ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від __ _____ 2022 р.
№__

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення практичних занять з навчальної дисципліни «ОСНОВИ КІБЕРБЕЗПЕКИ» (вибіркова)

для здобувачів вищої освіти освітнього ступеня «БАКАЛАВР»
спеціальностей та освітньо-професійний програм
Державного університету «Житомирська політехніка»
факультет інформаційно-комп'ютерних технологій
кафедра інженерії програмного забезпечення

Рекомендовано на засіданні кафедри інженерії програмного забезпечення
___ _____ 20__ р.,
протокол № ___

Розробник: канд. техн. наук, доц., доцент кафедри інженерії програмного забезпечення ЛОБАНЧИКОВА Надія,
старший викладач кафедри інженерії програмного забезпечення
ЮЩЕНКО Ольга

Житомир
2022

ЗМІСТ

ВСТУП

Постійний розвиток інформаційних технологій вносить свої коригування у життєдіяльність людини, як члена цифрового суспільства. Використання цифрового світу вимагає і нових рішень щодо захисту інформації. Для запобігання витоку інформації та протидії несанкціонованому доступу до неї, зокрема і цифрової, зменшення збитків від розголошення конфіденційної інформації та втрати даних, необхідно ретельно вибирати заходи та засоби захисту інформації та коректно використовувати сучасні інформаційні технології

Дані методичні рекомендації розроблені для студентів, які навчаються за різними спеціальностями та освітніми програмами Державного університету «Житомирська політехніка» та обрали дану освітню компоненту для розширення своїх компетентностей в межах здобуття освітнього ступеня «бакалавр».

Освітня компонента «Основи кібербезпеки» є вибірковою освітньої компонентною, метою якої є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки та захисту інформації в інформаційно-телекомунікаційних системах, методологічними та законодавчими основами організації, планування та впровадження систем кібербезпеки та захисту інформації в інформаційних системах управління на підприємствах та організаціях. Направлена на представлення основних аспектів практичної діяльності по створенню, забезпеченню функціонування та оцінці ефективності систем захисту з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Дисципліна «Основи кібербезпеки» потребує систематичного вивчення теоретичного матеріалу та його послідовного закріплення шляхом виконання практичних завдань та самостійної роботи студентів. Виконання студентами практичних робіт з курсу «Основи кібербезпеки» дозволяє закріпити теоретичні знання, здобути загальні компетентності та отримати програмні результати навчання.

Практичне заняття №1
СКЛАДАННЯ ІМОВІРНІСНОГО ПРОГНОЗУ ТА МОДЕЛІ ПОРУШНИКА

Мета – здобуття практичних навиків визначення несанкціонованого доступу до інформації та складання ймовірнісного прогнозу, прогнозування та оцінки моделей порушника.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Оцінка можливостей порушника щодо подолання засобів захисту систем

Для проведення оцінки нам необхідно визначити компетентності порушника. В якості порушника розглядається суб'єкт, який має доступ до роботи зі штатними засобами інформаційно-телекомунікаційних систем (ІТС) і ПК як частини ІТС. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами ІТС, інформаційними систем (ІС). Класифікація є ієрархічною, тобто кожен наступний рівень включає в себе функціональні можливості попереднього.

Виділяється чотири рівні цих можливостей [1-4]:

Перший рівень визначає найнижчий рівень можливостей ведення діалогу в ІТС (ІС) - запуск програмного забезпечення та задач з визначеного набору, що реалізують, заздалегідь передбачені функції по обробці інформації відповідно до посадових функцій.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації, що передбачені політикою безпеки підприємства (організації).

Третій рівень визначається можливістю управління функціонуванням ІТС (ІС), тобто з можливістю впливу на базове програмне забезпечення системи, її на склад, конфігурацію та устаткування.

Четвертий рівень визначається всім обсягом можливостей осіб, які здійснюють проектування, реалізацію та ремонт технічних засобів ІТС (ІС), аж до включення до складу ІТС власних технічних засобів з новими функціями з обробки інформації.

Вважаємо, що у своєму рівні порушник є фахівцем вищої кваліфікації, знає все про ІТС і, зокрема, про систему і засоби її захисту.

Крім рівня знань порушника, його кваліфікації, підготовленості до реалізації своїх задумів, для формування найбільш повної моделі порушника

необхідно визначити категорію осіб, до яких може належати порушник.

В загальному випадку порушників можна розділити на **внутрішніх та зовнішніх**. Отримуємо наступні відкриті класифікаційні угрупування:

$\mathbf{N} = \bigcup_{\gamma} N_{\gamma}$ – множина персоналу, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність ІТС (ІС);

$\mathbf{Z} = \bigcup_{j} Z_{j}$ – множина потоку відвідувачів та контрагентів, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність ІТС (ІС)

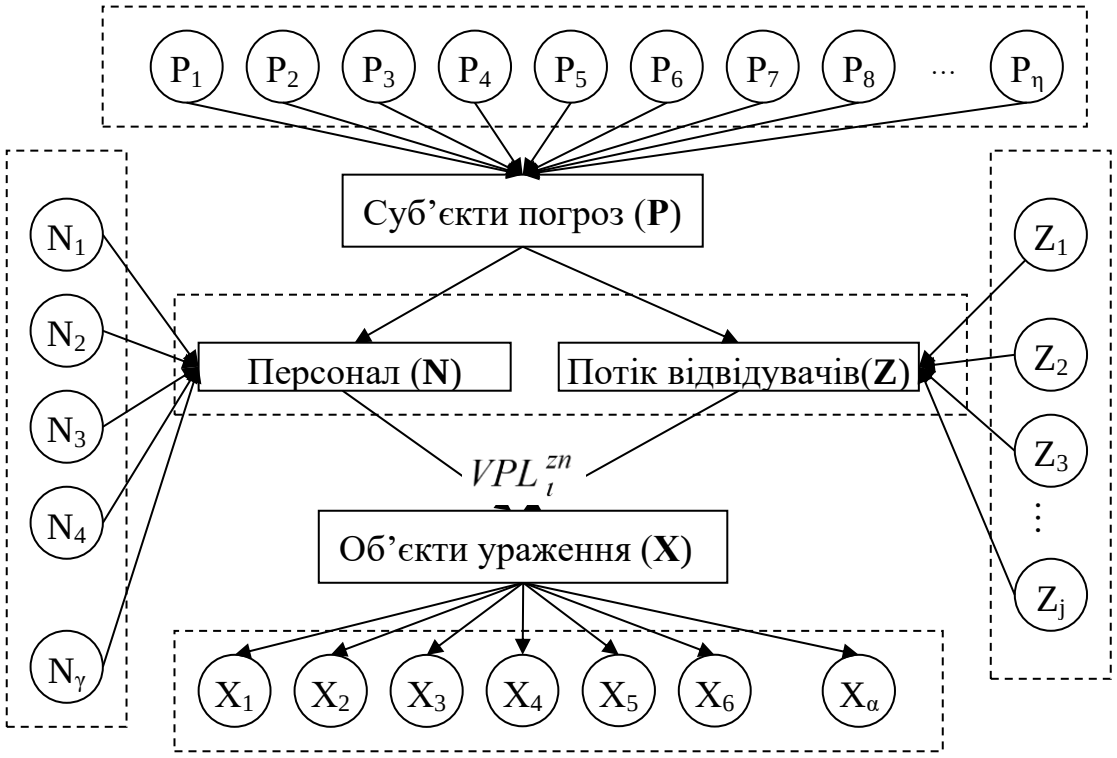

Рисунок 1.1. Модель прояву суб'єктів погроз виникнення НС на території аеропорту

Виходячи з рис. 1.1, маємо відкрите класифікаційне угрупування суб'єктів погроз, представлене у вигляді об'єднання множин потенційних учасників (реалізаторів) погроз виникнення загроз безпеки:

$$\mathbf{P} = \mathbf{N} \bigcup \mathbf{Z} = (N \setminus Z) \vee (Z \setminus N) \vee (Z \wedge N) \quad (1)$$

Таким чином, визначено джерела небезпеки у вигляді множини суб'єктів погроз (P), які можуть реалізувати свої погрози через потік відвідувачів (клієнтів, контрагентів) (Z) або (та) персонал (N), які, в свою чергу, можуть здійснити дії (впливи) на об'єкти ураження та спровокувати виникнення загрози кібервтручання. Неважливо, чи є у вашої системи зв'язок із зовнішнім світом, і чи є зовнішній захист, **але захист від внутрішніх порушників повинен бути обов'язково**.

Враховуючи той факт, що кожна організація має свою специфіку діяльності, не може існувати єдиної моделі порушника. Тому, при розробці заходів безпеки необхідно розглядати всі можливі для даної організації категорії порушників, яких можна класифікувати наступним чином, таблиця 1.1:

Таблиця 1.1. Класифікація порушників

Зовнішні порушники	Внутрішні порушники
Конкуренти	Системні адміністратори
Клієнти, контрагенти	Співробітники IT-відділу
Відвідувачі	Користувачі (оператори) системи
Хакери	Керівний склад організації
Злочинні організації	Технічний персонал
Звільнені співробітники	Співробітники служб безпеки

При створенні моделі порушника й оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників по їх можливостям доступу до системи і, отже, по потенційному збитку від кожної категорії користувачів. Наприклад, оператор або програміст ІС може завдати незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал.

Таким чином, кожен користувач у відповідності зі своєю категорією ризику може завдати більший або менший збиток системі. Крім того, необхідно враховувати, що користувачі різних категорій розрізняються не тільки за ступенем ризику, а й по тому, якого елементу системи вони загрожують найбільше. В результаті можна *оцінити ступінь ризику даної категорії користувачів щодо даного елемента системи* і представити результати аналізу у вигляді таблиці відповідностей.

Одним з варіантів градації ризику може бути наступний [1,2]:

- Найбільший ризик - 5
- Підвищений ризик - 4
- Середній ризик - 3

- Обмежений ризик - 2
- Низький ризик - 1
- Немає загрози – 0

Нижче наводиться таблиця 1.2, в рядках якої перераховані що наведені вище категорії користувачів, а в стовпцях – найбільш вразливі елементи системи. Таблиця показує, який ступінь ризику даної категорії користувачів щодо даного елемента систем.

Таблиця 1.2. Ступінь ризику для різних категорій користувачів

	Елементи АС																	
	I			**II**			**III**			**IV**			**V**			**VI**		
Види збитків Категорії користувачів	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C
Інженер системних магнітних носіїв											4	4		3	3		3	3
Користувач-операціоніст	2	2	2		1	1				2	2	2		1	1			
Оператор системи	1	5	5		5	5		5	5	1	3	3						
Оператор периферійного обладнання											3	3		4	4		1	1
Оператор завдань											3	3		4	4			
Оператор вводу та підготовки даних	3	3	3		4	4		5	5	3	3	3		4	4		1	5
Менеджер обробки	1	5	5		5	5		5	5	1	3	3		4	4		1	5
Адміністратор баз даних	3	3	3							3	3	3						
Системний програміст		5	5		5	5	5	5	5							5	1	5
Прикладний програміст	1	1	1	2	2	2							2	2	2			
Користувач- програміст	1	1	1	2	2	2							2	2	2			
Менеджер програмного забезпечення	1	1	1	4	4	4							4	4	4			
Інженер/оператор по зв’язку		5	5															
Інженер системи							2	2	2									
Адміністратор безпеки	5	5	5	5	5	5	5	5	5	3	3	3	4	4	4	5	5	5
Системний адміністратор	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Уразливі компоненти системи:

I - внутрішні дані

II - внутрішні прикладні програми

III - внутрішні системні модулі

IV - зовнішні дані

V - зовнішні системні модулі

VI - елементи комп'ютера та ін апаратура.

Види загроз:

A - модифікація,

B - знищення,

C - компрометація (розкриття) інформації.

Як видно з таблиці, різні категорії користувачів можуть по-різному впливати на різні частини ІТС. Ці тонкощі корисно враховувати як при проектуванні системи, так і при її експлуатації.

Далі кожну групу ймовірних порушників необхідно проаналізувати окремо за наступними параметрами:

- Дані необхідні порушнику і період їх актуальності;
- Технічна оснащеність і використовувані для вчинення порушення методи та засоби;
- Передбачувані місця і час здійснення незаконних дій порушника;
- Обмеження і припущення про характер можливих дій;
- Кількісна оцінка часу, який порушник може витратити для подолання захисту (рисунок 1.2).

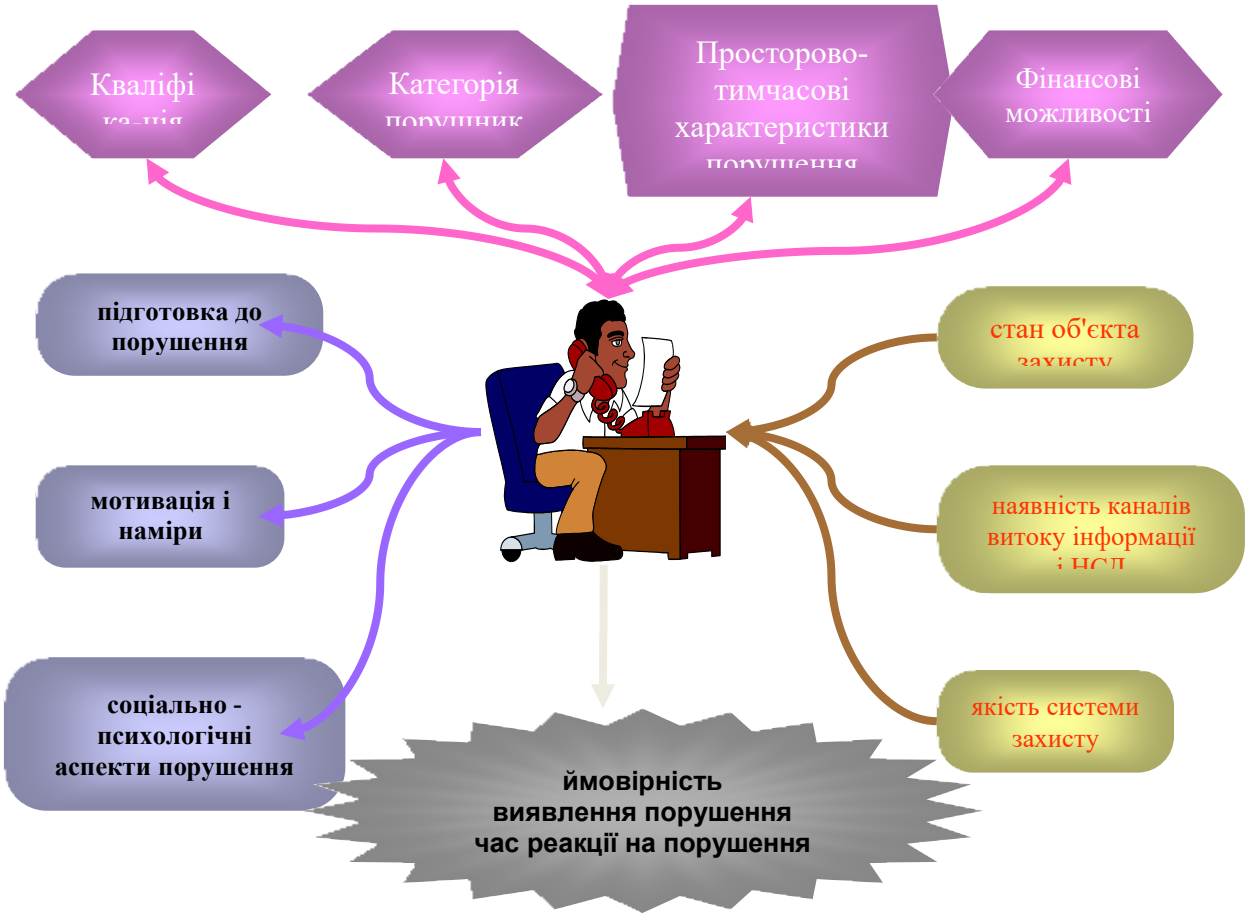

Рисунок 1.2. Схематична модель дій порушника

За технічної оснащеності та методами і засобами, що використовуються, порушники поділяються на тих, що:

- застосовують пасивні засоби (засоби перехоплення без модифікації компонентів системи);

- використовують тільки штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів);

- застосовують методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

Наведена класифікація передбачає, перш за все, знання і постійне їх поповнення про характеристики технічних і програмних засобів ведення розвідки і забезпечення доступу до інформації.

Незаконні дії порушник може здійснювати:

- *В різний час* (в процесі функціонування ІС, під час роботи компонентів системи, під час планових перерв у роботі ІС, в неробочий час, в перерви для обслуговування і ремонту і т.п.);

- *З різних місць* (за меж контрольованої зони ІС; всередині контрольованої зони ІС, але без доступу в виділені для розміщення компонентів ІС приміщення; всередині виділених приміщень, але без доступу до технічних засобів ІС; з доступом до технічних засобів ІС і з робочих місць кінцевих користувачів; з доступом в зону даних, архівів тощо; з доступом в зону управління засобами забезпечення безпеки ІС).

Облік місця і часу дій зловмисника також дозволить конкретизувати його можливості по доступу до інформаційних ресурсів і врахувати їх для підвищення якості системи захисту інформації.

Визначення значень можливих характеристик порушників в значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду.

Для того, щоб розроблена модель порушника приносила користь у вирішенні проблем інформаційної безпеки, а не була простою формальністю, вона повинна бути строго адаптована до конкретного об'єкта інформаційної захисту. Крім того, кожен блок моделі порушника повинен мати продовження як у вигляді причинно-наслідкових зв'язків між окремими блоками, так і у вигляді деталізації інформації, що міститься в кожному блоці. Така деталізація передбачає побудову ланцюжків передбачуваних наслідків настання тих чи

інших висновків щодо вигляду порушника.

Наявність сукупності моделей дій порушника може бути корисною з точки зору прогнозування можливих подій у всьому розмаїтті ситуацій, що складаються, запобігання дій порушника, побудови надійної системи захисту інформації, використання сучасних засобів інтелектуальної підтримки для управління системою захисту.

Серед обмеження і припущення про характер дій можливих порушників можуть бути наступні:

- робота з підбору кадрів та спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об’єднання (змови) і цілеспрямованих дій щодо подолання підсистеми захисту двох і більше порушників;

- порушник, плануючи спроби НСД, приховує свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, що експлуатує та обслуговуючого персоналу, а також недоліків прийнятої технології обробки інформації і т.д.

Один зі спрощених варіантів табличного оформлення моделі порушника наведено Таблиці 1.3-1.10 [4, стор.31-34]. Для побудови даної моделі використовується 4-х бальна шкала оцінювання

Таблиця 1.3. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Побудова причинно - наслідкових зв’язків між елементами моделі і ланцюжків передбачуваних наслідків вимагає знань в області соціально-

психологічних аспектів діяльності порушника, в галузі техніки промислового шпигунства, можливостей засобів інформаційного захисту та цілого ряду інших, нерозривно пов'язаних з проблемою захисту інформації.

Таблиця 1.4. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 1.5. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 1.6. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.7. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 1.8. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Далі виводимо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Зведемо все у таблицю 1.9.

Таблиця 1.9. Сумарна рівень загроз дляокремих категорій порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
прибиральник	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	

Продовження таблиці 1.9

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
електрик	ПВ1	М1	К1	З1	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	20
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	З1	Ч4	Д3	12
	2	1	2	1	4	2	
	ПЗ4	М4	К4	З4	Ч4	Д3	22
	4	4	4	4	4	2	
юрист	ПВ3	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З4	Ч3	Д2	21
	4	4	4	4	3	2	
адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	24
	4	4	4	4	4	4	
працівник служби безпеки	ПВ5	М1	К1	З1	Ч4	Д3	14
	4	1	1	1	4	3	
	ПЗ4	М4	К4	З4	Ч4	Д3	23
	4	4	4	4	4	3	

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну «Модель внутрішнього порушника політики безпеки інформації», таблиця 1.10.

Таблиця 1.10. Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Служба безпеки	М1	К1	З1	Ч4	Д3	14
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	17
Користувач	М1	К2	З1	Ч3	Д2	11
Технік ІТС	М1	К2	З1	Ч4	Д3	12
Електрик	М1	К1	З1	Ч1	Д1	8
Прибиральник	М1	К1	З1	Ч4	Д1	9

Аналіз останньої таблиці показує, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Таким чином представлено побудову моделі порушника та досліджено її особливості формування.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Провести вибір об’єкту захисту та представити короткий опис діяльності.
3. Визначити організаційну структуру об’єкту дослідження та представити її у звіті.
4. Провести оцінку ступеня ризику для різних категорій користувачів відносно елементу системи відповідно до таблиці 1.2.
5. Побудувати модель порушника відповідно до наведених таблиць 1.3-1.10 для вибраного об’єкту дослідження.
6. Зробити висновки та оформити звіт.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть основні типи та мотивацію порушень концепції безпеки підприємства.
2. Які категорії порушників Ви знаєте?
3. Назвіть типи конфліктів, які можуть виникати в організації?
4. Назвіть категорії порушників, які є потенційно небезпечними.
5. Назвіть основні заходи та методи захисту інформації від НСД.
6. Яким чином, на вашу думку, можна заохотити персонал до якісного виконання професійних обов’язків?
7. Якою є мотивація до роботи для Вас особисто?
8. Які наслідки можуть бути від розголошення інформації для організації?
9. Які наслідки розголошення інформації можуть бути для працівника?
10. Перерахуйте засоби та технології захисту інформації в кібернетичному просторі, які Ви знаєте?

Практичне заняття №2
МЕТОДИ КІБЕРЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Мета - здобуття практичних навиків захисту інформації від несанкціонованого доступу шляхом накладання паролів на документи, створених засобами Microsoft Office, архівних документів.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Методи та засоби накладання паролів на офісні документи Microsoft Office.

1.1. Методи та засоби накладання паролів на документи текстового редактора Microsoft Word

Для захисту текстових документів створених засобами Microsoft Word використовується наступна послідовність дій:

1. Пуск→Програми→ Microsoft Office→ Microsoft Word, рисунок 2.1.

Рисунок 2.1. Іконка для запуску Microsoft Word

2. Створюємо будь-який документ (може містити фразу, малюнок, таблицю), рисунок 2.2, та зберігаємо його під наступною назвою: **номер групи_Прізвище студента**. Наприклад, КБ_21_1_Лобанчикова.

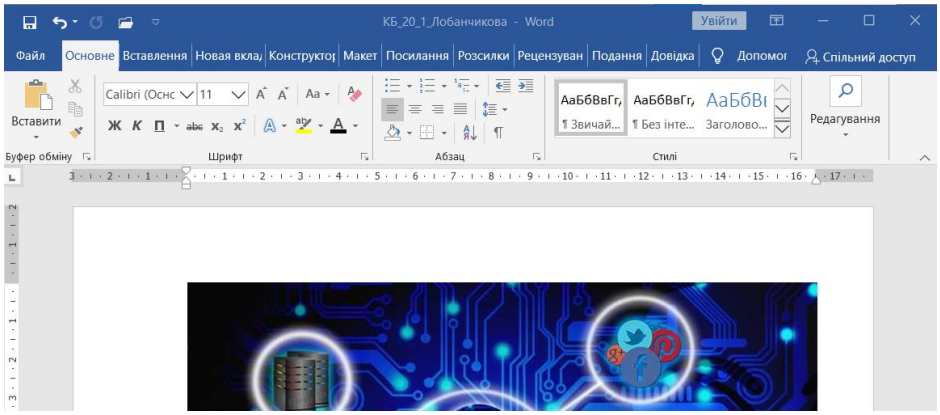

Рисунок 2.2. Вигляд документу

3. Відкриваємо: Рецензування→Захист.

Я видно з вікна, що представлено на рисунку 2.3-2.5 пропонується декілька варіантів використання параметрів безпеки.

