним пристроєм (зчитувачем) на відстані.

Найдешевші, але найменш захищені - карти формату EM-Marin (ім'я компанії EM Microelectronic-Marin). Це найпоширеніший формат карт, що використовуються в СКУД. Його єдиний недолік – відносна простота клонування, що може бути визначним тільки для об'єктів, що під особливою охороною. Тим паче, що ряд алгоритмів СКУД робить неможливим використання клонованої карти. Крім того, для захисту від підроблених карт існують спеціальні зчитувачі з функцією «антиклон». Ці карти мають і передають засобу зчитування унікальний код. Десятичне значення цього коду вказуються на самій карті. Існує однозначна відповідність між кодом, що сприймає контролер СКУД та числом на карті.

Зчитування ключа Em-Marine здійснюється на відстані від декількох сантиметрів до метра (залежить від зчитувача і ключа). При піднесенні ідентифікатора до зчитувача RFID циклічно передається 64 біти інформації з амплітудною модуляцією носія. Робоча частота - 125 кГц. 40 з 64 переданих біт займає повний номер картки. 32 біти з них є унікальним номером картки, а 8

біт - номер партії (ідентифікатор виробника). Решта 24 біти - це технічна інформація (біти заголовка, парність і стоп-біт).

Електронні замки - це повноцінні замикаючі пристрої, корпус яких містить всі механічні та електронні компоненти, необхідні для їх роботи. Поняття «електронний замок» включає електричні замки, соленоїдні замки, замки з електроблокуванням, електромагнітні замки, електромеханічні замки, комбіновані замки, невидимі замки, біометричні замки і деякі інші види замків, що працюють на електриці або пов'язані з електронікою.

Вважається, що електронний замок має дві основні переваги перед традиційною механічною конструкцією. По-перше, це набагато вищий рівень секретності і надійності, а, по-друге, можливість дистанційного відкриття. До переваг електронних замків, звичайно ж, можна віднести і можливість ведення електронного журналу обліку операцій, що дозволяє точно визначити, хто і коли відкрив замок. Рівень секретності електронного замка сильно варіюється в залежності від пристрою, який використовується для його відкриття.

Види електронних замків:

- врізні електронні замки;
- накладні електронні замки;
- ручки-накладки;
- розумні циліндри.

Апаратне шифрування – процес шифрування, що реалізується за допомогою спеціалізованих обчислювальних пристроїв. До переваг апаратного шифрування можна віднести:

- цілісність;
- швидкість;
- виключення загрози зчитування ключової інформації по коливанням електромагнітного випромінювання, що виникає при шифруванні даних;

- спеціалізований процесор вивантажує центральний процесор комп’ютера;
- можливість реалізації системи розмежування доступу до комп’ютера та захисту інформації від несанкціонованого доступу.

У сучасному ринку представлено 3 різновиди апаратних засобів шифрування інформації:

- блоки шифрування по каналах зв’язку;
- самодостатні шифрувальні модулі;
- шифрувальні плати розширення для встановлення у персональні комп’ютери.

Плати розширення для персональних комп'ютерів є більш універсальним засобом апаратного шифрування і, як правило, дуже прості в налаштуванні таким чином, щоб вся інформація записувалась на жорсткий диск або відправлялася в порти і диски [3]. Додатковими можливостями апаратного шифрування є довірене завантаження, контроль цілісності файлів операційно системи і генератор випадкових чисел.

2.4.3. Опис програмних засобів захисту інформації

Програмні засоби – це система спеціальних програм, що реалізують функції захисту інформації та збереження цілісності та конфіденційності.

Avanpost FAM – система єдиної аутентифікації співробітників у корпоративних ресурсах компанії. Перевагами є:

- одноразова /уніфікована багатофакторна аутентифікація в ОС, мобільних, настільних і веб-додатках;
- аутентифікація в хмарних/ SaaS додатках з використанням єдиного посвідчення співробітника;
- перехресна аутентифікація співробітників в довірених ресурсах партнерських організацій через федерацію ідентичності;

- самообслуговування співробітників з управлінням їх факторами аутентифікації та сценаріями відновлення;
- адаптивна аутентифікація з вибором відповідного ланцюжка перевірок для різних співробітників і даних середовища;
- багатофакторна аутентифікація за допомогою смарт-карток, одноразових кодів, сертифікатів EP, середовища і домену.

Для посилення аутентифікації в Avanpost FAM є можливість використання одноразової технології паролів TOTP (Time-based One Time Password Algorithm). На даний момент підтримується реалізація цієї технології у вигляді додатку Google Authenticator. Користувач встановлює відповідний мобільний додаток на свій телефон і отримує там одноразові паролі, які необхідно ввести при аутентифікації в Avanpost FAM на додаток до основного логіна і пароля. Налаштування додаткового фактора аутентифікації може здійснюватися в тому числі для окремих критичних додатків.[4]

Avanpost FAM підтримує весь арсенал сучасних фізичних факторів, включаючи ключові засоби масової інформації, біометричні зчитувачі та зчитувачі тегів. Платформа, яка поєднує в собі функції ESSO і Web SSO, дозволяє компанії здійснювати єдині проходи співробітників. Цей пропуск може бути використаний як для проходу на територію підприємства, так і в якості додаткового фактора аутентифікації в корпоративну мережу і будь-які додатки.

Програмне забезпечення для шифрування є відмінним інструментом для захисту даних від інших користувачів і від вірусів. Одна програма може підтримувати шифрування декількома алгоритмами - за вибором користувача. Функціональність також може включати повне або часткове шифрування розділів жорсткого диска. Коли ви шифруєте розділ, всі файли на ньому більше не будуть доступні, тому, якщо це системний розділ, то при шифрі операційна система не завантажиться з нього. Крім того, деякі програми мають додаткові функції, які дозволяють, наприклад, постійне видалення файлів.

