Хмельницький національний університет
Факультет програмування та комп'ютерних
і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система захисту об'єкту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз
Назва теми

КвРКБ.170144.17.01.05. ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *Кібербезпека*

Виконала студентка IV курсу, група КБ-17-1 _____ О.О Зацепіна
Підпис Ініціали, прізвище

Керівник _____ В.Ю. Тітова
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки,
та комп'ютерних систем
і мереж _____ Ю.П. Кльоц
Підпис, дата Ініціали, прізвище

7 червня 2021 р.

Хмельницький, 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра кібербезпеки та комп'ютерних систем та мереж
Освітній рівень *бакалавр*
Галузь знань *12 «Інформаційні технології»*
Спеціальність *125 «Кібербезпека»*
Освітня програма *освітньо-професійна програма підготовки бакалавра*

ЗАТВЕРДЖУЮ:
Завідувач кафедри _____
_____
5.01 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Зацепіні Ориславі Олександрівні
Прізвище, ім'я, по батькові студента

1 Тема роботи «Система захисту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз»
Керівник роботи Тітова Віра Юріївна, к.т.н, доцент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від ___ ____ 2021р. № ___
2 Строк подання студентом роботи на кафедру: _____
3 Вихідні дані до роботи системи захисту інформації ,методи забезпечення інформаційної безпеки ,методика оцінювання ризиків, види внутрішніх загроз

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз об'єкта захисту, обгрунтування вибору засобів для побудови системи захисту, проектування системи захисту, реалізація роботи

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
«Класифікація загроз», «Схема відеостеження», «Алгоритм шифрування AES»

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийня
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ		
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ		

7 Дата видачі завдання 5 лютого 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Пр
1	Вибір та затвердження теми кваліфікаційної роботи.	Січень	
2	Аналіз об'єкта захисту.	Січень–лютий	
3	Проектування та розробка загальної архітектури і структури системи захисту.	Лютий–березень	
4	Програмна реалізація запропонованого рішення та тестування системи; аналіз результатів і оцінювання прийнятих рішень.	Квітень	
5	Написання тексту пояснювальної записки та розробка графічних матеріалів.	Травень	
6	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника.		
7	Оформлення кваліфікаційної роботи як документа відповідно до вимог.		
8	Отримання супровідних документів. Нормоконтроль.	Червень	
9	Підготовка до захисту та захист кваліфікаційної роботи.		

Студент

Керівник роботи

Підпис Іщенко О.О.
Ініціали, прізвище

Підпис Ігнатов В.Г.
Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз.

Автор роботи: Зацепіна Орислава Олександрівна.

Керівник роботи: Тітова Віра Юріївна.

Обсяг – 59 с., 13 рис., 3 додатки, 18 джерел.

Графічна частина: 8 презентаційних слайдів, 3 плакати.

ЗАГРОЗИ, ВНУТРІШНІ ЗАГРОЗИ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, ФІЗИЧНИЙ ЗАХИСТ, РИЗИКИ, СИСТЕМИ ЗАХИСТУ.

Метою роботи є проєкування та реалізація системи захисту інформації від внутрішніх загроз, оцінка ризиків інформаційної безпеки, криптографічний та фізичний захист.

У цій роботі були проаналізовані усі можливі методи та засоби захисту інформаційних ресурсів підприємства. Також були досліджені найпоширеніші проблеми інформаційної безпеки та запропоновані можливі шляхи їх подолання.

В ході кваліфікаційної роботи була розроблена система захисту інформації ТОВ «ХмельницькІнфоком» від внутрішніх загроз.

Підпис студента: _____

Дата: 05.06.21р.

Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
	1		Завдання на дипломний	1	
			проект		
	2		Анотація	1	
	3	КвРКБ.170144.17.01.05 ПЗ	Система захисту	1	
			Інформаційної діяльності		
			ТОВ «ХмельницькІнфоком»		
			від внутрішніх загроз		
			Пояснювальна записка		
	4	КвРКБ.170144.17.01.05 Е8	Класифікція загроз	1	
			Схема структурна		
	5	КвРКБ.170144.17.01.05 Е8	Алгоритм шифрування AES	1	
			Алгоритм роботи		
	6	КвРКБ.170144.17.01.05 Е8	Система відеоспостереження	1	
			Схема структурна		

КвРКБ.170144.17.01.05 ВП

Арк.	№ Докум.	Підп.	Дата
робив	Зацепіна О.О.		06.06.20 р.
рев.	Тітова В.Ю.		
контр.	Муляр І.В.		
в.	Кльоц Ю.Й.		

Система захисту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз
Відомість проекту

Літера	Аркуш	Аркушів
в	1	1

ХНУ, КБ-17-1

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – база даних

ЕОМ – електронно-обчислювальна машина

ІБ –інформаційна безпека

ІС – інформаційна система

ІТ – інформаційні технології

IoT – інтернет речей

КС – комп’ютерна система

НСД – несанкціонований доступ

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

AES – Advanced Encryption Standard

DES – Data Encryption Standard

DLP – Data Leak Prevention

RSA – Rivest, Shamir и Adleman

ВСТУП

У XXI столітті важко уявити будь-яку сферу життя без використання інформаційних технологій. Щодня ми використовуємо різні гаджети та пристрої і більшість з нас навіть не уявляє, який величезний потік даних циркулює навколо нас. З кожним днем додатки та соціальні мережі поповнюють свої бази нашими даними, тому і з'явилася необхідність у захисті важливої інформації, наприклад, такої як персональна.

Але варто зазначити, що на сьогоднішній день інформація стала дуже цінним продуктом, який часто хочуть отримати незаконним способом. Гостро питання інформаційної безпеки стоїть на підприємствах та установах, і неважливо чи це мала фірма, чи велика корпорація. Керівництво з відповідальністю має ставитись до питання захисту інформації, адже від стану захищеності буде залежати подальша доля компанії.

Для того щоб якісно захистити інформацію, потрібно створити цілу систему, тому що загрози мають різну природу і важливо враховувати всі потенційні атаки.

Як вже зазначалось, загрози можуть бути різними від простої неуважності працівника, де наслідками, наприклад, буде часткова втрата інформації, до цілеспрямованої атаки зловмисника, яка крім матеріальних втрат може призвести і взагалі до припинення існування компанії.

Отже, тема кваліфікаційної роботи бакалавра є дійсно дуже актуальною, тому що небезпека для інформації є не лише ззовні, а й всередині компанії і ніхто не знає напевно де і коли чекати на загрози, проте за допомогою системи захисту можна максимально убезпечити своє підприємство.

Метою даної кваліфікаційної роботи являється закріплення, систематизація, узагальнення та підтвердження знань набутих в процесі навчання за спеціальністю «Кібербезпека», набуття практичних навичок проєктування, моделювання та дослідження інформаційних управляючих систем за допомогою сучасних програмних засобів та технологій.

Завданнями кваліфікаційної роботи є:

- узагальнення, закріплення, застосування теоретичних та практичних навиків з вивчених дисциплін;
- вдосконалення навиків у користуванні сучасними засобами та системами програмування, вирішені інженерних задач, проєктуванн захищених інформаційних систем, а також їх елементів за допомогою використовування сучасних методологій та інформаційніих технологій;
- використовування знань в комп'ютерному моделюванні, а також вміння обробляти та систематизувати результати досліджень, за допомогою відповідних інструментальних засобів.

Структура кваліфікаційної роботи складається зі вступу, основної частини, висновків, списку використаної літератури, а також додатків.

1 АНАЛІЗ ОБ'ЄКТА ЗАХИСТУ

1.1 Характеристика предметної області

Щороку кількість кіберзлочинів та атак в світі збільшується з величезною швидкістю. За останні кілька років в Україні кількість навмисних втручань у роботу інформаційних систем більшості державних та комерційних установ різко зросла. В більшості випадків, після хакерських атак, робота компаній може блокуватися від кількох годин до пари десятків днів, а це носить негативний вплив та значні фінансові витрати.

Сучаснв інформаційні технології (IT) постійно змінюють як робочі процеси компаній, так і повсякденне життя звичайних людей. Кожна компанія має в своїх володіннях котфіденційну інформацію. Бувають випадки, коли вартість такої секретної інформації в кілька сотень раз перевищує мережеву вартість усієї інфраструктури підприємства. Витік конфіденційних даних, частіше за все, може призвести до значних фінансових втрат, а особливо коли йде мова про розробки нових технологій чи продуктів. Сьогодні інформація стала цінним товаром, який можна купити, продати чи обміняти.

Окрім витоку конфіденційний даних існують й інші типи інформаційних загроз, які призначені для часткової/повної зупинки робочих процесів на підприємстві, блокування доступу до важливих зовнішніх чи внутрішніх інформаційних ресурсів, зменшення рівня продуктивності мережевої інфраструктури або ж її повної зупинку, фізичного пошкодження окремих елементів технічного обладнання.

Інформаційна безпека - це захищеність мережевої інфраструктури і інформаційних систем від випадкового або навмисного втручання (внутрішнього або зовнішнього), крадіжки інформації та / або блокування робочих процесів, що завдають шкоди власникам і користувачам інформації [1].

Сучасні інформаційні системи складаються з великої кількості елементів і вузлів різного ступеня автономності. Оскільки усі елементи з'єднані між собою та обмінюються даними, то на кожен елемент по- різному може впливати зовнішня загроза або несправність.

Усі елементи сучасноих інформаційних систем можна поділяють на чотири групи:

- апаратні;
- програмне забезпечення (ПЗ);
- дані ;
- персонал.

Для компанії дуже важливо створювати резервні копії важливої інформації та копіювати фрагменти системного диска, коли персональні комп'ютери та сервери працюють нормально. Комбінування цих методів надають змогу відновити роботу в найкоротші терміни.

Введення обмеження прав доступу до зміни системної інформації, регулярне оновлення та контроль систем, а також своєчасний збір і аналіз інформаційної діяльності впродовж роботи користувача запобігатимуть випадковим помилкам в ІС. Правильні дії в напрямку забезпечення ІБ напряму залежать від кваліфікації адміністратора ІС.

Останнім часом комп'ютерні віруси найчастіше потрапляють в систему через електронні листи та заражені носії даних.

На сьогодні антивірусний захист не може обмежуватись просто встановленням антивірусних програм. Тому зараз використовують комплексні програми захисту від вірусів, які допомагають захистити файли та обладнання від шкідливих програм, таких як хробаки, троянські коні та шпигунські програми, а також можуть запропонувати додатковий захист, такий як налаштовувані брандмауери та блокування веб-сайтів.

Антивірусні програми та програмне забезпечення захисту комп'ютера призначені для оцінки таких даних, як веб-сторінки, файли, програмне

забезпечення та додатки, щоб допомогти якнайшвидше знайти та викорінити шкідливе програмне забезпечення.

Більшість із них забезпечують захист у режимі реального часу, який може захистити пристрої від вхідних загроз; потрібно регулярно перевіряти ПК на наявність відомих загроз .

Оскільки зараз багато операцій ведеться в Інтернеті, і постійно з’являються нові загрози, важливіше, ніж будь-коли, встановити захисну антивірусну програму. На щастя, сьогодні на ринку є ряд чудових товарів, з яких можна вибрати.

Антивірусне програмне забезпечення починає працювати, перевіряючи комп'ютерні програми та файли на базу даних відомих типів шкідливих програм. Оскільки хакери постійно створюють і розповсюджують нові віруси, він також буде перевіряти комп’ютери на наявність нових або невідомих типів шкідливих програм.

Як правило, більшість програм використовуватимуть три різні пристрої виявлення: специфічне виявлення, яке ідентифікує відоме шкідливе програмне забезпечення; загальне виявлення, яке шукає відомі частини або типи шкідливого програмного забезпечення або шаблони, пов’язані загальною кодовою базою; та евристичне виявлення, яке сканує невідомі віруси, виявляючи відомі підозрілі файлові структури. Коли програма знаходить файл, що містить вірус, вона, як правило, поміщає його на карантин та / або позначає для видалення, роблячи його недоступним та усуваючи ризик для вашого пристрою.

1.2 Аналіз відомих методів забезпечення захисту інформації

На сьогоднішній день існує величезне різноманіття методів захисту інформаційних ресурсів. Найкращим з яких засобів є комплекс, який дозволяє

повністю захистити інформацію, тобто фізично, апаратно, інженерно-технічно та програмно.

Технічний захист відноситься до ряду методів, що використовуються для автентифікації та захисту від крадіжки конфіденційних даних та інформації, як правило, в організаціях. Він автентифікує логін та дані користувачів таким чином, що лише перевірені користувацькі програми можуть читати та отримувати доступ до даних та програм. Технічна безпека має ряд компонентів, серед яких:

- Кібербезпека та розслідування
- Архітектура безпеки для програмних додатків
- Стратегія IT-безпеки
- Управління автентифікацією мережі
- Спеціалізовані інженерні рішення для організаційної безпеки

Організація зазвичай може адаптувати тип послуг, необхідних відповідно до потреб ресурсів.

Технічний захист – це дуже поширений тип захисту, який використовується в організаціях, що використовують комп'ютери чи майже будь-який тип технології. Він займається виявленням лазів у системі безпеки та пошуком адекватних рішень для усунення ризику технічної несправності або злому [2].

Оскільки більшість даних існує у нефізичній формі, з перенесенням даних на хмарні диски та портативні пристрої важко забезпечити безпечний сеанс та передачу інформації. У ненадійних мережах і пристроях, а також у взаємодії з несанкціонованими системами відсутні засоби контролю.

Фізичний захист – це захист людей, майна та матеріального майна від дій та подій, які можуть спричинити шкоду чи збитки [3]. Незважаючи на те, що часто не помічають на користь кібербезпеки, фізична безпека є однаково важливою. Усі брандмауери у світі не можуть вам допомогти, якщо зловмисник вилучить ваш носій інформації з камери зберігання.

По суті, фізична безпека полягає у захисті своїх об’єктів, людей та активів від реальних загроз. Він включає фізичне стримування, виявлення зловмисників та реагування на ці загрози.

Незважаючи на те, що це може відбуватися внаслідок екологічних подій, цей термін, як правило, застосовується для утримання людей - незалежно від того, чи є зовнішні актори чи потенційні загрози внутрішньої інформації - доступу до територій або активів, яким вони не повинні. Це може бути заборона загальної публіки у вашому штабі, третіх осіб на місцях із районів, де триває делікатна робота, або ваших працівників із критично важливих місць, таких як серверна кімната.

Фізичні атаки можуть потрапити у захищений центр обробки даних, пробратися в обмежені райони будівлі або скористатися терміналами, до яких вони не мають доступу. Зловмисники можуть викрасти або пошкодити важливі IT-активи, такі як сервери або носії інформації, отримати доступ до важливих терміналів для критично важливих додатків, викрасти інформацію через USB або завантажити шкідливе програмне забезпечення у ваші системи.

Ретельний контроль на зовнішньому периметрі повинен мати можливість захищати від зовнішніх загроз, тоді як внутрішні заходи щодо доступу повинні зменшувати ймовірність внутрішніх зловмисників (або, принаймні, позначати незвичну поведінку).