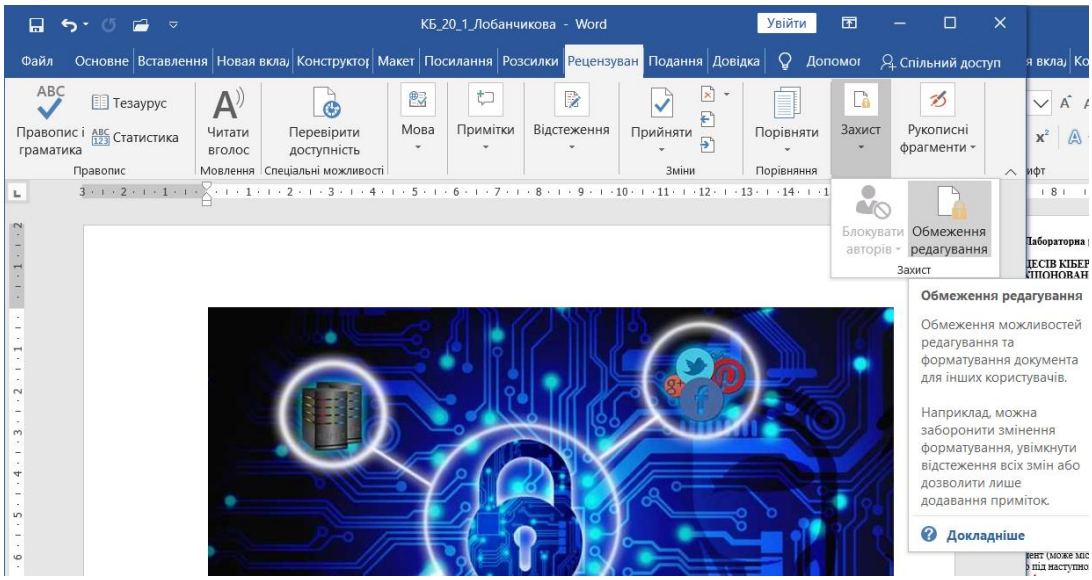

Рисунок 2.3. Обмеження редагування

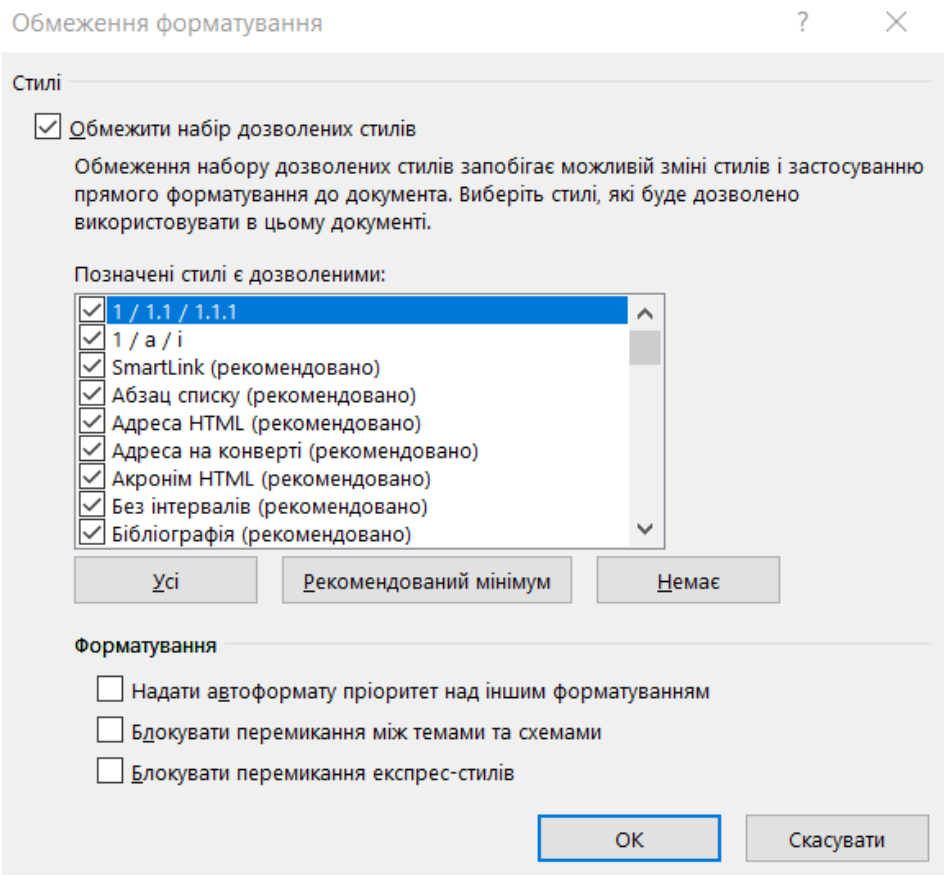

Рисунок 2.4. Обмеження форматування

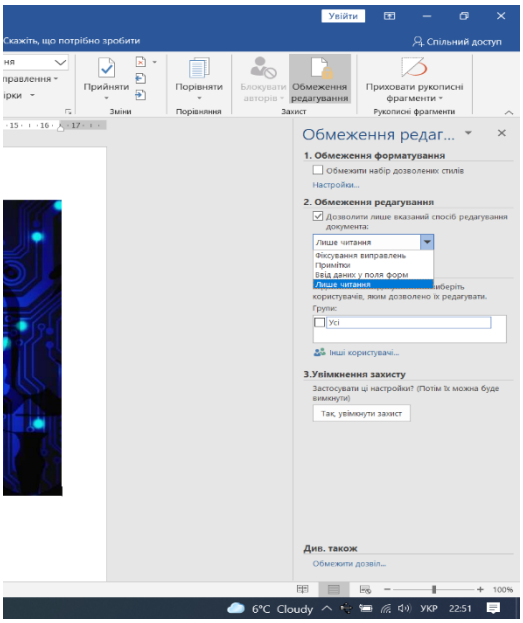

Рисунок 2.5. Обмеження редагування

2. Встановлення паролю

Рецензування → Захист →3. Увімкнення захисту →Так, увімкнути захист, рисунок 2.6.

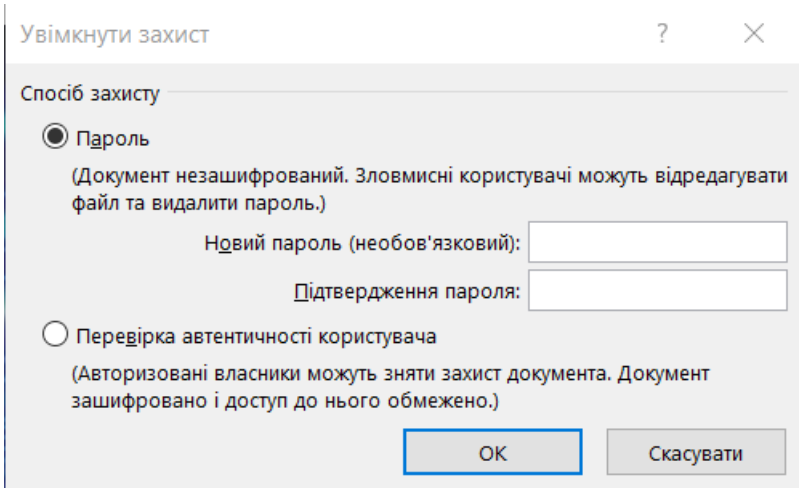

Рисунок 2.6. Вікно для встановлення паролю

Другий варіант: Для того, щоб встановити пароль, необхідно виконати наступні дії (рисунок 2.7):

1. Вибрати команду *Файл → Зберегти як… і* у вікні, що відкрилося вибрати команду *Сервіс → Загальні параметри,* рисунок 2.7.

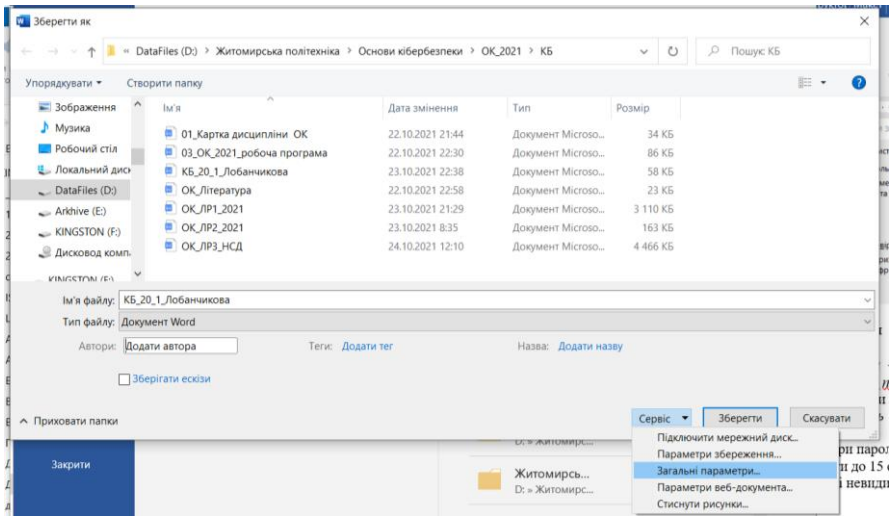

Рисунок 2.7. Вікно переходу до налаштування загальних параметрів

У нижній частині вкладки *Збереження* знаходяться поля введення: *Пароль для відкриття файлу, Пароль дозволу запису* і прапорець *Рекомендувати доступ тільки для читання*, рисунок 2.8

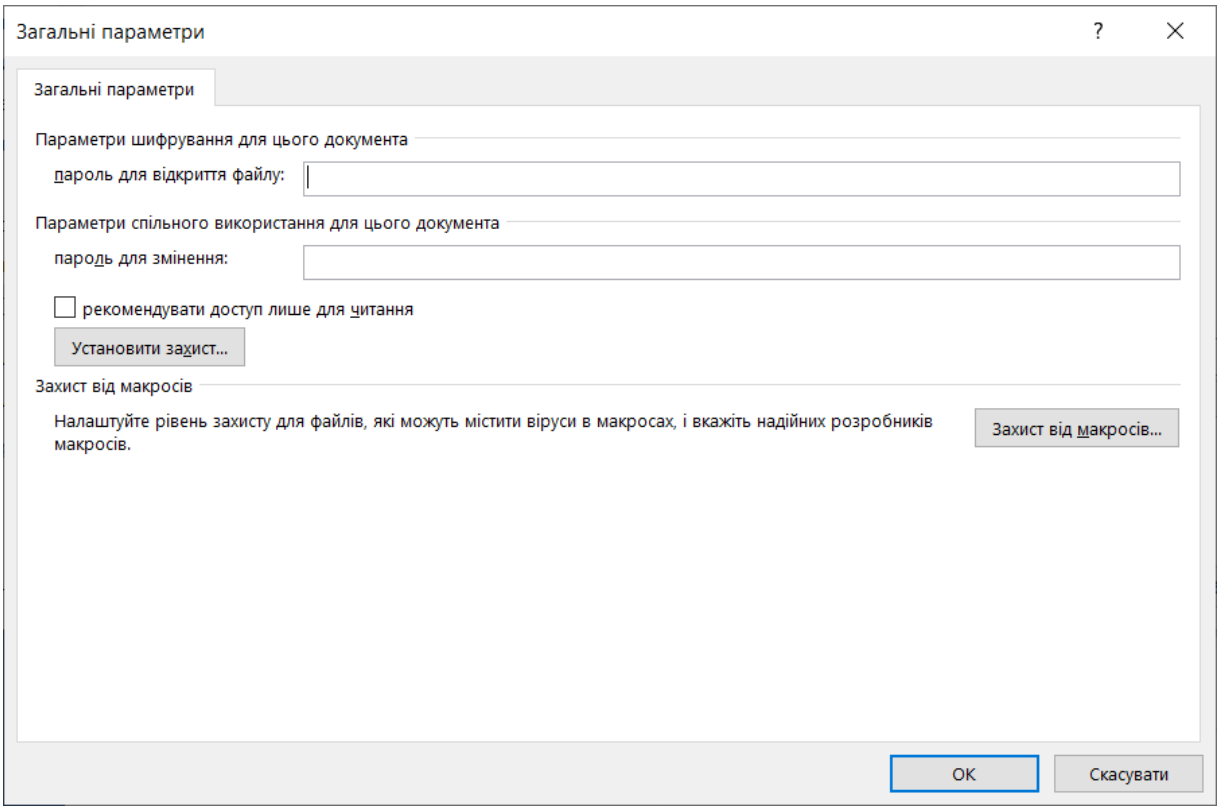

Рисунок 2.8. Вікно налаштувань загальних параметрів

2. Ввести з клавіатури пароль.

Пароль може містити до 15 символів, включаючи букви, цифри, значки і пропуски. Пароль в цьому полі невидимий (головне, його запам'ятати).

3. Натиснути *ОК*. З'явиться вікно діалогу *Підтвердження пароля*.

4. Повторно ввести пароль і знову натиснути *ОК*.

5. Зберегти документ із внесеними змінами, натиснувши клавішу *Сохранить*.

3. Шифрування документів

У відкритому документі послідовно виберіть елементи *Файл* → *Відомості* → *Захист документа*, рисунок 2.9.

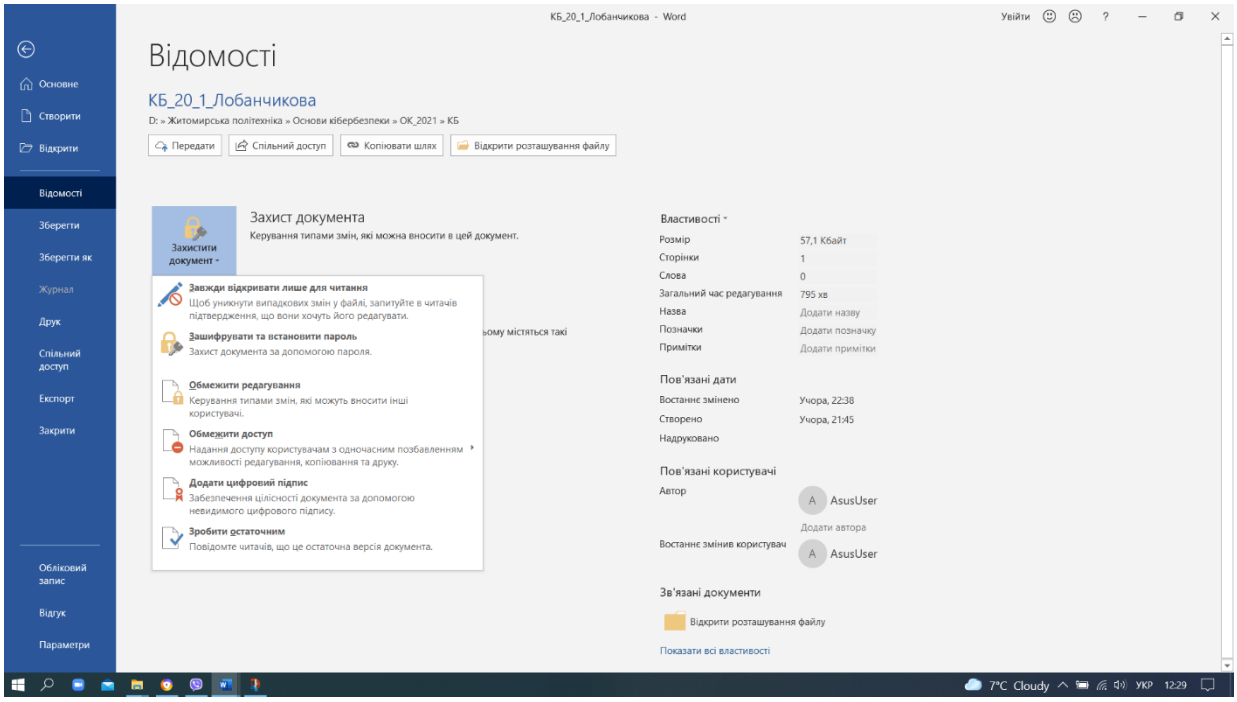

Рисунок 2.9. Вікно з параметрами захисту документу

Відобразяться такі параметри:

Завжди відкривати лише для читання. Встановлення даного параментру дозволяє уникнути випадкових змін у файлі, шляхом запиту у читача підтвердження внесених змін.

Зашифрувати та встановити пароль. Відбувається процедура шифрування файлу із встановленням паролю. У разі вибору параметра *Шифрувати паролем* відображається діалогове вікно *Зашифрувати документ*. У полі *Пароль* введіть пароль. Увага! Корпорація Майкрософт не може відновити втрачені або забуті паролі, тому зберігайте список паролів і відповідних імен файлів у безпечному місці.

Обмежити редагування. Керування типами змін, які можна внести в документ. Якщо вибрати команду *Обмежити редагування*, відобразиться три

параметри. *Обмеження форматування* Завдяки цьому обмежуються параметри форматування та зберігається зовнішній вигляд. Щоб вибрати, які стилі дозволено, виберіть елемент *Налаштування*. *Обмеження редагування*. Можна контролювати, як можна редагувати файл або вимкнути редагування. Щоб керувати тим, хто може редагувати, виберіть елемент Винятки або Інші користувачі.

Увімкнення захисту. Щоб вибрати захист паролем або автентифікація користувача, виберіть команду *Так, увімкнути захист*. Щоб додати або видалити редакторів з обмеженими дозволами, можна також вибрати команду *Обмежити дозвіл*. *Обмежити дозвіл за користувачем*. Використання ідентифікатора Windows Live ID для обмеження дозволів. Щоб обмежити дозволи, використовуйте ідентифікатор Windows Live ID або обліковий запис Microsoft Windows. Дозволи можна застосовувати через шаблон, який використовується в організації або можна додати дозволи вибравши команду

Обмежити доступ. Докладні відомості про керування правами доступу до інформації див. у статті Керування правами доступу до інформації в системі Office.

Додати цифровий підпис. Додавання видимого або невидимого цифрового підпису. Цифрові підписи дають змогу автентифікувати цифрові відомості, зокрема документи, повідомлення електронної пошти й макроси, за допомогою комп’ютерної криптографії. Цифрові підписи створюються шляхом введення підпису або додавання зображення підпису, щоб установити автентичність, цілісність і неможливість зречення.

Зробити остаточним. Перетворення документа лише для читання з повідомлення читачів про те, що документ є остаточним. Коли документ позначається як остаточний, функція введення тексту, команди редагування та перевірки правопису вимикаються, а документ стає доступний лише для читання. За допомогою команди *Позначити як остаточний* можна повідомити, що надається доступ до остаточної версії документа. Вона також допомагає уникнути внесення випадкових змін у документ редакторами або читачами.

3.2. Методи та засоби накладання паролів на документи програми обробки електронних таблиць Microsoft Excel

Для захисту документів, створених засобами Microsoft Excel виконується наступна послідовність дій:

1. Запускаємо програму обробки електронних таблиць Microsoft Excel.

2. Створюємо будь-яку таблицю (може містити особисті наді, форми звітності, рейтинг студентів, тощо) та зберігаємо її під наступною назвою: **номер групи_Прізвище студента**. Наприклад, КБ_20_1_Лобанчикова.

3. Для того, щоб встановити пароль, необхідно виконати наступні дії (рисунок 2.7):

1. Вибрати команду *Файл → Зберегти як… і* у вікні, що відкрилося вибрати команду *Сервіс → Загальні параметри*.

У нижній частині вкладки *Збереження* знаходяться поля введення: *Пароль для відкриття файлу, Пароль для зміни* і прапорець *Рекомендувати доступ тільки для читання* та *Завжди створювати резервну копію*.

2. Ввести з клавіатури пароль, рисунок 2.10.

Пароль може містити до 15 символів, включаючи букви, цифри, значки і пропуски. Пароль в цьому полі невидимий (головне, його запам'ятати).

3. Натиснути *ОК*. З'явиться вікно діалогу *Підтвердження пароля*.

4. Повторно ввести пароль і знову натиснути *ОК*.

5. Зберегти документ із внесеними змінами, натиснувши клавішу *Зберегти.*

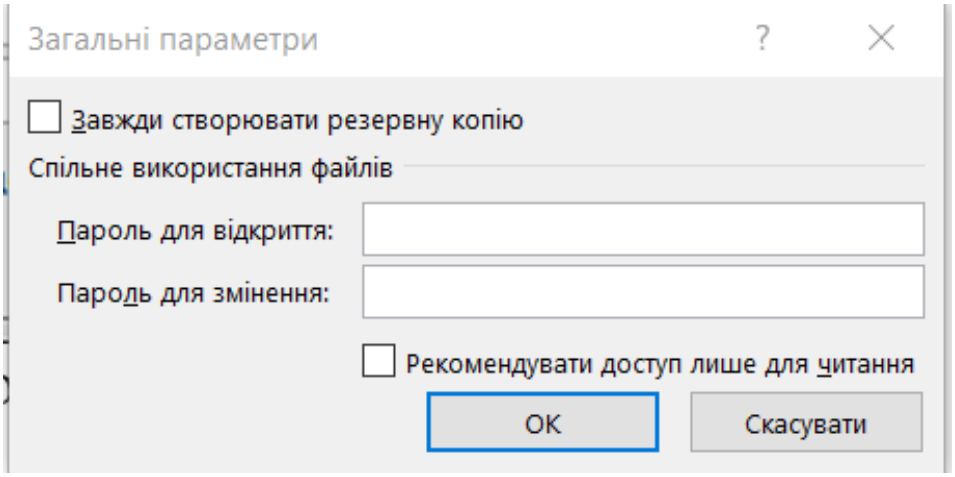

Рисунок 2.10. Вікно накладання паролю

Додатковими параметрами є встановлення паролю на відкриття документів на дозвіл запису.

4. Захист аркуша Excel

На відкритому аркуші послідовно виберіть елементи *Файл → Відомості → Захист книги*, рисунок 2.9.

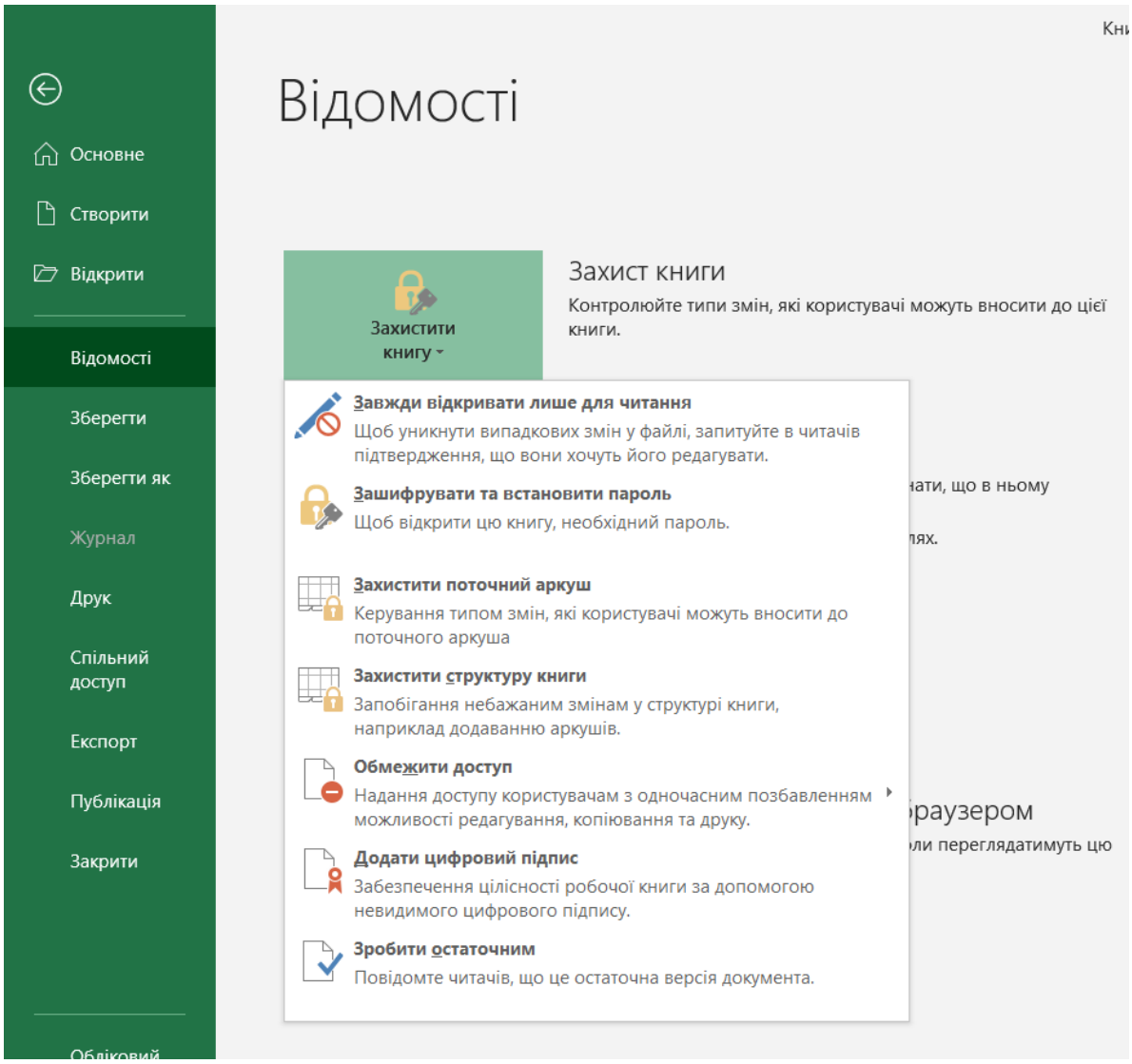

Рисунок 2.11. Вікно встановлення параметрів захисту на Excel документи

Відобразяться такі параметри, рис. 2.11, що ідентичні до Word, однак є відмінності у застосуванні, зокрема захистити можна поточний аркуш або захистити структуру книги.

1.3. Методи та засоби накладання паролів на відкриття архівних документів.

Для дослідження процедури захисту архівних документів від відкриття при їх пересиланні засобами електронної пошти та Інтернет необхідно:

1. Вибрати будь-яких документ та запустити програму створення архівів, рисунок 2.12:

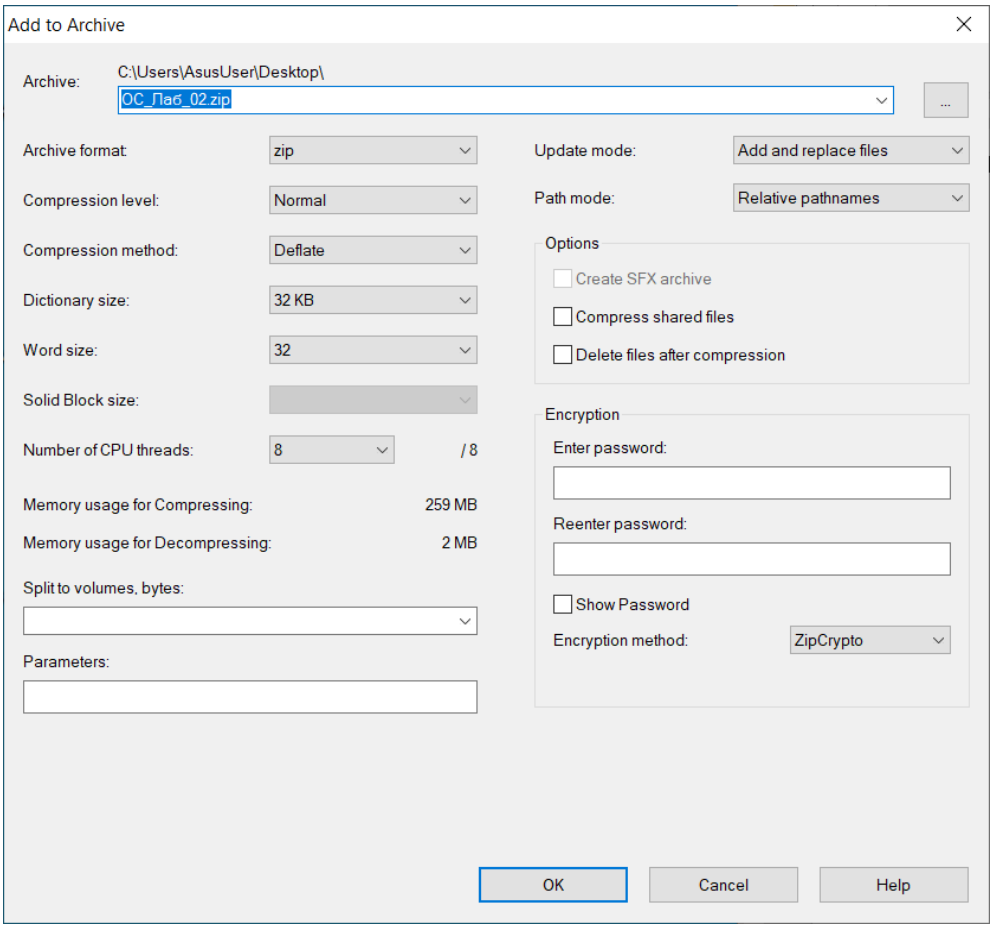

Рисунок 2.12. Вікно накладання паролів на архів

2. Далі, зазвичай вибирається метод стиснення даних, обмеження розміру (при необхідності). Праворуч міститься розділ вікна Encryption, де можна ввести ароль на шифрування, його підтвердження та вибрати метод шифрування: ZipCrypto або AES-256.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.