VeraCrypt

VeraCrypt є одним з найпопулярніших інструментів безпеки. Це програма з відкритим вихідним кодом, яка використовується для шифрування даних на жорстких дисках. З його допомогою можна створити окремий віртуальний том з даними або повністю зашифрувати розділ жорсткого диска, включаючи системний. При використанні останньої функції користувачеві доведеться вводити пароль кожного разу, коли пк запускається. Програма також надає можливість «приховати» зашифрований том від сторонніх очей. Базова версія програмного забезпечення абсолютно безкоштовна.

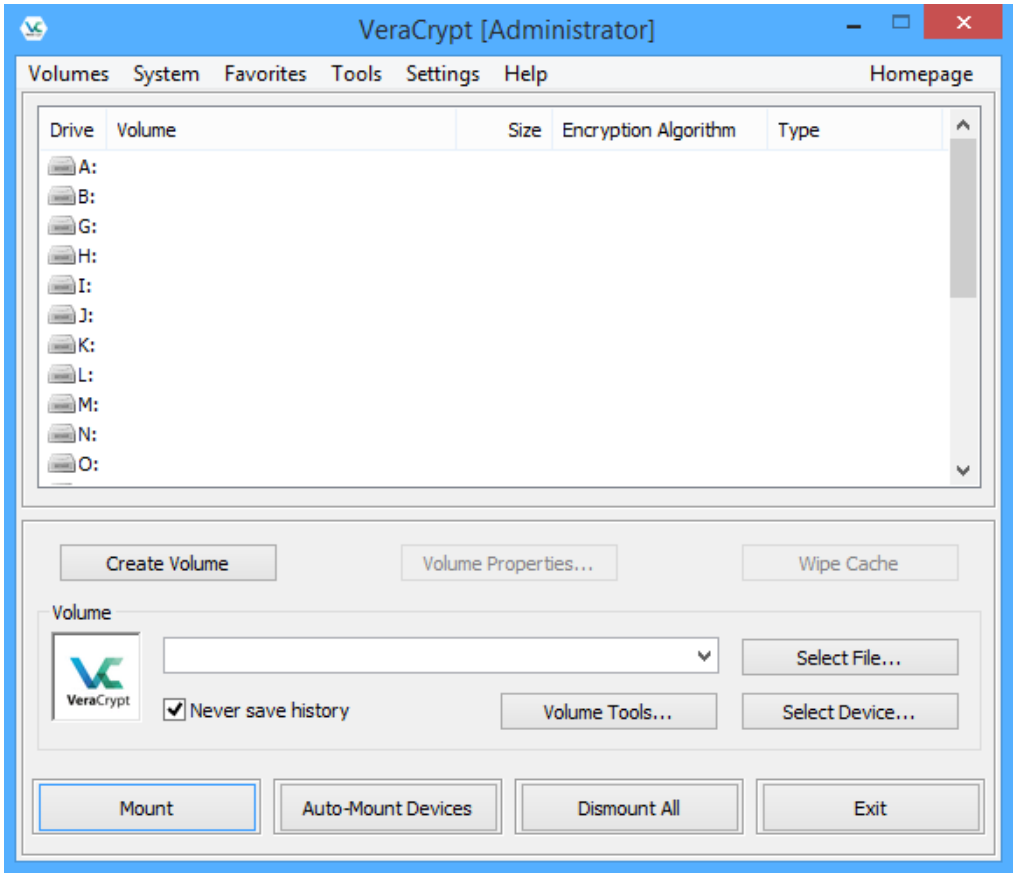


Рисунок 2.1 Інтерфейс VeraCrypt

CryptoExpert

CryptoExpert - це настільне програмне забезпечення Windows, яке пропонує безпечні сховища даних для всіх ваших даних, гарантуючи, що воно завжди захищене від потенційних порушень. Він забезпечує більш потужне шифрування, ніж деякі інші інструменти та програми, перераховані в цій статті, може похвалитися швидкою операцією на льоту. Система може створити резервну систему різних файлів, включаючи сертифікати, файли Word, Excel і PowerPoint, мультимедійні файли та бази даних електронної пошти. Надається безкоштовна 30-денна пробна версія.