За допомогою програмних засобів захисту та мережевих вразливостей, на які постійно націлюються хакери, захист апаратних компонентів набуває все більшої важливості, оскільки він стає більш безпечним, а кіберзлочинцям буде важко змінити фізичний рівень для своїх цілей.

Будь-який компроміс із цілісністю, автентифікацією та доступністю робить програмне забезпечення небезпечним. Програмні системи можуть бути атаковані з метою викрадення інформації, моніторингу вмісту, появи вразливих місць та пошкодження поведінки програмного забезпечення.

Шкідливе програмне забезпечення може спричинити DoS (відмова в обслуговуванні) або вивести з ладу саму систему.

Переповнення буфера, переповнення стека, введення команд та ін'єкції SQL - найпоширеніші атаки на програмне забезпечення.

Атаки переповнення буфера та стека перезаписують вміст купи або стека відповідно, записуючи зайві байти.

Введення команд можна здійснити за допомогою програмного коду, коли переважно використовуються системні команди. Шкідлива атака додає нові системні команди до існуючих команд. Іноді системна команда може зупинити служби і спричинити DoS.

Ін'єкції SQL використовують шкідливий код SQL для отримання або модифікації важливої інформації із серверів баз даних. Ін'єкції SQL можна використовувати для обходу облікових даних для входу. Іноді ін'єкції SQL отримують важливу інформацію з бази даних або видаляють усі важливі дані з бази даних.

Єдиний спосіб уникнути подібних атак - це практикувати хороші техніки програмування. Безпека на рівні системи може бути забезпечена за допомогою кращих брандмауерів. Використання виявлення та запобігання вторгненню також може допомогти зупинити зловмисників від легкого доступу до системи.

Криптографічний захист – це тактика інформаційної безпеки, яка використовується для захисту корпоративної інформації та комунікацій від кіберзагроз за допомогою кодів [4]. Ця практика стосується захищених інформаційних та комунікаційних методів, отриманих із математичних концепцій, та набору розрахунків, заснованих на правилах, які називаються алгоритмами, для перетворення повідомлень способами, які важко розшифрувати.

Потім ці алгоритми використовуються для генерації криптографічного ключа, цифрового підписання, перевірки для захисту конфіденційності даних,

перегляду веб-сторінок в Інтернеті та конфіденційного спілкування, таких як операції з кредитними картками та електронні листи.

Криптографія досягає кількох цілей, пов'язаних з інформаційною безпекою, включаючи конфіденційність, цілісність та автентифікацію та відмову від використання.

Криптографія також підтримує доступність даних, гарантуючи, що особи, які мають відповідний дозвіл, можуть використовувати системи та отримувати дані надійно та своєчасно. Це гарантує надійність та доступність інформаційних систем.

Стеганографія – це практика приховування секретного повідомлення всередині (або навіть поверх нього) чогось, що не є секретним [5]. Що щось може бути майже про все, що ти хочеш. У наші дні багато прикладів стеганографії передбачають вбудовування секретного фрагмента тексту всередину картинки. Або приховування секретного повідомлення чи сценарію всередині документа Word або Excel.

Мета стеганографії – приховування та обман. Це форма прихованого спілкування і може передбачати використання будь-якого засобу для приховування повідомлень. Це не форма криптографії, оскільки вона не передбачає скремблювання даних або використання ключа. Натомість це форма приховування даних і може бути виконана розумними способами. Якщо криптографія – це наука, яка значною мірою забезпечує конфіденційність, стеганографія – це практика, яка забезпечує секретність і обман.

1.3 Аналіз наявних проблем досліджуваної області

Наразі інформаційна безпека не може бути більш актуальною, і інформація (часто зберігається на декількох пристроях) зараз така ж цінна для злочинців, як і наше фізичне майно. Це означає, що таким же чином ви

встановлюєте сигналізацію про вторгнення та інвестуєте в страхування житла, вживаючи захисних заходів щодо вашої інформації та даних, має бути пріоритетом для всіх.

Зараз технологія справді є найкращим другом людини. Ми так сильно покладаємося на це для зберігання та передачі даних одним натисканням кнопки, і значна частина цієї інформації може бути дуже цінною, якщо вона потрапить у чужі руки. Наша довіра до технології означає, що вона створила нову породу злочинців - тих, хто готовий скористатися будь-якими уразливими місцями інформаційної безпеки, які вони можуть знайти, щоб отримати несанкціонований доступ до даних. Вони можуть націлюватись як на окремих людей, так і на цілі організації залежно від їхньої кваліфікації та рівня прихильності. Відносна легкість вчинення кіберзлочинів (наприклад, легко надіслати десятки тисяч фішингуелектронна пошта за секунду), і величезна кількість інформації, що зберігається на комп'ютерах, означає, що цифрова інформаційна безпека є, мабуть, найбільш загроженою; факт, який означає, що кроки, які ми робимо для захисту себе, повинні бути вдосконалені.

Щодня відбувається приблизно 4000 атак шкідливого програмного забезпечення, багато з яких є вимогами, де злочинці блокують / шифрують пристрій користувача та вимагають платежу, щоб скасувати їх дії. У поєднанні з тим, що щодня розробляється 230 000 нових форм шкідливих програм, заривання голови в пісок точно не допоможе зменшити ризики.

Важливо пам'ятати, що жодна організація не застрахована від порушень інформаційної безпеки. Багато бізнес-важкоатлетів зазнали жертв кіберзлочинів. Наприклад, Ebay, гіганта інтернет-аукціону, було зламано в 2014 році, в результаті зловмисники отримали дані про 145 мільйонів користувачів. Зловмисники змогли потрапити в мережу, використовуючи повноваження трьох співробітників корпорації. Ця точка входу надала їм

доступ до всього, врешті-решт оголивши бази даних інформацією про клієнтів.

Імена, адреси та паролі були порушені, хоча, на щастя, дані кредитної картки користувачів зберігалися деінде. В той же час, компанія зазнала критики через кількість часу, який їм знадобився для зв'язку з користувачами щодо порушення та запрошення їх змінити свої паролі. Це рішення мало бути застосовано набагато швидше, ніж було раніше, і поставити дані людей на непотрібний ризик - особливо тих, хто повторно використовує паролі на інших платформах та службах. В результаті скандалу активність користувачів на eBay зменшилася, підкресливши, що навіть найуспішніші імена домогосподарств можуть бути заплямовані порушеннями інформаційної безпеки.

Зловмисники можуть використовувати електронні листи для надсилання шкідливого програмного забезпечення, наприклад, у зловмисних вкладеннях, або спонукаючи одержувачів натискати гіперпосилання, які дійсно починають процес завантаження. Завантажуючи невідомі вкладення або натискаючи такі посилання, користувачі ненавмисно можуть завантажувати шкідливе програмне забезпечення, яке може заразити всю мережу організації. Вони також можуть завантажити засіб, за допомогою якого хакери можуть мати постійні точки входу на сервери компанії, бази даних тощо. Вони можуть залишатися невидимими і не виявленими протягом місяців і років.

Фішинг-листи - це ще один спосіб, яким злочинці можуть знайти спосіб отримати доступ до конфіденційної інформації електронною поштою. Представляючи себе законним джерелом, таким як ваш банк, злочинці запитують інформацію за допомогою автентичних, фірмових електронних листів та підроблених веб-сайтів. Потрібно лише одному тисячі одержувачів впасти на шахрайство, щоб зробити його вартим хакерського часу. Отримавши інформацію про вхід або дані облікового запису,

кіберзлочинці можуть отримати доступ до вашого реального облікового запису або продати інформацію.

Наша любов до соціальних мереж – це те, що не скоро зникне найближчим часом. У середньому людина витрачає до двох годин на день, перевіряючи та обмінюючись інформацією на платформах. Проблема в цьому полягає в кількості інформації, якою ми готові ділитися, і все тому, що ми розглядаємо її як неформальний, веселий простір, а не як місце, яке може опинитися під загрозою з боку злочинців. На жаль, саме таке ставлення означає, що саме туди злітаються хакери, коли шукають нову жертву.

Кіберзлочинці можуть використовувати соціальні медіа для створення підроблених профілів та спілкування з багатьма людьми в надії потрапити до їх списку друзів. Подібно до електронних листів, лише одному користувачеві потрібно прийняти запит, щоб кіберзлочинцям стало набагато простіше зв’язуватися зі своїми зв’язками більш законно, як у «друзі друга».

Хакери іноді можуть використовувати вразливості програм, щоб вставити шкідливий код. Часто вразливість виявляється в полі введення тексту для користувачів, наприклад, для імені користувача, куди вводиться оператор SQL, який працює в базі даних, у так званій атаці ін'єкції SQL. Інші види атак введення коду включають введення оболонки, атаки команд операційної системи, введення скриптів та атаки динамічної оцінки.

Атаки цього типу можуть призвести до викрадених облікових даних, знищення даних або навіть втрати контролю над сервером. Вони також є напрочуд поширеними, оскільки Фонд OWASP (Відкритий проект безпеки веб-додатків) займає перше місце серед перших 10 ризиків безпеки додатків .

Існує два способи запобігти введенню коду: уникати вразливого коду та фільтрувати введення. Додатки можуть захищатись від вразливого коду, зберігаючи дані окремо від команд та запитів, наприклад, використовуючи безпечний API з параметризованими запитами. Компанії також повинні використовувати перевірку вхідних даних і дотримуватися принципу

найменших привілеїв, застосовуючи елементи керування, такі як функція SQL LIMIT, щоб зменшити шкоду від успішної атаки.

Вартість даних порушень добре задокументовані. Вони часто спричинені скомпрометованими обліковими даними , але цілий ряд інших поширених причин включає неправильну конфігурацію програмного забезпечення, втрату обладнання або шкідливе програмне забезпечення.

Запобігання порушенням даних вимагає низки передових практик. Трафік сайту та транзакції повинні бути зашифровані за допомогою SSL , дозволи повинні бути ретельно встановлені для кожної групи користувачів, а сервери повинні бути перевірені. Співробітників слід навчити, як уникнути фішингових атак , і як правильно дотримуватися гігієни паролів. Тут також варто зауважити принцип найменшої привілеї.

Більшість підприємств усвідомлюють на певному рівні загрозу безпеці, яку створює шкідливе програмне забезпечення, проте багато людей не знають, що електронна пошта все ще є головним вектором шкідливих атак.

Оскільки зловмисне програмне забезпечення походить з різних джерел, для запобігання зараженню потрібно кілька різних інструментів. Необхідна надійна система сканування та фільтрації електронної пошти, а також сканування зловмисного програмного забезпечення та вразливості. Як і порушення, які часто спричинені зараженням шкідливим програмним забезпеченням, освіта працівників життєво необхідна для захисту підприємств від шкідливих програм.

Будь-який пристрій або система, інфіковані шкідливим програмним забезпеченням, повинні бути ретельно очищені, що означає виявлення прихованих частин коду та видалення всіх заражених файлів перед їх реплікацією. Це практично неможливо вручну, тому потрібен ефективний автоматизований інструмент.

Частиною виклику для кібербезпеки бізнесу є підтримка та використання повного набору інструментів, необхідних для того, щоб не

відставати від мінливого ландшафту загроз. По мірі розвитку бот-мереж IoT, зловмисного програмного забезпечення та інших нових загроз організаціям стає все нереальніше не відставати самостійно. Однак підготовка залишається критично важливою для збереження ділових операцій та продуктивності.

2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ДЛЯ ПОБУДОВИ СИСТЕМИ

2.1 Загальні методи захисту інформації

Оскільки комп’ютери стають все більш зрозумілими, кожен день приносить нові програми. Багато з цих нових додатків передбачають як зберігання інформації, так і одночасне використання кількома особами. Ключовою проблемою у цій роботі є багаторазове використання. Для тих додатків, в яких усі користувачі не повинні мати однакових повноважень, потрібна певна схема, яка гарантує, що комп’ютерна система реалізує бажану структуру повноважень.

Фахівці з питань інформаційної безпеки вважають за корисне розподілити потенційні порушення безпеки у три категорії.

1. Несанкціоноване оприлюднення інформації: несанкціонована особа може прочитати та скористатися інформацією, що зберігається в комп’ютері. Ця категорія занепокоєння іноді поширюється на «аналіз трафіку», коли зловмисник дотримується лише закономірностей використання інформації, і з цих моделей можна зробити висновок про деякий інформаційний зміст. Він також включає несанкціоноване використання власної програми.
2. Несанкціонована модифікація інформації: несанкціонована особа може вносити зміни до збереженої інформації - форма саботажу. Зверніть увагу, що такого роду порушення не вимагає, щоб зловмисник бачив інформацію, яку він змінив.
3. Несанкціонована відмова у використанні: зловмисник може перешкодити уповноваженому користувачеві посилатися на інформацію або змінювати її, навіть якщо зловмисник може не мати змоги посилатися на неї або модифікувати її. Причини відмови

системи, порушення алгоритму планування або стрільба кулею в комп'ютер - приклади відмови у використанні. Це ще одна форма саботажу.

Прикладами методів безпеки, які іноді застосовуються до комп'ютерних систем, є такі:

- маркування файлів зі списками авторизованих користувачів;
- перевірка особистості потенційного користувача, вимагаючи пароль;
- екранування комп'ютера для запобігання перехоплення і подальшої інтерпретації електромагнітного випромінювання;
- шифрування інформації, що надсилається по телефонних лініях;
- замикання кімнати з комп'ютером;
- контроль, кому дозволено вносити зміни в комп'ютерну систему (як її апаратне, так і програмне забезпечення);
- використання надлишкових схем або запрограмованих перехресних перевірок, які підтримують безпеку внаслідок відмов апаратного або програмного забезпечення;
- підтвердження того, що апаратне та програмне забезпечення насправді реалізовано за призначенням.

2.2 Криптографічний захист

Криптографія забезпечує безпечне спілкування у присутності зловмисних третіх сторін, відомих як супротивники. Шифрування використовує алгоритм і ключ для перетворення вхідних даних (тобто відкритого тексту) у зашифрований вихід (тобто зашифрованого тексту) [8]. Заданий алгоритм завжди перетворює один і той же відкритий текст в один і той же зашифрований текст, якщо використовується той самий ключ.

Алгоритми вважаються безпечними, якщо зловмисник не може визначити будь-які властивості відкритого тексту або ключа, враховуючи зашифрований текст. Зловмисник не повинен мати змоги визначити що-небудь про ключ, враховуючи велику кількість комбінацій відкритого/зашифрованого тексту, в яких використовувався ключ.

При симетричному шифруванні один і той же ключ використовується як для шифрування, так і для дешифрування. Відправник і одержувач вже повинні мати спільний ключ, який відомий обом. Розподіл ключів є складною проблемою і послужив поштовхом для розвитку асиметричної криптографії.

При асиметричній криптографії для шифрування та дешифрування використовуються два різні ключі. Кожен користувач асиметричної криптосистеми має як відкритий, так і приватний ключ. Приватний ключ постійно тримається в таємниці, але відкритий ключ може вільно розповсюджуватися.

Дані, зашифровані за допомогою відкритого ключа, можуть дешифруватися лише за допомогою відповідного приватного ключа.