2. Створити документи Word (може містити фразу, малюнок, таблицю), рисунок 2.2, та зберігаємо його під наступною назвою: **номер групи_Прізвище студента**. Наприклад, КБ_21_1_Лобанчикова.

3. Дослідити процедуру «обмеження на форматування», рисунок 2.4, «обмеження на редагування», рисунок 2.5. Представити у звіті послідовність процедур та описати значення параметрів.

4. Дослідити процедуру встановлення паролю на відкриття документів, процедуру встановлення паролю на дозвіл запису, параметри налаштування захисту конфіденційності інформації та захисту від макросів. Представити у звіті

послідовність процедур та описати значення параметрів. Визначити поняття «макросу» та необхідності захисту від макросів (рисунок 2.7-2.8).

5. Дослідити процедуру «позначити як остаточний», «шифрування паролем», «обмежити редагування», «обмежити форматування», «обмеження редагування». Представити у звіті послідовність процедур та описати значення параметрів. Визначити поняття «цифровий підпис».

6. Створити документи засобами Microsoft Excel (може містити фразу, діаграму, таблицю) та зберігаємо його під наступною назвою: **номер групи_Прізвище студента**. Наприклад, КБ_21_1_Лобанчикова.

7. Дослідити процедуру встановлення паролю на відкриття документів Microsoft Excel, процедуру встановлення паролю на дозвіл запису. Представити у звіті послідовність процедур та описати значення параметрів.

8. Провести дослідження процедури кожного виду захисту, рисунок 2.11, навести у звіті порядок виконання операції та представити результати роботи в вигляді скріншотів та коротких нотацій.

9. Аналогічним чином провести дослідження методів та засобів захисту документів, створених за допомогою програми PowerPoint, Access. Представити скіншоти послідовності операцій та результатів ваших дій. Коротко описати процедури та параметри захисту документів у різних програмах.

10. Вибрати будь-який доступний документ, запустити процедуру архівування, встановити пароль на відкриття документу та перевірити його дію. Навести скріншоти виконання операції.

11. Всі результати проведених досліджень представити викладачу у порядку їх виконання. Зі створених файлів сформувати архів (без паролю) та надіслати викладачу разом зі звітом.

12. Підготувати звіт в установленому порядку. Всі результати проведених дій та операцій в звіті відобразити у вигляді скріншотів та нотацій.

КОНТРОЛЬНІ ПИТАННЯ

1. Які особливості захисту документів *Microsoft Office*?
2. Які недоліки розглянутих методів захисту інформації?
3. Для яких документів варто використовувати такі методи захисту?
4. Які вимоги до паролю ви вважаєте достатніми для захисту документів?
5. За допомогою яких програм можна спробувати зламати встановлений таким чином пароль?

Практичне заняття №3
ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Мета – здобуття практичних навичок шифрування текстової інформації із використанням криптографічного шифру гамування

ТЕОРЕТИЧНІ ВІДОМОСТІ

Перетворення відкритого тексту часто виконується за допомогою обчислень, що здійснюються над літерами алфавіту, яким попередньо присвоєні деякі числові значення. Наприклад [2,3], літери алфавіту нумеруються з нуля, а їх числові значення збігаються з цими номерами. Для латинського алфавіту літері A можна приписати значення 0, літері B – значення 1, літері C – значення 2 і так далі до літери Z, якій приписується значення, що рівне 25. Для того, щоб скласти літери B і D складемо їх числові значення: 1 + 3 = 4. Розглянемо суму як числове значення деякої літери латинського алфавіту. Легко бачити, що такою літерою є літера E. Вважаємо тому: $B + D = E$. При додаванні літери Z з літерою C числове значення дорівнює 27 і, мабуть, не відповідає жодній літері алфавіту. В таких випадках вважають, що в алфавіті за літерою Z йде літера A, потім B і т. д. У другому алфавіті літері A приписане числове значення рівне 26, літері B – 27 і так до літери Z. Потім йде третій алфавіт, четвертий алфавіт і так далі необхідну кількість разів. Таким чином, можна додавати кілька букв в одному виразі, виконувати множення букв або множити літери на константи. В даному випадку: $Z + C = B$. Зазначені дії над числовими значеннями букв відповідають операціям, виконуваним над числами за модулем m, де модуль дорівнює кількості знаків в алфавіті.

Часто величину m називають модулем алфавіту. Під час виконання модульних операцій однаковим літерам, які знаходяться в різних, послідовно записаних алфавітах повинні відповідати однакові числові значення. Наприклад, значення 1, 27, 53 задають ту саму букву B і вони, у цьому розумінні, еквівалентні. Неважко бачити, що ці числа відрізняються на величину, кратну m, тобто мають один і той же залишок під час ділення на модуль алфавіту. Такі числа називаються порівняними за модулем m, що записується у вигляді так званих порівнянь: $a = b(\text{mod } m)$, тобто $1 = 27(\text{mod } 26)$, або $1 = 27(26)$. При переході до порівнянь, числові значення і модуль алфавіту маються на увазі, а самі порівняння часто записуються як рівності: $Z + C = B$, замість $Z + C = B(\text{mod } 26)$.

Для отримання шифрованого тексту S існує три способи накладання гами Г

на відкритий текст *O:* додавання гами і тексту *S* = Г + *O,* віднімання гами з тексту *S* = *O* – Г і віднімання тексту з гами *S* = *Г* – *O*. Під операціями додавання і віднімання розуміються як звичайні операції за модулем *m,* так і застосування замість них відповідних таблиць. Процедура розшифрування, очевидно, будується природним чином, використовуючи обернені перетворення *O* = *S* — Г, *O* = *S* + Г, *O* = *Г* – *S* або обернені таблиці, відповідно.

3.1.Створення ключа

Для шифрування методом гамування необхідно визначити алфавіт, на основі якого будуть створюватись повідомлення та ключ. Також кожному символу треба надати послідовний номер (код), який буде використовуватись при гамування, таблиця 3.1.

Таблиця 3.1.Таблиця кодування символів

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

У якості основи гами (ключ) зручно обрати ***слово-гасло***. Нехай це буде ***«amusement»***. Сама гама має довжину відкритого повідомлення і складається із повторення гасла [2].

3.2. Шифрування

Необхідно зашифрувати наступний відкритий текст:

«Unix is user-friendly. It's just very selective about who its friends are».

Приводимо даний текст до канонічного вигляду, тобто відкидаємо усі символи, що відсутні в означеному алфавіті. Отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Складаємо таблицю із трьох рядків. Перший ряд О містить відкрите повідомлення, другий Г – гаму, третій S – шифрований текст.

За умовою завдання гамування необхідно здійснити за формулою 3.1.

$$S = Г - O(\text{mod } 26). \quad (3.1)$$

Це означає, що для отримання поточного символу шифротексту треба від коду відповідного символу гами відняти код відповідного символу відкритого тексту.

Таким чином перший символ гами «a», що має код 0, відняти по модулю 26 перший символ відкритого тексту «u» із кодом 20 дає у результаті код 6, тобто

символ «g» шифротексту. В результаті виконання усього процесу гамування отримуємо таблицю 3.2:

Таблиця 3.2. Шифрування відкритого тексту

O	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
Г	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
O	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	
Г	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	

Зашифроване повідомлення має такий вигляд:

gzmvwukvpjhdkazbcvstcjkulspjocoticulfiurqslrmmebazvwjgxuuba

3.3. Дешифрування

Дешифрування відбувається у зворотньому порядку за формулою 3.2.

$$O = Г - S(\text{mod } 26). \quad (3.2)$$

Так перший символ гами «a» (0) відняти по модулю 26 перший символ шифротексту «g» (6) буде 20, тобто «u», таблиця 3.3.

Таблиця 3.3. Дешифрування текстового повідомлення

S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
Г	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
O	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	
Г	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
O	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	

Після розшифрування отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

Для формування зашифрованого тексту використовуються наступні формули шифрування 3.3 – 3.5:

$$S=(O+ Г)\text{mod}N \quad (3.3)$$

Наприкла: N=26, O=14, Г=20. $S = (14 + 20)\text{mod}26 = 34\text{mod}26 = 8$;

N=26, O=14, Г=10. $S = (14 + 10)\text{mod}26 = 24\text{mod}26 = 24$.

$$S=(О – Г) \quad (3.4)$$

Наприклад: N=26, О=14, Г=20.

Якщо О< Г тоді S = (О+N)–Г = (14+26)-20 = 20;

N=26, О=14, Г=10. S = (14 - 10) = 4.

$$S = (Г – О) \quad (3.5)$$

Обчислення відбуваються аналогічно як у випадку з формулою 3.4.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Провести шифрування та розшифрування за допомогою криптографічного алгоритму гамування. Завдання до виконання представлено у таблиці 3.4. Варіант здобувачем вищої освіти вибирається відповідно до списку в журналі відвідування академічної групи.

Таблиця 3.4. Варіанти завдань до виконання

Варіант	Формула	Текст для шифрування
1.	S = (О + Г)modN	Вимоги безпеки до технологічного обладнання та процесів
2.	S = (О - Г)	Для створення шифрованого тексту на вихідний накладається гама.
3.	S = (Г - О)	Атака, що має на меті змусити сервер не відповідати на запити
4.	S = (О + Г)modN	Безліч людей розмовляють в масштабі реального часу шляхом набору повідомлень на клавіатурі
5.	S = (О - Г)	Сьогодні є чимало каналів просочування інформації з організації
6.	S = (Г - О)	У першій частині розглядаються загальні проблеми безпеки інформаційних систем
7.	S = (О + Г)modN	У другій частині увага приділяється методам та засобам можливого вирішення цих проблем
8.	S = (О - Г)	Роль інформації в сучасному світі та необхідність її захисту
9.	S = (Г - О)	Разом з поняттям інформація, важливе значення має поняття дані
10.	S = (О + Г)modN	Від інформації дані відділяються конкретною формою подань.
11.	S = (О - Г)	Інформація на стадії даних характеризується певною формою подання й додатковою характеристикою
12.	S = (Г - О)	Нематеріальність інформації полягає у тому, що не можна виміряти параметри відомими фізичними методами
13.	S = (О + Г)modN	Таким чином, інформація зберігається і передається на матеріальних носіях

Продовження таблиці 3.4

Варіант	Формула	Текст для шифрування
14.	S = (О - Г)	Все що є матеріальним об’єктом, інформацією бути не може
15.	S = (Г - О)	Інформація не може існувати сама по собі, у відриві від матеріального носія
16.	S = (О + Г)modN	Матерія ж не може не нести інформації, оскільки завжди перебуває в певному стані
17.	S = (О - Г)	Матеріальними носіями інформації можуть бути мозок людини, звукові та електромагнітні хвилі
18.	S = (Г - О)	Інформація, якщо вона міститься на матеріальному носієві, доступна людині.
19.	S = (О + Г)modN	Цінність інформації визначається мірою її корисності для власника
20.	S = (О - Г)	Якщо доступ до інформації обмежується, то така інформація є конфіденційною
21.	S = (Г - О)	Для позначення цінності конфіденційної комерційної інформації використовується категорія конфіденційно
22.	S = (О + Г)modN	Інформацію правочинно розглядати як товар, що має певну цінність
23.	S = (О - Г)	Кількість інформації тим більша, чим нижча ймовірність події
24.	S = (Г - О)	Підхід ентропії широко використовується при визначенні кількості інформації, переданої по каналах зв’язку
25.	S = (О + Г)modN	Тезарусний підхід заснований на розумінні інформації як знань
26.	S = (О - Г)	У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна зменшується
27.	S = (Г - О)	Проблеми захисту інформації непокоїли людство з давніх-давен

ЗАВДАННЯ НА САМОСТІЙНУ ПІДГОТОВКУ

Реалізувати програмно варіант завдання. Продемонструвати викладачу робочу програму та отримати додатково 3 бали в рейтинг-лист.

КОНТРОЛЬНІ ПИТАННЯ

1. Які недоліки притаманні моноалфавітним криптографічним алгоритмам?
2. У чому складність використання такого роду криптографічних алгоритмів?

Практичне заняття №4
МЕТОДИ НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ЗОБРАЖЕННЯ

Мета – здобуття практичних навичок нанесення цифрових водяних знаків у зображення просторовим методом LSB в інтегрованому середовищі розробки програмного забезпечення Microsoft Visual Studio.

ТЕОРЕТИЧНІ ВІДОМОСТІ

4.1. LSB (Least Significant Bit, найменший значущий біт)

Суть цього методу полягає в заміні останніх значущих бітів в контейнері (зображення, аудіо або відеозапису) на біти приховуваного повідомлення [2,5]. Різниця між порожнім і заповненим контейнерами має бути незначна для органів сприйняття людини.

Суть методу полягає в наступному: Нехай, є 8-бітове зображення в градаціях сірого. 00h (00000000b) означає чорний колір, FFh (11111111b) - білий. Всього є 256 градацій (2^8). Також припустимо, що повідомлення складається з 1 байта – наприклад, 01101011b. При використанні 2 молодших біт в описах пікселів, нам буде потрібно 4 пікселі. Допустимо, вони чорного кольору. Тоді пікселі, що містять приховане повідомлення, виглядатимуть таким чином: 00000001 00000010 00000010 00000011. Тоді колір пікселів зміниться: першого - на 1/255, другого і третього - на 2/255 і четвертого - на 3/255. Такі градації, мало того що непомітні для людини, можуть взагалі не відобразитися при використанні низькоякісних пристроїв виводу.

Головне вікно програми просторового алгоритму нанесення цифрових водяних знаків (LSB) на зображення наведено на рис. 4.1.

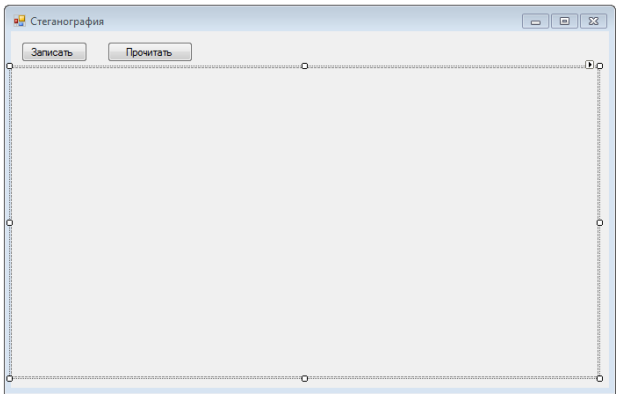

Рисунок 4.1. Головне вікно програми нанесення водяних знаків на зображення

Використаємо для шифрування/дешифрування bmp файл, який не містить палітру. У такому bmp файлі кожні 3 байти визначають 3 кольори пікселя.

Оскільки, ми працюватимемо з бітами інформації, а колір одного пікселя займає один байт, то буде потрібно методи перетворення байта в біти і навпаки, які представлені нище:

```
private BitArray ByteToBit(byte src) {
        BitArray bitArray = new BitArray(8);
        bool st = false;
        for (int i = 0; i < 8; i++)
        {
           if ((src >> i & 1) == 1) {
              st = true;
           } else st = false;
           bitArray[i] = st;
        }
        return bitArray;
    }
private byte BitToByte(BitArray scr) {
        byte num = 0;
        for (int i = 0; i < scr.Count; i++)
           if (scr[i] == true)
              num += (byte)Math.Pow(2, i);
        return num;
    }
```

Розташування в bmp інформації буде наступним:

– Піксель 0.0: ознака того, що у файлі є текстова інформація. Як ознака використовується символ /

– Пікселі 0.1 - 0.3: розмір текстової інформації, записаної у файл.

– Пікселі 0.4 і до кінця файлу: власне текстова інформація.

Спершу розглянемо код, що записує в піксель 0.0 ознака зашифрованого файлу.

```
byte [] Symbol = Encoding.GetEncoding(1251).GetBytes("/");
        BitArray ArrBeginSymbol = ByteToBit(Symbol[0]);
        Color curColor = bPic.GetPixel(0, 0);
        BitArray tempArray = ByteToBit(curColor.R);
        tempArray[0] = ArrBeginSymbol[0];
        tempArray[1] = ArrBeginSymbol[1];
        byte nR = BitToByte(tempArray);
        tempArray = ByteToBit(curColor.G);
        tempArray[0] = ArrBeginSymbol[2];
        tempArray[1] = ArrBeginSymbol[3];
        tempArray[2] = ArrBeginSymbol[4];
        byte nG = BitToByte(tempArray);

        tempArray = ByteToBit(curColor.B);
        tempArray[0] = ArrBeginSymbol[5];
        tempArray[1] = ArrBeginSymbol[6];
        tempArray[2] = ArrBeginSymbol[7];
        byte nB = BitToByte(tempArray);
```

```
Color nColor = Color.FromArgb(nR, nG, nB);
bPic.SetPixel(0, 0, nColor);
```

У коді в змінній Symbol зберігається код символу "/". Далі цей код перетвориться в масив біт (змінна ArrBeginSymbol). Колір пікселя 0.0 зберігається в змінній curColor. Далі кожна з трьох складових кольорів пікселя перетвориться в масив біт, потім в червоному кольорі замінюються молодші 2 біта на біти символу "/", в зеленому замінюються молодші 3 біта на біти символу "/" і в синьому так само замінюються молодші 3 біта кольору. З 3 нових отриманих кольорів створюється новий колір пікселя (nColor) і встановлюється замість попереднього кольору. Усе, ознака того, що у файлі є інформація записаний в bmp файл. Спосіб запису інформації, тобто 2 біта, 3 біта і 3 біта вибраний для зручності роботи, бо в один піксель записується відразу байт інформації.

Далі розглянемо метод перевірки ознаки, описаної вище

```
/*Перевіряє, чи зашифрований файл, повертає true, якщо символ в першому пиксилі рівний / інакше false */
private bool isEncryption(Bitmap scr)
    {
      byte[] rez = new byte[1];
      Color color = scr.GetPixel(0, 0);
      BitArray colorArray = ByteToBit(color.R); //отримуємо байт кольору і перетворюємо в масив біт
      BitArray messageArray = ByteToBit(color.R); ;//ініціалізуємо результуючий масив біт
      messageArray[0] = colorArray[0];
      messageArray[1] = colorArray[1];

      colorArray = ByteToBit(color.G);//отримуємо байт кольору і перетворюємо в масив біт
      messageArray[2] = colorArray[0];
      messageArray[3] = colorArray[1];
      messageArray[4] = colorArray[2];

      colorArray = ByteToBit(color.B);//отримуємо байт кольору і перетворюємо в масив біт
      messageArray[5] = colorArray[0];
      messageArray[6] = colorArray[1];
      messageArray[7] = colorArray[2];
      rez[0] = BitToByte(messageArray); //отримуємо байт символа, записаного в 1 пікселі
      string m = Encoding.GetEncoding(1251).GetString(rez);
      if (m == "/")
      {
        return true;
      }
      else return false;
    }
```

Метод аналогічний коду приведеному вище з точністю до навпаки. Якщо в пікселі 0.0 записаний символ "/", то функція повертає true, інакше - false.

Далі у файл записується розмір текстової інформації. Розглянемо метод

детальніше:

```
/*Записує кількість символів для шифрування в перші біти картинки */
      private void WriteCountText(int count, Bitmap src) {
         byte[] CountSymbols = Encoding.GetEncoding(1251).GetBytes(count.ToString());
         for (int i = 0; i < 3; i++)
         {
            BitArray bitCount = ByteToBit(CountSymbols[i]); //біти кількості символів
            Color pColor = src.GetPixel(0, i + 1); //1, 2, 3 пікселі
            BitArray bitsCurColor = ByteToBit(pColor.R); //біт кольорів поточного пікселя
            bitsCurColor[0] = bitCount[0];
            bitsCurColor[1] = bitCount[1];
            byte nR = BitToByte(bitsCurColor); //новий біт кольору пікселя

            bitsCurColor = ByteToBit(pColor.G);//біт кольорів поточного пікселя
            bitsCurColor[0] = bitCount[2];
            bitsCurColor[1] = bitCount[3];
            bitsCurColor[2] = bitCount[4];
            byte nG = BitToByte(bitsCurColor);//новий колір пікселя

            bitsCurColor = ByteToBit(pColor.B);//біт кольорів поточного пікселя
            bitsCurColor[0] = bitCount[5];
            bitsCurColor[1] = bitCount[6];
            bitsCurColor[2] = bitCount[7];
            byte nB = BitToByte(bitsCurColor);//новий колір пікселя

            Color nColor = Color.FromArgb(nR, nG, nB); //новий колір із отриманих бітів
            src.SetPixel(0, i + 1, nColor); //записали отриманий колір в картинку
         }
            }
```

У CountSymbols записується кількість символів початкового тексту. Кожна цифра займає один байт, тому максимальна довжина початкового тексту: 999 - 4 = 995 символів (4 - це один піксель на ознаку присутності інформації у файлі і три пікселі на розмір текстової інформації).

При необхідності можна збільшити, узявши пікселі не з 0.1 по 0.3, а з 0.1 по 0.4 наприклад, і так далі. У циклі for кожна цифра кількості початкового тексту перетвориться в масив біт і записується в молодші пікселі кольору за принципом, описаним вище.

Метод читання розміру текстової інформації :

```
/*Зчитує кількість символів для дешифрування з перших біт картинки*/
      private int ReadCountText(Bitmap src) {
         byte[] rez = new byte[3]; //масив на 3 елемента, тобто максимум 999 символів шифрується
         for (int i = 0; i < 3; i++)
         {
            Color color = src.GetPixel(0, i + 1); //колір 1, 2, 3 пікселів
            BitArray colorArray = ByteToBit(color.R); //біти кольору
```

```
            BitArray bitCount = ByteToBit(color.R); ; //ініціалізація результуючого масиву біт
            bitCount[0] = colorArray[0];
            bitCount[1] = colorArray[1];

            colorArray = ByteToBit(color.G);
            bitCount[2] = colorArray[0];
            bitCount[3] = colorArray[1];
            bitCount[4] = colorArray[2];

            colorArray = ByteToBit(color.B);
            bitCount[5] = colorArray[0];
            bitCount[6] = colorArray[1];
            bitCount[7] = colorArray[2];
            rez[i] = BitToByte(bitCount);
        }
        string m = Encoding.GetEncoding(1251).GetString(rez);
        return Convert.ToInt32(m, 10);
    }
```

4.2. Реалізація програми нанесення цифрових водяних знаків у зображення просторовим методом LSB

Приведемо код, який відкриває/закриває файл, перевіряє на помилки, та власне і записує інформацію у файл. Деякий код вже був приведений вище. Bitmap bPic - відкритий файл з картинкою.

```
/* Відкрити файл для шифрування */
    private void button1_Click(object sender, EventArgs e)
    {
        string FilePic;
        string FileText;
        OpenFileDialog dPic = new OpenFileDialog();
        dPic.Filter = "Файлы изображений (*.bmp)|*.bmp|Все файлы (*.*)|*.*";
        if (dPic.ShowDialog() == DialogResult.OK)
        {
            FilePic = dPic.FileName;
        }
        else
        {
            FilePic = "";
            return;
        }

        FileStream rFile;
        try
        {
            rFile = new FileStream(FilePic, FileMode.Open); //відкриваємо поток
        }
        catch (IOException)
        {
            MessageBox.Show("Ошибка открытия файла", "Ошибка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
```

```
            return;
        }
        Bitmap bPic = new Bitmap(rFile);

        OpenFileDialog dText = new OpenFileDialog();
        dText.Filter = "Текстовые файлы (*.txt)|*.txt|Все файлы (*.*)|*.*";
        if (dText.ShowDialog() == DialogResult.OK)
        {
            FileText = dText.FileName;
        }
        else
        {
            FileText = "";
            return;
        }

        FileStream rText;
        try
        {
            rText = new FileStream(FileText, FileMode.Open); //відкриваємо поток
        }
        catch (IOException)
        {
            MessageBox.Show("Ошибка открытия файла", "Ошибка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
            return;
        }
        BinaryReader bText = new BinaryReader(rText, Encoding.ASCII);

        List<byte> bList = new List<byte>();
        while (bText.PeekChar() != -1) { //зчитали увесь текстовий файл для шифрування в лист байт
            bList.Add(bText.ReadByte());
        }
        int CountText = bList.Count; // в CountText - кількість в байтах текста, який необхідно закодувати
        bText.Close();
        rFile.Close();

        //перевіримо, чи поміститься вихідний текст в картинці
        if (CountText > ((bPic.Width * bPic.Height)) - 4 ) {
            MessageBox.Show("Выбранная картинка мала для размещения выбранного текста", "Информация",
MessageBoxButtons.OK);
            return;
        }

        //перевіряємо, може бути картинка уже зашифрована
        if (isEncryption(bPic))
        {
            MessageBox.Show("Файл уже зашифрован", "Информация", MessageBoxButtons.OK);
            return;
        }

        byte [] Symbol = Encoding.GetEncoding(1251).GetBytes("/");
```

```
BitArray ArrBeginSymbol = ByteToBit(Symbol[0]);
Color curColor = bPic.GetPixel(0, 0);
BitArray tempArray = ByteToBit(curColor.R);
tempArray[0] = ArrBeginSymbol[0];
tempArray[1] = ArrBeginSymbol[1];
byte nR = BitToByte(tempArray);

tempArray = ByteToBit(curColor.G);
tempArray[0] = ArrBeginSymbol[2];
tempArray[1] = ArrBeginSymbol[3];
tempArray[2] = ArrBeginSymbol[4];
byte nG = BitToByte(tempArray);

tempArray = ByteToBit(curColor.B);
tempArray[0] = ArrBeginSymbol[5];
tempArray[1] = ArrBeginSymbol[6];
tempArray[2] = ArrBeginSymbol[7];
byte nB = BitToByte(tempArray);

Color nColor = Color.FromArgb(nR, nG, nB);
bPic.SetPixel(0, 0, nColor);
//тобто в першому пікселі буде символ /, який говорить про те, що картинка зашифрована

WriteCountText(CountText, bPic); //записуємо кількість символов для шифрування

int index = 0;
bool st = false;
for (int i = 4; i < bPic.Width; i++) {
   for (int j = 0; j < bPic.Height; j++) {
      Color pixelColor = bPic.GetPixel(i, j);
      if (index == bList.Count) {
         st = true;
         break;
      }
      BitArray colorArray = ByteToBit(pixelColor.R);
      BitArray messageArray = ByteToBit(bList[index]);
      colorArray[0] = messageArray[0]; //змінюємо
      colorArray[1] = messageArray[1]; // в нашому кольорі біти
      byte newR = BitToByte(colorArray);

      colorArray = ByteToBit(pixelColor.G);
      colorArray[0] = messageArray[2];
      colorArray[1] = messageArray[3];
      colorArray[2] = messageArray[4];
      byte newG = BitToByte(colorArray);

      colorArray = ByteToBit(pixelColor.B);
      colorArray[0] = messageArray[5];
      colorArray[1] = messageArray[6];
      colorArray[2] = messageArray[7];
      byte newB = BitToByte(colorArray);
```

```
            Color newColor = Color.FromArgb(newR, newG, newB);
            bPic.SetPixel(i, j, newColor);
            index ++;
          }
          if (st) {
            break;
          }
        }
        pictureBox1.Image = bPic;

        String sFilePic;
        SaveFileDialog dSavePic = new SaveFileDialog();
        dSavePic.Filter = "Файлы изображений (*.bmp)|*.bmp|Все файлы (*.*)|*.*";
        if (dSavePic.ShowDialog() == DialogResult.OK)
        {
          sFilePic = dSavePic.FileName;
        }
        else
        {
          sFilePic = "";
          return;
        };

        FileStream wFile;
        try
        {
          wFile = new FileStream(sFilePic, FileMode.Create); //відкриваємо поток на запис результату
        }
        catch (IOException)
        {
          MessageBox.Show("Ошибка открытия файла на запись", "Ошибка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
          return;
        }

        bPic.Save(wFile, System.Drawing.Imaging.ImageFormat.Bmp);
        wFile.Close(); //закриваємо поток
      }
```