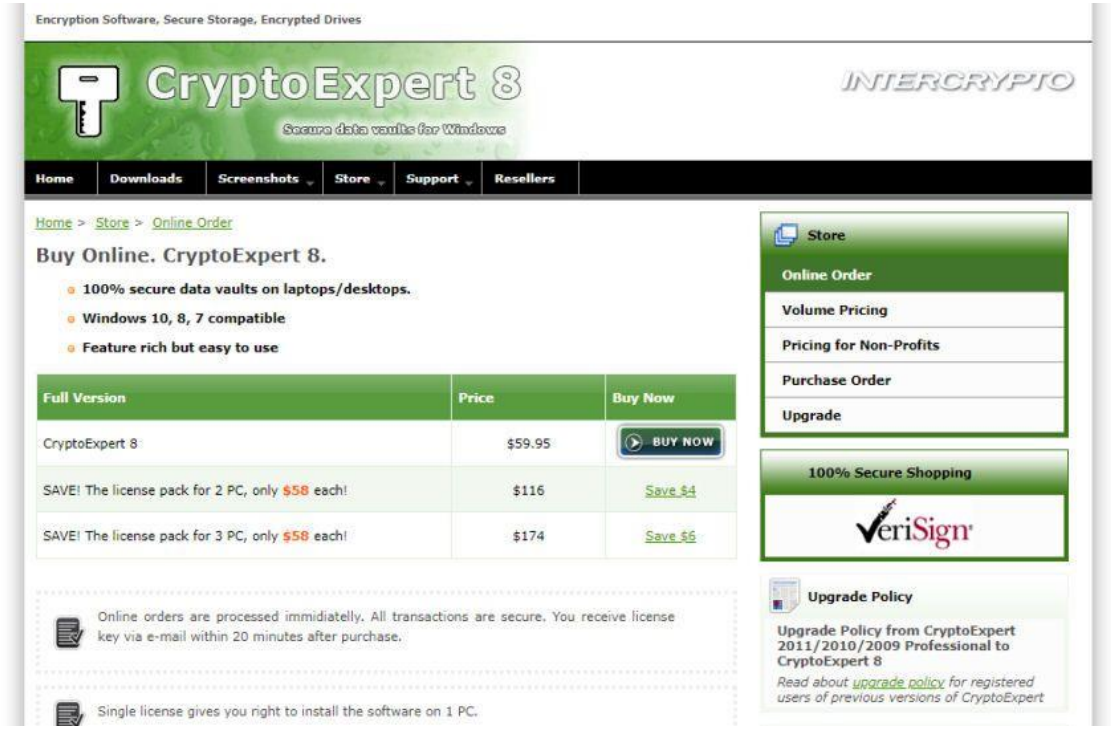


Рисунок 2.2 Інтерфейс CryptoExpert

Boxcryptor

Програмне забезпечення для шифрування Boxcryptor в основному фокусується на шифруванні ваших файлів у хмарі та полегшує шифрування, редагування та розшифрування файлів за допомогою більш ніж 30 різних постачальників хмар. Однак, у вас також є можливість зашифрувати локальні

файли. За допомогою плану Premium ви можете додати стільки просторів для зберігання, скільки потрібно зашифрувати сховище NAS, USB-накопичувачі, цілі жорсткі диски, розташування WebDAV тощо. Boxcryptor підтримує так зване шифрування на льоту. Замість того, щоб шифрувати всю папку, кожен файл в папці шифрується окремо. Таким чином, ви можете легко розшифрувати і відредагувати один файл без необхідності розшифровувати і повторно шифрувати всю папку. При такому підході вам не потрібно часто шифрувати файли вручну. Boxcrytor дозволяє визначати атрибути через ієрархію папок, які потім застосовуються до шифрування папок та параметрів спільного доступу. Наприклад, якщо потрібно додати файл до папки, яка вже зашифрована та передана спільному доступу працівнику, новий файл буде автоматично зашифровано та надано спільний доступ. Це економить багато роботи і часу.

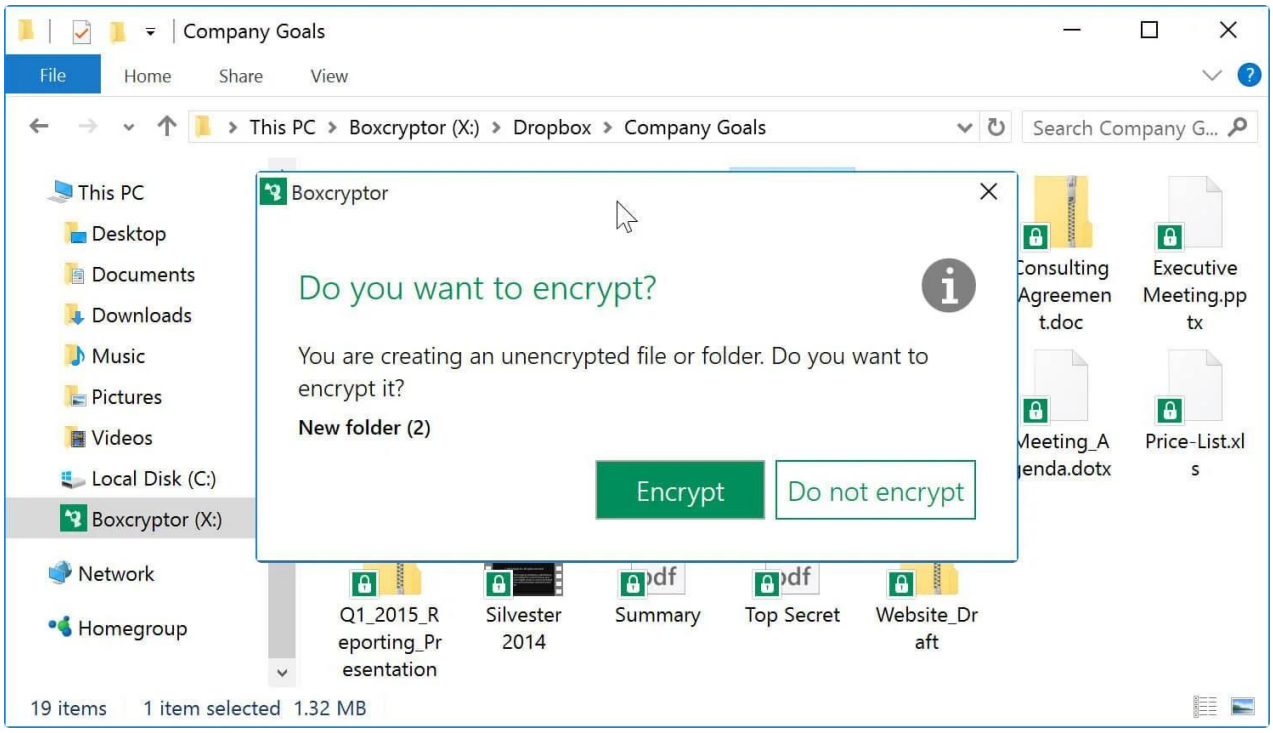


Рисунок 2.3 Boxcryptor

2.5. Висновки до розділу

У даному розділі було здійснено детальний аналіз загроз інформаційній безпеці компанії Golden Cooper, розроблено модель загроз і, з урахуванням технології обробки інформації та побудови моделі загроз інформації, – модель порушника. Також описано системи захисту інформації, інженерно-технічні, апаратні та програмні засоби.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ДОДАТКОВИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ITC GOLDEN COOPER

3.1. Методи і засоби захисту інформації, що впроваджені в інформаційну систему підприємства. Наявність (відсутність) служби з питань захисту інформації.

Форма захисту інформації в компанії - обліковий запис користувача на комп’ютерах. Це сукупність даних про користувача, що зберігається в комп'ютерній системі.