Як правило, симетричні алгоритми дуже швидкі і ідеально підходять для шифрування великих обсягів даних (наприклад, цілого розділу диска або бази даних). Асиметричний набагато повільніший і може шифрувати лише фрагменти даних, менші за розмір ключа (зазвичай 2048 біт або менше). Таким чином, асиметрична криптографія зазвичай використовується для шифрування симетричних ключів шифрування, які потім використовуються для шифрування набагато більших блоків даних. В цифрових підписів асиметрична криптографія зазвичай використовується для шифрування хеш-повідомлень, а не цілих повідомлень.

Криптосистема забезпечує управління криптографічними ключами, включаючи генерацію, обмін, зберігання, використання, відкликання та заміну ключів.

Безпечна система повинна забезпечувати декілька гарантій, таких як конфіденційність, цілісність та доступність даних, а також достовірність та невідмова. При правильному використанні криптографія допомагає надати ці запевнення. Криптографія може забезпечити конфіденційність та цілісність як даних, що передаються, так і даних у стані спокою. Він також може автентифікувати відправників та одержувачів один одного та захищати від відмови.

Програмні системи часто мають декілька кінцевих точок, як правило, декілька клієнтів та один або кілька внутрішніх серверів. Зв'язок між клієнтом та сервером відбувається через мережі, яким не можна довіряти. Зв'язок відбувається через відкриті, загальнодоступні мережі, такі як Інтернет, або приватні мережі, які можуть бути скомпрометовані зовнішніми зловмисниками або зловмисними інсайдерами.

Він може захистити комунікації, які перетинають ненадійні мережі. Існує два основних типи атак, які противник може спробувати здійснити в мережі. Пасивні атаки включають зловмисника, який просто слухає сегмент мережі і намагається прочитати конфіденційну інформацію під час подорожі. Пасивні атаки можуть бути онлайн (в яких зловмисник зчитує трафік у режимі реального часу) або офлайн (коли зловмисник просто фіксує трафік у режимі реального часу і переглядає його пізніше - можливо, витративши деякий час на його дешифрування). Активні атаки включають в себе зловмисника, який видає себе за клієнта або сервер, перехоплює комунікації в дорозі та переглядає та / або модифікує вміст перед тим, як передати його за призначенням (або повністю скинути).

Захист конфіденційності та цілісності, пропонований криптографічними протоколами, такими як SSL / TLS, може захистити комунікації від зловмисного прослуховування та втручання. Захист автентичності забезпечує впевненість у тому, що користувачі фактично спілкуються із системами за

призначенням. Наприклад, ви надсилаєте свій банківський пароль через Інтернет своєму банку чи комусь іншому?

Також його можна використовувати для захисту даних у стані спокою. Дані на знімному диску або в базі даних можуть бути зашифровані, щоб запобігти розголошенню конфіденційних даних у разі втрати чи викрадення фізичного носія. Крім того, він також може забезпечити захист цілісності даних у стані спокою для виявлення зловмисних фальсифікацій.

Єдине, що повинно бути «таємним», коли мова заходить про захищену криптосистему – самі ключі. Обов'язково повинні бути відповідних заходів для захисту будь-яких клавіш, якими користуються системи. Не можна зберігати ключі шифрування у чистому тексті разом із даними, які вони захищають. Це схоже на замикання вхідних дверей і підкладання ключа під килимок. Це перше місце, куди погляне зловмисник. Ось три найпоширеніші методи захисту ключів (від найменш захищеного до найбільш захищеного):

Зберігати ключі у файловій системі та захищайте їх за допомогою надійних списків контролю доступу (ACL) [9].

Шифрувати ключі шифруванням даних (DEK) за допомогою другого ключа шифрування ключа (KEK). KEK слід генерувати за допомогою шифрування на основі пароля (PBE). Пароль, відомий мінімальній кількості адміністраторів, може бути використаний для створення ключа за допомогою такого алгоритму, як bcrypt, scrypt або PBKDF2, і використовуваний для завантаження криптосистеми. Це позбавляє від необхідності зберігати незашифрований ключ у будь-якому місці.

Апаратний модуль безпеки (HSM) - це апаратний пристрій, захищений від втручання, який можна використовувати для надійного зберігання ключів. Код може здійснювати виклики API до HSM, щоб надавати ключі, коли це потрібно, або виконувати дешифрування даних на самому HSM [10].

Розширений стандарт шифрування (AES) (із 128, 192 або 256-бітними ключами) є стандартом симетричного шифрування. RSA та криптографія з

еліптичною кривою (ECC) із принаймні 2048-бітовими ключами є стандартом для асиметричного шифрування.

2.3 Відеоспостереження

Встановлення камер відеоспостереження допомагає не тільки запобігти злочинам завдяки візуальному контролю, але й звинуватити злочинців, використовуючи інформацію, записану відеокамерою.

Система відеоспостереження, встановлена на підприємствах або на складах, неодноразово доводила свою ефективність та окупність завдяки значному зменшенню ризиків.

Встановлення системи відео спостереження дає ряд функцій:

- контролювати кожен етап виробничого процесу;
- запобігати відмові якості, порушенню умов праці, правил техніки безпеки;
- мати повні та зафіксовані дані про виробничі аварії;
- запобігати крадіжкам та пошкодженню товарів та виробів, а також виробничого обладнання.

Система відеоспостереження безпеки призначена для захисту безпеки і включає: кілька відеокамер, пристрої обробки відеосигналів, пристрої відображення відеоінформації (монітори), обладнання для запису та зберігання відеоінформації [12].

Система відеоспостереження всередині приміщень та прилеглих територіях побудована на базі віддалених чутливих відеокамер. Камери можуть встановлюватися всередині або зовні.

Система безпеки відеоспостереження забезпечує:

1. Контроль за приміщеннями та територіями вдень та вночі з боку моніторів.
2. Опція запису за допомогою датчиків руху.

Системи відеоспостереження вже давно вийшли за рамки функцій безпеки. Сучасні системи забезпечують інтелектуальний аналіз отриманого відеопотоку.

За допомогою сучасної системи відеоаналітики можна значно розширити функціональність системи та зменшити кількість залученого персоналу. Оператору більше не потрібно постійно спостерігати за багатьма моніторами. Злочини виявляються на основі обробки подій за допомогою аналітичних програм, а також сигналів від різних детекторів. Оператор отримує сигнал про можливу небажану подію або подію, яка вже сталася.

Існує величезна кількість різноманітних камер, які можна використовувати для систем відеоспостереження. Однак усі камери поділяються на аналогові або IP / цифрові:

Аналогові камери – традиційні камери, які зазвичай пропонують лише нижчу роздільну здатність і вимагають підключення коаксіального кабелю для кожної камери до відеореєстратора та окремих дротових з'єднань для живлення [13]. Крім того, щоб забезпечити якісніші кадри, камери повинні розташовуватися біля відеореєстратора. Діапазон їхнього зору, як правило, менший, ніж IP-камер, тобто може знадобитися більше камер, щоб покрити таку ж кількість місця, ніж одна IP-камера. Нарешті, записані кадри ще більше спотворюватимуться при спробі збільшити зображення.

Однак ці камери дешевші, і вони мають широкий вибір варіантів дизайну, щоб ви могли знайти те, що вам потрібно, за розумною ціною. IP / Digital-камери – цифрові камери, які мають значно вищу роздільну здатність та чіткіші зображення, ніж аналогові. Вони підключаються до відеореєстратора через перемикач живлення за допомогою Ethernet і використовують лише один кабель для підключення як до відеореєстратора, так і до джерела живлення.

Для отримання якісних зображень IP-камери не повинні бути поруч із відеореєстратором, і їх зображення можна збільшити цифровим способом, не

погіршуючи якість зображення. Нарешті, IP-камери мають ширший діапазон зору та безліч додаткових спеціальних функцій, таких як автоматичний запис, викликаний рухом, розпізнавання об’єктів та опції смарт-технологій.

Недоліком цифрових IP-камер є те, що вони значно дорожчі, вони займають смугу пропускання від вашої мережі для передачі зображень, і їм потрібно більше місця для зберігання. Більше того, хоча вони забезпечують зручність бути камерами Wi-Fi, що робить їх стрічку дистанційно доступною, це також робить їх хакерськими, тому особливу увагу потрібно приділити їхнім функціям безпеки.

Як для аналогових, так і для цифрових камер існують додаткові спеціалізовані функції, такі як камери, які можуть записувати якісні зображення при поганому освітленні, камери з декількома напрямками, камери, які можуть робити знімки на великі відстані тощо.

Нижче наведено лише вибірку спеціалізованих опцій камери:

Внутрішні / зовнішні купольні камери: вандалостійкі та найпоширеніші для базового внутрішнього / зовнішнього спостереження, купольні камери не дають злочинцям знати, в який бік може спрямовувати камера.

Камери PTZ Pan / Tilt / Zoom: ці камери дозволяють оператору спостереження в реальному часі або охоронцю активно рухати камеру вліво або вправо, вгору або вниз, або збільшувати об'єктив далі або ближче.

Приховані камери: як випливає з назви, ці камери важко побачити і забезпечують чіткі кадри. Вони можуть бути замасковані під різноманітні предмети, можуть бути встановлені або підкріплені, і ідеально підходять для внутрішнього використання.

Камери-кулі: довгі та циліндричної форми, вони найбільш ефективні для використання на вулиці, оскільки забезпечують чіткі види на великі відстані.

Теплові фотокамери / інфрачервоні камери: використовуються багатьма аеропортами, морськими портами та приміщеннями, що забезпечують

критичну інфраструктуру, інфрачервоні камери можуть забезпечувати якісне цілодобове спостереження незалежно від часу доби та якості світла. Вони можуть фіксувати фігури, що рухаються навіть у темно-темній темряві, а лінзи мають дальність відстані понад 900 футів.

Камери ANPR / LPR: Камери автоматичного розпізнавання номерних знаків (ANPR) або Розпізнавання номерних знаків (LPR) - це вузькоспеціалізовані камери, здатні зчитувати та зберігати дані на номерних та реєстраційних номерах [14].

Камери високої чіткості: надають такі зображення з високою роздільною здатністю, що їх в основному використовують у закладах з дуже високим рівнем ризику, таких як казино та банки.

3 ПРОЕКТУВАННЯ СИСТЕМИ БЕЗПЕКИ

3.1 Аналіз джерел загроз на підприємстві

Носіями загроз інформаційної безпеки є їх джерела. Загрозами можуть виступати як фізичні особи, тобто суб'єкти, так і об'єктивні прояви. При цьому, джерела загроз можуть бути як всередині установи, так і за її межами.

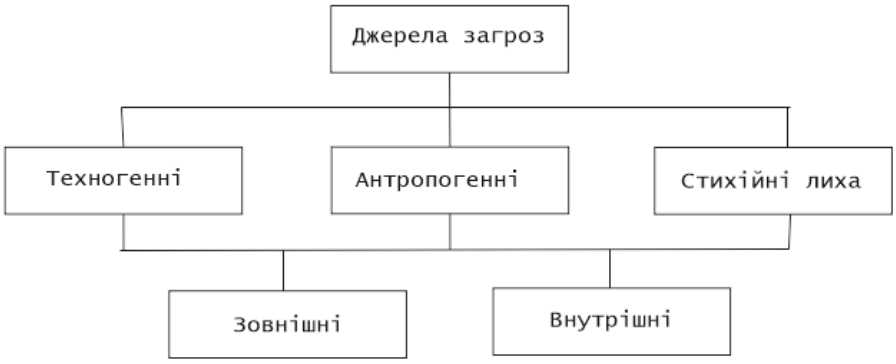


Рисунок 3.1 – Джерела загроз інформаційній безпеці

З рисунку 3.1 можемо зробити висновок, що загрози бувають техногенного, антропогенного характеру, в результаті стихійних лих, а також поділяються на зовнішні та внутрішні.

Антропогенними джерелами загроз являються суб'єкти, чиї дії можуть класифікуватися як навмисні, так і ненавмисні злочини. Це джерело є найбільш поширеним і являється найцікавішим з точки зору організації захисту, через те що дії суб'єкта завжди можна спрогнозувати та прийняти відповідно адекватні дії. Заходи протидії у цьому випадку піддаються контролю і напряму залежать від організаторів системи ІБ.

До антропогенних джерел належать суб'єкти, що мають санкціонований/несанкціонований доступ до роботи зі штатними засобами компанії, а їхні дії можуть бути і зовнішніми, і внутрішніми.

Джерела загроз, що з'явились в результаті діяльності людини та розвитку цивілізації, складніше піддаються прогнозуванню і є залежними від властивостей технічних засобів, і саме тому потребують особливої уваги. Цей вид джерел загроз надзвичайно актуальний в сучасному світі, через те, що експерти очікують різкого збільшення кількості техногенних катастроф, які викликані фізичним та моральним старіння технічної бази обладнання, а також відсутністю матеріального забезпечення для її оновлення.

Стихійні лиха та атмосферні явища відносяться до обставин, які не можливо передбачити та запобігти напевно, навіть при сучасних технологіях та людських знаннях. Такі джерела не піддаються прогнозуванню, а тому при розробці системи захисту мають бути присутні заходи захисту. Стихійні джерела потенційних загроз відносяться здебільшого до зовнішніх загроз, а під ними розуміються всякі природні катаклізми(урагани, повені, смерчі, тайфуни, виверження вулканів, тощо).

Зовнішні загрози виникають внаслідок діяльності шахраїв, хакерів та потенційних злочинців, недобросовісних партнерів, представників контролюючих органів, що зловживають службовим становищем.

Внутрішні випадкові загрози пов'язані з відмовами в обслуговуванні обчислювальної та комунікаційної техніки, помилками ПЗ, та іншими ненавмисними діями, котрі порушують нормальну роботу компанії.

На рисунку 3.1 зображено класифікацію антропогенних загроз.

Рисунок 3.1 – Класифікація антропогенних загроз

Аналіз класифікації зображеної на рисунку 3.1 свідчить про те, що випадкові загрози, які пов’язані з помилковими діями, здійснюються співробітниками випадково, через незнання, неуважність чи халатність, або ж просто з цікавості. При цьому, такі дії не мають якогось злого наміру. До основних ненавмисних загроз відносяться наступні:

- випадкові дії, що спричиняють часткові чи повні збої системного обладнання, програмного забезпечення та інформаційних ресурсів (ненавмисне пошкодження обладнання, видалення або спотворення файлів, що містять важливу інформацію або програми, включаючи системи тощо);
- неправомірне відключення пристроїв чи зміна режиму роботи програм та обладнання;
- ненавмисне пошкодження носіїв інформації;
- запуск технологічних програм, здатних при некомпетентному використовуванні викликати втрату працездатності системи або здійснити незворотні зміни в системі ;
- незаконне впровадження та використання необлікових програм, як наслідок, згодом це випливе необґрунтованою витратою ресурсів ;
- зараження комп’ютера вірусами;

- недбала поведінка, що призводять до розголошення або розкриття конфіденційної інформації;
- розголошення, передача чи втрата елементів розмежування доступу, включаючи паролі, ключі шифрування, ID карти тощо;
- ігнорування організаційних обмежень/правил при роботі в системі;
- вхід в корпоративеі облікові записи через обхід засобів захисту;
- некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки;
- відсилання даних на помилкову адресу отримувача/пристрою;
- введення помилкової інформації;
- ненавмисне пошкодження каналів зв'язку.