Код, який прочитує інформацію з bmp файл наведено нижче.

```
/*Відкрити файл для дешифрування */
      private void button2_Click(object sender, EventArgs e)
      {
        string FilePic;
        OpenFileDialog dPic = new OpenFileDialog();
        dPic.Filter = "Файлы изображений (*.bmp)|*.bmp|Все файлы (*.*)|*.*";
        if (dPic.ShowDialog() == DialogResult.OK)
        {
          FilePic = dPic.FileName;
        }
        else
```

```
        {
            FilePic = "";
            return;
        }
        FileStream rFile;
        try
        {
            rFile = new FileStream(FilePic, FileMode.Open); //відкриваємо поток
        }
        catch (IOException)
        {
            MessageBox.Show("Ошибка открытия файла", "Ошибка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
            return;
        }
        Bitmap bPic = new Bitmap(rFile);
        if (!isEncryption(bPic)) {
            MessageBox.Show("В файле нет зашифрованной информации", "Информация",
MessageBoxButtons.OK);
            return;
        }
        int countSymbol = ReadCountText(bPic); //зчитуємо кількість зашифрованих сисмволів
        byte[] message = new byte[countSymbol];
        int index = 0;
        bool st = false;
        for (int i = 4; i < bPic.Width; i++) {
            for (int j = 0; j < bPic.Height; j++) {
                Color pixelColor = bPic.GetPixel(i, j);
                if (index == message.Length) {
                    st = true;
                    break;
                }
                BitArray colorArray = ByteToBit(pixelColor.R);
                BitArray messageArray = ByteToBit(pixelColor.R); ;
                messageArray[0] = colorArray[0];
                messageArray[1] = colorArray[1];
                colorArray = ByteToBit(pixelColor.G);
                messageArray[2] = colorArray[0];
                messageArray[3] = colorArray[1];
                messageArray[4] = colorArray[2];
                colorArray = ByteToBit(pixelColor.B);
                messageArray[5] = colorArray[0];
                messageArray[6] = colorArray[1];
                messageArray[7] = colorArray[2];
                message[index] = BitToByte(messageArray);
                index++;
            }
            if (st) {
                break;
            }
        }
        string strMessage = Encoding.GetEncoding(1251).GetString(message);
```

```
        string sFileText;
        SaveFileDialog dSaveText = new SaveFileDialog();
        dSaveText.Filter = "Текстовые файлы (*.txt)|*.txt|Все файлы (*.*)|*.*";
        if (dSaveText.ShowDialog() == DialogResult.OK)
        {
           sFileText = dSaveText.FileName;
        }
        else
        {
           sFileText = "";
           return;
        };
        FileStream wFile;
        try
        {
           wFile = new FileStream(sFileText, FileMode.Create); //відкриваємо поток на запис результатів
        }
        catch (IOException)
        {
           MessageBox.Show("Ошибка открытия файла на запись", "Ошибка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
           return;
        }
        StreamWriter wText = new StreamWriter(wFile, Encoding.Default);
        wText.Write(strMessage);
        MessageBox.Show("Текст записан в файл", "Информация", MessageBoxButtons.OK);
        wText.Close();
        wFile.Close(); //закриваємо поток
    }}}
```

Ще один варіант програмної реалізації даного алгоритму представлено у роботі [5]. Авторами «…Розроблено алгоритм стеганографічного захисту інформації за методом LSB та реалізовано програмний код, що підвищує рівень захисту інформації від несанкціонованого доступу за рахунок приховування її у мультимедійних файлах, а саме у файлах зображень. Приховування даних відбувається у молодших бітах значення пікселів файлів зображень (по 1-му, 2-м або 3-м бітам приховуваного повідомлення на піксель контейнера). Алгоритм не змінює візуальну якість зображення, що унеможливлює виявлення факту приховування інформації. Програмний код розроблено з використанням обраної мови програмування C# в середовищі Visual Studio 2010. Проведене тестування повністю підтвердило правильність алгоритму та програмного засобу» [5, стор.8]. В результаті реалізації алгоритму отримані наступні зображення, рис. 4.2.

а) б)

Рисунок 4.2. Файл-зображення Windows 10.bmp:
а) початкове зображення; б) контейнер заповнений на 99%

Лістинг програми міститься за посиланням: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34816/93876.pdf?sequence=2&isAllowed=y.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Провести програмну реалізацію просторового алгоритму нанесення цифрових водяних знаків на власне зображення.
3. Провести перевірку правильності роботи програмного продукту.
4. Провести демонстрацію програмного продукту викладачу.
5. Зробити висновки та оформити звіт.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть переваги та недоліки даного алгоритму.
2. На який саме захист направлено даний метод?
3. Чи змінюється візуальне сприйняття зображення?
4. У чому складність програмної реалізації даного алгоритму?
5. Дайте визначення терміну «стеганографія».
6. Як перевірити наявність «повідомлення» у рисунку?
7. Які особливості приховування інформації у мультимедійних файлах?
8. Які методи стеганографії Ви знаєте?
9. Відмінність стеганографії та криптографії.
10. Які типи файлів можна використовувати для приховування інформації?

Практичне заняття № 5
НАЛАШТУВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS 10 ІЗ ЗАСТОСУВАННЯМ ПРОГРАМИ VIRTUALBOX

Мета – здобуття практичних навиків щодо налаштування параметрів безпеки операційної системи Windows 10 із застосуванням програми VirtualBox

ТЕОРЕТИЧНІ ВІДОМОСТІ

Для виконання завдання необхідно встановити програму для віртуальних машин Oracle VM VirtualBox (http://surl.li/amwgc) та імпортувати в неї образ Windows 10 (http://surl.li/amwfw).

Провести перейменування Віртуальної машини за зразком: W10_Прізвище студента_група. Використовуємо при вході в ОС **логін: Student, пароль 1111**. Відеоінструкція з послідовності виконання вказаних процедур знаходиться на освітньому порталі за посиланням: (http://surl.li/amwgd). Результат проведеної роботи представлено на рисунку 5.1.

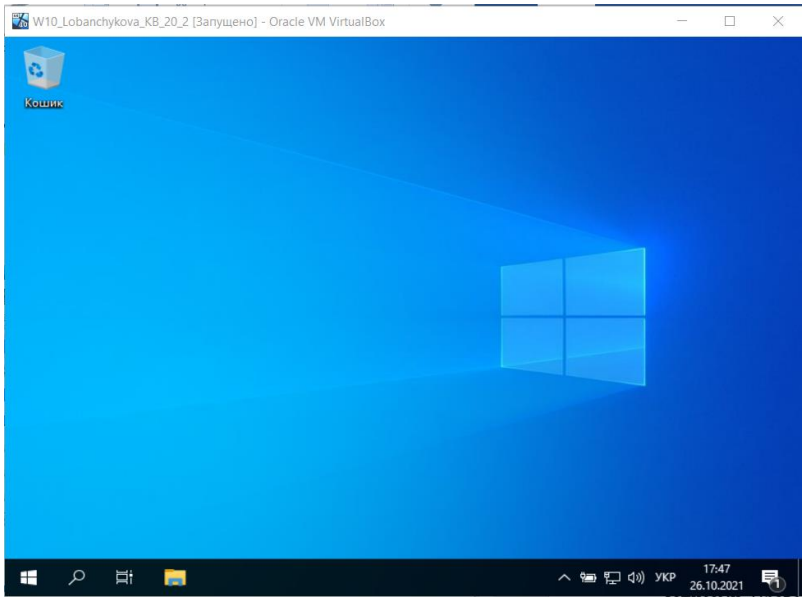

Рисунок 5.1. Вікно завантаженої віртуальної машини

Враховуючи те, що при налаштуванні віртуальної машини (ВМ) один із адаптерів включено у режимі використання NAT, ВМ отримала від «хостової машини» один із IP-адрес, що дозволяє нам отримати доступ до Інтернету, рис. 5.2, що відповідно робить можливим процес інсталювання.

Після інсталяції операційної системи, переконайтеся, що встановлено всі доступні оновлення. Це захистить та забезпечить виправлення помилок, а також «закриє» існуючі вразливості ОС. Для цього необхідно вибрати «Інсталювати

оновлення та перезавантажити» (рис. 5.3).

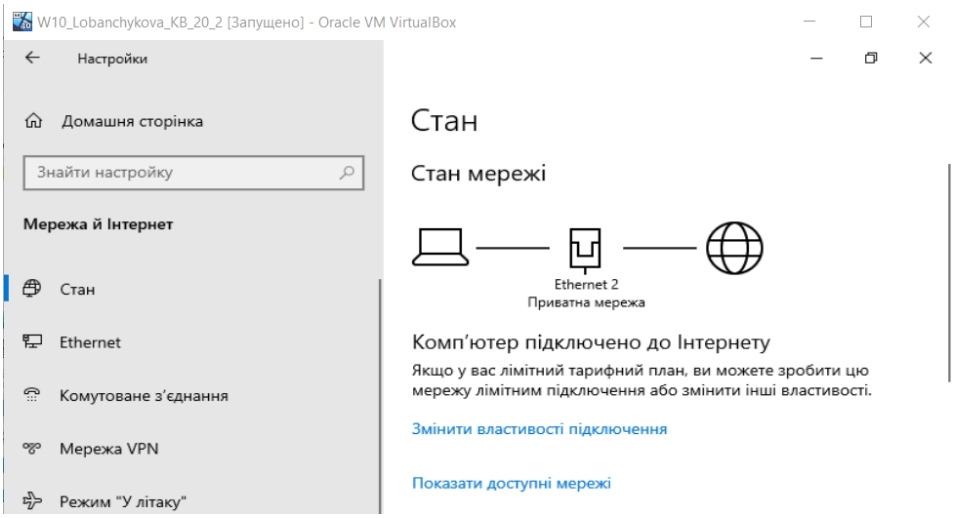

Рисунок 5.2. Параметри мережі ВМ

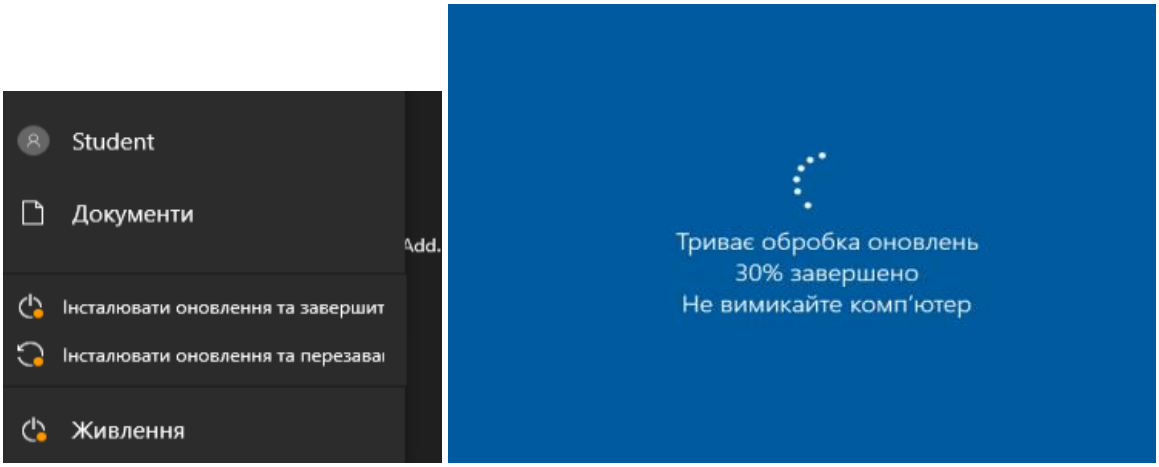

Рисунок 5.3. Встановлення оновлень

Наступним кроком є встановлення антивірусного програмного забезпечення. Вибір даного типу програмного продукту досить широко представлено на ринку. Тому необхідно провести аналіз та встановити антивірусну програму. Результати роботи представити у вигляді скріншоту.

Одним із засобів безпеки ОС Windows 10 є управління обліковими записами. Проведемо дослідження даної технології. Створимо додатковий обліковий запис для повсякденної роботи для підвищення рівня безпеки ОС та уникнення потенційних проблем при роботі під обліковим записом з підвищеними привілеями.

Для цього необхідно запустити файловий провідник, рис. 5.4 → Мій комп'ютер → правою кнопкою миші елемент Керування, рисунок 5.5.

Рисунок 5.4. Вибір параметру «Керування»

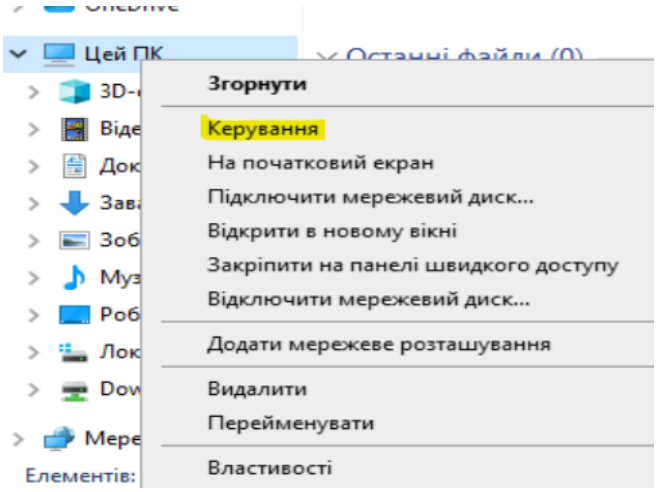

Рисунок 5.5. Вікно вибору елементу «Керування»

У вікні, що відкриється вибрати : «Локальні користувачі»-«Користувачі», рисунок 5.6.

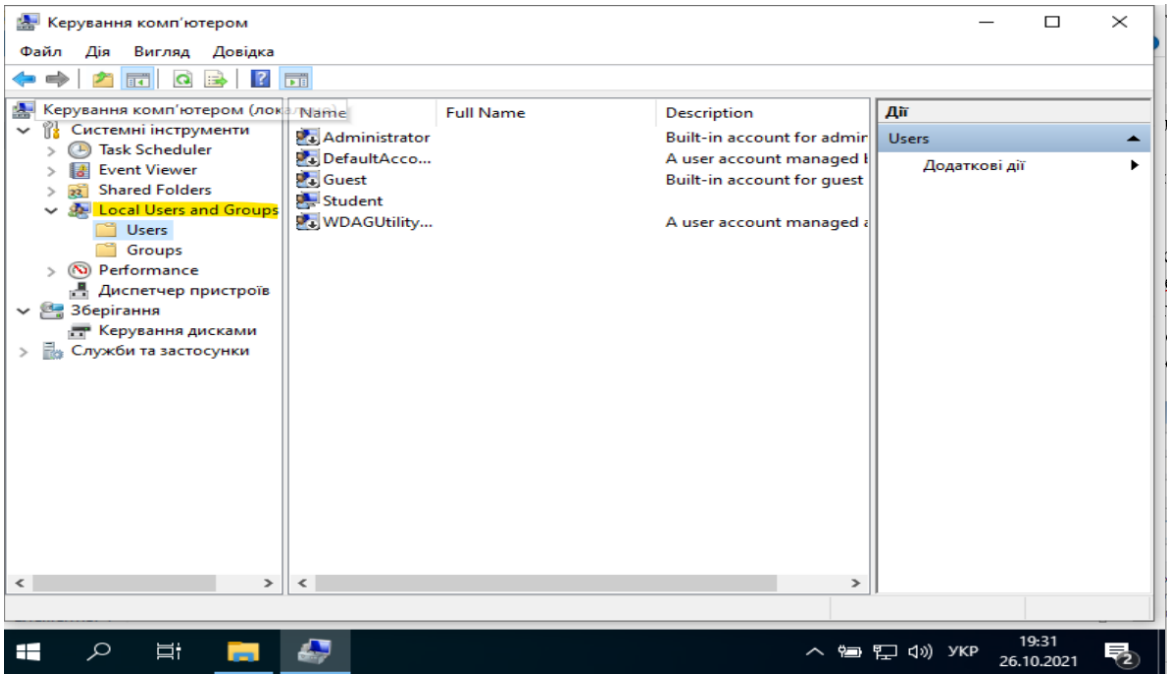

Рисунок 5.6. Вікно керування користувачами

Далі необхідно перейти у вікно «Дії», натиснути «Додаткові дії»→ «Новий користувач», рис. 5.7.

Створити користувача, в моєму випадку це **Student 2**. Це буде ваш

обліковий запис користувача для повсякденного використання. Заповнюємо поля та натискаємо «Створити», рис. 5.8. По замовчуванню встановлена позначка про необхідність зміни паролю при першому вході в систему. Цю позначку можна зняти. Є і ніші позначки, які можна встановити («користувач не може змінити пароль», «термін дії паролю не обмежений», «відключити обліковий запис»).

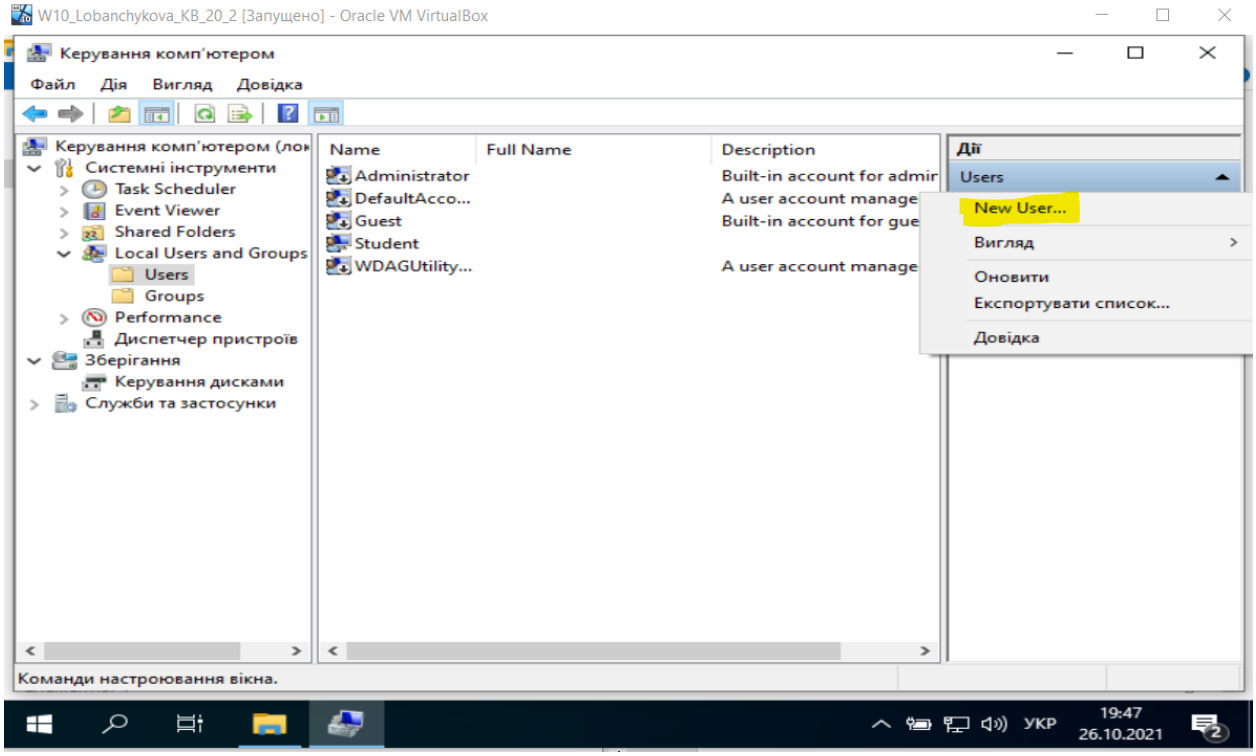

Рисунок 5.8 . Вікно для створення «Нового користувача»

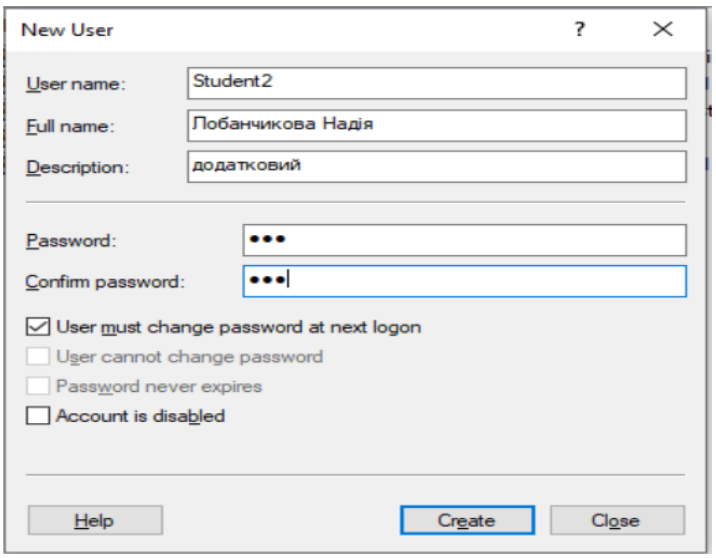

Рисунок 5.9. Вікно введення параметрів користувача

За потреби встановлення програмного забезпечення при вході в систему під

новостворeним користувачем, рис. 5.10, використовуйте функцію "Запуск от имени»". Натисніть клавішу Shift (праву кнопку миші) і виберіть "Запуск від імені іншого користувача", рисунок 5.11.

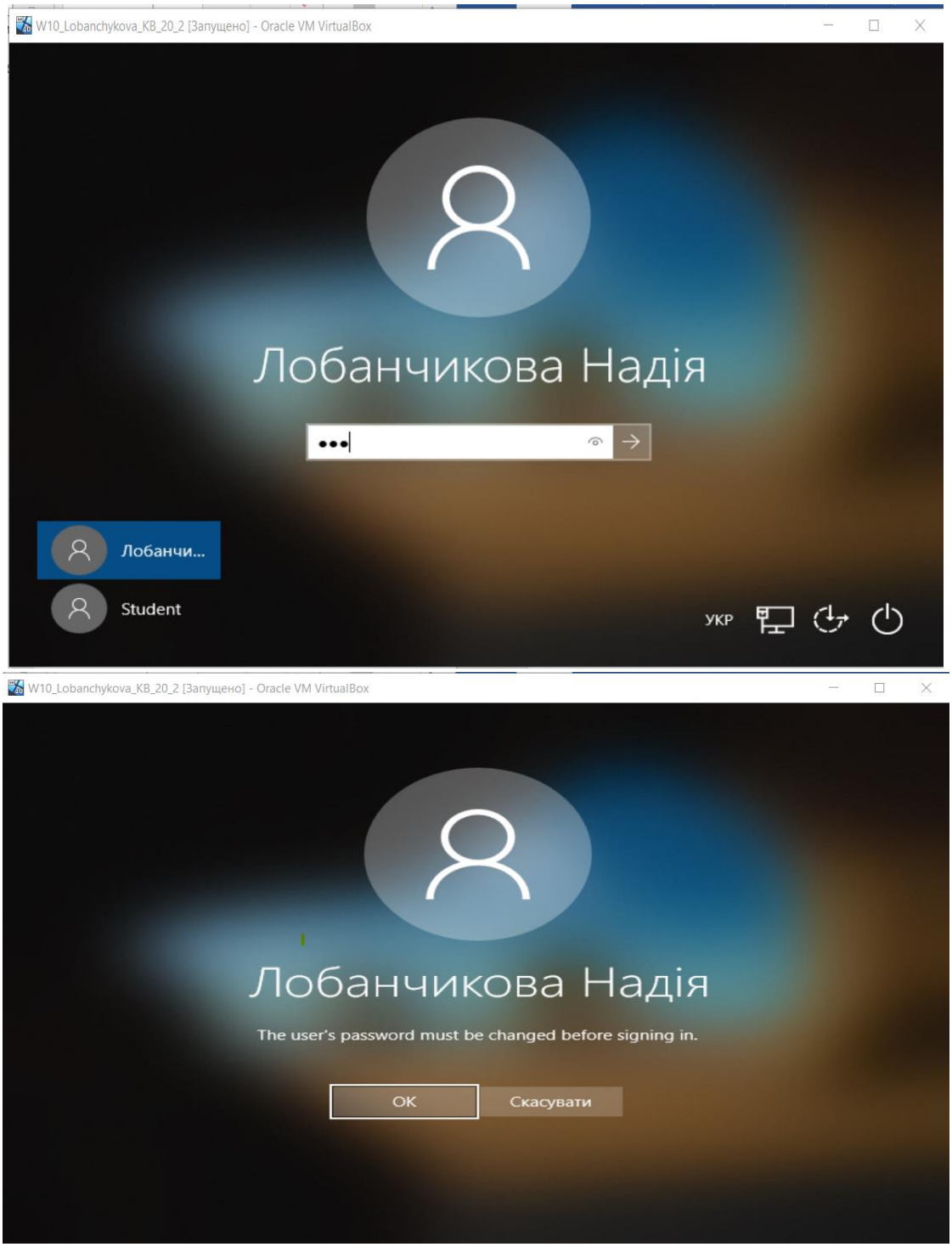

Рисунок 5.10. Вхід ОС під новим користувачем

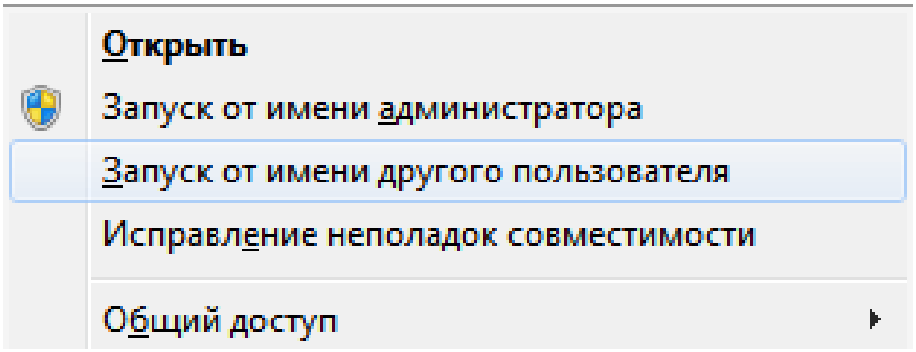

Рисунок 5.11. Вікно вибору типу запуску ПЗ

Важливим кроком у справі захисту ваших паролів буде відключити шифрування на LMHash. Вимкнення виконується через політику локальної безпеки або в реєстрі. В другому випадку необхідно відкрити редактор реєстру: пошук → Виконати → **regedit.exe,** рис. 5.12.