Щоб унеможливити неправомірний доступ до інформації застосовуються такі способи, як ідентифікація та аутентифікація.

Ідентифікація – це механізм надання власного унікального імені або образу користувачеві, який взаємодіє з інформацією.

Аутентифікація - це система способів перевірки збігу користувача з тим образом, якому дозволено допуск.

Найпростіший спосіб захисту – пароль. Пароль – це набір символів для захисту облікового запису. Логін – це слово (ідентифікатор), яке використовується для визначення користувачів у комп'ютерних системах з метою подальшого входу. Достовірна (еталонна) пара логін-пароль зберігається у спеціальній базі даних у комп'ютерному центрі (системі).

Аутентифікація має такий алгоритм: суб'єкт запитує доступ до системи та вводить особистий ідентифікатор (логін) та пароль. Оскільки пароль має зберігатися в таємниці, то він шифрується перед посилкою по незахищеному каналу зв'язку. Ідентифікатор та пароль надходять на сервер аутентифікації, де порівнюються із еталонними. У разі їх збігу, пароль вважається достовірним, а користувач – законним. При збігу з еталоном, автентифікація визнається успішною, при розбіжності – суб'єкт повертається на перший крок.

Іншою формою є наявність служби з питань захисту інформації.

ESET Server Security для Microsoft Windows Server — антивірус для сервера компанії. Він забезпечує безпеку персональних та платіжних даних, а також всіх даних CRM, поштових акаунтів, внутрішньої документації та файлів, що пересилаються. Продукт актуальний для таких компаній, як Golden Cooper. До переваг ESET Server Security можна віднести:

- антивірус та антишпіон;
- розширене сканування пам’яті;
- захист від програм-вимагачів;
- підтримка ESET Dynamic Threat Defense;
- 64-бітне ядро сканування;
- сканер UEFI;
- захист від ботнерів та експлойтів.

Також доступні спеціалізовані функції:

- сканування сховища;
- оптимізації для віртуального середовища;
- підтримка Microsoft Office 365 (після реєстрації на окремому сервері ESET може просканувати OneDrive, щоб забезпечити видимість та відстежувати довірені джерела даних компанії).

ESET Server Security для Microsoft Windows Server забезпечує ефективний захист файлових серверів, зберігаючи при цьому більше системних ресурсів для виконання інших завдань. Під час встановлення продукту можна вибрати необхідні компоненти. Продуктом ESET Server Security для Microsoft Windows Server можна віддалено керувати за допомогою ESET Protect.