Водночас навмисні джерела загроз пов'язані, найчастіше, зі свідомими діями працівників для досягнення своїх цілей.

До найбільш поширених навмисних загроз можна віднести такі:

- НДС до інформації, яка зберігається в пам'яті ПК або системи, з метою незаконного використання;
- розробка спеціального ПЗ, яке використовується для здійснення НСД або інших дій;
- заперечення дій, що пов'язані з маніпуляціями інформацією та інші злочинні дії;
- введення в ПЗ та проєкти «логічних бомб», які спрацьовують при виконанні певних умов або через якийсь певний період частково/повністю виводять з ладу КС;
- розробка та поширення вірусів
- халатність при розробці, підтримуванні та експлуатації ПЗ, що в свою чергу призводить до руйнування КС;
- фальсифікація цифрових підписів;
- розкрадання інформації з подальшим маскуванням;
- перехоплення даних;

- заперечення або приховування факту крадіжки інформації
- відмова в обслуговувані.

Залежність внутрішніх загроз передбачає можливість використання зловмисником помилок працівників, які мають закрий доступ до захищуваної інформації. А незалежність внутрішніх загроз передбачає відсутність вказаних особливостей, тобто внутрішня загроза виникає у результаті самостійних дій злочинця.

При реалізації внутрішньої загрози злочинець може наслідувати ціль порушення конфіденційності, цілісності або доступності інформації.

За характером порушення конфіденційності інформації може бути так само навмисним та випадковим. За способом порушення поділяється на незаконне ознайомлення з інформацією, копіюванням та викраденням. Користуватись конфіденційними даними можуть лише ті працівники, в яких є до них доступ, а також виконувати обмежений ряд дозволених функцій.

Цілісність передбачає забезпечення гарантії збереження даних шляхом заборони змін неавторизованих користувачів. Порушення цілісності може призвести до псування, видалення, модифікації, підміни інформації. Найчастіше зловмисники або модифікує дані, що знаходяться, наприклад, в базах даних, крадуть, копіюють, доповнюють інформацію. Також слід зазначити, що і ПЗ є потенційно вразливим.

Порушення доступності пов’язано, найчастіше, з порушення правил розмежування доступу, блокуванням інформації порушенням роботи компанії. Цілю зловмисника є обмеження або відсутність доступу в законних користувачів, коли в цьому є необхідність. Вимоги з забезпечення доступності в обов’язковому порядку повинні виконуватись.

Каналами витоку інформації можуть бути зовнішні та внутрішні канали зв’язку. До них належать: поштовий сервер(електронна пошта), відкритий веб-сервер, принтери, пристрої для збереження та передачі даних(CD, USB, drive).

Не менш важливий той факт, що внутрішні загрози можуть реалізовані і за допомого зорового нагляду, а також з використанням спеціальних оптичних засобів стеження, таких як мобільні, стаціонарні та комбіновані засоби, а також засоби відео нагляду із вмонтованими накопичувачами.

Всі види загроз несуть за собою наслідки – збитки для власників інформації. Вони можуть бути як матеріальні , так і моральні.

Також внутрішні загрози можна згрупувати за рівнем ризику для компанії: найбільший, підвищений, середній, обмежений та низький. Найбільший ризик можуть являти собою системний адміністратор та адміністратори безпеки. Підвищений ризик можна отримати внаслідок незаконних дій оператора системи, працівників підготовки, введення та обробки даних. Середній рівень ризику може бути викликаний незаконними діями менеджера ПЗ або інженера системи. Обмежений рівень належить прикладним програмістам, інженерам та операторам зв'язку, адміністратору БД, користувачам-програмістам.

3.2 Визначення об'єктів захисту

Основним об'єктом захисту на підприємстві являється інформація. Захищуваною інформацією називають таку інформацію, яка підлягає захисту відповідно до вимог правових документів або вимог, які встановлені власником інформації. Власником може бути фізична, юридична особа, держава, суб'єкт господарювання та муніципальне утворення.

У сучасному світі інформація є однією з найважливіших частин нашого життя. Інформація в організаціях повинна бути класифікована, тому що не всі дані/інформація мають однаковий рівень важливості або однаковий рівень релевантності / критичності для організації. Деякі дані є більш цінними для людей, які приймають стратегічні рішення (вищий менеджмент), оскільки вони допомагають їм у прийнятті довгострокових або короткотермінових

рішень у напрямку бізнесу. Деякі дані, такі як комерційна таємниця, формули (використовуються науковими та/або дослідницькими організаціями), та нова інформація про товар (наприклад, використання маркетинговим персоналом та торговим персоналом) настільки цінні, що їх втрата може створити значні проблеми для підприємства в ринку. Таким чином, очевидно, що інформація використовується для запобігання несанкціонованому розголошенню та наслідку порушення конфіденційності.

Інформація на державному рівні буває таких видів :

Відкрита - інформація, яка не є ні конфіденційною, ні секретною. Публічне оприлюднення цієї інформації не порушує конфіденційність.

Конфіденційна - несанкціоноване розголошення конфіденційної інформації може завдати шкоди національній безпеці країни.

Секретна - несанкціоноване розголошення цієї інформації може завдати серйозної шкоди національній безпеці країн.

Цілком таємна - це найвищий рівень класифікації інформації. Будь-яке несанкціоноване розголошення надсекретної інформації призведе до серйозної шкоди національній безпеці країни.

В приватних установих є такі види інформації:

Загальнодоступна - інформація, подібна до публічноїї. Однак, якщо це буде розкрито, не очікується, що воно серйозно вплине на компанію.

Чутлива - інформація, яка вимагала вищого рівня класифікації, ніж звичайні дані. Ця інформація захищена від втрати конфіденційності, а також від втрати цілісності внаслідок несанкціонованих змін.

Приватна – як правило, це інформація особистого характеру і призначена лише для використання компанією, її розголошення може негативно вплинути на компанію або рівень заробітної плати її працівників, а медичну інформацію можна розглядати як приклади «приватної інформації».

Отже, нам відомо, що на даному підприємстві зберігається загальнодоступна та інформація з обмеженим доступом, а саме конфіденційна, та «для службового користування».

3.3 Аналіз існуючих заходів заисту інформації на підприємстві від внутрішніх загроз

Захист інформації є одним із найважливіших частин інформаційної безпеки сфери бізнесу. Проблема захисту інформації на різних підприємствах, державних установах і звичайних користувачів є важливим завданням для спеціалістів з інформаційних технологій і потребує невідкладних відповідних рішень та індивідуального підходу для кожного.

Практично перед кожним підприємством гостро стоять проблеми забезпечення інформаційної безпеки. Це пов'язано з швидким розвитком інформатизації підприємства. Так інформація вже давно стала цінним ресурсом з постійно зростаючою вартістю, то щодня росте кількість зловмисників, які готові викрасти її як для задоволення своїх інтересів, так і працюючи на когось. Конфіденційна інформація використовується компаніями-конкурентами, шахраями, терористами у своїх корисливих цілях, що як наслідок, завдає збитки підприємству , тобто власникові цієї інформації.

Проблеми та завдання компаній сьогодні можні зрівняти із проблемами загальнодержавного рівня. Так само як і держави, вони працюють та воюють. Але війни в цьому випадку носять назву інформаційні: той хто має інформацію, якщо володіє не світом, то фінансовими потоками напевно. Це трішки дивно, але і сьогодні не всі керівники компаній усвідомлюють, що їм необхідно організувати на їхньому підприємстві системи захисту інформації.

Але серед тих, хто розуміє таку необхідність, не завжди знають, що потрібно робити, для збереження тих чи інших відомостей в таємниці, з вигідно все реалізувати і не зазнати збитків від їхнього витоку чи втрати.

Деякі обирають варіант оснащення підприємства лише технічними засобами захисту і повністю ігнорують організаційно-правові методи. Тобто створення нормативно-правової бази, а її прийняття і чітке дотримання дозволять фірмі не тільки зберегти і використати з вигодою важливу інформацію, але і у разі витоку інформації мати підстави для того, щоб подати позовну заяву.

Суб'єктом захисту є компанія інтернт-провайдера, на даний час вона має вже існуючу систему фізичного захисту, а саме. Найперше, підприємство має відділ охорони, які безперервно контролюють територію. На вході є пропускна система, для входу/виходу працівників використовуються ID-карти, на охороному пості є журнал відвідування для клієнтів, тобто це означає, що в офіс не може будь-хто пройти.

Також по всьому периметру встановленні камери віддеоспростереження, трансляція ведеться на ПК в охоронній будці , а також відбувається запис у хмарне сховище, де можна переглянути інформацію за певну дату. Окрім відеонагляду є ще системи сигналізації та протипожежні.

На всіх вікнах передбачені жалюзі щоб не можна було через монітори комп'ютерів зазнімкувати інформацію, а на першому поверсі встановленні грати, щоб запобігти незаконному проникненню в офіс.

Щодо апартного захисту, то ніяких нарікань немає, тому що мережі у даній компанії захищені на високом рівні, адже вона спеціалізується на їх побудові та безпечного підключення абонетнів до мережі Інтернет. Було б дивно, якщо б мережа немала ніякого захисту. На даний момент ТОВ «ХмельницькІнфоком» активно використовує обладнання фірми Cisco. А саме комутатори, маршрутизатори, сервери доступу, мережеві екрани різних типів та інше.

Cisco є найбезпечнішим обладнанням в світі, тому що компанія відповідально підходить до пошуку, обробки і виправлення вразливостей у своїх продуктах. Компанія Cisco займається виготовленням комутаторів, маршрутизаторів, серверів доступу й іншого обладнання, які відрізняються за

місцем розташування в мережі та її типом. Це означає, що може існувати кілька різних видів моделей з однаковими зовнішніми параметрами – кількістю й швидкістю портів, але вони будуть відрізнятися функціями ПЗ, продуктивністю, можливостями резервування і взаємодією із «сусідами» по мережі.

Щодо програмного забезпечення то зараз на ПК підприємства встановлений антивірус ESET для бізнесу, від має ряд функцій, таких як управління захистом, захист робочих станцій, файлових серверів, поштових серверів. Плюсом є те, що має невелике навантаження на комп'ютер.

Також компанія використовує системи автентифікації, вони користуються програмним забезпеченням,де передбачено розмежування доступу, тобто кожен працівник, авторизується під своїм ім'ям та має доступ лише до тієї інформаці, до якої дозволено.

Проте, більша частина традиційних засобів захисту, таких як антивіруси, фаєрволи і системи автентифікації все ж таки не здатні забезпечити ефективний захист від внутрішніх порушників. Тому в такому випадку використовують DLP-системи (системи запобігання втрати даних).

Запобігання втраті даних (DLP) - це набір інструментів та процесів, що використовуються для того, щоб несанкціоновані користувачі не втрачали, не використовували або не отримували доступ до конфіденційних даних[15].

Програмне забезпечення DLP класифікує регульовані, конфіденційні та важливі для бізнесу дані та виявляє порушення політик, визначених організаціями, або в межах заздалегідь визначеного пакета політик, як правило, внаслідок дотримання нормативних вимог, таких як HIPAA, PCI-DSS або GDPR. Після виявлення цих порушень DLP здійснює виправлення за допомогою попереджень, шифрування та інших захисних дій, щоб запобігти випадковому або зловмисному обміну даними, які можуть поставити організацію під загрозу.

Програмне забезпечення та засоби запобігання втраті даних контролюють і контролюють діяльність кінцевих точок, фільтрують потоки даних у корпоративних мережах і відстежують дані в хмарі для захисту даниху спокої, в русі та у використанні. DLP також надає звіти, щоб задовольнити вимоги щодо дотримання вимог та аудиту та виявити зони слабкості та аномалій для криміналістики та реагування на інциденти.

3.4 Оцінка можливої шкоди

Ризик ІБ – рівень збитку, який понесе компанія, в разі реалізації загрози з використанням уразливості місця зберігання і обробки інформації компанії [16].

Оцінка ризику є вирішальним, якщо не найважливішим аспектом будь-якого дослідження безпеки. За допомогою точного та всебічного вивчення та оцінки ризику можна визначити заходи щодо пом’якшення наслідків.

Метою оцінки ризиків є виявлення та оцінка потенційних загроз, вразливостей та ризиків, яким піддається об'єкт, що оцінюється, та їх впливу на основні послуги та діяльність.

Оцінка ризику також встановлює основу та обґрунтування заходів із пом'якшення наслідків, які слід планувати, розробляти та впроваджувати на об'єкті з метою захисту життя людей та зменшення шкоди майну від потенційних загроз.

Існує безліч методологій та технологій проведення оцінки ризику. Одним із підходів є збір результатів оцінки загроз, оцінки вразливості та оцінки впливу для визначення числового значення ризику для кожної пари активів та загроз.

Введена тут методологія оцінки ризику використовує як кількісні, так і якісні методи для отримання висновків, отриманих в результаті

систематичного обчислення рейтингів, що підтверджується логічними аргументами, підкріпленими фактичними даними.

Весь процес оцінки ризику може бути узагальнений як:

- визначення активів, які потребують захисту;
- оцінка загроз для виявлення та визначення загроз, які можуть завдати шкоди об'єкту. Визначення активів та загроз;
- Проведення оцінки вразливості для виявлення слабких місць, якими може скористатися зловмисник;
- Обчислення ризиків, використовуючи результати оцінки вартості активів, загроз та вразливості;

Перш ніж проводити оцінку ризику, найважливішим є виявлення всіх критичних активів на об'єкті, які потребують захисту.

Активи - це цінні для об'єкта ресурси, які можуть бути матеріальними (наприклад, орендарями, установками, спорудами, обладнанням, діяльністю, операціями та інформацією) або нематеріальними (наприклад, процеси або репутація компанії) [18]. Для досягнення найбільшого зниження ризику за найменших витрат життєво важливим є визначення та визначення пріоритетів критичних активів об’єкта. Цього можна досягти шляхом визначення/розуміння основних функцій та процесів об'єкта; а також шляхом виявлення інфраструктур / компонентів всередині об'єкта, які мають важливе значення для досягнення та підтримки таких основних функцій та процесів. Деталі можна скласти в таблиці для переліку цих активів та відповідних планів резервування та відновлення, щоб посилання можна було зробити під час оцінки ризику.

У таблиці 3.1 наведено приклад цього процесу.