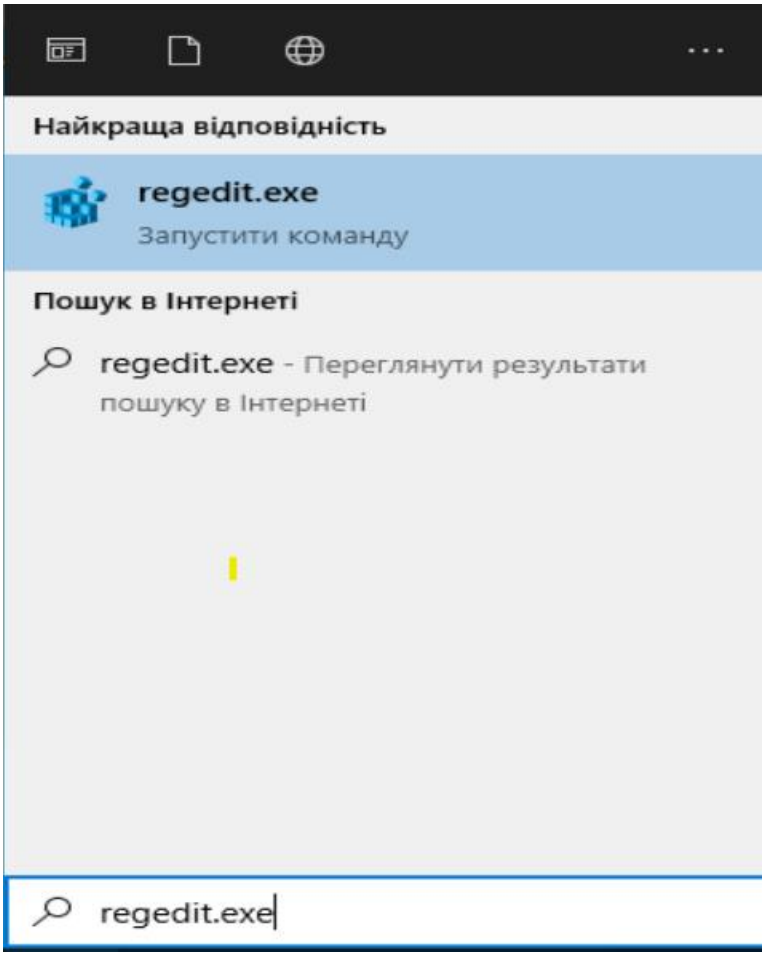

Рисунок 5.12. Знайдення та запуск реєстру

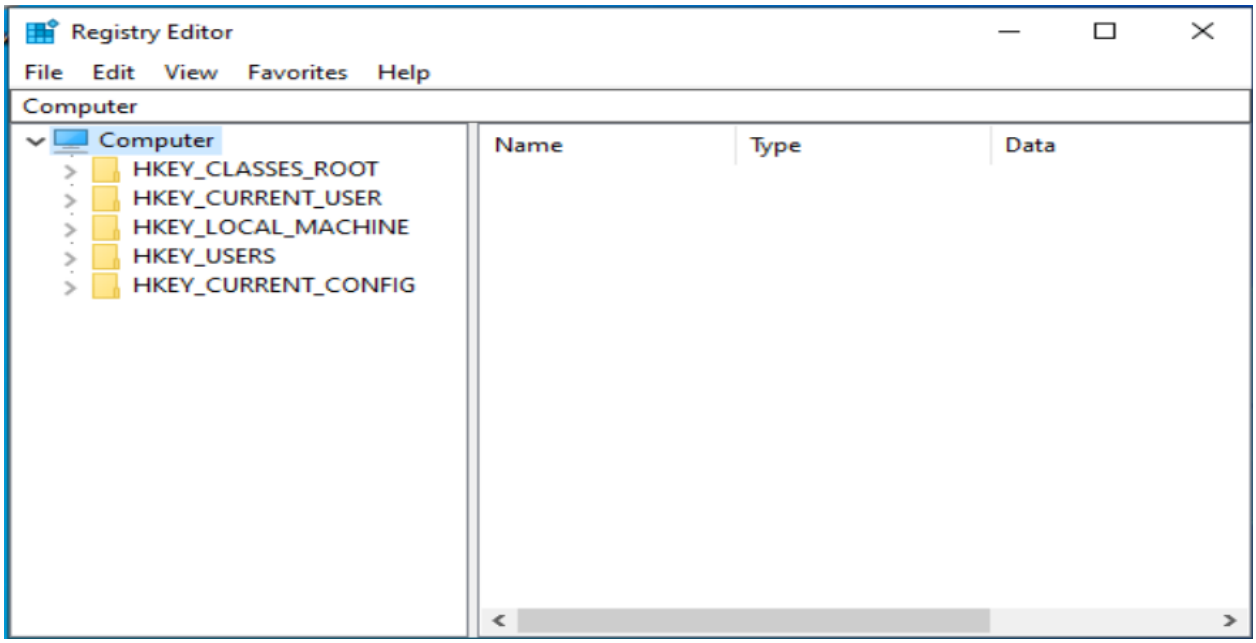

Рисунок 5.13. Вікно редактора реєстру

Знайти вітку:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

і перевірити параметр "NoLMHash" типу DWORD значення з значення даних 1.

Примітка: починаючи з Windows 7 SP1 у цього параметра вже встановлено по замовчуванню 1. У попередніх системах, або відсутній або дорівнює 0. Тому там необхідно було створювати його в ручному режимі.

В оснастці «Керування» шукаємо вкладку «Служби та застосунки», рисунок 15. Варто відзначити, що будь-яких служб дуже багато, але розглянемо найбільш популярні серед користувачів інтернету служби, видалення який забезпечить прискорення. Після того, як перед вами відкриється весь список служб можна натиснути на будь-який і в розділі «Властивості», «Тип запуску» встановити бажане значення. За допомогою цього ж меню можна просто провести відключення чи призупинити будь-яку службу в даний момент. Двічі клікнувши на будь-яку службу, можна зупинити або включити її, а також вибрати тип запуску: автоматичний – при включенні комп'ютера, вручну – за необхідності, відключено завантаження заборонена, служба не запускається, рис. 5.14.

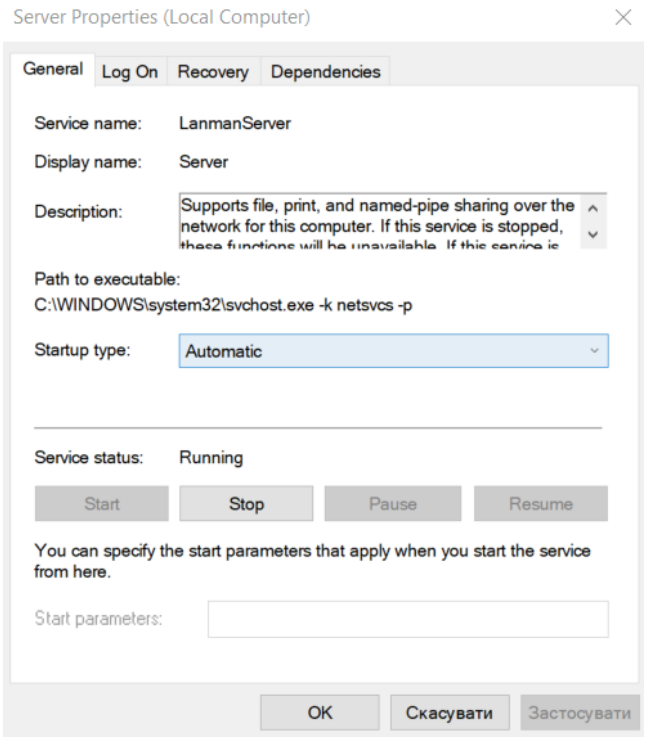

Рисунок 5.14

Крім цього, відключення здійснюється з використанням командного рядка (від Адміністратора), в яку вводиться sc config «Ім’я_служби» start=disabled. Всі дані для цієї команди знаходяться у верхній частині вікна при візуалізації відомостей про службу.

Далі проводимо відключення служб, які ми не використовуємо та тих служб, що нам не потрібні:

Microsoft Compatibility Telemetry. Служба, яка містить технічні дані про роботу пристрою і пов'язаного з ним програмного забезпечення. Вона періодично відправляє дані в Microsoft для подальшого поліпшення системи і підвищення зручності роботи користувачів. В цілому це важлива служба, але відключити її можна і нічого страшного з комп'ютером не відбудеться. Зупинити її роботу і прибрати компоненти можна в тому ж меню всіх сервісів, способом, описаним вище.

Windows Aero. Це графічна служба для красивого прозорого інтерфейсу. В цілому вона не потрібна і досить добре навантажує комп'ютер. Коли вона відключається, інтерфейс, зовнішній вигляд вікон і панелі завдань істотно може змінитися, але пристрій працювати стане краще.

Також до сервісів, що навантажує пристрій можна віднести Медіа центр Віндовс (Windows Media Center). Відключивши чи видаливши його, можна домогтися найкращої швидкодії - максимальної швидкості завантаження ОС

(навіть до 10 сек). Така оптимізація доступна в двох варіантах: з допомогою видалення назовсім і відключення з можливістю відновлення в майбутньому. Але, щоб відключити цей центр потрібно буде звернутися до реєстру regedit.exe і видаляти певні ключі.

- Автономні файли – на домашньому ПК не використовуються.
- Браузер комп'ютерів – якщо у вас немає робочої групи, то відключіть.
- Сервер – не потрібен на машинах, які не виділяються ресурси для спільний доступу у мережі.
- Прослуховувач домашньої групи – залежить від служби "Сервер" зупиниться при її відключенні.
- Віддалений реєстр – безумовно відключити, оскільки віддалений доступ до нього вдома не потрібен.

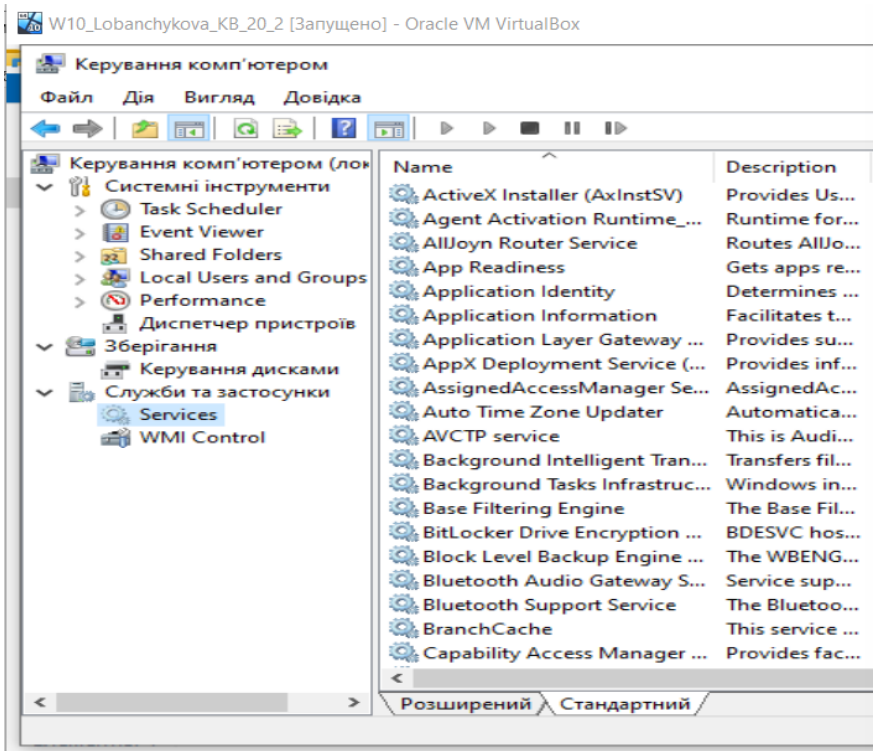

Рисунок 5.15. Вікно «Служби» керування комп’ютером

Переходимо до налаштувань локальних політик безпеки. Для відкриття локальної політики безпеки необхідно запустити secpol.msc (можна задати через пошук та запустити), рис. 5.16. «Встановлюємо наступні значення, рис. 5.17:

Політики облікових записів.

- Політика паролів – Мінімальна довжина пароля становить 10 символів.

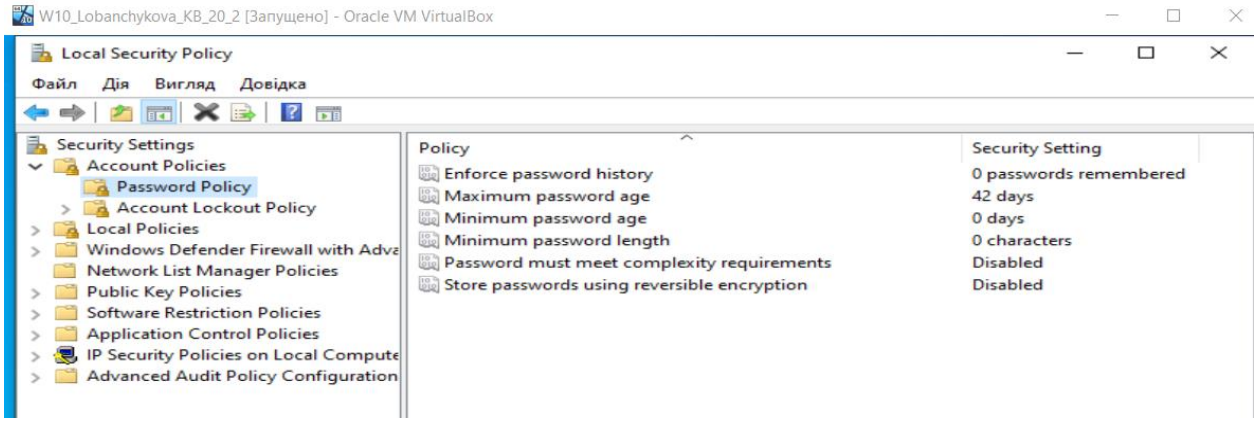

Рисунок 5.17. Встановлення параметрів політики паролю

- Політика блокування облікових записів – порогове значення блокування 5 спроб на 10 хвилин, рис. 5.18.

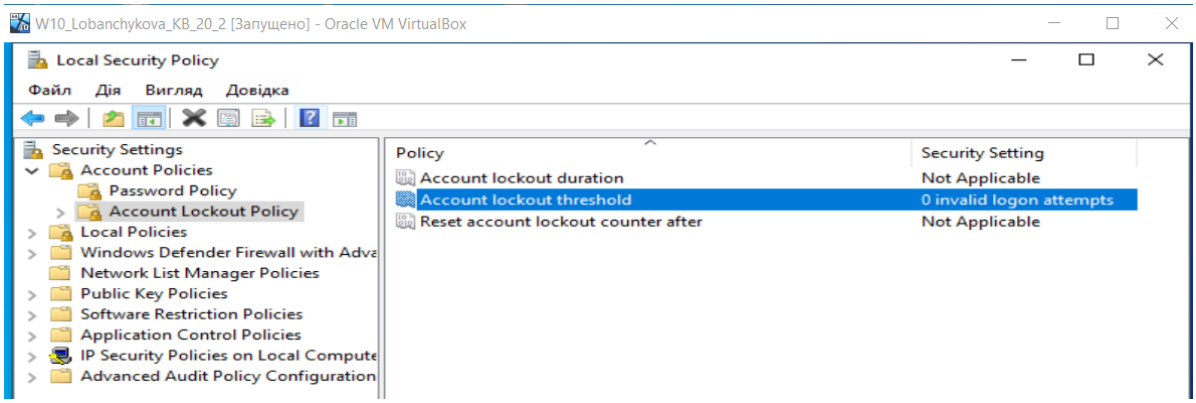

Рисунок 5.18. Встановлення параметрів блокування облікових записів

Локальні політики.

- Політика аудиту – Аудит входу в систему – Успіх та Відмова, рис. 5.19.

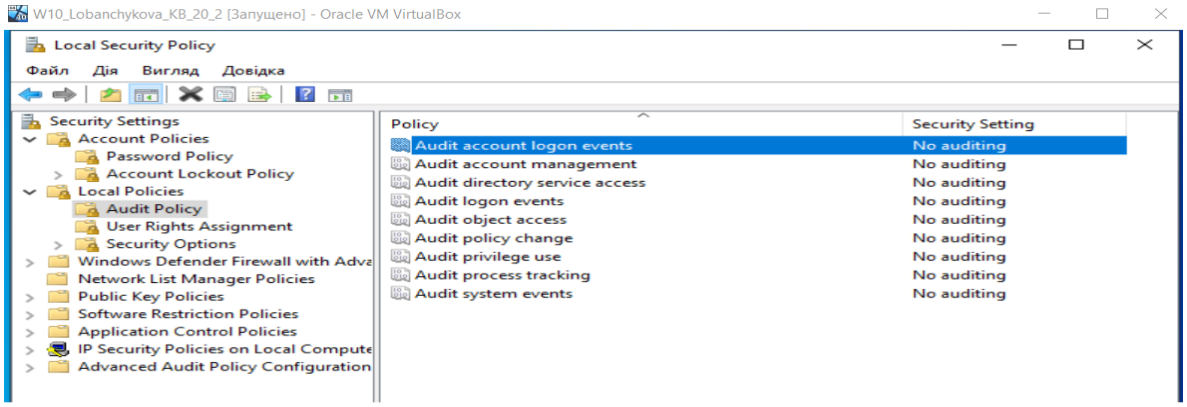

Рисунок 5.19. Встановлення параметрів аудиту входів у систему

- Політика аудиту – Аудит зміни політики – Успіх та Відмова, рис. 5.20.

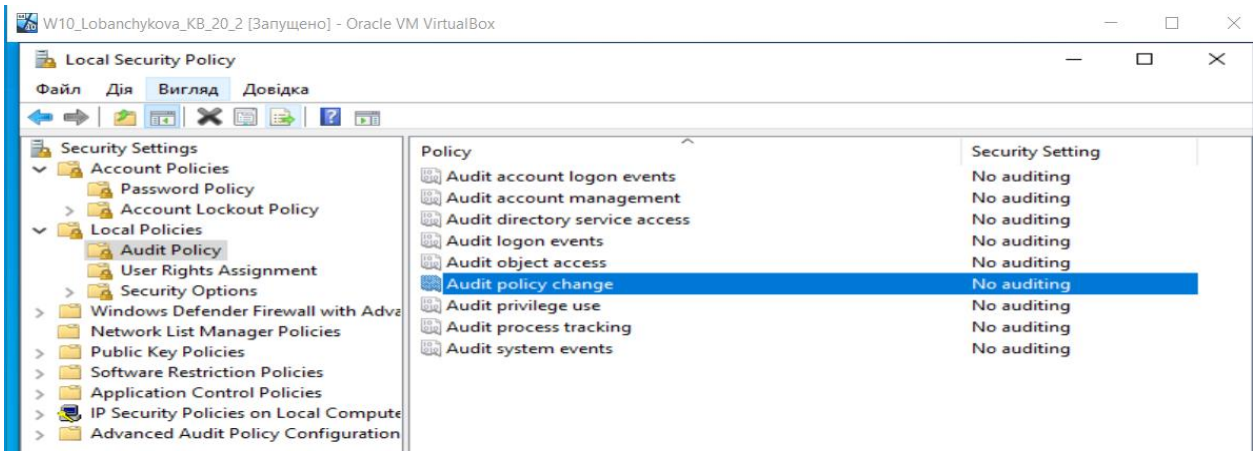

Рисунок 5.20. Встановлення параметрів аудиту зміни політики

- Політика аудиту – Аудит подій входу в систему – Успіх та Відмова, рис. 5.21.

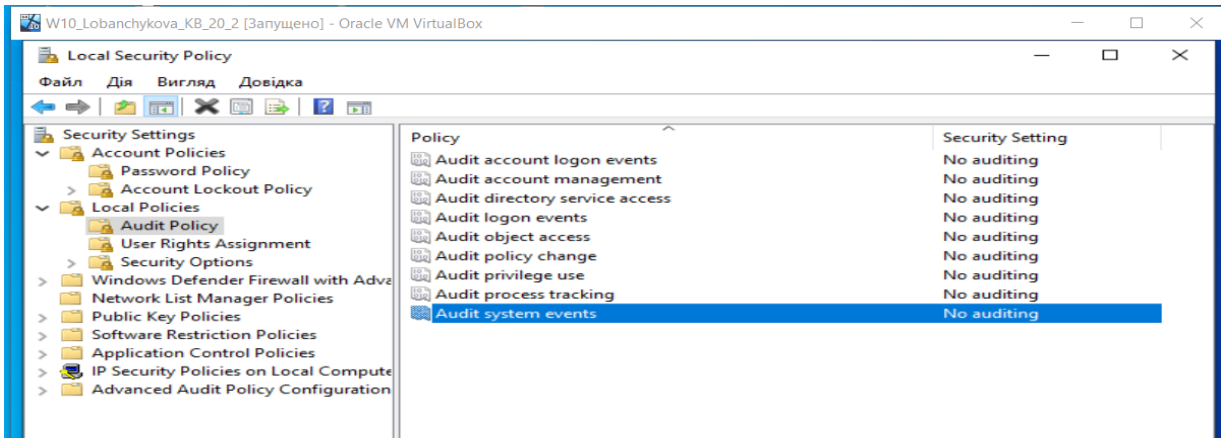

Рисунок 5.21. Аудит подій входу у систему

- Призначення прав користувача – Доступ до комп'ютера з мережі, рис. 5.12.

Проаналізувати потрібність всіх зазначених користувачів. Залишити тільки тих, кому дійсно можна дозволити доступ.

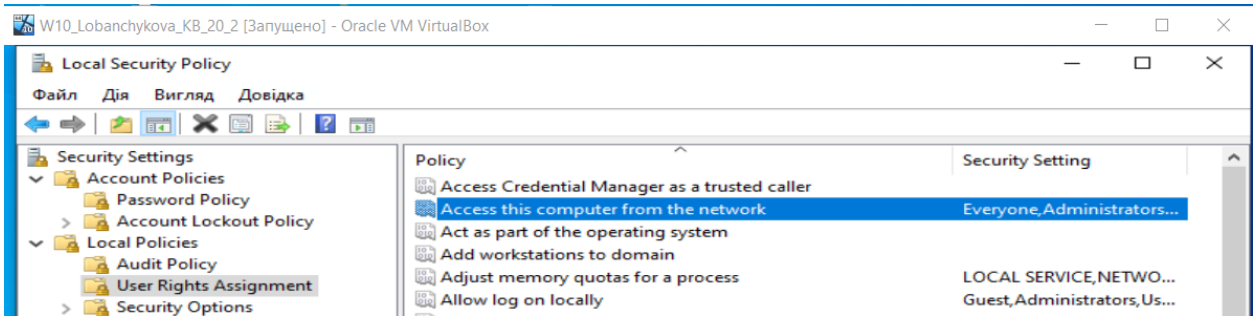

Рисунок 5.22. Вікно налаштування доступу до ПК з мережі

- Призначення прав користувача – Локальний вхід в систему – Видалити "Гість".
- Параметри безпеки – Облікові записи: перейменування облікового запису адміністратора – вказати нове ім'я (прізвище студента), рис. 5.23.

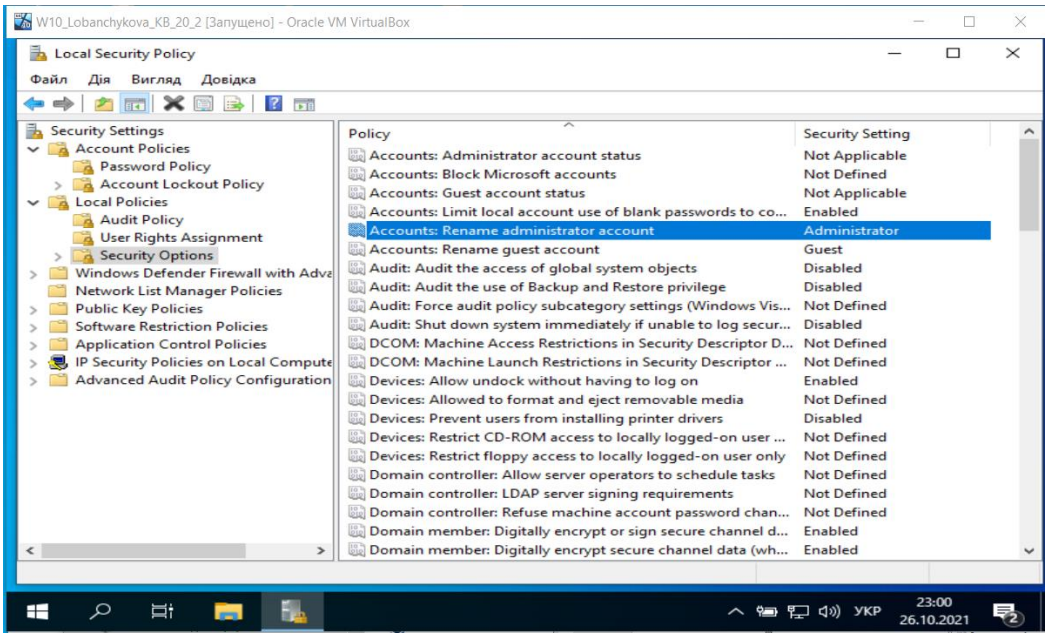

Рисунок 5.23. Вікно перейменування акаунту Адміністратора

- Параметри безпеки – Облікові записи: перейменування облікового запису гостя: вкажіть нове ім'я (скорочене прізвище студента).
- Параметри безпеки – Облікові записи: дозволити використання пустих паролів для входу тільки при консольному вході – Виключити.
- Безпека мережі: не зберігати хеш LAN Manager при наступній зміні пароля – Включено (увімкнуто),

P.S. вище зазначені параметри є достатніми для забезпечення безпечної експлуатації вашого комп'ютера.