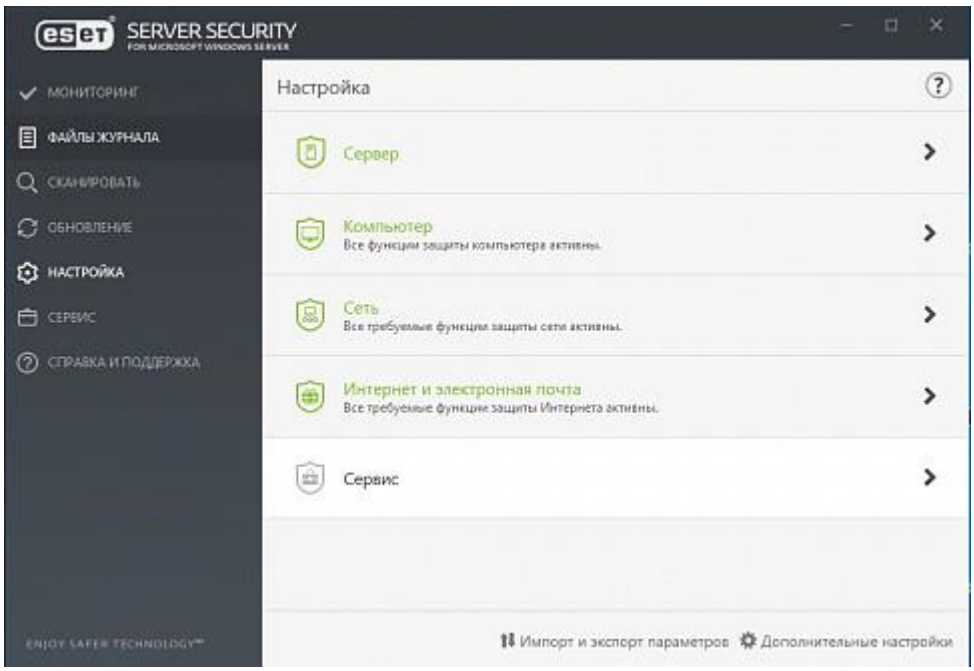


Рисунок 3.1 Інтерфейс ESET Server Security

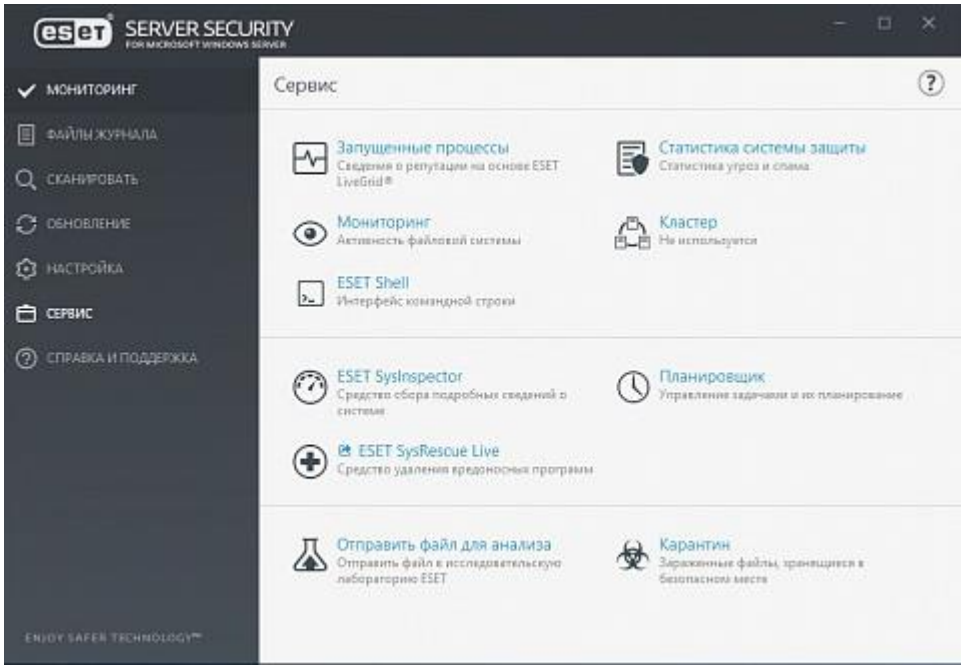


Рисунок 3.2 Інтерфейс ESET Server Security

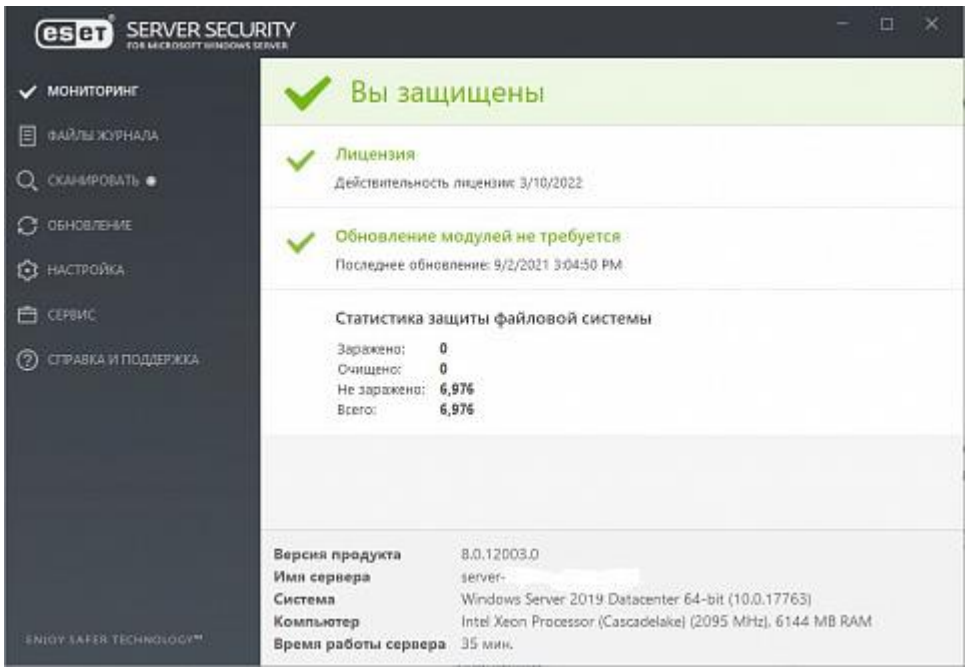


Рисунок 3.3 Інтерфейс ESET Server Security

3.2. Вибір, обґрунтування та опис функціонування додаткових програмно-апаратних засобів захисту інформації компанії Golden Cooper

Незважаючи на те, що компанія добре захищена від різного роду атак, найкращий спосіб підтримувати максимальний рівень безпеки на сервері – це регулярно оновлювати ESET Server Security. У розділі Оновлення можно перевірити поточний стан оновлення ESET Server Security, а також дату та час останнього успішного оновлення.

Найкращим варіантом є придбання оновлення до ESET NOD32 Antivirus Business Edition (NBE) та ESET NOD32 Smart Security Business Edition (SBE).

Отже, нові можливості додатка включають в себе:

- централізоване управління;
- захист робочих станцій;
- захист мобільних пристроїв;
- захист файлових серверів;
- розширений захист робочих станцій.

В пакет буде включено повнодискове шифрування.

Додатковий засіб, що бажано мати підприємству – це ESET Secure Authentication. Це додаток двохфакторної аутентифікації, який надає безпечний доступ до важливої чи конфіденційної інформації компанії. Рішення дозволяє захистити підключення, що знижує ризик витоку даних, зумовлений вибором ненадійних паролів. Переваги ESET Secure Authentication це:

- надійний та простий засіб двофакторної аутентифікації;
- при кожному підключенні формується додатковий тимчасовий пароль для запобігання витоку конфіденційних даних;
- немає потреби в керуванні апаратними пристроями;
- продукт легко інтегрується у існуючу інфраструктуру;
- ідеальне рішення для віддалених співробітників;
- мультиплатформне рішення на базі мобільних пристроїв;
- безпечний доступ до ресурсів системи 1С.

Додаткові можливості включають доставку тимчасових паролів, підтримку стандарту FIDO, підтримку вбудованої біометрії, push-автентифікацію, пакети API та SDK.

3.3. Код програмного модулю захисту інформації та середовище розробки.

Для розробки програмного модулю використовувалася Microsoft Visual Studio. Це інтегрована середа розробки, у якій дозволяється написання, налагодження та складання коду, а також подальша публікація додатків. Крім стандартного редактора і відладчика, які є в більшості середовищ IDE, Visual Studio включає компілятори, засоби автозавершення коду, графічні конструктори і багато інших функцій для поліпшення процесу розробки. Обрана мова програмування – C#. Це сучасна об’єктно-орієнтована мова, що дозволяє створювати різні типи безпечних та надійних додатків[5].

Принцип роботи додатку полягає у шифруванні важливого тексту повідомлень, документів, особистих даних клієнтів або замовників за допомогою шифру Цезаря.

Шифр Цезаря – один із найпростіших і найвідоміших алгоритмів шифрування текстових даних. Цей метод названо на честь римського полководця Гая Юлія Цезаря, який застосовував шифр для особистого листування з підлеглими.