Таблиця 3.1 – Оцінка інформаційних ризиків

№ п/п	Інформаційний актив	Наявні заходи захисту	Вразливості	Загрози	Ймовірність реалізації	Наслідки	Оцінка ризиків
1	2	3	4	5	6	7	8
1	Обладнання	Діагностика та технічне обслуговування, прибирання, стабілізатори напруги	Чутливість до температури, вологи, пилу, коливань напруги, тощо	Ц,Д	2	4	8
2	Програмне забезпечення	Резервне копіювання	Відсутність резервного копіювання, неправильне розмежування прав доступу	К, Ц, Д	3	4	12
3	Документи на паперових носіях	Цифрування паперових носіїв	Чутливість до вологи, вогню, часу, пошкоджень, викрадення	К, Ц, Д	2	3	6

Продовження таблиці 3.1

1	2	3	4	5	6	7	8
4	Документи на електронних носіях	Резевне копіювання в хмарні сховища	Чутливість до вологи, часу, пошкоджень, викрадення	К,Ц,Д	2	5	6
5	Бази даних	Резервне копіювання, автентифікація для користувачів	Втрата, тимчасова недоступність, модифікація даних	К,Ц,Д	3	5	15
6	Персонал	Відеоспостереження, розмежування доступу до інформації, авторизація та ентифікація, анкетування	Розголошення, крадіжка, продаж, необережне користування, неправильний підбір, відсутність механізмів моніторингу	К,Ц,Д	5	5	25

3.5 Політика безпеки

Загальні положення. Мета та сфера застосування. Інформація є цінним активом, який потрібно захищати від несанкціонованого розголошення,модифікація, використання або знищення. Необхідно вжити необхідних заходів, щоб забезпечити його конфіденційність, цілісність та доступність.

Політика безпеки надає єдиний набір політик захисту інформації для ТОВ «ХмельницькІнфоком»(надалі Товариство).

В додаток до визначення функцій та відповідальності політика інформаційної безпеки допоможе підвищити обізнаність користувачів про потенційні ризики, пов’язані з доступом до та використанням технологічних ресурсів. Поінформованість працівників через розповсюдження цієї політики

допомагає прискорити розробку нових прикладних систем і забезпечити

послідовне впровадження засобів контролю за інформаційними системами.

Політика інформаційної безпеки базується на міжнародному стандарті інформаційної безпеки - ISO27002 2005. Стандарти призначені длятого, щоб

дотримуватись чинного законодавства та нормативних актів. Стандарти визначають мінімальні вимоги щодо забезпечення безпечного середовища для розробки, впровадження та підтримки інформаційних технологій та систем.

Виконання

Політики повинні дотримуватися всі міські працівники та відділи, якщо не було виділено спеціально вийнятків. Керівництво та відділи можуть вводити санкції щодо працівників, згідно з прийнятими управлінням Товариства, за порушення стандартів.

2 Інформаційна безпека

Інформація є цінним активом Товариства та повинна бути захищена від несанкціонованого доступу розкриття, модифікації або знищення. Політика

інформаційної безпеки і відповідні процедури повинні бути впроваджені для забезпечення цілісності, конфіденційності та доступності інформації.

Технологічні ресурси в міру необхідності, але щонайменше щорічно переглядають найсучасніші найкращі практики щодо використання технологій та вносять зміни та/або видають нову політику, процедури та/або засоби контролю, щоб відобразити найбільш відповідне рішення щодо безпеки міста інформація

Технологічні ресурси надаються уповноваженим користувачам для сприяння ефективного та результативного виконання своїх обов'язків в захищеному електронному режимі середовищі. Використання таких ресурсів накладає певні обов'язки та зобов'язанння перед користувачами і підпорядковується всім чинним правилам Товариства.

3 Оцінка ризиків та загроз

Оцінка ризиків повинна проводитись щороку для дослідження чи змінювались/додавались ризики, активи, загрози, вразливості.

Оцінка ризиків має мати чітко визначений обсяг, щоб бути ефективною. Результатом оцінки ризиків повинен бути звіт, для визначення пріорітетів ризиків, на основі вразливостей та дестабілізуючого впливу на інформацію Товариства.

4 Організація безпеки

Керівництво Товариства повністю розуміє, що інформаційна безпека є основою функціонування Товариства та забезпечує впровадження, підтримку і контроль відповідного рівня безпеки іфнормації.

Управління Товариства активно підтримує інформаційну безпеку шляхом регулювання, розприділення обов'язків та призначення відповідальних за ІБ.

У Товаристві створений та працює Комітет з питань управління інформаційною безпекою ТОВ «ХмельницькІнфоком» (надалі – Комітет),

прийняті ним рішення являються обов’язковими для виконання усіма співробітниками Товариства.

Документація системи управління ІБ розробляється відділом інформаційної безпеки Товариства.

Документи системи управління ІБ доступні працівникам Товариства у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

5 Безпека доступу третьої сторони

Усім майбутнім стороннім особам буде надана копія Політики інформаційної безпеки Товариства, прийняття якої вони повинні підтвердити письмово та будуть зобов’язані дотримуватись зазначених правил.

У випадку, коли третім особам мають доступ до технологічних ресурсів, вони повинні дотримуватись тих же стандартів, що і співробітники Товариства. Якщо третя сторона працює в Товаристві, не будучи під безпосереднім наглядом, співробітники Товариства повинні бути пильними щодо виходу з сесії, вихід із системи або забезпечення доступу до ПК та збереження паперової інформації сналежним чином.

До облікових записів користувачів, які використовують віддалений доступ для входу, повинні застосовуватися жорсткі елементи керування. Якщо доступ сторонніх осіб передбачає підключення до мережі, використання брандмауера, реєстрація доступу та моніторинг систем є обов’язковим.

Порти мережевого підключення повинні постійно контролюватися на предмет невідомих пристроїв та несанкціоновані з'єднання.

5 Класифікація та контроль активів

Вся інформація та активи, пов’язані з обробкою інформації, будуть закріплені за відповідним співробітником(власником) Товариства. Власник активу нестиме відповідальність за:

- забезпечення того, щоб інформація та активи, пов’язані з інформацією переробні об'єкти класифіковані належним чином;

- визначення, надання та щорічний перегляд обмежень доступу та класифікації, враховуючи застосовну політику контролю доступу.

Звичайні завдання можуть бути делеговані, наприклад, зберігачу, який доглядає за активом, але остаточна відповідальність залишається за власником.

Інформаційні та технологічні ресурси Товариства надаються користувачам для сприяння ефективному та результативному виконанню своїх обов'язків. Використання таких ресурсів покладає на користувачів певні обов'язки та зобов'язання. Кожен користувач несе відповідальність за розуміння та дотримання політики Товариства прийнятного використання технологій та забезпечення наявності таких ресурсів.

Товариство залишає за собою право отримувати та читати будь-які дані, що отримуються, формуються та передаються через Інтернет-з'єднання та/або зберігаються на обладнанні Товариства.

Вся інформація Товариства поділяється на такі категорії:

- Конфіденційна;
- Для службового користування;
- Загальнодоступна(публічна).

Право власності та класифікація даних визначатимуться відповідно директором або адміністратором.

Перевірки будуть проведені для всіх працівників Товариства, підрядників та постачальників, коли визначається доступ до конфіденційної інформації.

Керівництво вимагатиме від працівників та сторонніх користувачів застосування захисту відповідно до Політики та процедур інформаційної безпеки Товариства.

Усі працівники повинні будуть проходити щорічне навчання з питань обізнаності про безпеку та концепції. Усі працівники негайно повинні повідомляти про випадки, що стосуються порушення безпеки Товариства. Усі

працівники повинні повідомляти про будь-які інциденти, занепокоєння або підозри в діяльності безпосереднього керівника, відділу кадрів або адміністраторів безпеки.

7 Фізична та екологічна безпека

Повинна бути проведена оцінка безпеки всіх основних засобів обробки інформації, а вподальшому щорічно має проводитись оцінка фізичної безпеки та готуватись звіт.

Доступ до будь-якого центру обробки даних, мережевого, операційного центру, телекомунікацій або інших подібних засобів обробки інформації має бути обмеженим і фізично контрольованим.

Доступ до будь-якого офісу, комп'ютерного кабінету або робочої зони, що містить конфіденційну інформацію повинна бути фізично обмежена.

Виробничі системи, включаючи, але не обмежуючись ними, сервери, мережеве обладнання, та телефонії ма.ть бути розташовані в межах фізично захищеної зони.

Відповідні запобіжні заходи, включаючи видалення або шифрування конфіденційних даних будуть прийняті під час відправлення обладнання за межі об'єкта на технічне обслуговування.

Носії інформації (дискети, компакт-диски, DVD-диски, касети тощо), які містять конфіденційну інформацію, але підлягають утилізації повинні бути знищені для запобігання витоку інформації.

Коли носій зношений, пошкоджений або іншим чином більше не потрібен, він має бути утилізованим безпечним способом. Щоб запобігти витоку конфіденційної інформації через необережне або неадекватне розпорядження комп’ютерними носіями, формально мають бути встановлені процедури щодо безпечного утилізації носіїв інформації.

8 Управління інцидентами інформаційної безпеки

Будь-яке підозрюване або спостерігане порушення конфіденційної або обмеженої інформації необхідно повідомити адміністратора безпеки або

керівництво.Інформація, отримана в результаті оцінки інцидентів інформаційної безпеки буде використовуватися для виявлення повторюваних або сильних наслідків.

4 РЕАЛІЗАЦІЯ РОБОТИ

4.1 Загальні відомості про алгоритм шифрування AES

Найбільш популярним та широко прийнятим алгоритмом симетричного шифрування, з яким сьогодні можна зіткнутися, є Розширений стандарт шифрування (AES). Це виявляється принаймні в шість разів швидше, ніж потрійний DES [12].

Потрібна була заміна DES, оскільки його розмір ключа був замалим. Зі збільшенням обчислювальної потужності він вважався вразливим перед вичерпною атакою ключового пошуку. Triple DES був розроблений, щоб подолати цей недолік, але виявився повільним.

Особливості AES такі:

- Симетричний ключ симетричний блок-шифр
- 128-бітні дані, 128/192/256-бітні ключі
- Сильніший і швидший, ніж Triple-DES
- Надайте повну специфікацію та деталі дизайну

AES - це ітераційний, а не шифр Фейстеля. Він базується на «мережі заміщення – перестановки». Він складається з ряду пов’язаних операцій, деякі з яких передбачають заміну входів на конкретні виходи (підстановки), а інші передбачають перемішування бітів навколо (перестановки) [13].

Цікаво, що AES виконує всі свої обчислення на байтах, а не на бітах. Отже, AES обробляє 128 біт блоку відкритого тексту як 16 байт. Ці 16 байтів розташовані у чотири стовпці та чотири рядки для обробки у вигляді матриці -

На відміну від DES, кількість раундів в AES є змінною і залежить від довжини ключа. AES використовує 10 раундів для 128-розрядних ключів, 12 раундів для 192-розрядних ключів і 14 раундів для 256-розрядних ключів. У кожному з цих раундів використовується інший 128-розрядний круглий ключ, який обчислюється за вихідним ключем AES [14].

Схема структури AES наведена на наступному рисунку 4.1

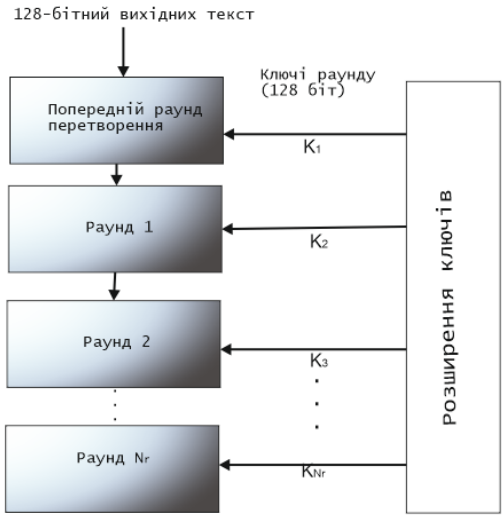


Рисунок 4.1 – Схема структури алгоритму шифрування AES

Процес шифрування. Тут ми обмежимося описом типового раунду шифрування AES. Кожен раунд складається з чотирьох підпроцесів. Процес першого туру зображений на рисунку 4.2.

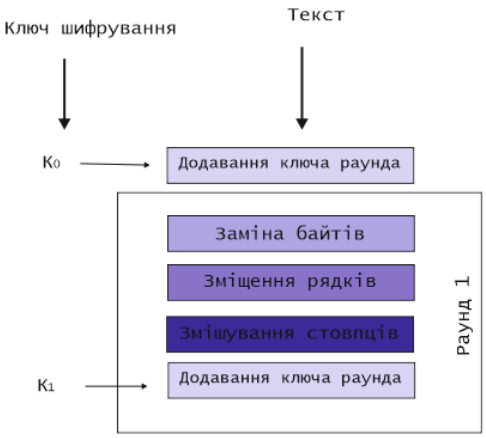


Рисунок 4.2 – Перший раунд алгоритму шифрування AES

Заміна байтів (SubBytes)

16 вхідних байтів замінюються пошуком фіксованої таблиці (S-box), заданої в дизайні. Результатом є матриця з чотирьох рядків і чотирьох стовпців.

Кожен з чотирьох рядків матриці зміщується вліво. Будь-які записи, які «відпадають», повторно вставляються з правого боку рядка. Зміна здійснюється наступним чином:

- Перший ряд не зміщується.
- Другий рядок зміщується на одне (байтове) положення вліво.
- Третій ряд зміщений на дві позиції вліво.
- Четвертий ряд зміщений на три позиції вліво.
- Результатом є нова матриця, що складається з тих самих 16 байтів, але зміщених відносно один одного.

MixColumns

Кожен стовпець із чотирьох байтів тепер перетворюється за допомогою спеціальної математичної функції. Ця функція бере як вхідні дані чотири байти одного стовпця і виводить чотири абсолютно нові байти, які замінюють вихідний стовпець. Результатом є ще одна нова матриця, що складається з 16 нових байт. Слід зазначити, що цей етап не виконується в останньому турі.

Додавання ключа раунду

16 байт матриці тепер розглядаються як 128 біт і XOR до 128 бітів круглого ключа. Якщо це останній раунд, то на виході буде зашифрований текст. В іншому випадку отримані 128 біт інтерпретуються як 16 байт, і ми починаємо ще один подібний раунд.

Процес розшифровки

Процес розшифровки шифротексту AES подібний до процесу шифрування в зворотному порядку. Кожен раунд складається з чотирьох процесів, що проводяться в зворотному порядку :

- Додати ключ раунду
- Змішати стовпці
- Змістити рядки
- Замінити байти

4.1 Реалізація програми

Переходимо до реалізації програми, алгоритм шифрування виконайний на мові програмуванння C# у середовищі для розробки Visual Studio 2019. На рисунку 4.3 зображено головне вікно, максимально просте в користуванні. Для того, щоб зашифрувати файл натискаємо кнопку «Оберіть файл», після чого відкривається діалогове вікно(рисунок 4.4), серед документів шукаємо потрібний, а вже потім натискаєм кнопку зашифрувати.