Правила:

1. Встановлюйте постійно оновлення.
2. Не використовуйте без необхідності обліковий запис «Адміністратор».
3. Не завантажувати програмне забезпечення із невідомих джерел. Намагайтеся завантажувати програмне забезпечення лише з сайту виробника.
4. Завантажуючи кряки і т. д. не забувайте про те, що таке програмне забезпечення може закінчиться негативно для вашого комп'ютера.
5. Виконуйте резервне копіювання даних.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Встановити оновлення та антивірусне програмне забезпечення на віртуальну машину з ОС Windows 10.
3. Створити 5 облікових записів за зразком Прізвище студента_N, де N – номер користувача (1,2,3,4,5).
4. Створити 2 групи користувачів за зразком Група_Р_К, де Р – порядковий номер студента у списку групи, К – порядковий номер групи (1,2).
5. Задати паролі для входу кожного користувача та змінити їх при першому вході в систему. Використання складного паролю (числа + букви спеціальних символів, принаймні 10 символів у довжину, але в ідеалі 15-16).
6. Провести налаштування служб у відповідності до теоретичних відомостей.
7. Провести дослідження налаштувань локальних політик безпеки відповідно до матеріалу, представленому у теоретичних відомостях.
8. Оформити звіт та зробити висновки.

КОНТРОЛЬНІ ПИТАННЯ

1. Для чого використовується «Родина та інші користувачі»?
2. Яку максимальну кількість користувачів можна зареєструвати в ОС Windows 10 ?
3. Яким чином можна визначити стійкість паролю до зламу?
4. Рекомендовані вимоги до логіну та паролю.
5. Диспетчер задач та його призначення.

ЗМІСТ ЗВІТУ

1. Назва, мета й завдання.
2. Опис дій в ході виконання роботи підтверджений відповідними рисунками (скріншотами).

При формуванні звіту скріншоти виконання завдання повинні містити **назву віртуальної машини**. Скріншоти повинні відображати всі завдання виконані студентом.

3. Дати відповіді на контрольні питання.
4. Висновки про виконану роботу.

Практичне заняття №6
РОЗРОБКА ДИСКРЕЦІЙНОЇ ПОЛІТИКИ БЕЗПЕКИ ТА ЇЇ ПРОГРАМНА РЕАЛІЗАЦІЯ

Мета – здобуття практичних навичок розробки дискреційної політики безпеки та реалізувати програмно дискреційної політики безпеки організації

ТЕОРЕТИЧНІ ВІДОМОСТІ

При розробці політики безпеки повинні бути враховані особливості організації, її розміщення, структура та корпоративна культура. Вона повинна враховувати вимоги сьогодення щодо необхідного рівня захисту та відповідати чинному законодавству [2,3]. Політика безпеки повинна містити:

- загальний опис сфери діяльності підприємства;
- розподіл ролей і функцій, необхідних для вирішення конкретних питань, закріплення за певними співробітниками (фахівцями, керівниками) обов'язків по виконанню необхідної роботи з метою рішення завдань у рамках цієї політики безпеки.

У таблиці 6.1 представлено розподіл ролей одного із співробітників. Таблиця містить прізвище, ім’я, по-батькові співробітника, його посаду та опис функціональних обов’язків.

Таблиця 6.1.Розподіл ролей і функцій

№ з/п	ПІБ співробітника	Посада	Функціональні обов’язки
1.	Сидорчук Ольга Андріївна	Менеджер	Прийом замовлень від клієнтів, контроль за виконанням замовлень, аналіз запасів товарів і т.д.

Кожному працівнику організації необхідно присвоїти унікальний ідентифікатор та пароль для проведення аутентифікації при роботі з інформаційною системою.

Наступним є побудова матриці доступу до інформаційної системи підприємства, яка включає всі інформаційні ресурси, що представляють собою об’єкти інформаційної діяльності, O_n, перелік усіх користувачів інформаційної системи, S_m та визначені права щодо доступу до об’єктів інформаційної системи, P_i. Також слід визначити права користувачів щодо доступу до об’єктів інформаційної діяльності, як правило, це читання – 1, редагування – 2 та видалення – 3. Орієнтовний вигляд матриці доступу представлено у таблиці 6.2.

Таблиця 6.2 Матриця доступу до ресурсів інформаційної системи

	O_1	O_2	O_3	O_4
S_1	1	2	2	1
S_2	1	2	3	3
S_3	2	2	2	2
S_4	3	3	3	3
S_5	1	1	2	1

Для програмної реалізації розробленої політики безпеки першим етапом є розробка підсистеми аутентифікація користувачів, а другим – перевірка прав доступу до об’єктів інформаційної системи.

Приклад. Для наочності розглянемо підприємство, яке займається випуском кондитерської продукції [2,3]. В інформаційній системі зберігаються дані про споживачів, постачальників, співробітників, структуру управління підприємством, конфіденційна та комерційна інформація про виробництво. Побудуємо таблицю розподілу ролей та функцій та представимо дані у формі таблиці 6.3.

Таблиця 6.3. Розподіл ролей і функцій

№ з/п	ПІБ співробітника	Посада	Функціональні обов’язки
1.	Талько В.С.	Директор	Управління керівництвом, працює з конфіденційною та комерційною інформацією
2.	Лайко О.В.	Секретар	Працює з неконфіденційною документацією, веде облік запису на прийом до директора
3.	Сарган О.В.	Оператор	Обслуговування технічних установок
4.	Сидорчук О.А.	Менеджер	Представлення виготовленої продукції на ринок
5.	Михайлова В.І.	Адміністратор	Підтримує нормальне функціонування інформаційної системи та бази та сайту підприємства

На наступному етапі кожному працівнику організації присвоїмо унікальний ідентифікатор та пароль для проведення аутентифікації при роботі з інформаційною системою. В межах прикладу використовуємо простий 4-хзначний цифровий пароль (в реальних системах використання такого паролю

значно знижує рівень захищеності системи від зламу)

Таблиця 6.4. Ідентифікатори та паролі працівників

№ з/п	ПІБ співробітника	Ідентифікатор	Пароль
1.	Талько В.С.	director	111111
2.	Лайко О.В.	secretar	222222
3.	Сарган О.В.	operator	333333
4.	Сидорчук О.А.	meneger	444444
5.	Михайлова В.І.	admin	555555

Будуємо матрицю доступу до інформаційної системи підприємства, таблиця 6.5.

Таблиця 6.5. Матриця доступу до інформаційної системи

	O_1	O_2	O_3	O_4
S_1	2	2	2	2
S_2	4	1	1	1
S_3	4	1	1	1
S_4	4	1	2	2
S_5	4	3	3	3

S_1–директор;

S_2–секретар;

S_3–оператор;

S_4–менеджер;

S_5–адміністратор.

O_1–комерційна, конфіденційна інформація підприємства;

O_2–дані про робітників;

O_3–дані про споживачів;

O_4–дані про клієнтів.

P_i – права користувачів щодо доступу до об'єктів:

1) читання даних;
2) редагування;
3) видалення;
4) не має права доступу.

Розробляємо програму для реалізації розробленої політики безпеки (приклад лістингу програми знаходиться у викладача.

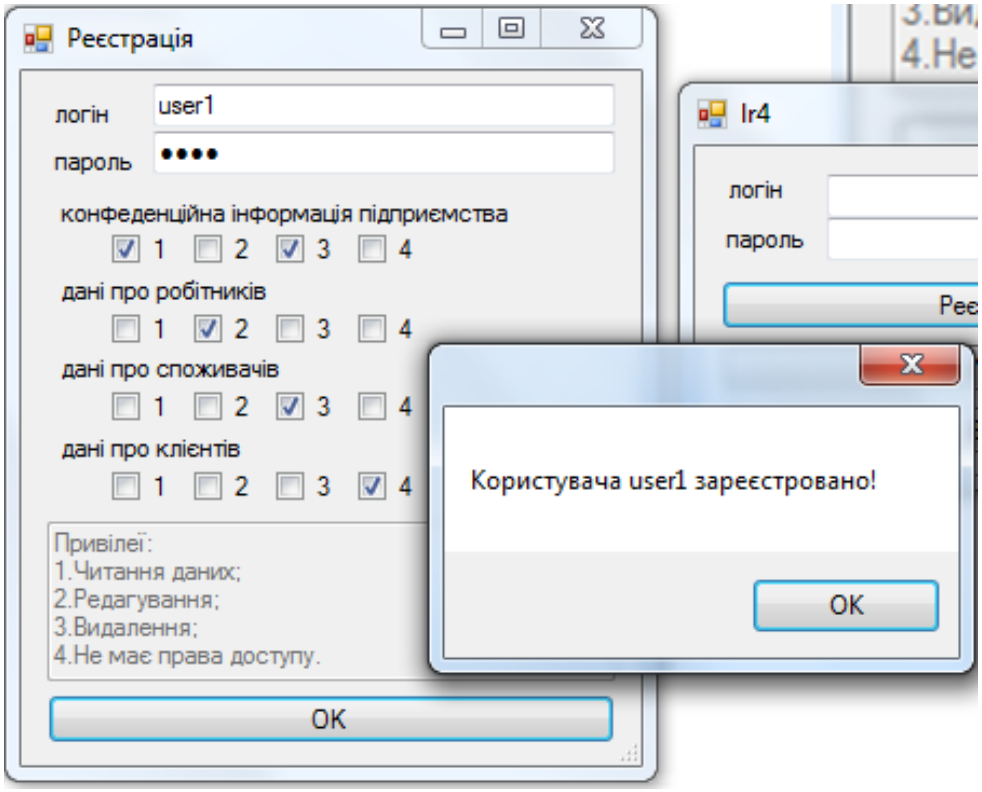

Рисунок 6.1. Вікно реєстрації користувачів

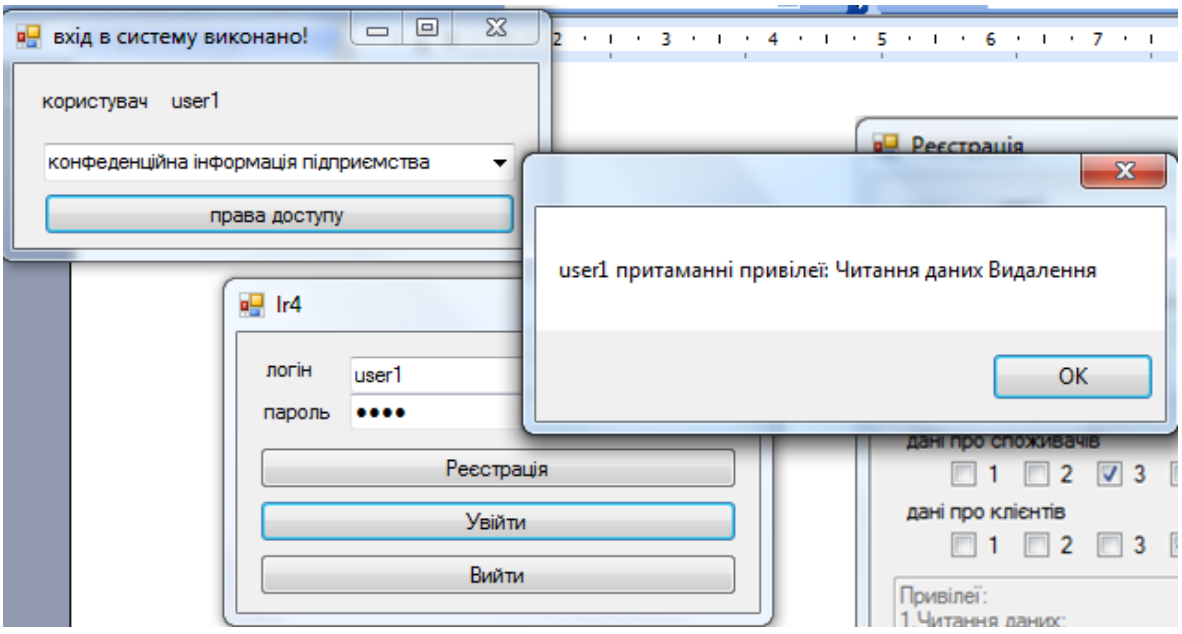

Рисунок 6.2. Перевірка прав доступу зареєстрованих користувачів

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Вибрати підприємство для дослідження процесів розробки політики безпеки.
3. Здійснити загальний опис сфери діяльності обраного підприємства.
4. Дослідити функціональні обов'язки співробітників та визначити їх роль та функції, необхідних для вирішення конкретних питань та виконання посадових обов'язків. Дані представити у вигляді таблиці 6.1 (таблиці 6.3).
5. Створити ідентифікатори та паролі кожному працівнику та представити їх у вигляді таблиці 6.4.
6. Визначити інформаційні ресурси підприємства, O_n та провести їх категоріювання. Привести перелік усіх користувачів інформаційної системи, S_m та визначені права щодо доступу до об'єктів інформаційної системи, P_i. Також визначити права користувачів щодо доступу до об'єктів інформаційної діяльності.
7. Побудувати матрицю доступу до ресурсів інформаційної системи відповідно до таблиці 6.5.
8. Провести програмну реалізацію розробленої політики та продемонструвати її викладачу.
9. Оформити звіт та дати відповіді на контрольні питання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Призначення політики безпеки на підприємстві.
2. Дайте визначення поняттю «дискреційна політика безпеки».
3. Назвіть переваги і недоліки дискреційної політики безпеки.
4. Дайте коротку характеристику мандатної політики безпеки.
5. Назвіть переваги і недоліки мандатної політики безпеки.
6. Дайте коротку характеристику рольової політики безпеки.
7. Назвіть переваги і недоліки рольової політики безпеки.
8. Назвіть етапи формального підходу до перевірки СЗІ на повноту і коректність.
9. Назвіть основні принципи захисту інформації від НСД.
10. Структура монітора звернень.
11. Основні характеристики моделі Белла-Ла Падула.
12. Дайте визначення поняттям «ідентифікація», «аутентифікація».
13. Перерахуйте засади, яким доцільно керуватися при формалізації політики захисту інформації.

Практичне заняття №7
МЕТОДИ, ЗАСОБИ ТА ТЕХНОЛОГІЇ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Мета – здобуття практичних навичок технічного захисту інформації у визначеному приміщенні, проведення аналізу об'єкту захисту, виявлення каналів витоку інформації та визначення засобів захисту інформації.

ТЕОЕРЕТИЧНІ ВІДОМОСТІ

1. Загальні теоретичні відомості

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне й системне ПЗ;
- апаратна частина серверів і робочих станцій;
- комунікаційне устаткування й канали зв'язку;
- периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікації;
- системи аудиту й моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі;
- системи сигналізації;
- засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мереженого захисту інформації:

– міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

– системи виявлення вторгнень (IDS - Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;

– засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

– засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й керування доступом (СККД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

В межах виконання завдання необхідно провести аналіз приміщення в

якому проводяться переговори і робота з документами в твердому і електронному вигляді, дати оцінку захищеності об'єкту від витоку інформації по технічних каналах і сформувати рекомендації по захисту інформації на об'єкті.

2. Просторова і структурна моделі приміщення переговорів

Під кімнатою, приміщенням розуміється службове приміщення, у якому ведуться розмови (переговори) конфіденційного характеру. Тут мова йде про службові приміщення, у яких відсутні які-небудь технічні засоби обробки (передачі) конфіденційної інформації. До таких приміщень відносяться, насамперед, кімнати для переговорів в офісах, де ведуться ділові переговори, що містять конфіденційну інформацію.

Слід зазначити, що переговірні кімнати використаються все частіше і на сьогодні вони є практично невід'ємним атрибутом фірми (компанії). Тому буде цікаво розглянути питання забезпечення безпеки інформації у виділених приміщеннях, маючи на увазі, насамперед, кімнати для ведення переговорів.

По-перше, необхідно зрозуміти основну мету і завдання захисту, тому що правильне з'ясування мети і завдань захисту визначить надалі клад комплексу проведених заходів, їх вартість і ефективність захисту в цілому.

Оскільки при роботі обробляється інформація, що носить конфіденційний характер (відомості про осіб, факти, події і інше, таке, що стосується фінансової діяльності підприємства), то можна зробити висновок про незаперечну необхідність побудови системи захисту даного приміщення.

Клас захищеності автоматизованої системи від несанкціонованого доступу до інформації згідно керівному документу Державної технічної комісії при Президенті України «Класифікація автоматизованих систем і вимог по захисту інформації»: 3.К. Проведемо аналіз даного приміщення.

Виділене приміщення знаходиться на четвертому поверсі будівлі. Схема комплексу рішень по захисту кімнат переговорів, кабінетів керівників, службових приміщень від просочування конфіденційної інформації по технічних каналах представлений на рисунку 7.1. Розміри приміщення: висота 3,5 метра, ширина 6 метрів, довжина 9 метрів. Приміщення знаходиться в межах контрольованої зони, відстань до межі якої не менше 40 метрів. Приміщення має одне вікно, яке виходить на внутрішню частину території. Двері виходять в коридор, в якому можуть знаходитися як працівники самої організації, так і сторонні люди.

Меблі кімнати складаються з двох столів (один стіл керівника, один стіл для переговорів), восьми стільців. Так само в приміщенні знаходиться шафа, три

полки під документи, сейф та прилади захисту інформації.

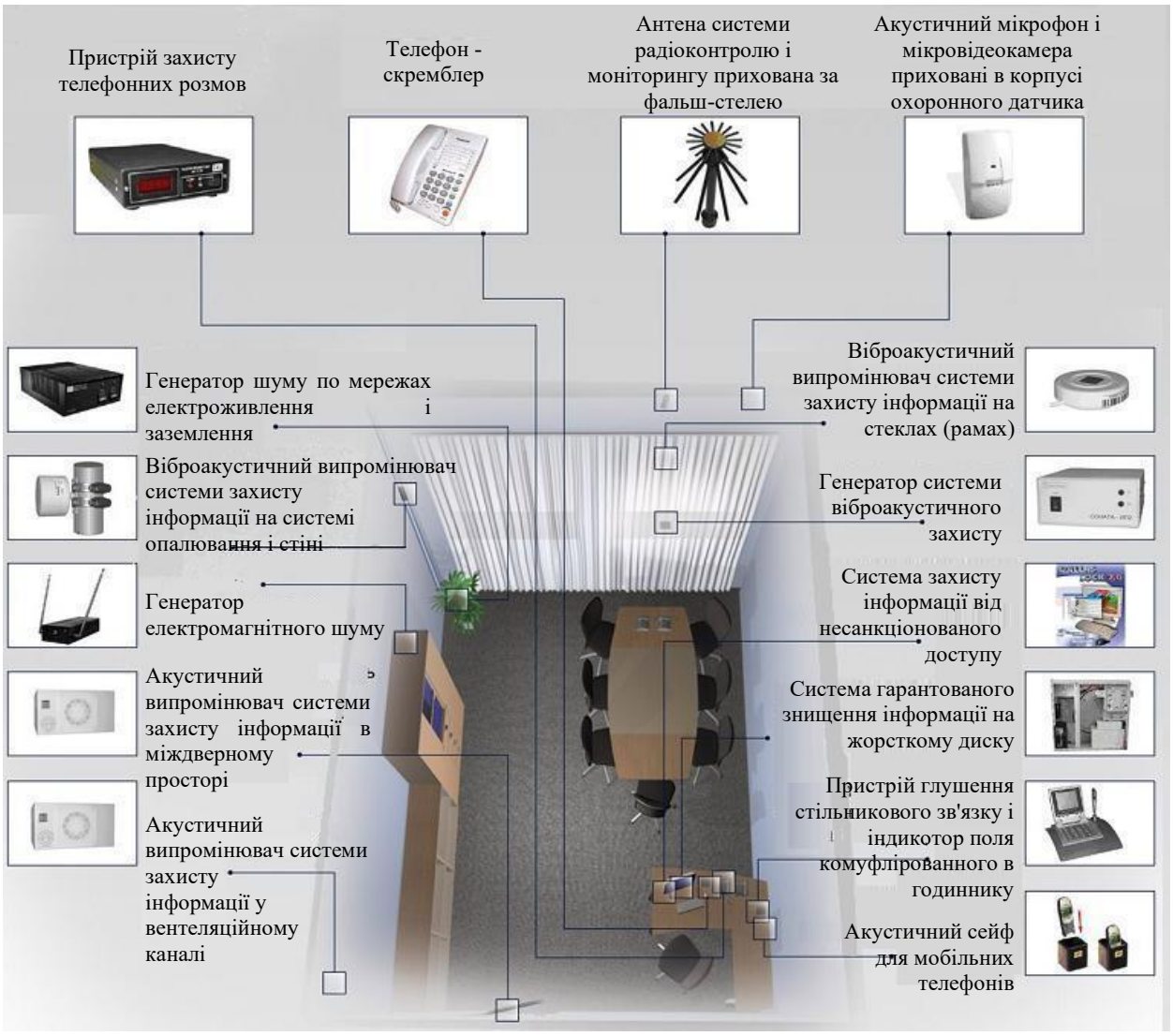

Рисунок 7.1.Схема комплексу рішень по захисту кімнат переговорів, кабінетів керівників, службових приміщень від просочування конфіденційної інформації по технічних каналах

Всі стіни виконані з червоної цегли. Ліва та права стіни приміщення товщиною 200 мм, і 400 мм стіна, що виходить в коридор і на вулицю. Всі стіни обштукатурені і пофарбовані з обох боків. Приміщення обладнане двома батареями опалення радіаторного типу. Приток води по батареях здійснюється з приміщення, розташованого над контрольованим приміщенням, а стік з батарей здійснюється по трубах в приміщення за стіною №2. Зліва від входу за стіною №1 знаходиться допоміжне приміщення, яке є власністю організації, але доступ в нього мають сторонні люди. За стіною №2 (праворуч від входу) знаходиться приміщення №404. Це приміщення, так само як і

попереднє, належить організації. Там знаходиться аудиторія.

Таблиця 7.1. Перелік меблів і побутових приладів, встановлених в кабінеті

Найменування	*Кількість, шт.*	*Обліковий номер*
Стіл робочий	*1*	*006*
Стіл для нарад	*1*	*007*
Стільці	*8*	*008-015*
Комп'ютер	*1*	*016*
Шафа	*1*	*017*
Полка для документів	*3*	*018-020*
Сейф	*1*	*021*

Двері в приміщенні звукоізольовані, подвійні із зазором більше 200 мм, габарити 1500×2300 мм.

Вікно має подвійне скління, при цьому відстань між шибками дорівнює 57 мм, товщина скла 5 мм. Розмір отвору: 2200×1200 мм. Візуальному огляду виділеного приміщення ззовні (через вікно) перешкоджають жалюзі.

Перекриття – стеля і підлога виконані з бетонних плит з круглими порожнечами, 220 мм. На підлозі постелений паркет. Оскільки будівля чотириповерхова, то над стелею приміщення, що захищається, горище, вхід в який закритий на замок. Приміщенням під підлогою є аудиторія.

Отвір припливної вентиляції знаходиться відразу при вході (зліва від дверей), а другий отвір в кінці цієї ж стіни (також ліворуч від дверей). Діаметр отвору складає 20 сантиметрів.

У мережу електроживлення подається напруга 220 В з постійною промисловою частотою 50 Герц. Офіс, що захищається, обладнаний дванадцятьма розетками.

Проаналізувавши приведені вище початкові дані, вивчивши теоретичні, аналітичні матеріали, а так само нормативні і керівні документи в даній області захисту інформації, потрібно скласти план проведення робіт на об'єкті, визначити склад заходів і їх послідовність, виробити вимоги до спеціальних технічних засобів, які використовуватимуться для дослідження об'єкту. Далі потрібно привести результати обстеження об'єкту, на їх підставі зробити висновки про захищеність досліджуваного приміщення і сформувати рекомендації по захисту.

В ході обстеження приміщення потрібно перевірити всю радіоелектронну апаратуру, предмети меблів і інтер'єру, що несуть конструкції, системи комунікації на наявність закладених пристроїв (ЗП). Провести дану перевірку

слід в два етапи:

– візуальний огляд;

– пошук ЗП з використанням спеціального устаткування.

Для захисту від несанкціонованого доступу співробітників фірми і сторонніх осіб в неробочий час, приміщення обладнане дверима із замком і охоронною сигналізацією. Так само пожежна і охоронна сигналізації виведені на пульт чергового. Черговий знаходитися при вході в будівлю. Пульт чергового обладнаний світловою і звуковою індикацією, і у разі спрацьовування сигналізації спалахує відповідна лампа і подається звуковий сигнал високих частот.

Основна мета забезпечення безпеки конфіденційної інформації в переговірних кімнатах – виключити доступ до її змісту при проведенні переговорів (розмов).