Алгоритм шифрування Цезаря полягає у заміні кожного символу вхідного повідомлення на символ, який знаходиться на певній константній відстані праворуч або ліворуч. Відстань при цьому називають ключем.

Математично шифр Цезаря можна описати наступними формулами:

- $Encrypt(m_n) = (Q + m_n + k) \% Q$;
- $Decrypt(c_n) = (Q + c_n - k) \% Q$.

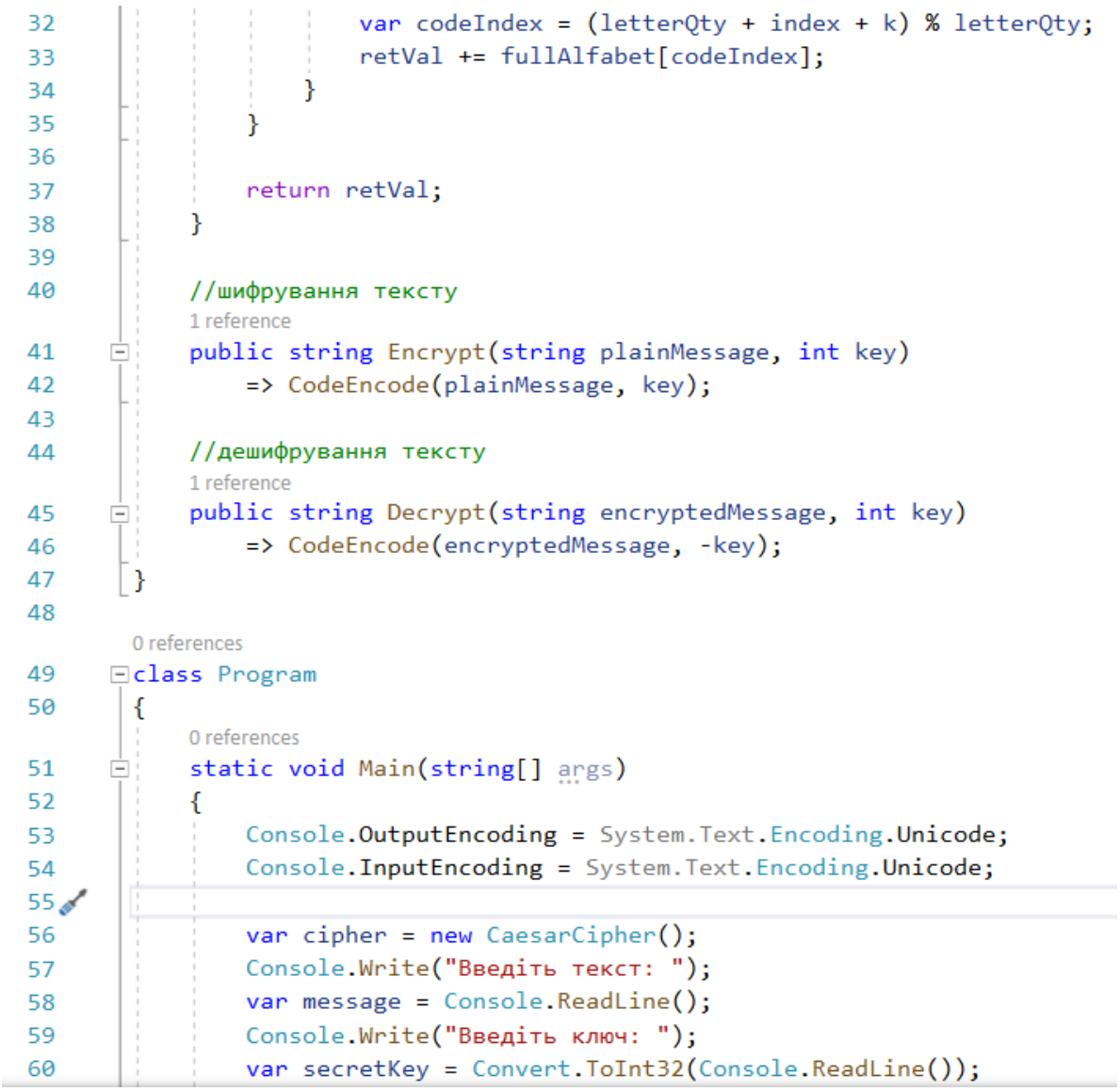
де m - відкритий текст, k - ключ шифрування, Q - кількість символів у алфавіті, c - зашифрований текст.

Отже, спочатку користувач вводить у текстове поле інформацію, дані, повідомлення, які бажано зашифрувати. Далі обирає ключ шифрування. І програма видає зашифрований та одразу розшифрований текст.

Реалізація шифрування Цезаря:

```
1   using System;
2   using System.Collections.Generic;
3   using System.Linq;
4   using System.Text;
5   using System.Threading.Tasks;
6
7
8   namespace Encryption { }
9
        1 reference
10  public class CaesarCipher
11  {
12      //символи української абетки
13      const string alfabet = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ";
14
            2 references
15      private string CodeEncode(string text, int k)
16      {
17          //додаємо в алфавіт маленькі літери
18          var fullAlfabet = alfabet + alfabet.ToLower();
19          var letterQty = fullAlfabet.Length;
20          var retVal = "";
21          for (int i = 0; i < text.Length; i++)
22          {
23              var c = text[i];
24              var index = fullAlfabet.IndexOf(c);
25              if (index < 0)
26              {
27                  //якщо символ не знайдений, то додаємо його в незмінному вигляді
28                  retVal += c.ToString();
29              }
30              else
31              {
```