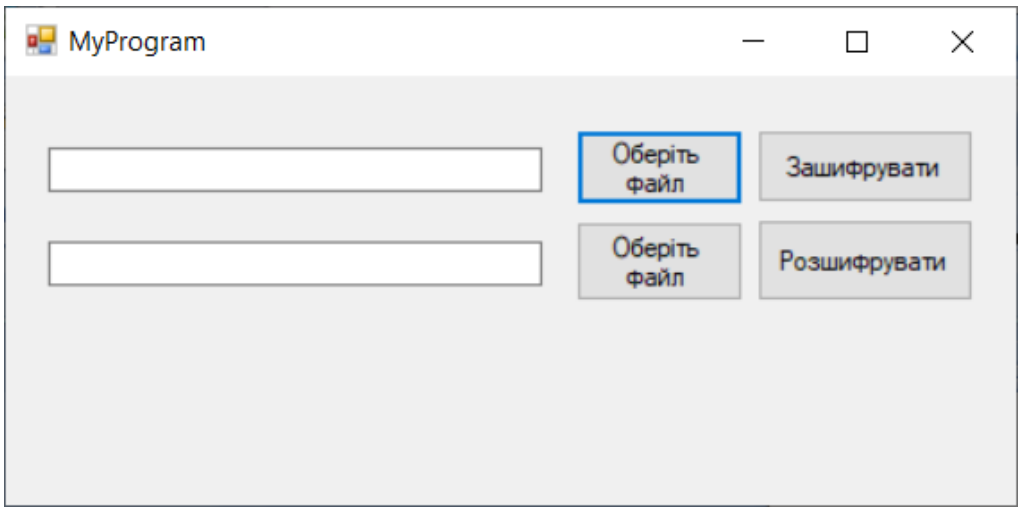


Рисунок 4.3 – Головне вікно програми

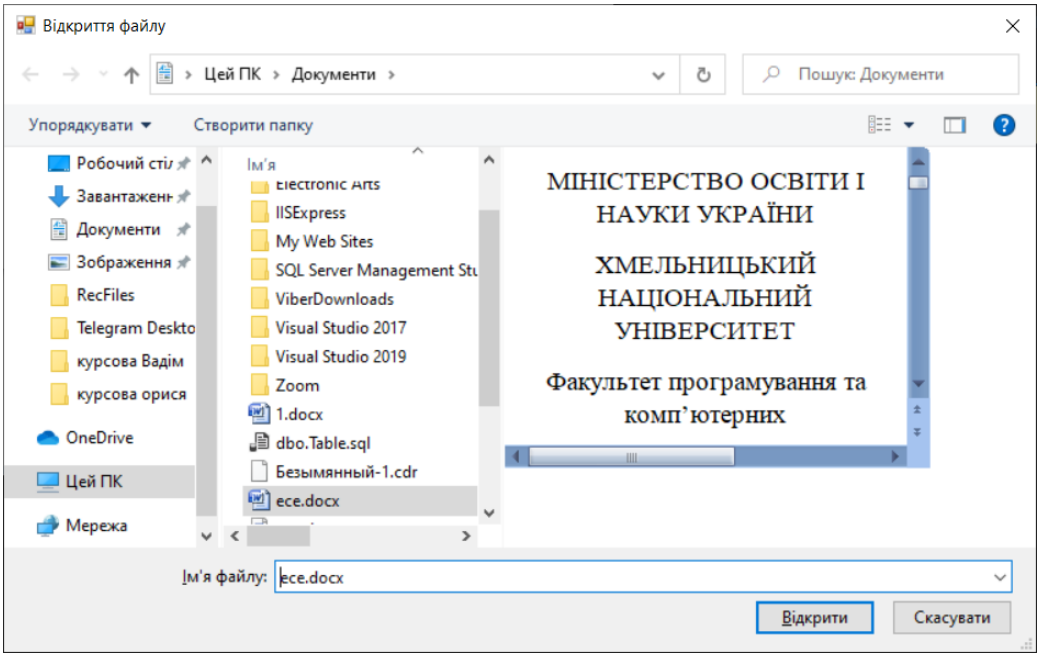


Рисунок 4.4 – Діалогове вікно відкриття файлу

Після того, як була нанисnута кнопка «Зашифрувати» виконується процес шифрування наступним чином:

```
static void CryptFile ( string fileIn, string fileOut, SymmetricAlgorithm
algo, byte[] rgbKey, byte[] rgbIV ) {
if ( string.IsNullOrEmpty( fileIn ) )
throw new FileNotFoundException( string.Format( "Неправильний шлях до файлу:
{0}.", fileIn ) );

if ( !File.Exists( fileIn ) )
throw new FileNotFoundException( string.Format( "Файл '{0}' не знайдений!",
fileIn ) );

byte[] buff = null;
const string CRYPT_EXT = ".crypt";

using ( var sa = algo )
using ( var fsw = File.Open( fileOut + CRYPT_EXT, FileMode.Create,
FileAccess.Write ) )
using ( var cs = new CryptoStream( fsw,
sa.CreateEncryptor( rgbKey, rgbIV ), CryptoStreamMode.Write )
) {
using ( var fs = File.Open( fileIn, FileMode.Open, FileAccess.Read ) ) {
buff = new byte[fs.Length + sizeof( long )];
fs.Read( buff, sizeof( long ), buff.Length - sizeof( long ) );
int i = 0;
foreach ( byte @byte in BitConverter.GetBytes( fs.Length ) )
buff[i++] = @byte;
}

cs.Write( buff, 0, buff.Length );
cs.Flush();
}

Array.Clear( rgbKey, 0, rgbKey.Length );
Array.Clear( rgbIV, 0, rgbIV.Length );
```

Після шифрування створюється файл з розширенням .crypt і має наступний вигляд (рисунок 4.5):

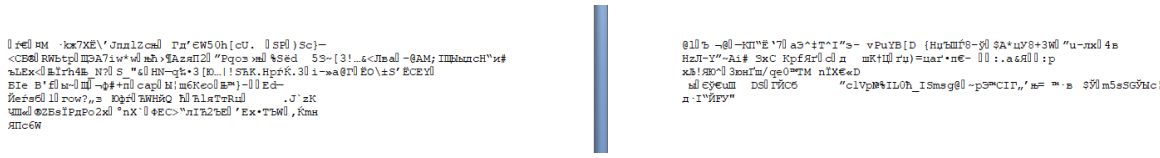


Рисунок 4.5 – Зашифрований файл

Для того, щоб розшифрувати цей файл, відриваємо знову нашу програму, натискаємо кнопку «Оберіть файл», після чого відкриється діалогове вікно, де потрібно обрати зашифрований файл (рисунок 4.4).

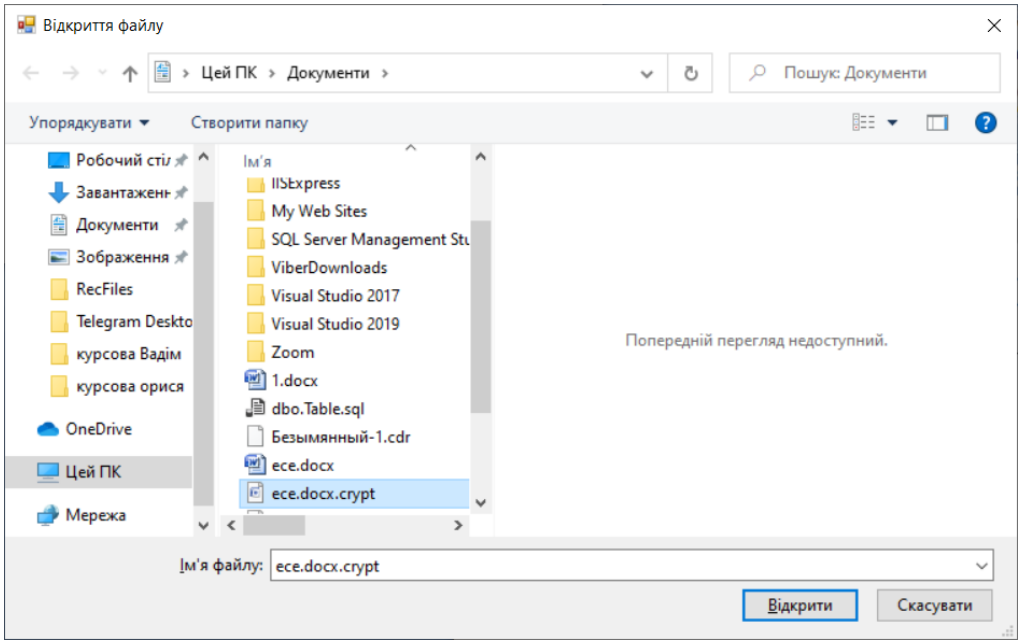


Рисунок 4.6 – Діалогове вікно для вибору файлу

Процес шифрування відбувається після натискання кнопки розшифрувати і має наступний вигляд програмного коду:

```
static void DecryptFile ( string fileIn, string fileOut, SymmetricAlgorithm
algo, byte[] rgbKey, byte[] rgbIV ) {
if ( string.IsNullOrEmpty( fileIn ) )
throw new FileNotFoundException( string.Format( "Непривильний шлях до файлу
файлу: {0}.", fileIn ) );

if ( !File.Exists( fileIn ) )
throw new FileNotFoundException( string.Format( "Файл '{0}' не знайдений!",
fileIn ) );

byte[] buff = null;
const string DECRYPT_EXT = ".decrypt";


using ( var sa = algo )
using ( var fsr = File.Open( fileIn, FileMode.Open, FileAccess.Read ) )
using ( var cs = new CryptoStream( fsr,
sa.CreateDecryptor( rgbKey, rgbIV ), CryptoStreamMode.Read )
) {
buff = new byte[fsr.Length];
cs.Read( buff, 0, buff.Length );
using ( var fsw = File.Open( fileOut + DECRYPT_EXT, FileMode.Create,
FileAccess.Write ) ) {
int len = (int)BitConverter.ToInt64( buff, 0 );
fsw.Write( buff, sizeof( long ), len );
fsw.Flush();
}
}

Array.Clear( rgbKey, 0, rgbKey.Length );
Array.Clear( rgbIV, 0, rgbIV.Length );
}
```

4.3 Система відеоспостереження

Як вже зазначалось у 3 розділі ТОВ «ХмельницькІнфоком» має існуючу систему відеоспостереження, але після проведеного аналізу було виявлено, що декілька об’єктів не потрапляють у поле зору камер, а саме біля запасного виходу, а також над постом охорони була становлена лише одна камера з недостатнім кутом огляду.

Тому після модернізації системи відеонагляду план-схема має наступний вигляд(рисунок 4.7).

Рисунок 4.7 – Схема системи відеонагляду

За допомогою програми IP Video System Design Tool було відтворено план приміщення підприємства. Через функцію 3D-моделювання можна розташувати та підібрати камери, щоб в кут огляду потрапили важливі елементи, на рисунку 4.8 зображено поле зору камери в кабінеті відділу кадрів.

Рисунок 4.8 – Поле зору камери у відділі кадрів

Для системи відеоспостереження будуть використані камери фірми Cisco IP-камери Cisco Video Surveillance 6030.

IP-камера Cisco Video Surveillance 6030 – повнофункціональна кінцева точка відеозйомки високої чіткості з провідною якістю та роздільною здатністю. Завдяки своєму відкритому, заснованому на стандартах дизайну, камера забезпечує ідеальну платформу для інтеграції та роботи як незалежний пристрій або як частина мережі відеоспостереження.

4.4 Тестування системи

4.4.1 Тестування системи відеонагляду

За допомогою 3D моделі можемо перевірити кут огляду встановлених камер. В холі було встановлено 2 камери, одна над постом охорони, інша на проти, в кутку, направлена на пропускну систему. На рисунку 4.9 та 4.10 можемо побачити, що саме таке розміщення камер дозволяє відслідковувати хто заходить та виходить з офісу, хто заходить у кабінет директора та у підсобне приміщення, де є запасний вихід.

Рисунок 4.9 – Камера №1

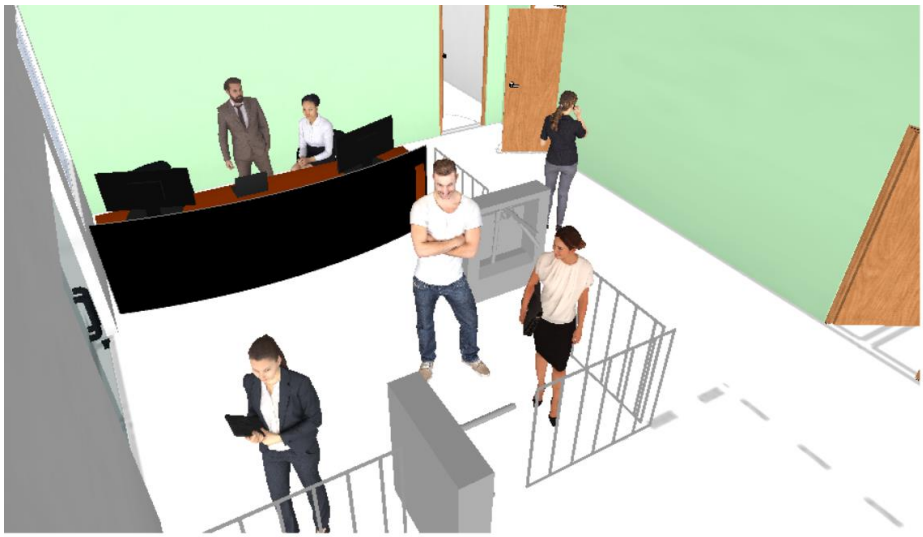


Рисунок 4.10 – Камера №2

А в кабінеті керівництва раніше камера була встановлена вкутку біля вікна, і шафа частково закривала одне робоче місце. Тому було прийнято рішення переустановити камеру в протилежний кут, і як видно з рисунку 4.11 тепер вхід в кабінет, в сереверну, робочі місця та шафа з сейфом у полі зору.

Рисунок 4.11 – Камера №3

4.4.2 Тестування програми шифрування

Тестування частково було організовано через автоматизовані тести, тобто окрема програма генерувала файли, шифрувала їх в обидві сторонни(шифрувала/розшифровувала), а потім звіряла результати з очікуваними.

Вважається, що використовування в алгоритмі шифрування AES ключа довжиною в 128 біт є досить надійним захистом проти лобової атаки, це означає, що суто з математичної точки зору підібрати один правильний пароль практично неможливо, тому що це займе декілька сотень тисяч років. Незважаючи дрібні недоліки AES, зламати захищену за допомогою цього алгоритму інформацію фактично неможливо.

ВИСНОВКИ

Першочерговою умовою і головною запорукою успішного розвитку будь-якої сфери діяльності на сьогоднішній день залишається інформація. Це продукт, на який не лише завжди буде попит, а й в боротьбі за який є і буде величезна конкуренція, і далеко не всі досягають бажаного чесними методами. Тому щоб захистити інформацію на даний час людство використовує найрізноманітніші засоби, які поєднують між собою в систему для комплексного забезпечення інформаційної безпеки.

В ході кваліфікаційної роботи було спроектовано систему захисту інформації ТОВ «ХмельницькІнфоком», а саме від внутрішніх загроз. Після дослідження об’єкту та проведеного аналіз були визначені всі можливі загрози та вразливості, зроблена оцінка ризиків інформаційної безпеки. Проаналізувавши усе це був зроблений висновок про стан безпеки в компанії.