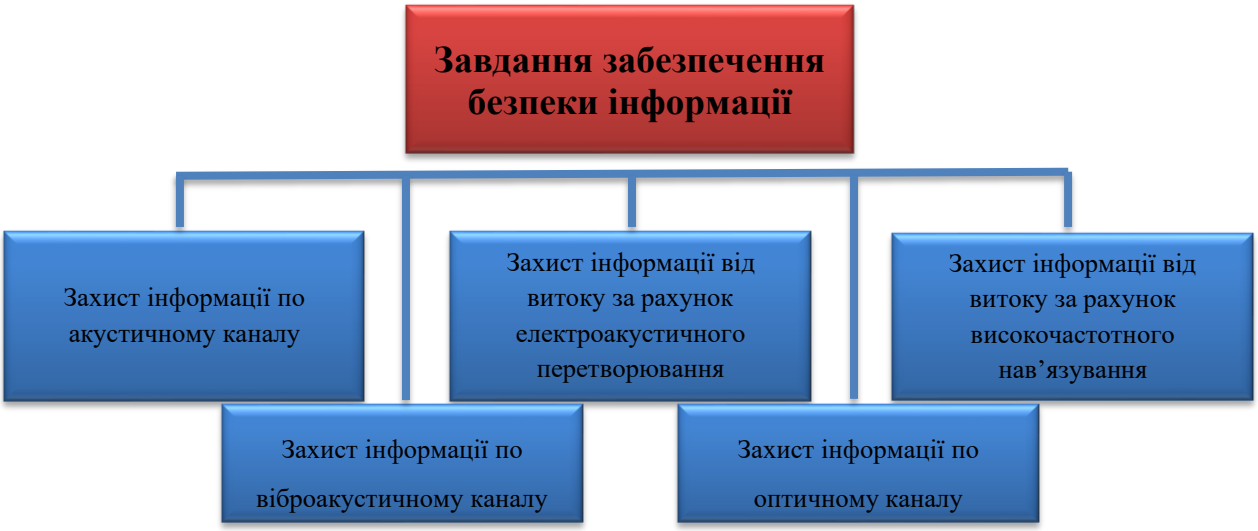

Рисунок 7.2. Завдання забезпечення безпеки конфіденційної інформації в кімнаті для переговорів

Першорядними завданнями забезпечення безпеки інформації (рисунок 7.2.) є:

– захист інформації від витоку по акустичному каналі (АК);

– захист інформації від витоку по віброакустичному каналу (ВАК);

– захист інформації від витоку за рахунок електроакустичного перетворення (ЕАП);

– захист інформації від витоку за рахунок високочастотного нав'язування (ВЧН);

– захист інформації від витоку по оптичному каналі (ОК).

Усвідомивши основну мету і завдання захисту інформації, можна перейти до розробки моделі погроз для конфіденційної інформації, що мають місце при веденні переговорів (розмов). Моделі погроз доцільно розробляти, погодившись із завданнями захисту.

Модель погроз для інформації через акустичний канал витоку

Несанкціонований доступ до конфіденційної інформації з акустичного каналу витоку (рисунок 7.3) може здійснюватися:

Рисунок 7.3. Несанкціонований доступ до конфіденційної інформації з акустичного каналу витоку

Модель погроз для інформації через віброакустичний канал витоку

Несанкціонований доступ до вмісту переговорів (розмов) зловмисниками може бути також здійснений (рисунок 7.4) за допомогою стетоскопів і гідроакустичних датчиків.

Рисунок 7.4. Несанкціонований доступ до вмісту переговорів

За допомогою стетоскопів можливе прослуховування переговорів через стіни товщиною до 1 м 20 см (залежно від матеріалу).

Залежно від виду каналу передачі інформації від самого вібродатчика стетоскопи підрозділяються на:

- провідні (провідний канал передачі);
- радіо - (канал передачі по радіо);
- інфрачервоні (інфрачервоний канал передачі).

Не виключена можливість використання і гідроакустичних датчиків, що дозволяють прослуховувати розмови в приміщеннях, використовуючи труби водопостачання і опалення. Правда, випадки застосування таких пристроїв на практиці дуже рідкі.

Модель погроз для інформації за рахунок електроакустичного перетворення і гетеродинного встаткування

Витік конфіденційної інформації при веденні переговорів (розмов) можлива через вплив звукових коливань на елементи електричної схеми деяких технічних засобів обробки інформації, що одержали в літературі назва "Допоміжні засоби".

До допоміжних засобів ставляться ті, які особистої участі в обробці конфіденційної інформації не приймають, але можуть бути причиною її витоку. Доступ до змісту переговорів (розмов) може бути здійснений на значному видаленні від приміщення, що становить у деяких випадках сотні метрів, залежно від виду каналу витоку (рисунок 7.5).

Рисунок 7.5. Доступ до конфіденційної інформації в залежності від виду каналу витоку

Подібні канали витоку існують при наявності в приміщеннях телефонних апаратів з дисковим номеронабирачем, телевізорів, електричних годин, підключених до системи годинофікації, приймачів і т.д.

Причому у випадку з телефонними апаратами і електричними годинниками витік інформації здійснюється за рахунок перетворення звукових коливань в електричний сигнал, що потім поширюється по провідних лініях (телефонним або по проводам системи годинофікації). Доступ до конфіденційної інформації може здійснюватися шляхом підключення до цих ліній.

Що стосується телевізорів і приймачів, то витік конфіденційної інформації відбувається тут за рахунок наявних у них гетеродинів (генераторів частоти). Причина витоку – модуляція звуковим коливанням при веденні розмови несучої частоти гетеродина, просочування її в систему з наступним випромінюванням у вигляді електромагнітного поля.

Модель погроз для інформації з оптичного каналу і за рахунок високочастотного нав'язування

Якщо переговори ведуться в кімнаті, вікна якої не обладнані шторами або жалюзі, то в цьому випадку в зловмисника є можливість за допомогою оптичних приладів з більшим посиленням (біноклів, підзорних труб) переглядати приміщення. Сутність прослуховування переговорів за допомогою високочастотного нав'язування складається в підключенні до телефонної лінії генератора частоти і наступного прийому "відбитого" від телефонного апарата промодельованого розмовою, що ведеться в кімнаті, сигналу.

Таким чином, аналіз погроз для конфіденційної інформації, які мають місце

при веденні переговорів (розмов) показує, що якщо не прийняти мір захисту, те можливий доступ зловмисників до її змісту.

3. Рекомендації із захисту

Перш ніж перейти до заходів та засобів захисту, необхідним є складання моделі порушника. Передбачуваний порушник – це людина добре підготовлена, знаюча всі канали витоку інформації в кімнатах для ведення переговорів, професійно володіє способами і засобами добування відомостей, що містять конфіденційну інформацію. Тому необхідно розробити і реалізувати комплекс заходів, що забезпечують надійний захист під час ведення переговорів (розмов).

1. Особливо важливий вибір місця проведення переговорів – переговірної кімнати. Її доцільно розмістити по можливості на верхніх поверхах. Бажано, щоб кімната для переговорів не мала вікон, або ж вони виходили у внутрішній двір.

2. У кімнаті для переговорів не повинно бути зайвої техніки, як наприклад телевізор, приймач, ксерокс, годинник, системи годонофікації, телефонних апаратів.

3. Вхід у переговірну кімнату повинен бути обладнаний тамбуром, а внутрішня сторона тамбура оббита звукоізоляційним матеріалом. Необхідно пам'ятати, що незначна щілина (одиниці міліметрів) багаторазово знижує звукоізоляцію.

4. При наявності в кімнаті для переговорів вентиляційних каналів потрібно подбати, щоб вони були обладнані спеціальними ґратами, що дозволяють закривати отвір вентиляційного каналу при веденні переговорів і відкривати його, коли переговори не ведуться.

5. Якщо в переговірній є вікна, то повинні бути вжиті наступні заходи обережності:

- Проводити переговори при закритих кватирках.
- На вікнах повинні бути штори або жалюзі.
- Шибки повинні бути обладнані вібродатчиками.

6. При наявності в переговірної телефонного апарата повинні бути вжиті наступні заходи захисту. Наявність телефонного апарату з дисковим номеронабирачем вимагає захисту дзвінкового ланцюга. Тому доцільно використати фільтр "Корунд-М", що забезпечує загасання сигналу витоку порядку 80 дБ. Для захисту від високочастотного нав'язування рекомендується підключити паралельно мікрофону (для будь-яких телефонних апаратів) конденсатор ємністю С = 0,01 - 0,05 мкФ. На практиці можуть зустрічатися і

більше складні схеми захисту дзвінкового і мікрофонного ланцюга телефонних апаратів.

7. Для захисту від провідних мікрофонів, що використають для передачі інформації по мережі електроживлення в 220 В, рекомендується використовувати генератор типу "Соната-С1", що має гарні тактико-технічні характеристики і ефективно виконує функції захисту.

Для захисту переговірних від спеціальних технічних засобів добре скористатися генератором віброакустичного шуму "Соната-АВ" і генератором радіоперешкод "Барикада-1". Генератор віброакустичного шуму "Соната-АВ" захищає від: безпосереднього підслуховування в умовах поганої звукоізоляції; застосування радіо і провідних мікрофонів, установлених у порожнинах стін, надстельному просторі, у вентиляційних проходах і т.д.; використання стетоскопів, установлених на стінах, стелях, підлогах, трубах водо і теплопостачання і т.д.; застосування лазерних і інших типів спрямованих мікрофонів. Генератор радіошуму "Барикада-1" забезпечує захист переговорів від всіх радіозакладок, створюючи в крапці прийому зловмисником перевищуючого рівня перешкоди над рівнем випромінюваного радіозакладкой сигналу. Важливий також контроль над станом безпеки конфіденційної інформації в переговірних кімнатах, що здійснюється при періодичному проведенні спецобстежень і атестацій. По закінченні складається акт спецобстеження і атестат відповідності. Таким чином, запропоновані нами рекомендації дозволять забезпечити безпека переговорів, проведених у спеціально виділені для цієї мети приміщеннях.

ЗАВДАННЯ ДО ВИКОНАННЯ

1.1. Провести дослідження приміщення з метою оформлення опитового листа.

Необхідно захистити мовну інформацію в приміщенні, призначеному для проведення конфіденційних переговорів. Забезпечити аудіо-відео протоколізацію переговорів, що проводяться в приміщенні.

Загальні відомості про приміщення

Призначення приміщення:

Міра конфіденційності (секретності) інформації, що заявляється:

Поверх:

Площа (кв. м), висота стель (м):

Перекриття (потовк, пів), товщина (мм):

Стінні перегородки:

Стіни зовнішні:

Вікна:

Двері:

Опис суміжних приміщень:

Система електроживлення (освітлення):

Система заземлення:

Системи сигналізації (тип):_

Система вентиляції (тип):

Система опалення:

Телефонні лінії:

Інші дротяні лінії:

Засоби зв'язку:

Оргтехніка:

Побутова техніка:

Спеціальні технічні засоби захисту інформації:

Опис обстановки довкола об'єкту:

1.2. Описати та представити склад та опис виявлених функціональних каналів витоку інформації.

1.3. Визначити можливості порушника по перехопленню мовної інформації.

1.4. На підставі проведеного аналізу представити вимоги до системи захисту інформації.

1.5. Провести вибір обладнання для захисту мовної інформації для дослідженого приміщення та розробити рекомендації із захисту.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яку направленість мають системи технічного захисту інформації?
2. Назвіть основні джерела витоку аудіоінформації.
3. Назвіть основні джерела витоку відеоінформації.
4. Назвіть засоби зняття аудіоінформації.
5. Назвіть засоби зняття відеоінфрмації.
6. Наведіть приклад засобів апаратного захисту інформації.
7. Наведіть приклад засобів захисту програмного забезпечення.

Практичне заняття №8
МЕТОДИ ВИЗНАЧЕННЯ МІЦНОСТІ ЗАХИСТУ ІНФОРМАЦІ

Мета – здобуття практичних навичок визначення міцності захисту інформації з використанням різних моделей систем захисту інформації, дослідження процесів оцінки стійкості парольного захисту інформації

ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Оцінка моделей систем захисту інформації

У загальному випадку найпростіша модель елементарного захисту будь-якого предмету може бути у вигляді представленому на рис. 8.1.

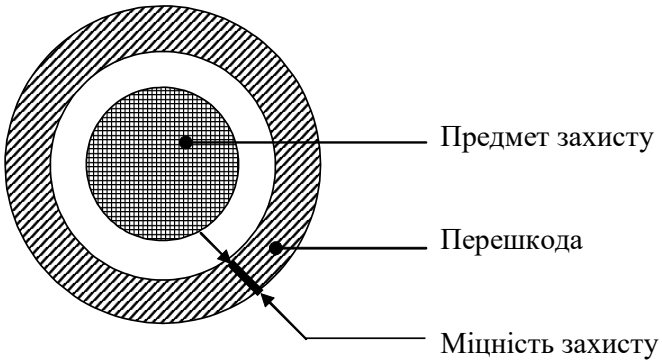

Рисунок 8.1. Модель елементарного захисту

Якщо позначити імовірність неподолання перешкоди порушником через $P_{сзі}$, час життя інформації через $t_ж$, очікуваний час подолання перешкоди порушником через $t_{под}$, імовірність обходу перешкоди порушником через $P_{обх}$, то для випадку старіння інформації умову достатності захисту одержимо у виді наступних відношень:

$$P_{сзі}=1, \text{ якщо } t_ж<t_{под} \text{ і } P_{обх}=0,$$

де $P_{обх}$, яке рівне нулю, відбиває необхідність замикання перешкоди навколо предмету захисту. Якщо $t_ж > t_{под}$, а $P_{обх}=0$, то

$$P_{сзі}=(1-P_{под}), \qquad (8.1)$$

де $P_{под}$ - імовірність подолання перешкоди порушником за час, менший ніж $t_ж$.

Для реального випадку, коли $t_ж > t_{под}$ і $P_{обх} > 0$, міцність захисту можна представити у виді:

$$P_{сзі}=(1-P_{под})(1-P_{обх}),$$

де $P_{под}=0$, якщо $t_ж<t_{под}$, $P_{под}>0$, якщо $t_ж>t_{под}$.

Слід зазначити, що ця формула справедлива для випадку, коли порушників двоє, тобто коли один переборює перешкоду, а другий її обходить.

Припустимо, що порушник буде один і йому відомі міцність перешкоди і складність шляху її обходу. Оскільки одночасно по двох шляхах він йти не зможе, він вибере один з них – найбільш простий, тобто по формулі "або". Тоді формальний вираз міцності захисту в цілому для даного випадку буде відповідати формулі

$$P_{сзі}=\min\{(1-P_{под}),(1-P_{обх})\}. \quad (8.2)$$

Отже, міцність перешкоди після визначення і порівняння величин $(1 – P_{под})$ і $(1 – P_{обх})$ буде дорівнювати найменшому значенню однієї з них.

Вибір і визначення конкретної величини $P_{обх}$ спочатку можна проводити експертним шляхом на основі досвіду фахівців. Величина $P_{обх}$ повинна приймати значення від 0 до 1. При $P_{обх}=1$ захист втрачає всякий зміст.

Можливо також, що в однієї перешкоди може бути кілька шляхів обходу. Тоді формула (8.2) прийме вид:

$$P_{сзі}=\min\{(1-P_{под}),(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхк})\}, \quad (8.3)$$

де к – число шляхів обходу перешкоди.

Для випадку, коли порушників більше ніж один і вони діють одночасно (організована група) по кожному шляху, цей вираз з урахуванням сумісності подій буде мати вигляд:

$$P_{сзі}=(1-P_{под})(1-P_{обх1})(1-P_{обх2})(1-P_{обх3})...(1-P_{обхк}).$$

У цьому випадку, міцність перешкоди буде визначатись добутком результатів віднімання з одиниці значень ймовірності доступу порушників до предмету захисту по кожному можливому шляху подолання цієї перешкоди.

У тому випадку, коли інформація, що підлягає захисту, не застаріває або періодично обновляється, тобто коли нерівність $t_ж>t_{под}$ постійна або ж коли забезпечити $t_{под}>t_ж$ за будь-якими причинами неможливо, звичайно застосовується постійно діюча перешкода, що володіє властивостями виявлення і блокування доступу порушника до предмета або об'єкта захисту

Умову міцності перешкоди з виявленням і блокуванням НСД можна представити у виді співвідношення

$$\frac{T_{оп}+t_{спр}+t_в+t_{бл}}{t_{под}}<1, \quad (8.4)$$

де $T_{оп}$ – період опитування датчиків;

$t_{спр}$– час спрацьовування тривожної сигналізації; $t_в$– час визначення місця доступу;

$t_{бл}$– час блокування доступу.

Якщо позначимо суму ($T_{оп}+t_{спр}+t_в+t_{бл}$) через $T_{вбл}$, одержимо співвідношення:

$$\frac{T_{вбл}}{t_{под}} < 1. \qquad (8.5)$$

Процес контролю НСД і несанкціонованих дій порушника в часі представлений на рис. 8.2. З діаграми на рис. 8.2 зрозуміло, що порушник може бути не виявлений у двох випадках:

а) коли $t_{под} < T_{оп}$;

б) коли $T_{оп} < t_{под} < T_{вбл}$.

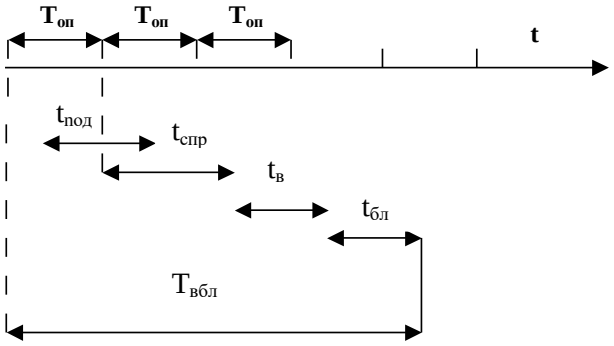

Рисунок 8.2. Діаграма дій порушника

У першому випадку потрібна додаткова умова – влучання інтервалу часу $t_{под}$ в інтервал $T_{оп}$, тобто необхідна синхронізація дій порушника з частотою опитування датчиків виявлення. Для розв'язання цієї задачі порушникові прийдеться таємно підключити вимірювальну апаратуру в момент виконання несанкціонованого доступу до інформації, що є досить складною задачею для сторонньої людини. Тому вважаємо, що свої дії з частотою опитування датчиків він синхронізувати не зможе і може розраховувати лише на деяку ймовірність успіху, що виражається в імовірності влучення відрізка часу $t_{под}$ у проміжок часу між імпульсами опитування датчиків, рівний $T_{оп}$.

Відповідно до визначення геометричної ймовірності з курсу теорії ймовірності одержимо вираз для визначення ймовірності успіху порушника в наступному виді:

$$P_{под} = \frac{T_{оп} - t_{под}}{T_{оп}} = 1 - \frac{t_{под}}{T_{оп}}. \quad (8.6)$$

Тоді ймовірність виявлення несанкціонованих дій порушника буде визначатися виразами:

$$P_в = 1 - P_{под}, \quad (8.7)$$

$$P_в = \frac{t_{под}}{T_{оп}}. \quad (8.8)$$

При $t_{под} > T_{оп}$ порушник буде виявлений напевно, тобто $P_в = 1$. В другому випадку, коли $T_{оп} < t_{под} < T_{вбл}$, імовірність успіху порушника буде визначатися за аналогією з попереднім співвідношенням:

$$P_{под} = 1 - \frac{t_{под}}{T_{вбл}}. \quad (8.9)$$

Імовірність виявлення і блокування несанкціонованих дій порушника:

$$P_{вбл} = (1 - P_{под}), \quad (8.10)$$

$$P_{вбл} = \frac{t_{под}}{T_{вбл}}. \quad (8.11)$$

При $t_{под} > T_{вбл}$ спроба НСД не має сенсу, тому що вона буде виявлена напевно. У цьому випадку $P_{вбл} = 1$.

Таким чином, розрахунок міцності перешкоди з властивостями виявлення і блокування можна робити по формулі

$$P_{сзі} = \min\{P_{вбл,}(1 - P_{обх1}),(1 - P_{обх2}),...,(1 - P_{обхj})\}, \quad (8.12)$$

де j – число шляхів обходу цієї перешкоди.

Для більш повного представлення міцності перешкоди у виді автоматизованої системи виявлення і блокування НСД необхідно враховувати надійність її функціонування і шляхи можливого обходу її порушником.

Імовірність відмовлення системи визначається по відомій формулі

$$P_в(t) = e^{-\lambda t}, \quad (8.13)$$

де λ – інтенсивність відмовлень групи технічних засобів, що складають систему виявлення і блокування НСД;

t – інтервал часу функціонування системи виявлення і блокування НСД.

З урахуванням можливого відмовлення системи контролю міцність перешкоди буде визначатися за формулою

$$P_{сзік}=\min\{P_{вбл}(1-P_{в}),(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхj})\}, \quad (8.14)$$

де $P_{вбл}$ і $P_{в}$ визначаються відповідно по формулах (8.11) і (8.13);

$P_{обх}$ і кількість шляхів обходу j визначаються експертним шляхом на основі аналізу принципів побудови системи контролю і блокування НСД.

На підставі викладеного підбиваємо деякі підсумки і робимо висновок про те, що захисні перешкоди бувають двох видів: контрольовані і не контрольовані людиною. Міцність неконтрольованої перешкоди розраховується за формулою (8.3), а контрольованої – за формулою (8.14).

1.2. Оцінка моделі багатоланкового захисту інформації

Прикладом такого виду захисту може служити приміщення, у якому зберігається апаратура. Як перешкоди з різною міцністю тут можуть служити стіни, стеля, підлога, вікна і замок на дверях.

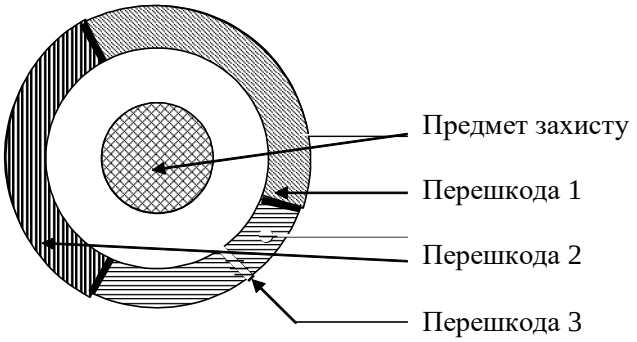

Рисунок 8.3. Модель багатоланкового захисту

Формальний опис для міцності багатоланкового захисту практично збігається з виразами (8.2) і (8.14), тому що наявність декількох шляхів обходу однієї перешкоди, що не задовольняє заданим вимогам, зажадає їхнього перекриття відповідними перешкодами. Тоді вираз для міцності багатоланкового захисту при використанні неконтрольованих перешкод може бути представлене у виді:

$$P_{сзі}=\min\{P_{сзі1},P_{сзі2},...,P_{сзіі},(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхк})\}, \quad (8.15)$$

де $P_{сзіі}$ – міцність і-ї перешкоди.

Вираз для міцності багатоланкового захисту з контрольованими перешкодами буде в наступному виді:

$$P_{сзік}=\min\{P_{сзік1},P_{сзік2},P_{сзік3},...,P_{сзікn},(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхj})\}, \quad (8.16)$$

де $P_{сзік}$ – міцність к-ї перешкоди.

Тут варто підкреслити, що розрахунки підсумкової міцності захисту для неконтрольованих і контрольованих перешкод повинні бути роздільними, оскільки вихідні дані для них різні, і, отже, це різні задачі, два різних контури захисту.

Якщо міцність слабкої ланки задовольняє пред'явленим вимогам контуру захисту в цілому, виникає питання про надмірність міцності на інших ланках даного контуру. Звідси випливає, що економічно доцільно застосовувати в багатоланковому контурі захисту рівні за міцністю перешкоди.

Тоді сумарна міцність дубльованих перешкод буде визначатися за формулою

$$P_{\Sigma} = 1 - \prod_{i=1}^{m}(1 - P_i), \quad (8.17)$$

де i=1,m – порядковий номер перешкоди;

P_i– міцність і-ї перешкоди.

У відповідальних випадках при підвищених вимогах до захисту застосовується багаторівневий захист, модель якого представлена на рис. 8.4.

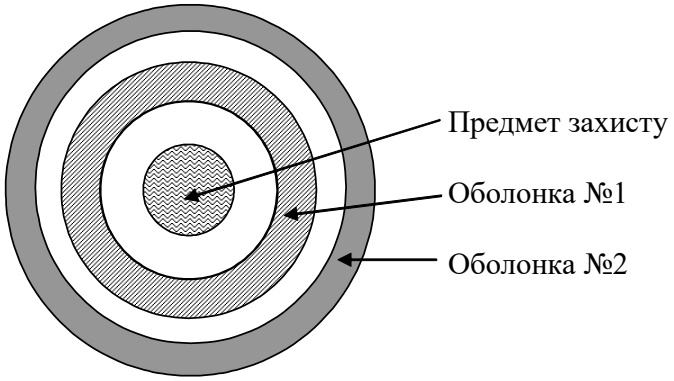

Рисунок 8.4. Модель багаторівневого захисту

Під час розрахунку сумарної міцності декількох контурів захисту у формулу (8.17) замість P_i включається $P_{кі}$ – міцність кожного контуру, значення якої визначається по одній з формул (8.15) і (8.16), тобто для контрольованих і неконтрольованих перешкод знову розрахунки повинні бути роздільними і

проводитись для різних контурів, що утворять кожний окремий багаторівневий захист. При $Р_{кі} = 0$ даний контур у розрахунок не приймається. При $Р_{кі.} = 1$ інші контури захисту є надлишковими. Підкреслимо також, що дана модель справедлива лише для контурів захисту, що перекривають ті самі канали несанкціонованого доступу до предмета захисту.

1.3. Методика розрахунку міцності захисту

У табл. 8.1 не приведені засоби контролю цілісності програмного забезпечення і інформації в АС, а також засоби реєстрації, рекомендовані звичайно сучасними фахівцями і нормативними документами. Ці засоби не мають досить швидкої реакції на НСД і є необхідними лише для оцінки наслідків після того, як подія вже здійснилася, і порушник може бути вже далеко. Їхні функції захисту ефективні лише в стримуванні потенційного некваліфікованого порушника. Процедура контролю цілісності в принципі видає операторові інформацію про порушення, але тільки в момент проведення цієї процедури. Її частота проведення, як правило, встановлюється організаційно і проводиться відносно рідко через великий час процедури і відволікання значних ресурсів ЕОМ. Однак необхідність у застосуванні цих засобів не заперечується. Вони необхідні для дублювання основних засобів, але насамперед для проведення аналізу події і виявлення випадкових впливів.

Таблиця 8.1. Розподіл засобів захисту по можливих каналах НСД

№ п/п	Найменування можливого каналу НСД	Клас захисту			Засоби захисту	Міцність
		I	II	III		
1	2	3	4	5	6	7
1	Пристрій введення (виводу) інформації	+	+	+	Система контролю і розмежування доступу в приміщення.	Р1
		+	+	-	Програмно-апаратний комплекс контролю входу в систему.	Р2
		+	+	+	Програма контролю і розмежування доступу до ПЗ й інформації АС.	Р3
		+	+	+	Антивірусні засоби.	Р4
2	Апаратура відображення і документуван-	+	+	+	Система розмежування і контролю доступу в приміщення.	Р1

№ п/п	Найменування можливого каналу НСД	Клас захисту			Засоби захисту	Міцність
		I	II	III		
1	2	3	4	5	6	7
	ня інформації					
3	Апаратура, що ремонтується та знаходиться на профілактиці	+ + + + +	+ + + - -	- - + - -	Система розмежування і контролю доступу в приміщення. Система контролю введення (виводу) апаратури в (з) робочий контур обміну інформацією. Засоби стирання залишків інформації. Засоби накладення на залишки інформації випадкової послідовності символів і чисел. Засоби знищення носіїв секретної інформації.	Р1 Р5 Р14 Р15 Р16
4	Машинні носії інформації	+ + + +	+ - - +	+ - - -	Облік і розмежування доступу до носіїв. Електронна ідентифікація носіїв. Шифрування інформації. Резервування інформації з охороною її копії.	Р6 Р7 Р8 Р9
5	Документи	+	+	+	Облік, реєстрація і розмежування доступу до документів.	Р10
6	Носії програмного забезпечення	+ + +	+ + +	+ + +	Облік, реєстрація і розмежу-вання доступу до носіїв ПЗ. Верифікація і контроль цілісності ПЗ. Резервування ПЗ з контролем доступу до його копії.	Р11 Р12 Р13
7	Машинні носії з залишками інформації (диски, стрічки)	+ + +	+ + -	+ + -	Облік, реєстрація і розмежування доступу. Засоби стирання інформації. Накладення випадкової послідовності символів і чисел.	Р6 Р14 Р15

№ п/п	Найменування можливого каналу НСД	Клас захисту			Засоби захисту	Міцність
		I	II	III		
1	2	3	4	5	6	7
		+	-	-	Засоби знищення носіїв.	Р16
8	Паперові носії з залишками інформації	+	+	-	Засоби знищення носіїв.	Р17
9	Засоби завантаження ПЗ	+	+	+	Засоби контролю і розмежування доступу в приміщення.	Р1 Р18
		+	+	-	Засоби контролю і блокування доступу до завантаження ПЗ.	Р4
		+	+	+	Антивірусні засоби.	
10	Пульти й органи керування, внутрішній монтаж апаратури	+	+	-	Засоби контролю і розмежування доступу в приміщення.	Р1
		+	+	-	Система контролю розкриття апаратури.	Р19
11	Внутрішні лінії зв'язку між апаратними засобами АС	+	+	-	Засоби контролю доступу на територію АС.	Р1
		+	+	-	Засоби контролю розкриття апаратури.	Р19
		-	+	-	Схована прокладка ліній зв'язку.	
		+	-	-	Шифрування переданої інформації.	Р20 Р21
12	Зовнішні канали зв'язку АС	+	+	+	Програма контролю і розмежування доступу до інформації АС (на вході АС).	Р24
		+	-	-	Шифрування інформації, що передається.	Р22
		+	+	+	Антивірусі засоби	
13	Побічне Електромагніт-	+	-	-	Засоби зниження або зашум-лення рівня випромінювання і наведень	Р23

№ п/п	Найменування можливого каналу НСД	Клас захисту			Засоби захисту	Міцність
		I	II	III		
1	2	3	4	5	6	7
	не випромінювання і наведення інформації				інформації на границі контрольованої зони об'єкта АС.	
14	Сміттєвий кошик	+	+	-	Засоби знищення носіїв закритої інформації.	Р17
Примітка: Знак "+" - наявність засобу захисту; знак "-" - відсутність засобу захисту.						

Для розрахунку міцності захисту інформації в АС проводиться аналіз можливого каналу НСД на предмет відповідності їхнього складу і кількості заданому класу захисту, поділу їх на контрольовані і неконтрольовані, наявність відповідних засобів захисту і можливе їхнє дублювання. До контрольованого в нашому прикладі по I класу захисту пропонується віднести засоби зі значеннями міцності: Р1, Р2, Р3, Р5, Р6, Р10, Р11, Р18, Р19, Р24. Перераховані значення обчислюються за формулою (8.14).

Для кожного можливого каналу НСД з урахуванням дублювання засобів захисту обчислюється значення міцності захисту. У нашому випадку такий розрахунок для каналів NN1, 3, 9, 10, 11 виробляється за формулою (8.17).

Після порівняння отриманих значень вибираємо менше з них, що і буде значенням міцності захисної оболонки, утвореної даними засобами, тобто використовуємо формулу (8.16).

До неконтрольованого можна віднести засоби з наступними значеннями міцності: Р8, Р14, Р15, Р16, Р17, Р21, Р23.

Розрахунок міцності захисту для кожного каналу ведемо аналогічним способом, використовуючи відповідні формули (8.1), (8.2), (8.12), оболонки в цілому - за формулами (8.10), (8.15) (8.16).

Чим більша довжина пароля, тим більшу безпеку буде забезпечувати система, тому що будуть потрібні великі зусилля для відгадування пароля. Цю обставину можна представити в термінах очікуваного часу розкриття пароля, або очікуваного безпечного часу. Очікуваний безпечний час – напівдобуток числа можливих паролів і часу, необхідного для того, щоб спробувати кожен пароль з послідовності запитів, тобто

$$t_{БЧ} = \frac{N_{ПАР} \cdot t_{ПАР}}{2} = \frac{N_{ПАР} \cdot N_{СИМ}}{2 \cdot R}, \quad N_{ПАР} = A^S, \tag{8.18}$$

де R - швидкість передачі (у симв/хв) у лінії зв'язку;

$N_{СИМ}$ - кількість символів у кожному переданому повідомленні при спробі одержати доступ (включаючи пароль і службові сим-воли);

$N_{ПАР}$ – кількість всіляких паролів;

$t_{ПАР}$ – час, необхідний для того, щоб спробувати кожен пароль з послідовності запитів;

S - довжина пароля;

A - число символів в алфавіті, з якого складається пароль (тобто для англійського A=26).

Приклад. Якщо R=60 млн. симв/хв, $N_{СИМ}$=20, S=8 і A=26, то безпечний час, що очікується,

$$t_{БЧ} = \frac{N_{ПАР} \cdot N_{СИМ}}{2 \cdot R} = \frac{A^S N_{СИМ}}{2 \cdot R} = \frac{26^8 \cdot 20}{2 \cdot 60 \cdot 10^6} = 34804{,}511 \text{ хв} \approx 24{,}2 \text{ доби}.$$

Якщо після кожної невдалої спроби автоматично передбачається десятисекундна затримка, то цим самим очікуваний час, необхідний для розкриття пароля, збільшується в шість разів і стає рівним приблизно шістдесяти рокам.

Якщо на додаток до R, $N_{СИМ}$, $N_{ПАР}$, S і A, визначеним вище, приймемо, що P - ймовірність того, що відповідний пароль може бути розкритий сторонньою особою, і $t_{ВІДКР.ПАР}$ - період часу, протягом якого можуть бути здійснені систематичні спроби, то P має нижню границю P_O, де

$$P_O = \frac{N_{ВІДКР.ПАР}}{N_{ПАР}}, \tag{8.19}$$

де $N_{ВІДКР.ПАР}$ - кількість спроб відкриття пароля за час $t_{ВІДКР.ПАР}$, дорівнює

$$N_{ВІДКР.ПАР} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ}}.$$

Тоді (1.2) можна представити у виді:

$$P_O = \frac{N_{ВІДКР.ПАР}}{N_{ПАР}} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} N_{ПАР}} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} A^S}, \tag{8.20}$$

оскільки $P \geq P_O$, то

$$P \geq \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} A^S}. \quad (8.21)$$

Переписавши (16.21) інакше, отримаємо формулу Андерсена

$$A^S \geq \frac{R \cdot t_{ВІДКР.ПАР}}{P \cdot N_{СИМ}}. \quad (8.22)$$

Якщо R, $N_{СИМ}$, $t_{ВІДКР.ПАР}$ і A фіксовані, то кожне значення S (довжина пароля) буде давати різну ймовірність P правильного його відгадування. Тоді для побудуви системи, де незаконний користувач мав би ймовірність відгадування правильного пароля не більшу, ніж P, варто вибрати таке S, що задовольняє виразу (8.22).

Приклад. Припустимо, що ми хочемо, використовуючи стандартний англійський шрифт, встановити такий пароль, щоб ймовірність його відгадування була не більшою 1/1000 (0,001) після тримісячного систематичного тестування. Припустимо, що швидкість передачі по лінії зв'язку $60 \cdot 10^6$ симв/хв і що за одну спробу посилається 20 символів. Використовуючи співвідношення (5.22), отримуємо

$$26^S \geq \frac{60 \cdot 10^6 \cdot 3 \cdot 30 \cdot 24 \cdot 60}{20 \cdot 0{,}001} = 3{,}888 \cdot 10^{15}.$$

Для S=6 отримаємо $26^S=3{,}089 \cdot 10^8$, і для S=7 – $26^7=8{,}03 \cdot 10^9$. Отже, за даних обставин нам варто вибрати S=7.

Як бачимо, на ймовірність P розкриття пароля робить вплив величина S. Збільшення довжини пароля тільки на один символ значно збільшує час, необхідний зловмисникові для розкриття цього пароля при систематичних спробах, організованих за допомогою ЕОМ. Так, якщо при відповідних умовах очікуваний безпечний час для семисимвольного пароля, обраного з 36-символьного алфавіту, складе близько 9 діб, очікуваний безпечний час для восьмисимвольного пароля складе 11 місяців.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Провести оцінку моделей систем захисту інформації.

1.1. Визначити імовірність неподолання перешкоди порушником $P_{сзі}$, при $P_{обх}=0$ і $t_ж > t_{под}$, користуючись даними таблиці. Зробити висновки.

Таблиця 8.2. Вихідні дані для розраху

№ варіанту	$P_{под}$
1.	0,25
2.	0,28
3.	0,25
4.	0,28
5.	0,31
6.	0,34
7.	0,37
8.	0,4
9.	0,43
10.	0,46
11.	0,49
12.	0,52
13.	0,55
14.	0,58
15.	0,61
16.	0,64
17.	0,67
18.	0,7
19.	0,73
20.	0,76
21.	0,79
22.	0,82
23.	0,85
24.	0,88
25.	0,91
26.	0,94
27.	0,97
28.	1
29.	1,03
30.	1,06

1.2 Провести розрахунок $P_{сзі}$ по формулі 8.2, відповідно до варіанту та даних таблиці 8.3. Зробити висновки.

Таблиця 8.3. Вихідні дані для розрахунку

№ варіанту	$P_{под}$	$P_{обх}$
1.	0,83	0,44
2.	0,89	0,97
3.	0,43	0,5
4.	0,13	0,69
5.	0,98	0,26
6.	0,75	0,83
7.	0,13	0,78
8.	0,64	0,42
9.	0,14	0,25
10.	0,55	0,43
11.	0,04	0,33
12.	0,18	0,92
13.	0,89	0,23
14.	0,01	0,17
15.	0,9	0,75

№ варіанту	$P_{под}$	$P_{обх}$
16.	0,63	0,14
17.	0,22	0,35
18.	0,06	0,11
19.	0,23	0,47
20.	0,89	0,62
21.	0,49	0,76
22.	0,94	0,57
23.	0,19	0,13
24.	0,59	0,26
25.	0,19	0,96
26.	0,73	0,72
27.	0,53	0,52
28.	0,63	0,44
29.	0,82	0,97

1.3. Провести розрахунок $P_{сзі}$ по формулі 8.3, відповідно до варіанту та даних таблиці 8.4.

Таблиця 8.4. Вихідні дані для розрахунку

№ варіанту	$P_{под}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$	$P_{обх4}$	$P_{обх5}$
1.	0,74	0,81	0,33	0,82	0,15	0,16
2.	0,74	0,44	0,18	0,77	0,92	0,16
3.	0,48	0,7	0,29	0,92	0,76	0,13
4.	0,61	0,57	0,99	0,62	0,43	0,79
5.	0,67	0,55	0,28	0,49	0,28	0,08
6.	0,42	0,57	0,92	0,68	0,47	0,85
7.	0,64	0,21	0,85	0,73	0,28	0,38
8.	0,91	0,71	0,95	0,17	0,8	0,95
9.	0,39	0,97	0,57	0,35	0,23	0,48
10.	0,71	0,97	0,92	0,43	0,53	0,03
11.	0,84	0,06	0,23	0,35	0,94	0,5
12.	0,11	0,36	0,31	0,05	0,83	0,87
13.	0,6	0,81	0,85	0,47	0,61	0,67
14.	0,05	0,61	0,93	0,25	0,36	0,53

№ варіанту	$P_{под}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$	$P_{обх4}$	$P_{обх5}$
15.	0,86	0,52	0,15	0,83	0,42	0,93
16.	0,02	0,59	0,05	0,62	0,38	0,46
17.	0,89	0,2	0,83	0,99	0,76	0,49
18.	0,15	0,01	0,03	0,61	0,28	0,99
19.	0,11	0,24	0,71	0,97	0,3	0,3
20.	0,33	0,29	0,93	0,71	0,63	0,25
21.	0,07	0,59	0,57	0,37	0,23	0,13
22.	0,15	0,18	0,61	0,64	0,66	0,16
23.	0,21	0,99	0,14	0,62	0,45	0,83
24.	0,55	0,03	0,72	0,89	0,82	0,13
25.	0,8	0,99	0,47	0,84	0,93	0,57
26.	0,96	0,81	0,11	0,81	0,5	0,73
27.	0,02	0,21	0,4	0,77	0,23	0,76
28.	0,29	0,62	0,61	0,69	0,92	0,63
29.	0,23	0,57	0,61	0,95	0,32	0,48
30.	0,2	0,4	0,89	0,06	0,52	0,16
31.						

1.4. Провести підбір параметрів $T_{оп}$, $t_{спр}$, $t_{в}$, $t_{бл}$, при $t_{под}$=0,7 для задоволення умови (8.4) або (8.5).

1.5.Провести підбір параметрів Топ, tпод, щоб Рпод=Х відповідно до формули (8.6). Х вибирається з таблиці 8.5 відповідно до варіанту:

Таблиця 8.5.

№ варіанту	Х
1.	0,1
2.	0,15
3.	0,25
4.	0,2
5.	0,18
6.	0,21
7.	0,23
8.	0,16

№ варіанту	X
9.	0,22
10.	0,27
11.	0,3
12.	0,31
13.	0,32
14.	0,33
15.	0,34
16.	0,35
17.	0,36
18.	0,37
19.	0,38
20.	0,39
21.	0,12
22.	0,13
23.	0,14
24.	0,17
25.	0,19
26.	0,11
27.	0,4
28.	0,41
29.	0,42
30.	0,43

1.6. Провести розрахунок $P_{сзі}$ по формулі 8.3, відповідно до варіанту та даних таблиці 8.6.

Таблиця 8.6. Вихідні дані для розрахунку

№ варіанту	$t_{под}$, с	$T_{оп}$ с	$t_{спр}$ с	$t_в$ с	$t_{бл}$ с	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	130	82	25	35	15	0,17	0,25	0,45
2.	131	81	26	34	16	0,81	0,54	0,48
3.	132	80	27	33	17	0,43	0,39	0,64
4.	133	79	28	32	18	0,83	0,17	0,7
5.	134	78	29	31	19	0,49	0,07	0,53
6.	135	77	30	30	20	0,24	0,63	0,09
7.	136	76	31	29	21	0,62	0,46	0,73
8.	137	75	32	28	22	0,73	0,01	0,51
9.	138	74	33	27	23	0,49	0,14	0,11
10.	139	73	34	26	24	0,62	0,98	0,15
11.	140	72	35	25	25	0,63	0,34	0,91
12.	141	71	36	24	26	0,52	0,44	0,36
13.	142	70	37	23	27	0,49	0,63	0,57
14.	143	69	38	22	28	0,91	0,38	0,26
15.	144	68	39	21	29	0,02	0,26	0,63
16.	145	67	40	20	30	0,94	0,43	0,49
17.	146	66	41	19	31	0,29	0,75	0,04
18.	147	65	42	18	32	1	0,65	0,8
19.	148	64	43	17	33	0,03	0,14	0,71
20.	149	63	44	16	34	0,61	0,77	0,43
21.	150	62	45	15	35	0,15	0,68	0,76
22.	151	61	46	14	36	0,16	0,17	0,97
23.	152	60	47	13	37	0,54	0,52	0,79
24.	153	59	48	12	38	0,27	0,96	0,82
25.	154	58	49	11	39	0,72	0,25	0,41
26.	155	57	50	10	40	0,53	0,13	0,54
27.	156	56	51	9	41	0,29	0,34	0,11
28.	157	55	52	8	42	0,76	0,82	0,7
29.	158	54	53	7	43	0,41	0,38	0,18
30.	159	53	54	6	44	0,23	0,65	0,69

1.7. Підібрати параметри λ , t , імовірність відмовлення системи відповідно до формули (8.13) складала 0,05.

2. Провести оцінку моделі багатоланкового захисту.

2.1. Розрахувати міцність захисту при використанні неконтрольованих перешкод відповідно до формули (8.15) при наступних параметрах, таблиця 8.7.

Таблиця 8.7.

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	0,04	0,99	0,64	0,75	0,57	0,09
2.	0,09	0,91	0,07	0,74	0,73	0,85
3.	0,25	0,62	0,28	0,03	0,38	0,77
4.	0,52	0,4	0,53	0,21	0,73	0,79
5.	0,21	0,45	0,27	0,89	0,26	0,92
6.	0,52	0,83	0,63	0,35	0,6	0,16
7.	0,71	0,78	0,59	0,32	0,3	0,8
8.	0,81	0,46	0,96	0,75	0,27	0,51
9.	0,93	0,35	0,41	0,94	0,77	0,23
10.	0,54	0,65	0,26	0,5	0,44	0,04
11.	0,22	0,96	0,56	0,58	0,01	0,29
12.	0,65	0,3	0,74	0,36	0,87	0,99
13.	0,29	0,07	0,82	0,05	0,46	0,44
14.	0,51	0,86	0,41	0,32	0,16	0,9
15.	0,23	0,17	0,74	0,04	0,82	0,06
16.	0,78	0,5	0,96	0,98	0,59	0,87
17.	0,18	0,57	0,86	0,51	0,58	0,49
18.	0,43	0,05	0,23	0,86	0,66	0,44
19.	0,2	0,18	0,98	0,81	0,07	0,68
20.	0,14	0,77	0,83	0,43	0,61	0,34
21.	0,47	0,83	0,28	0,65	0,88	0,52
22.	0,09	0,18	0,3	0,01	0,42	0,75
23.	0,02	0,86	0,64	0,75	0,94	0,14
24.	0,55	0,42	0,93	0,74	0,03	0,5
25.	0,03	0,54	0,08	0,03	0,92	0,47
26.	0,19	0,2	0,9	0,21	0,03	0,53
27.	0,13	0,88	0,4	0,89	0,84	0,55

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
28.	0,42	0,63	0,36	0,35	0,62	0,96
29.	0,77	0,42	0,2	0,32	0,56	0,51
30.	0,53	0,65	0,61	0,75	0,17	0,02

2.2. Провести розрахунок міцності багатоланкового захисту з контрольованими перешкодами відповідно до формули 8.16 при наступних параметрах, таблиця 8.8.

Таблиця 8.8

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	0,02	0,84	0,62	0,17	0,28	0,33
2.	0,37	0,87	0,02	0,08	0,36	0,1
3.	0,4	0,87	0,82	0,47	0,94	0,23
4.	0,41	0,19	0,29	0,94	0,61	0,26
5.	0,26	0,67	0,73	0,37	0,58	0,28
6.	0,33	0,68	0,18	0,89	0,15	0,9
7.	0,86	0,21	0,04	0,59	0,76	0,98
8.	0,6	0,78	0,11	0,77	0,07	0,02
9.	0,76	0,06	0,61	0,29	0,4	0,49
10.	0,49	0,99	0,51	0,35	0,07	0,62
11.	0,21	0,03	0,18	0,19	0,76	0,02
12.	0,56	0,92	0,58	0,52	0,57	0,6
13.	0,2	0,48	0,17	0,39	0,1	0,31
14.	0,6	0,03	0,27	0,64	0,06	0,48
15.	0,72	0,17	0,82	0,02	0,92	0,25
16.	0,43	0,89	0,36	0,39	0,48	0,08
17.	0,79	0,41	0,64	0,99	0,9	0,87
18.	0,71	0,25	0,35	0,94	0,89	0,96
19.	0,01	0,39	0,74	0,36	0,55	0,96
20.	0,94	0,52	0,8	0,65	0,19	0,9
21.	0,39	0,6	0,06	0,84	0,96	0,98
22.	0,28	0,4	0,38	0,8	0,77	0,89
23.	0,43	0,08	0,01	0,17	0,88	0,04
24.	0,79	0,35	0,62	0,12	0,05	0,28
25.	0,51	0,46	0,18	0,39	0,99	0,9

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
26.	0,19	0,71	0,1	0,53	0,98	0,01
27.	0,97	0,94	0,87	0,12	0,45	0,27
28.	0,99	0,91	0,56	0,76	0,29	0,5
29.	0,69	0,46	0,67	0,65	0,2	0,28
30.	0,1	0,94	0,29	0,7	0,28	0,76

2.3. Провести розрахунок сумарної міцності.

3. Провести розрахунок міцності захисту.

Провести розрахунок міцності контрольованого по І класу захисту інформації при наступних параметрах, таблиця 8.9:

Таблиця 8.9

№ варіанту	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
1.	0,02	0,84	0,62	0,17	0,28	0,33	0,03	0,5	0,4	0,08	0,09	0,1
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,37	0,87	0,02	0,08	0,36	0,1	0,4	0,87	0,82	0,47	0,94	0,23
2.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,37	0,87	0,02	0,08	0,36	0,1	0,02	0,84	0,62	0,17	0,28	0,33
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,02	0,84	0,62	0,17	0,28	0,33	0,03	0,5	0,4	0,08	0,09	0,1
3.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,4	0,87	0,82	0,47	0,94	0,23	0,03	0,5	0,4	0,08	0,09	0,1
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,41	0,19	0,29	0,94	0,61	0,26	0,26	0,67	0,73	0,37	0,58	0,28
4.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,67	0,73	0,37	0,58	0,28	0,26	0,26	0,67	0,73	0,37	0,58
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,33	0,68	0,18	0,89	0,15	0,9	0,26	0,26	0,67	0,73	0,37	0,58
5.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,86	0,21	0,04	0,59	0,76	0,98	0,26	0,26	0,67	0,73	0,37	0,58
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,6	0,78	0,11	0,77	0,07	0,02	0,49	0,99	0,51	0,35	0,07	0,62
6.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,76	0,06	0,61	0,29	0,4	0,49	0,56	0,92	0,58	0,52	0,57	0,6

№ варіанту	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,49	0,99	0,51	0,35	0,07	0,62	0,6	0,03	0,27	0,64	0,06	0,48
7.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,21	0,03	0,18	0,19	0,76	0,02	0,43	0,89	0,36	0,39	0,48	0,08
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,56	0,92	0,58	0,52	0,57	0,6	0,86	0,21	0,04	0,59	0,76	0,98
8.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,2	0,48	0,17	0,39	0,1	0,31	0,6	0,78	0,11	0,77	0,07	0,02
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,6	0,03	0,27	0,64	0,06	0,48	0,76	0,06	0,61	0,29	0,4	0,49
9.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,72	0,17	0,82	0,02	0,92	0,25	0,21	0,03	0,18	0,19	0,76	0,02
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,43	0,89	0,36	0,39	0,48	0,08	0,2	0,48	0,17	0,39	0,1	0,31
10.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,79	0,41	0,64	0,99	0,9	0,87	0,49	0,99	0,51	0,35	0,07	0,62
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,71	0,25	0,35	0,94	0,89	0,96	0,43	0,89	0,36	0,39	0,48	0,08
11.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,01	0,39	0,74	0,36	0,55	0,96	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,94	0,52	0,8	0,65	0,19	0,9	0,72	0,17	0,82	0,02	0,92	0,25
12.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,39	0,6	0,06	0,84	0,96	0,98	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,28	0,4	0,38	0,8	0,77	0,89	0,33	0,68	0,18	0,89	0,15	0,9
13.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,43	0,08	0,01	0,17	0,88	0,04	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,79	0,35	0,62	0,12	0,05	0,28	0,33	0,68	0,18	0,89	0,15	0,9
14.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,51	0,46	0,18	0,39	0,99	0,9	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,19	0,71	0,1	0,53	0,98	0,01	0,2	0,48	0,17	0,39	0,1	0,31
15.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25

№ варіанту	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,99	0,91	0,56	0,76	0,29	0,5	0,6	0,03	0,27	0,64	0,06	0,48
16.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,69	0,46	0,67	0,65	0,2	0,28	0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,1	0,94	0,29	0,7	0,28	0,76	0,2	0,48	0,17	0,39	0,1	0,31
17.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,03	0,5	0,4	0,08	0,09	0,1	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,03	0,5	0,4	0,08	0,09	0,1	0,33	0,68	0,18	0,89	0,15	0,9
18.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,03	0,5	0,4	0,08	0,09	0,1	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
19.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
							0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,97	0,94	0,87	0,12	0,45	0,27
20.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,2	0,48	0,17	0,39	0,1	0,31
21.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,97	0,94	0,87	0,12	0,45	0,27
22.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
							0,72	0,17	0,82	0,02	0,92	0,25
23.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,33	0,68	0,18	0,89	0,15	0,9
24.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,2	0,48	0,17	0,39	0,1	0,31	0,2	0,48	0,17	0,39	0,1	0,31

№ варіанту	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,33	0,68	0,18	0,89	0,15	0,9	0,97	0,94	0,87	0,12	0,45	0,27
25.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
26.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
27.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
28.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
29.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,33	0,68	0,18	0,89	0,15	0,9	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
30.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25

4. Провести оцінку довжини паролів і безпечного часу їх використання.

Використовуючи англійський шрифт та клавіші CapsLock, Shift, та цифрові клавіші встановити таку довжину, щоб ймовірність його відгадування була не більшою 1/1000 (0,001) після тримісячного систематичного тестування. Припустимо, що швидкість передачі по лінії зв'язку $50 \cdot 10^6$ симв/хв і що за одну спробу посилається 25 символів.

5. Зробити висновки та оформити звіт.

СПИСОК ЛІТЕРАТУРИ

1. ISO/IEC 27002:2022 (en). Information security, cybersecurity and privacy protection – Information security controls// Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en.

2. Лобанчикова Н.М. Захист інформації в АСУ : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

3. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.

4. Гребенніков В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій. 2013. Ужгород: Електронний репозитарій ДВНЗ "УжНУ". URI: https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070.

5. Денисюк В. О. Програмна реалізація стеганографічного алгоритму захисту інформації [Електронний ресурс] / В. О. Денисюк, А. В. Денисюк, Н. В. Денисюк // Ефективна економіка. – 2018. – № 4. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=6223.