Рисунок 3.4 Програмний код



```
32                  var codeIndex = (letterQty + index + k) % letterQty;
33                  retVal += fullAlfabet[codeIndex];
34              }
35          }
36
37          return retVal;
38      }
39
40      //шифрування тексту
        1 reference
41      public string Encrypt(string plainMessage, int key)
42          => CodeEncode(plainMessage, key);
43
44      //дешифрування тексту
        1 reference
45      public string Decrypt(string encryptedMessage, int key)
46          => CodeEncode(encryptedMessage, -key);
47  }
48
    0 references
49  class Program
50  {
        0 references
51      static void Main(string[] args)
52      {
53          Console.OutputEncoding = System.Text.Encoding.Unicode;
54          Console.InputEncoding = System.Text.Encoding.Unicode;
55
56          var cipher = new CaesarCipher();
57          Console.Write("Введіть текст: ");
58          var message = Console.ReadLine();
59          Console.Write("Введіть ключ: ");
60          var secretKey = Convert.ToInt32(Console.ReadLine());
```

Рисунок 3.5 Програмний код

```
61          var encryptedText = cipher.Encrypt(message, secretKey);
62          Console.WriteLine("Зашифроване повідомлення: {0}", encryptedText);
63          Console.WriteLine("Розшифроване повідомлення: {0}", cipher.Decrypt(encryptedText, secretKey));
64          Console.ReadLine();
65      }
66  }
```

Рисунок 3.6 Програмний код

Результат роботи програми:

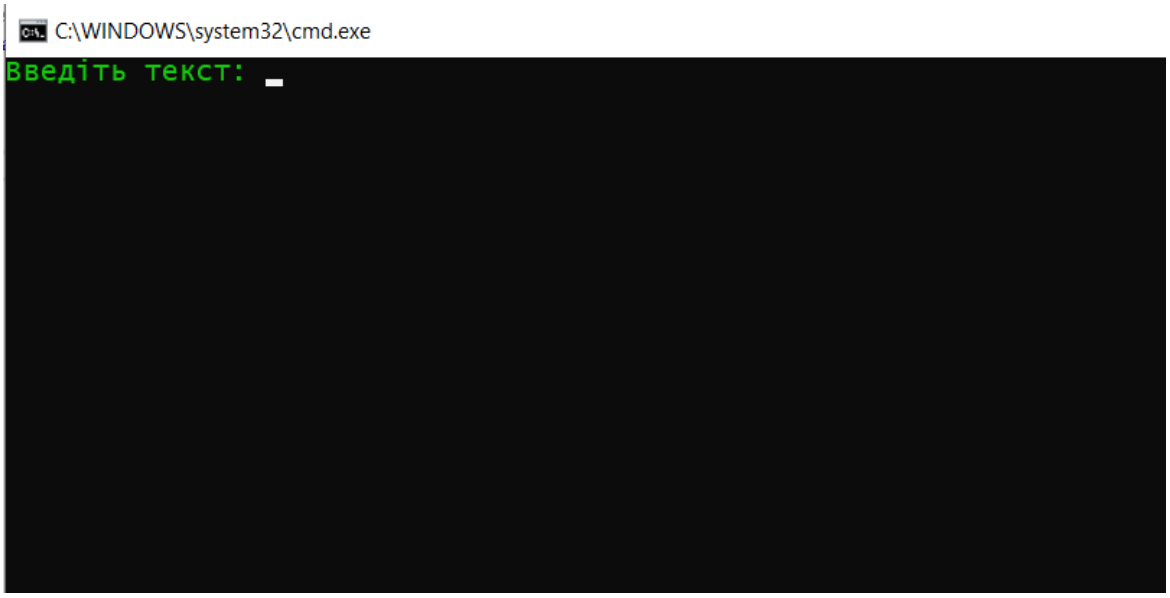


Рисунок 3.7 Введення тексту

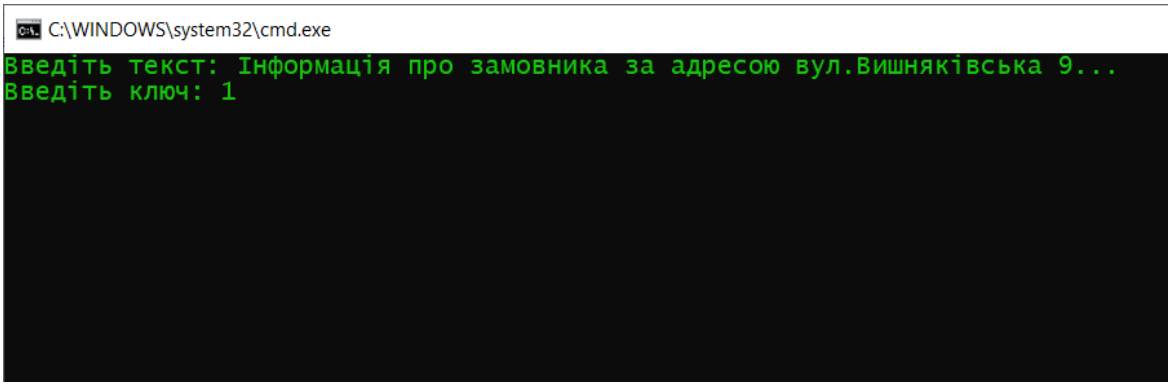


Рисунок 3.8 Введення ключа

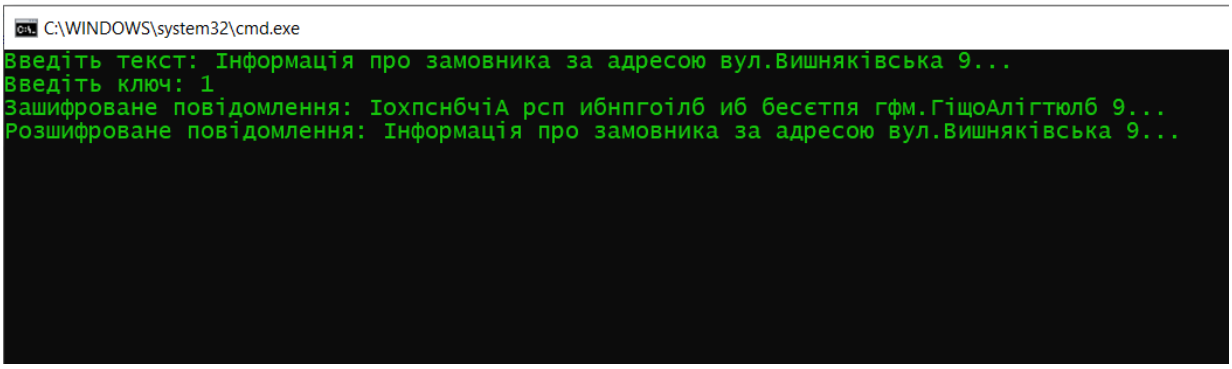


Рисунок 3.9 Шифрування та дешифрування

3.4. Висновки до розділу

У даному розділі було реалізовано додатковий програмний модуль захисту інформації в компанії, описано основні методи і засоби захисту інформації в ІТС компанії, обрано та описано додаткові програмні та апаратні засоби захисту. Також була вказана інформація про мову програмування та середовище розробки програмного додатку для шифрування інформації.

ВИСНОВКИ

У результаті виконання курсової роботи «Комплексний підхід до забезпечення захисту конфіденційної інформації в компанії Golden Cooper» було доведено актуальність та важливість теми інформаційної безпеки не тільки в корпоративних мережах, а й при персональному використанні. Адже діяльність будь-якої організації в наш час пов'язана з отриманням і передачею інформації. Інформація зараз є стратегічно важливим товаром. Втрата інформаційних ресурсів або вилучення конкурентами секретної інформації, як правило, завдає істотної шкоди підприємству і може навіть призвести до банкрутства.

Також було проведено аналіз основних загроз інформаційній безпеці і визначено методи боротьби з цими загрозами. Загрози інформаційній (комп'ютерній) безпеці - це різні дії, які можуть призвести до порушень стану захисту інформації. Іншими словами, це потенційні події, процеси або дії, які можуть пошкодити інформацію та комп'ютерні системи.

Сформовано комплекс заходів для управління інформаційною безпекою, таких як: шифрування, контроль користувачів, управління обліковими даними, тощо.

Підсумком виконаної курсової роботи на тему «Комплексний підхід до захисту конфіденційної інформації в компанії Golden Cooper» є готовий програмний модуль, що може бути використаний компанією для забезпечення конфіденційності даних співробітників та клієнтів і в подальшому – кращої та надійнішої роботи компанії.

Середовищем розробки було обрано Microsoft Visual Studio. Це швидке і просте забезпечення для різних платформ (Windows, Mac OS, Linux), що дозволяє розробляти веб-додатки, додатки для хмарних сервісів, мобільних та десктопних платформ. Visual Studio підтримує розробку мовою програмування C#. Це одна з найпопулярніших мов програмування, якій легко навчитися та просто

використовувати. Надає чітку структуру програмам і дозволяє повторно використовувати код.

Для реалізації програми використовувався метод шифрування Цезар - простий тип шифру, де кожна буква звичайного тексту замінюється буквою з фіксованою кількістю позицій вниз по алфавіту.

Було досліджено внутрішню систему доступу працівників та покращено системи та умови захисту інформації, розроблено додатковий засіб для шифрування цінної інформації. Отже, ціль та завдання курсової роботи було виконано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 1.3 Класифікація загроз електронної пошти. [Електронний ресурс] // - Режим доступу: https://radio.bobrodobro.ru/17044
2. Моделі порушників інформаційної безпеки на об’єкті. Форми злочинного посягання на інформаційну безпеку. [Електронний ресурс] // - Режим доступу: https://studopedia.org/11-88311.html
3. Апаратне шифрування. [Електронний ресурс] // - Режим доступу: https://ru.wikipedia.org/wiki/Аппаратное_шифрование
4. Avanpost FAM. [Електронний ресурс] // - Режим доступу: https://avanpost.ru/products/avanpost-fam/
5. Короткий огляд мови C# [Електронний ресурс] // - Режим доступу: https://docs.microsoft.com/ru-ru/dotnet/csharp/tour-of-csharp/

ДОДАТКИ

Додаток А

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;


namespace Encryption { }

public class CaesarCipher
{
    //символи української абетки
    const string alfabet = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ";

    private string CodeEncode(string text, int k)
    {
        //додаємо в алфавіт маленькі літери
        var fullAlfabet = alfabet + alfabet.ToLower();
        var letterQty = fullAlfabet.Length;
        var retVal = "";
        for (int i = 0; i < text.Length; i++)
        {
            var c = text[i];
            var index = fullAlfabet.IndexOf(c);
            if (index < 0)
            {
                //якщо символ не знайдений, то додаємо його в незмінному вигляді
                retVal += c.ToString();
            }
            else
            {
                var codeIndex = (letterQty + index + k) % letterQty;
                retVal += fullAlfabet[codeIndex];
            }
        }

        return retVal;
    }

    //шифрування тексту
    public string Encrypt(string plainMessage, int key)
        => CodeEncode(plainMessage, key);

    //дешифрування тексту
    public string Decrypt(string encryptedMessage, int key)
        => CodeEncode(encryptedMessage, -key);
}

class Program
{
    static void Main(string[] args)
    {
        Console.OutputEncoding = System.Text.Encoding.Unicode;
        Console.InputEncoding = System.Text.Encoding.Unicode;

        var cipher = new CaesarCipher();
        Console.Write("Введіть текст: ");
```

```
        var message = Console.ReadLine();
        Console.Write("Введіть ключ: ");
        var secretKey = Convert.ToInt32(Console.ReadLine());
        var encryptedText = cipher.Encrypt(message, secretKey);
        Console.WriteLine("Зашифроване повідомлення: {0}", encryptedText);
        Console.WriteLine("Розшифроване повідомлення: {0}", cipher.Decrypt(encryptedText,
secretKey));
        Console.ReadLine();
    }
}
```