В цілому ТОВ «ХмельницькІнфоком» має задовільний рівень безпеки, проте були виявлені суттєві прогалини, найперше – це необізнаність працівників в основах інформаційної безпеки, друге – система відеонагляду має сліпі зони, а в них потрапляють критично важливі об’єкти.

Компанія зберігає багато конфіденційної та персрнальної інформації, яка практично є незахищеною, тому для запобігання витоку даних мною була розроблена програма для шифрування файлів за допомого алгоритму AES. Також був редагований наявний план розміщення відеокамер, а також розроблена політика інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

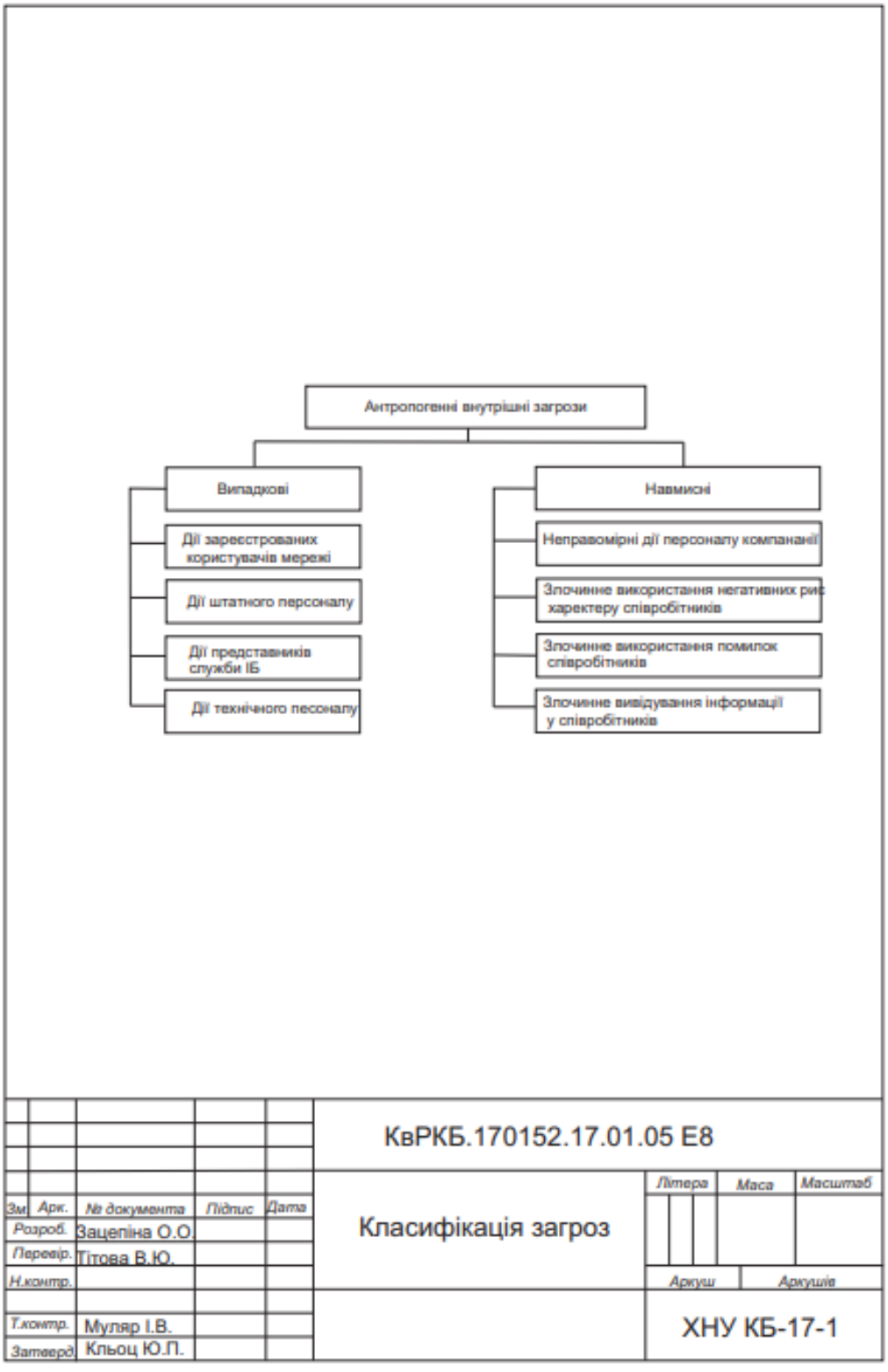
1. IT безпека і захист інформації. [Електронний ресурс] – Режим доступу:
2. https://infotel.ua/ua/IT-bezopasnost-i-zacshita-informatsii-1/ (дата звернення 28.03.2021). – Назва з екрану
3. Офіційний сайт ТОВ «ХмельницькІнфоком». [Електронний ресурс] – Режим доступу: https://www.ic.km.ua/index_km.html (дата звернення 19.04.2021). – Назва з екрану
4. AES шифрование. [Електронний ресурс] – Режим доступу: https://www.technodor.info/2020/05/aes.html (дата звернення 09.05.2021). – Назва з екрану
5. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. − 104 с.
6. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
7. Технології захисту інформації / Ю. А. Тарнавський – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
8. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
9. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.
10. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

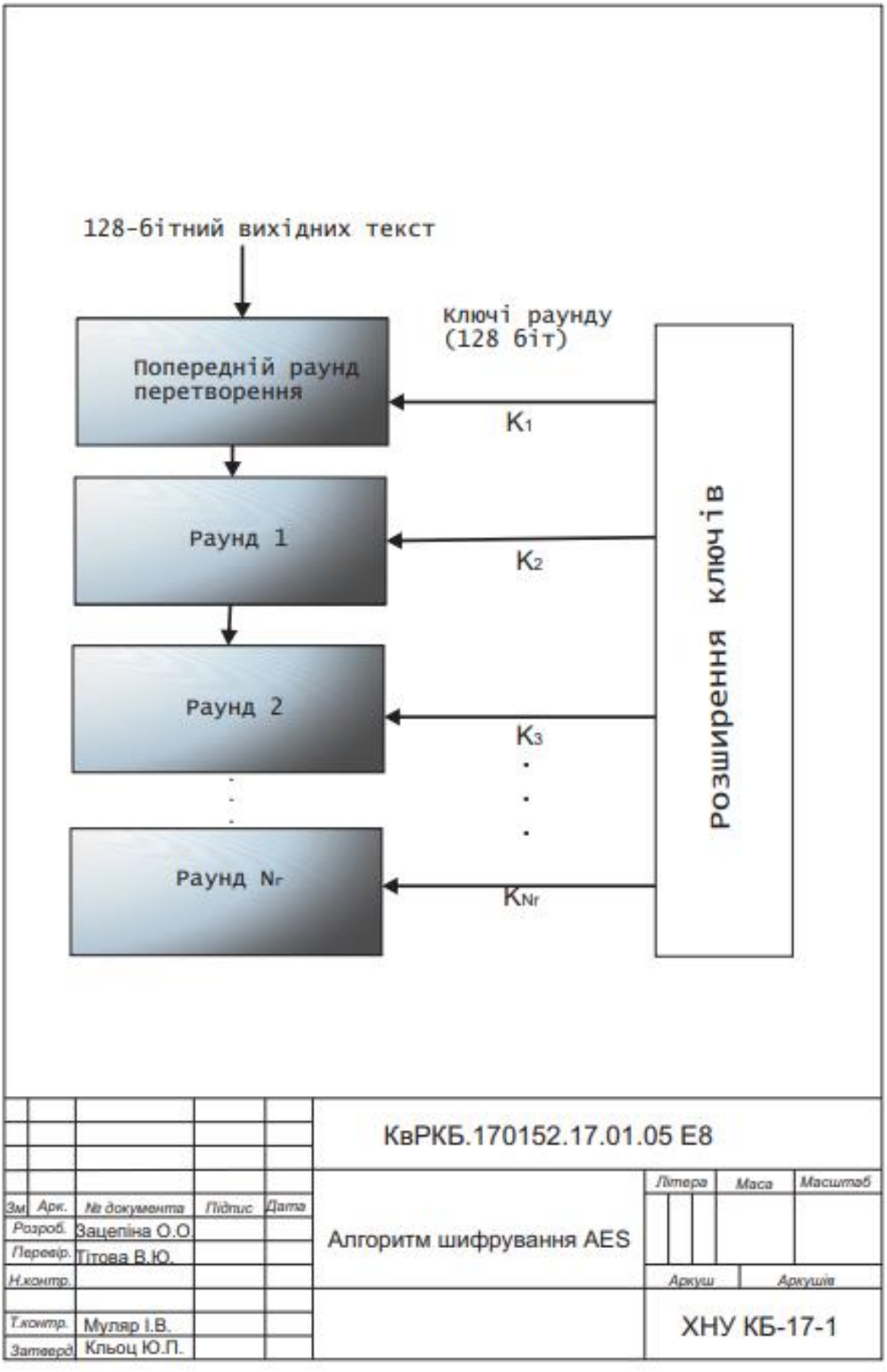
11. Девянин П. Н. Модели безопасности компьютерных систем : учебное пособие для студ. Высш. Учеб. Заведений – М. : Издательский центр "Академия", 2005. – 144 с.
12. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. / В. В. Домарев. – К. : ТИД "ДС", 2004. – 688 с.
13. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
14. Курило А. П. Аудит информационной безопасности. / [Курило А. П., Зуфиров С. Л., Голованов В. Б. и др.]. – М. : Издательская группа "БДЦ-пресс", 2006. – 304 с.
15. Малюк А. А. Информационная безопасность : концептуальне и методологические основы защиты информации : учебное пособие для вузов. – М. : Горячая линия – Телеком, 2004. – 280 с.
16. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
17. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов.. – М.: Горячая линия - Телеком, 2006. – 544 с.
18. Романец Ю.В. Защита информации в компьютерных системах и 328 с.– М.: Радио и связь, 1999. –сетях / Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин 2006. – 520 с.

ДОДАТОК А

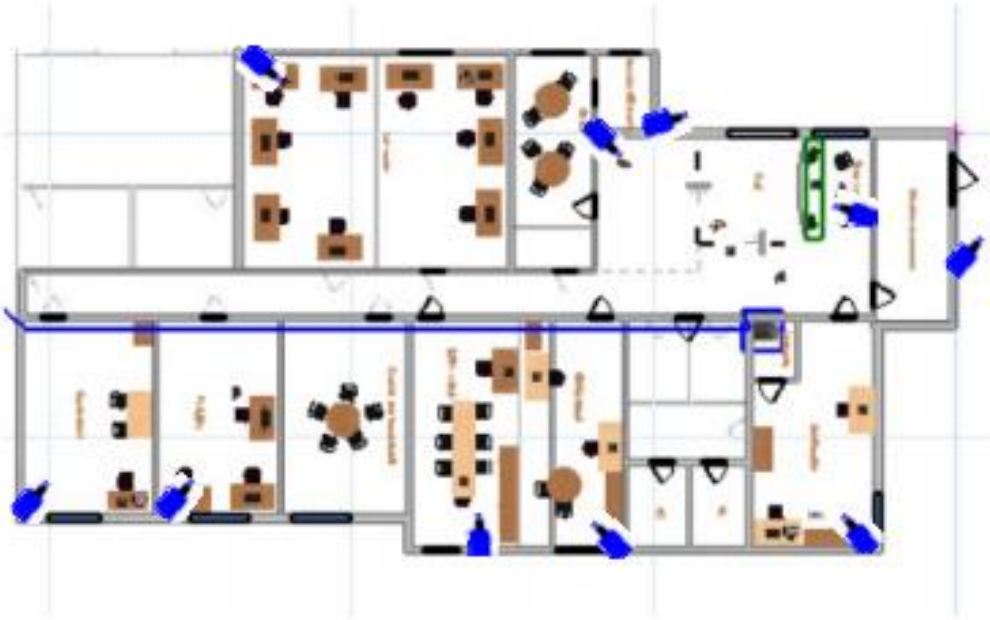
(обов’язковий)

Копія графічної частини





					КвРКБ.170152.17.01.05 Е8			
						Літера	Маса	Масштаб
Зм.	Арк.	№ документа	Підпис	Дата	Алгоритм шифрування AES			
Розроб.		Зацепіна О.О.						
Перевір.		Тітова В.Ю.				Аркуш	Аркушів	
Н.контр.								
Т.контр.		Муляр І.В.				ХНУ КБ-17-1		
Затверд.		Кльоц Ю.П.						



					КвРКБ.170152.17.01.05 Е8			
						Літера	Маса	Масштаб
Зм.	Арк.	№ документа	Підпис	Дата				
Розроб.		Зацепіна О.О.			Система відеоспостереження			
Перевір.		Тітова В.Ю.						
Н.контр.						Аркуш	Аркушів	
Т.контр.		Муляр І.В.				ХНУ КБ-17-1		
Затверд.		Кльоц Ю.П.						

ДОДАТОК Б

(обов’язковий)

Приклад програмного коду

```
using System;
using System.Collections.Generic;
using System.Drawing;
using System.Windows.Forms;
using System.IO;
using System.Text;
using System.Security.Cryptography;
using System.Xml.Linq;

namespace EDS_File
{

public partial class MainForm : Form
{
OpenFileDialog openfile = new OpenFileDialog();
SaveFileDialog save_encrypt = new SaveFileDialog();
string ext1,ext2;
string fName_enc, fName_dec;

public MainForm ( ) {

}

void Button1Click ( object sender, EventArgs e ) {
string dest = Path.Combine(
Application.StartupPath,
"keys"
);

Directory.CreateDirectory( dest );
dest = Path.Combine(
dest,
Path.GetFileName( textBox1.Text ) +
".key"
);

using ( var fs = File.Open( dest, FileMode.Create, FileAccess.Write ) )
using ( var aes = new AesCryptoServiceProvider() ) {
var rnd = RNGCryptoServiceProvider.Create();
byte[] buff0 = new byte[aes.KeySize / 8],
buff1 = new byte[16];

rnd.GetNonZeroBytes( buff0 );
rnd.GetNonZeroBytes( buff1 );

fs.Write( buff0, 0, buff0.Length );
fs.Write( buff1, 0, buff1.Length );

CryptFile(
textBox1.Text,
textBox1.Text,
```

```
aes, buff0, buff1
);
}
}

void Button3Click ( object sender, EventArgs e ) {
if ( openfile.ShowDialog() == DialogResult.OK ) {
textBox1.Text = openfile.FileName;
ext1 = Path.GetExtension( textBox1.Text );
fName_enc = Path.GetFileNameWithoutExtension( openfile.FileName );
}
}

void Button4Click ( object sender, EventArgs e ) {
if ( openfile.ShowDialog() == DialogResult.OK ) {
textBox2.Text = openfile.FileName;
ext2 = Path.GetExtension( textBox2.Text );
fName_dec = Path.GetFileNameWithoutExtension( openfile.FileName );
}
}

void Button2Click ( object sender, EventArgs e ) {
string dest = Path.Combine(
Application.StartupPath,
"keys",
Path.GetFileNameWithoutExtension( textBox2.Text ) +
".key"
);

using ( var fs = File.Open( dest, FileMode.Open, FileAccess.Read ) )
using ( var aes = new AesCryptoServiceProvider() ) {
byte[] buff0 = new byte[aes.KeySize / 8],
buff1 = new byte[16];

fs.Read( buff0, 0, buff0.Length );
fs.Read( buff1, 0, buff1.Length );

DecryptFile(
textBox2.Text,
Path.Combine(
Path.GetDirectoryName( textBox2.Text ),
Path.GetFileNameWithoutExtension( textBox2.Text )
),
aes, buff0, buff1
);
}
}

private void MainForm_Load(object sender, EventArgs e)
{

}

static void CryptFile ( string fileIn, string fileOut, SymmetricAlgorithm algo, byte[] rgbKey, byte[] rgbIV
) {
if ( string.IsNullOrEmpty( fileIn ) )
throw new FileNotFoundException( string.Format( "Неверный путь к файлу: {0}.", fileIn ) );
```

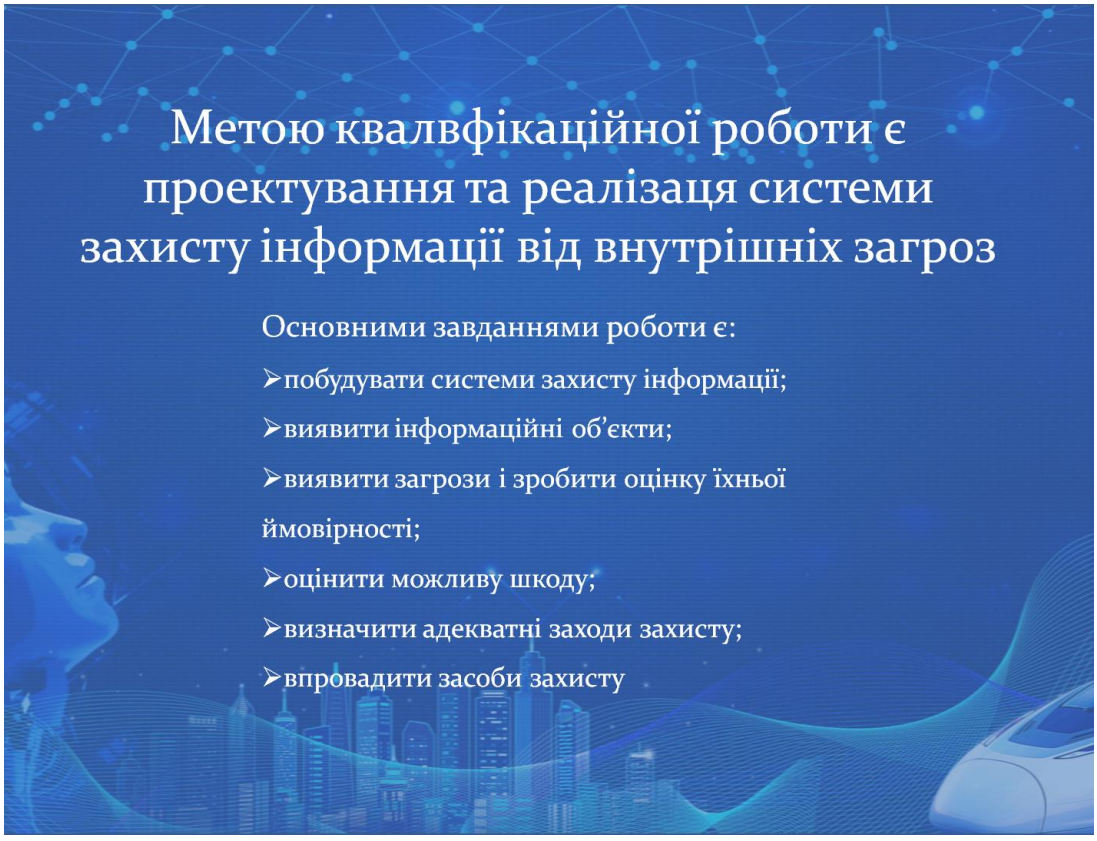
```
if ( !File.Exists( fileIn ) )
throw new FileNotFoundException( string.Format( "Файл '{0}' не найден.", fileIn ) );

byte[] buff = null;
const string CRYPT_EXT = ".crypt";

using ( var sa = algo )

using ( var fsw = File.Open( fileOut + CRYPT_EXT, FileMode.Create, FileAccess.Write ) )
using ( var cs = new CryptoStream( fsw,
sa.CreateEncryptor( rgbKey, rgbIV ), CryptoStreamMode.Write )
) {
using ( var fs = File.Open( fileIn, FileMode.Open, FileAccess.Read ) ) {
buff = new byte[fs.Length + sizeof( long )];
fs.Read( buff, sizeof( long ), buff.Length - sizeof( long ) );
int i = 0;
foreach ( byte @byte in BitConverter.GetBytes( fs.Length ) )
buff[i++] = @byte;
}

cs.Write( buff, 0, buff.Length );
cs.Flush();
}

Array.Clear( rgbKey, 0, rgbKey.Length );
Array.Clear( rgbIV, 0, rgbIV.Length );
}

static void DecryptFile ( string fileIn, string fileOut, SymmetricAlgorithm algo, byte[] rgbKey, byte[]
rgbIV ) {
if ( string.IsNullOrEmpty( fileIn ) )
throw new FileNotFoundException( string.Format( "Неверный путь к файлу: {0}.", fileIn ) );

if ( !File.Exists( fileIn ) )
throw new FileNotFoundException( string.Format( "Файл '{0}' не найден.", fileIn ) );

byte[] buff = null;
const string DECRYPT_EXT = ".decrypt";

using ( var sa = algo )
using ( var fsr = File.Open( fileIn, FileMode.Open, FileAccess.Read ) )
using ( var cs = new CryptoStream( fsr,
sa.CreateDecryptor( rgbKey, rgbIV ), CryptoStreamMode.Read )
) {
buff = new byte[fsr.Length];
cs.Read( buff, 0, buff.Length );
using ( var fsw = File.Open( fileOut + DECRYPT_EXT, FileMode.Create, FileAccess.Write ) ) {
int len = (int)BitConverter.ToInt64( buff, 0 );
fsw.Write( buff, sizeof( long ), len );
fsw.Flush();
}
}

Array.Clear( rgbKey, 0, rgbKey.Length );
Array.Clear( rgbIV, 0, rgbIV.Length );
}
```

```
}
}
```

```
using System;
using System.Windows.Forms;

namespace EDS_File
{

internal sealed class Program
{

[STAThread]
private static void Main(string[] args)
{
Application.EnableVisualStyles();
Application.SetCompatibleTextRenderingDefault(false);
Application.Run(new MainForm());
}

}
}
```

ДОДАТОК В

Копія презентаційних слайдів



Аналіз внутрішніх загоз

Аналіз наявних заходів безпеки

№	Актив	Наявний захист	Вразливості	Загрози
1	Обладнання	Діагностика та технічне обслуговування, прибирання, стабілізатори напруги	Чутливість до температури, вологи, пилу, коливань напруги, тощо	Ц,Д
2	Програмне забезпечення	Резервне копіювання	Відсутність резервного копіювання, неправильне розмежування прав доступу	К,Ц,Д
3	Документація	Резервне копіювання в хмарні сховища, цифрування паперових носіїв	Чутливість до вологи, часу, пошкоджень, викрадення	К,Ц,Д
4	Бази даних	Розмежування доступу	Втрата, тимчасова недоступність, модифікація даних	К,Ц,Д
5	Персонал	Відеоспостереження, розмежування доступу до інформації, авторизація та ідентифікація, анкетування	Розголошення, крадіжка, продаж, необережне користування, неправильний підбір, відсутність механізмів муніторингу	К,Ц,Д

Алгоритм шифрування AES

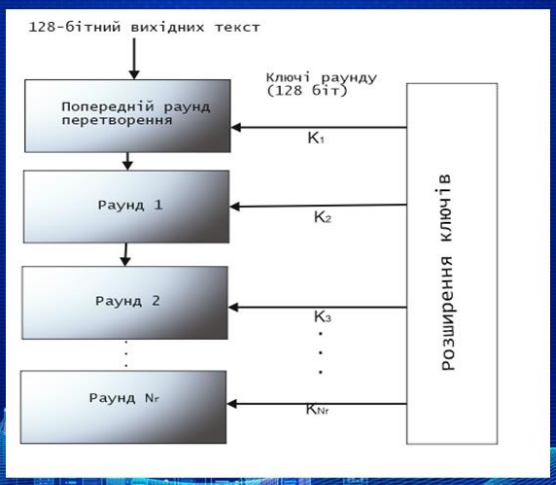


Схема відеоспостереження ТОВ "ХмельницькІнфоком"

Тестування розміщення камер в холі компанії

Висновки

В ході кваліфікаційної роботи було спроектовано систему захисту інформації ТОВ «ХмельницькІнфоком», а саме від внутрішніх загроз.

Після дослідження об'єкту та проведеного аналіз були визначені всі можливі загрози та вразливості, зроблена оцінка ризиків інформаційної безпеки.

Для захисту конфіденційної інформації реалізований алгоритм шифрування AES.

З точки зору фізичного захисту редаговано схему розміщення відеокамер в системі відеонагляду, щоб уникнути сліпих зон.

З організаційних заходів було розроблено політику безпеки.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту об'єкту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз

Автор: Зацепіна Орислава Олександрівна

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Керівник: Тітова Віра Юріївна, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2,4% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.Ю. Тітова

Завідувач кафедри КбКСМ, гарант ОП _____ Ю.П. Кльоц

Дата: 07.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студентка Зацепіна Орислава Олександрівна

Тема Система захисту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 59.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та розроблено систему захисту від внутрішніх загроз.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено предмет та об'єкт дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено дослідження предметної області а також загальний огляд технологій та методів забезпечення інформаційної безпеки, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби і технології використані для побудови системи захисту. В третьому розділі визначено основні положення системи захисту від внутрішніх загроз та розроблено алгоритми її роботи. У четвертому розділі був реалізований алгоритм шифрування та вдосконалення системи відеоспостереження.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці модуля лексичного аналізу з допомогою якого визначається ступінь конфіденційності даних. На основі даного аналізу в подальшому здійснюється керуючий вплив на витік конфіденційних даних. Практична цінність результатів кваліфікаційної роботи полягає у створені системи захисту від витоків даних, що може бути підлаштована для будь якої категорії даних, і у описі оптимальних моделей функціонування систем захисту подібного характеру.

5. Негативні сторони роботи Реалізований алгоритм шифрування має мінімальний ряд функцій.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

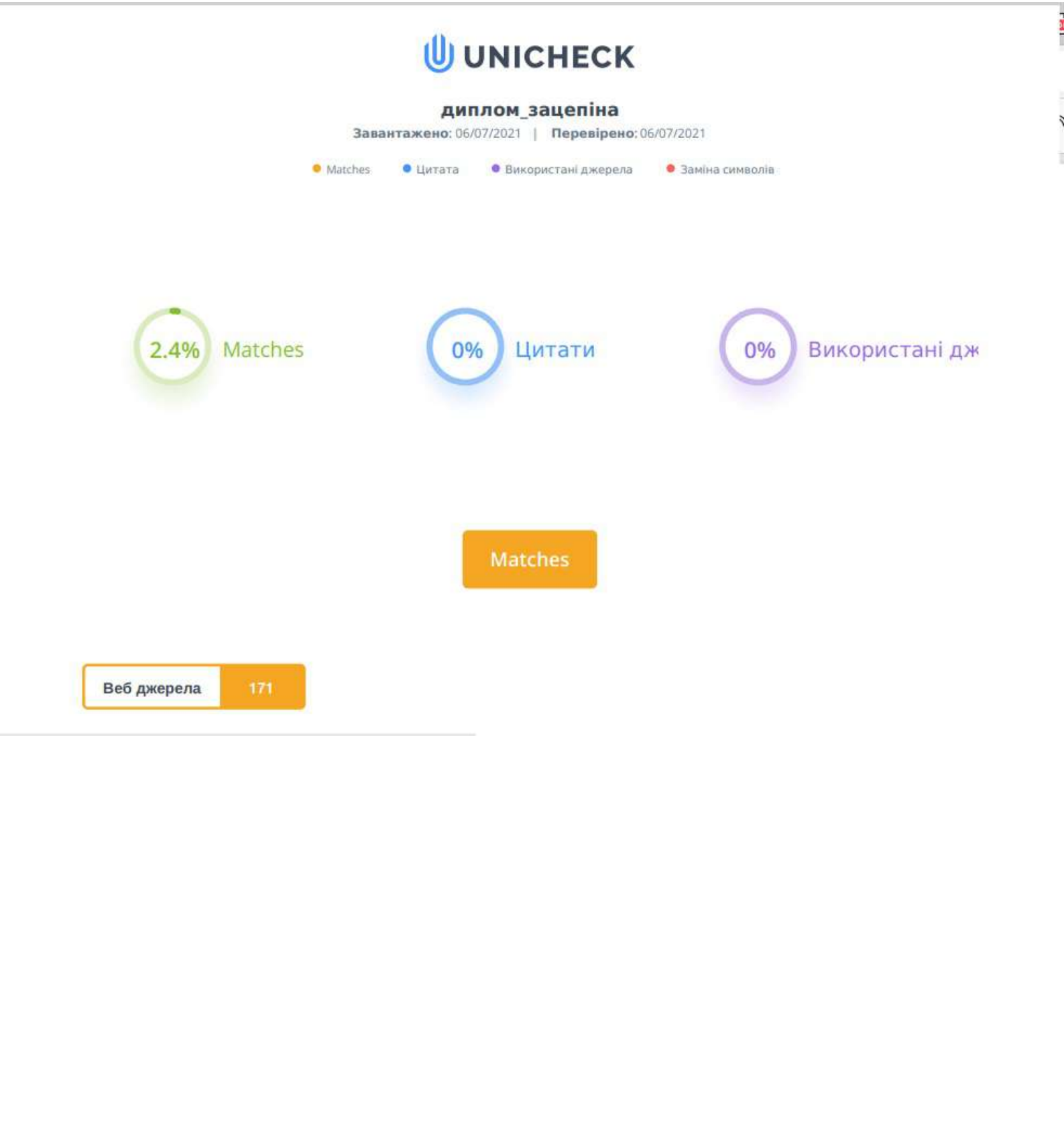
7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) К.Т.Н., доцент, доцент каф. КІСП Нікітчук А.О.

«07» 06 2021. (підпис)


UNICHECK
диплом_зацепіна
Завантажено: 06/07/2021 | Перевірено: 06/07/2021
Matches
Цитата
Використані джерела
Заміна символів
2.4% Matches
0% Цитати
0% Використані дж
Matches
Веб джерела 171

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 8%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 92430 Название: Система захисту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз Добавлено в БД: 2021-06-07 Авторы: Зацепіна О.О. Руководители: Тітова В.Ю. Консультанты: Оппоненты:	Символы	Лексемы	Символы	Лексемы
	71589	567	1299 (2%)	23 (4%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы