КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет автоматизації і інформаційних технологій

Кафедра управління проєктами

П О Я С Н Ю В А Л Ь Н А З А П И С К А
ДО АТЕСТАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

на тему:

Управління проєктом створення комплексної системи захисту інформації на підприємстві

Никифорчук Вадим Дмитрович
(прізвище, ім’я та по батькові студента повністю)

Київ 2024 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій
Кафедра: Управління проєктами
Освітній рівень: Магістр за освітньо-професійною програмою
Галузь знань: 12 Інформаційні технології
Спеціальність: 122 «Комп'ютерні науки»
Освітня програма: «Управління проєктами»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Сергій БУШУЄВ
„___"_____2024 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

Никифорчук Вадим Дмитрович

(прізвище, ім'я та по батькові студента)

1. Тема роботи: " Управління проєктом створення комплексної системи захисту інформації на підприємстві."

затверджена наказом ректора КНУБА № № 1666/2 від « 20 » серпня 2024 року

2. Керівник роботи: Бушуєва Наталія Сергіївна, д.т.н., професор

(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Строк подання студентом роботи до захисту: 11.11.2024

4. Зміст пояснювальної записки (перелік питань, які слід розробити):

а)теоретичний розділ: загальні положення про комплексні системи захисту інформації; означення, позначення та скорочення; сутність та задачі комплексної системи захисту інформації; основні підходи до створення комплексної системи захисту інформації; поняття комплексної системи захисту інформації ; призначення комплексної системи захисту інформації; основні стратегії захисту інформації; розробка політики безпеки; основні напрямки захисту інформаційних ресурсів; виклики та можливості сучасності: комплексна система захисту інформації.

б)дослідницько-аналітичний розділ: побудова комплексної системи захисту інформації; побудова комплексної системи захисту інформації для туристичної фірми; опис діяльності туристичної фірми; етапи створення КСЗІ; статут проєкту створення КСЗІ;

в)рекомендаційний розділ: модель управління проєктом створення комплексної системи захисту інформації; управління змістом проєкту; організаційна структура проєкту; формування команди проєкту; управління термінами проєкту; управління вартістю проєкту; управління ризиками проєкту.

г) дослідження з використанням комп'ютерних технологій: Microsoft Office Word для оформлення роботи, таблиць, схем; Power Point для створення презентації; Microsoft Office Project для створення моделі проєкту.

5. Графічний матеріал за розділами:

графіки, таблиці, малюнки, структура декомпозиції робіт проєкту, організаційна структура проєкту, календарно-мережевий графік робіт проєкту.

6. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Збір матеріалів обраного напряму роботи	16.08.24-21.08.24
Опрацювання та аналіз матеріалів роботи	22.08.24-27.08.24
Вступ	28.08.24-01.09.24
Розділ 1.	02.09.24- 20.09.24
Розділ 2.	21.09.24-15.10.24
Розділ 3.	16.10.24-05.11.24
Висновки	06.11.24-07.11.24
Остаточне оформлення роботи	08.11.24-09.11.24
Перевірка роботи на плагіат	10.11.2024
Попередній захист роботи на кафедрі	11.11.2024
Направлення роботи на рецензування	12.11.2024

7. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Розділ 1.	---	---	---
Розділ 2.	----	---	---
Розділ 3.	-----	---	----

8. Дата видачі завдання 16.08.2024

Зав. кафедри Сергій БУШУЄВ
(підпис) (прізвище та ініціали)

Керівник Наталія БУШУЄВА
(підпис) (прізвище та ініціали)

Студент Вадим НИКИФОРЧУК
(підпис) (прізвище та ініціали)

РЕЗЮМЕ (summary) *до атестаційної випускної роботи студента:*			**Никифорчук В.Д.**
ЗВО	Київський національний університет будівництва і архітектури		
Тема	Управління проєктом створення комплексної системи захисту інформації на підприємстві		
Освітній ступінь	Магістр за освітньо-професійною програмою навчання		
Факультет	Автоматизації і інформаційних технологій		
Кафедра	Управління проєктами		
Спеціальність	122 «Комп'ютерні науки»		
Освітня програма	Управління проєктами		
Керівник	Бушуєва Наталія Сергіївна, д.т.н., професор		
Обсяг роботи:	*пояснювальна записка, стор.*	*розділів*	*слайдів презентації*
	105	*3*	*20*
Розділ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	Розділ присвячений фундаментальним аспектам комплексних систем захисту інформації (КСЗІ). В ньому детально розглядається поняття КСЗІ, її призначення та основні складові. КСЗІ – це не просто сукупність технічних засобів, а скоріше комплексний підхід, який включає організаційні, технічні та правові заходи. Розглядаються основні цілі створення КСЗІ. Серед них: забезпечення конфіденційності, цілісності та доступності інформації, захист від несанкціонованого доступу, витоків інформації та інших кіберзагроз. Проаналізовано різноманітні підходи до побудови ефективних КСЗІ, підкреслюючи важливість комплексного аналізу ризиків та розробки відповідних стратегій захисту. Окремий акцент робиться на сучасних викликах та можливостях у сфері кібербезпеки. Розглянуто вплив нових технологій на розвиток КСЗІ, а також проаналізовано зростаючі кіберзагрози та способи протидії їм. Загалом, розділ пропонує всебічне уявлення про сучасний стан та перспективи розвитку комплексних систем захисту інформації.		

Розділ 2. ПОБУДОВА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	Цей розділ присвячений практичному застосуванню концепції комплексної системи захисту інформації (КСЗІ) на прикладі туристичної фірми. Спочатку надається короткий опис діяльності типової туристичної фірми, включаючи її основні бізнес-процеси, типи інформації, що обробляються, та потенційні загрози інформаційній безпеці. Далі детально розглядаються етапи створення КСЗІ для туристичної фірми. Починаючи з аналізу ризиків та визначення вимог до безпеки, описано процес вибору та впровадження технічних та організаційних заходів захисту, таких як системи контролю доступу, антивірусне програмне забезпечення, політики безпеки та навчання персоналу. Розділ завершується розглядом статуту проєкту створення КСЗІ, який визначає цілі, завдання, ресурси, терміни та відповідальних осіб. В цілому, розділ надає практичні рекомендації щодо побудови ефективної КСЗІ для туристичної фірми, враховуючи специфіку її діяльності та інформаційні ризики.
Розділ 3. МОДЕЛЬ УПРАВЛІННЯ ПРОЄКТОМ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	Розділ фокусується на застосуванні принципів управління проєктами до процесу створення комплексної системи захисту інформації (КСЗІ). Детально розглянуто ключові аспекти управління проєктом КСЗІ, такі як управління змістом, організаційна структура, формування команди, управління термінами та вартістю, а також управління ризиками. В розділі підкреслюється важливість чіткого визначення змісту проєкту КСЗІ, включаючи цілі, завдання, вимоги до системи та очікувані результати. Описано різні організаційні структури проєкту, які можуть бути використані для ефективного управління процесом створення КСЗІ, та надано рекомендації щодо формування команди проєкту, підбору фахівців з необхідними компетенціями. Окрема увага приділяється управлінню термінами та вартістю проєкту КСЗІ. Розглянуто методи планування та контролю виконання робіт, а також методи бюджетування та контролю витрат. Важливою частиною розділу є аналіз ризиків, пов'язаних з проєктом КСЗІ. Описано процес ідентифікації, аналізу та оцінки ризиків, а також розглянуто стратегії управління ризиками, які спрямовані на мінімізацію негативного впливу на проєкт.

Висновки по роботі:	В даному досліджені продемонстровано створення ефективної комплексної системи захисту інформації (КСЗІ). Це одне з найважливіших завдань для будь-якої організації, особливо в умовах стрімкого розвитку інформаційних технологій та зростання кіберзагроз. Розроблена в роботі модель КСЗІ для туристичної фірми демонструє, що системний підхід до забезпечення інформаційної безпеки дозволяє ідентифікувати та мінімізувати ризики, пов'язані з захистом конфіденційних даних клієнтів та внутрішньої інформації компанії. Ключовим аспектом успішної реалізації проєкту з впровадження КСЗІ є чітке планування та управління усіма етапами цього процесу. Розглянуті в роботі методи управління проєктом дозволяють забезпечити своєчасне виконання завдань, ефективне використання ресурсів та досягнення поставлених цілей.
Ключові слова: комплексна система захисту інформації (КСЗІ), інформаційна безпека, кібербезпека, захист даних, інформаційні технології, туристична фірма **Keywords:** integrated information security system (IIS), information security, cybersecurity, data protection, information technology, travel agency	

Укладач: Вадим НИКИФОРЧУК

Керівник: Наталія БУШУЄВА

«8» листопада 2024 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет автоматизації і інформаційних технологій
Кафедра управління проєктами

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Сергій БУШУЄВ
“___” _____2024 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

Управління проєктом створення комплексної системи захисту інформації на підприємстві

(назва)

Виконав студент групи: _____

Никифорчук Вадим Дмитрович
(прізвище, ім’я та по батькові повністю)

Спеціальність: 122 «Комп’ютерні науки»

Освітня програма: Управління проєктами

Керівник: Бушуєва Н.С.
(прізвище, ініціали,)
д.т.н., професор
науковий ступінь, вчене звання

Рецензент:_____
(прізвище, ініціали,)
_____
науковий ступінь, вчене звання

Київ 2024р

ЗМІСТ

ВСТУП

Науково-технічна революція останнім часом прийняла грандіозні масштаби в сфері інформатизації суспільства на базі сучасних засобів обчислювальної техніки, зв'язку, а також сучасних методів автоматизованої обробки інформації. Застосування цих засобів і методів прийняло загальний характер, а створювані при цьому інформаційно-обчислювальні системи і мережі стають глобальними як в сенсі територіального розподілення, так і в сенсі широти охоплення в рамках єдиних технологій процесів збирання, передачі, накопичення, зберігання, пошуку, переробки інформації і видачі її для використання. Іншими словами, людство почало реалізацію завдання створення і використання цілої індустрії переробки інформації.

У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку. Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху в будь-якій сфері господарської діяльності. Монопольне володіння певною інформацією виявляється найчастіше вирішальною перевагою в конкурентній боротьбі і зумовлює, тим самим, високу ціну «інформаційного чинника». Широке впровадження персональних ЕОМ вивело рівень «інформатизації» ділового життя на якісно новий щабель. Нині важко уявити собі фірму або підприємство (навіть найдрібніші), що не були б озброєні сучасними засобами обробки і передачі інформації. У ЕОМ на носіях даних накопичуються значні обсяги інформації, яка часто має конфіденційний характер або становить велику цінність для її власника.

В даний час характерними і типовими стають такі особливості використання обчислювальної техніки:

− зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;

− наростаюча важливість і відповідальність рішень, прийнятих в автоматизованому режимі і на основі автоматизованої обробки інформації;

− збільшення концентрації в автоматизованих системах (АС) обробки даних інформаційно-обчислювальних ресурсів;
− велике територіальне розподілення компонентів АС;
− ускладнення режимів функціонування технічних засобів АС;
− накопичення на технічних носіях величезних обсягів інформації, причому для багатьох видів інформації стає все більш важким (і навіть неможливим) виготовлення немашинних аналогів (дублікатів);
− інтеграція в єдиних базах даних інформації різного призначення і різної належності;
− довготривале зберігання великих масивів інформації на машинних носіях;
− безпосередній і одночасний доступ до ресурсів (в тому числі і до інформації) АС великого числа користувачів різних категорій та різних установ;
− інтенсивна циркуляція інформації між компонентами АС, у тому числі і розташованих на великих відстанях один від одного;
− зростаюча вартість ресурсів АС.

Проте створення індустрії переробки інформації, даючи об'єктивні передумови для грандіозного підвищення ефективності життєдіяльності людства, породжує цілий ряд складних і великомасштабних проблем. Однією з таких проблем є надійне забезпечення збереження встановленого статусу використання інформації, що циркулює і обробляється в інформаційно-обчислювальних установках, центрах, системах і мережах, або коротко – в автоматизованих системах обробки даних. Дана проблема увійшла в побут під назвою проблеми захисту інформації або забезпечення безпеки інформації.

Актуальність дослідження. У сучасному світі, де інформація стала одним з найцінніших активів підприємств, забезпечення її безпеки набуває все більшої важливості. Зростання кіберзагроз, постійна еволюція технологій та посилення вимог до захисту даних роблять створення ефективних систем захисту інформації критично важливим завданням. Управління проєктом, спрямованим на розробку та впровадження такої системи, є складним і багатоаспектним процесом, який вимагає застосування сучасних методологій і інструментів.

Мета дослідження. Метою даного дослідження є розробка теоретико-методичних основ та практичних рекомендацій щодо ефективного управління проєктом створення комплексної системи захисту інформації на підприємстві.

Предмет і об'єкт дослідження. Предметом дослідження є процес управління проєктом створення комплексної системи захисту інформації. Об'єктом дослідження є підприємство, на якому реалізується проєкт.

Для досягнення мети дослідження необхідно вирішити наступні завдання:

1. Проаналізувати сучасний стан та тенденції розвитку систем захисту інформації. Визначити основні загрози, що виникають перед підприємствами, та проаналізувати існуючі підходи до забезпечення інформаційної безпеки.
2. Дослідити теоретичні основи управління проєктами в сфері інформаційної безпеки. Виявити специфічні особливості таких проєктів та визначити вимоги до компетенцій проєктного менеджера.
3. Розробити модель управління проєктом створення комплексної системи захисту інформації. Створити деталізовану модель, яка включатиме всі етапи проєкту, від планування до впровадження та супроводу.
4. Оцінити ефективність різних методів і інструментів управління проєктами в контексті створення систем захисту інформації. Провести порівняльний аналіз популярних методологій (наприклад, Waterfall, Agile, Scrum) та інструментів (MS Project) для визначення оптимального підходу.

Для вирішення поставлених завдань будуть використані наступні методи дослідження:

- Теоретичні методи: аналіз наукової літератури, систематизація та узагальнення теоретичних положень, абстрагування, синтез.
- Системний аналіз: виявлення взаємозв'язків між елементами системи захисту інформації та процесами управління проєктом.
- Методи управління проєктами: планування, організація, контроль, координація, аналіз ризиків.

РОЗДІЛ 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

«Хто володіє інформацією, той володіє світом» -
одного разу сказав Ротшильд.
«Хто володіє інформацією, той володіє світом.
Інше повідомлення коштує дорожче життя » -
з часом доповнив Черчілль, крилату фразу Ротшильда.

Реалії ж сучасного бізнесу такі, що інформацією потрібно не тільки володіти, а й вміти її ефективно захищати. Згідно оглядам міжнародних агентств з інформаційної безпеки можна констатувати наступне:

- ✓ інформація стає основною метою нових організаторів атак;
- ✓ метою створення шкідливих програм і проведення атак стає, крім отримання грошового прибутку, крадіжка і подальше використання будь-якої можливої інформації;
- ✓ з'являється Spyware 2.0 - новий клас шкідливих програм, націлений як на крадіжку персональної інформації користувачів (identity theft), так і на тотальну крадіжку всіх інших даних.

Саме на вирішення питань ефективного захисту інформації, як від зовнішніх, так і від внутрішніх загроз, направлено створення комплексної системи захисту інформації (КСЗІ) в автоматизованих системах підприємства.

Комплексні системи захисту інформації – це сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Організаційні заходи є обов'язковою складовою побудови КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

КСЗІ є глобальною концепцією безпеки і основою для безпеки інфраструктури підприємства в цілому.

1.1 Означення, позначення та скорочення

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Система ТЗІ – сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Контрольована зона – територія, на якій унеможливлюється несанкціоноване перебування сторонніх осіб.

Модель загроз – формалізований опис методів та засобів здійснення загроз для інформації.

Інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку.

Виділені приміщення – приміщення, в яких циркулює інформація з обмеженим доступом.

Контрольно-інспекційна робота з питань ТЗІ – діяльність, спрямована на визначення та вдосконалення стану ТЗІ органів, щодо яких здійснюється ТЗІ, та на проведення контролю за виконанням суб'єктами системи ТЗІ завдань або проведенням діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями.

Атестація виділених приміщень – комплекс робіт, спрямованих на реалізацію заходів з ТЗІ, метою яких є приведення виділених приміщень відповідно до вимог нормативних документів з ТЗІ та визначення відповідності захищеності виділеного приміщення встановленій категорії.

Порушення з ТЗІ – невиконання вимог нормативно-правових актів з питань ТЗІ, яке створює умови або реальну можливість порушення конфіденційності, цілісності або доступності інформації.

Інші терміни використовуються згідно з:

– НД ТЗІ 1.1–003–99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»;

– ДСТУ 3396.2 «Захист інформації. Технічний захист інформації. Терміни та визначення»;

– «Термінологічний довідник з технічного захисту інформації на 11 об’єктах інформаційної діяльності».

Позначення і скорочення:

БД – база даних;

ДТЗ – допоміжні технічні засоби;

ЕОМ – електронно-обчислювальна машина;

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КРТ – копіювально-розмножувальна техніка;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ОТЗ – основні технічні засоби;

ПЗІ – підрозділ захисту інформації;

ПЕМВН – побічні електромагнітні випромінювання і наведення;

ПЗ – програмне забезпечення;

ПЗП – постійний запам’ятовувальний пристрій;

ПРД – правила розмежування доступу;

ПМА – програми та методики атестації;

ТЗІ – технічний захист інформації.

1.2 Сутність та задачі комплексної системи захисту інформації

1.2.1 Основні підходи до створення комплексної системи захисту інформації

Існує думка, що проблеми захисту інформації стосуються виключно інформації, що обробляється комп'ютером. Це, мабуть, пов'язано з тим, що комп'ютер і, зокрема, персональний комп'ютер є «ядром», центром зберігання інформації. Об'єкт інформатизації, стосовно якого спрямовані дії щодо захисту інформації, видається більш широким поняттям порівняно з персональним комп'ютером.

У реальному житті всі ці окремі «об'єкти інформатизації» розташовані в межах одного підприємства і являють собою єдиний комплекс компонентів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д.

Сучасне підприємство – велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх і зовнішніх чинників, які часто не піддаються чіткому кількісному оцінюванню, призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентам.

Характерною особливістю подібних систем є, насамперед, наявність людини в кожній зі складових підсистем і віддаленість людини від об'єкта її діяльності. Це відбувається у зв'язку з тим, що безліч компонентів, які складають об'єкт інформатизації, інтегрально може бути подано сукупністю трьох груп систем: 1) люди (біосоціальні системи); 2) техніка (технічні системи та приміщення, в яких вони розташовані); 3) програмне забезпечення, яке є інтелектуальним посередником між людиною і технікою (інтелектуальні системи). Сукупність цих трьох груп утворює соціотехнічну систему. Таке уявлення про соціотехнічну систему є досить поширеним і може стосуватися

багатьох об'єктів. Коло наших інтересів обмежується дослідженням безпеки систем, призначених для обробки вхідної інформації і видачі результату.

Якщо звернутися до історії цієї проблеми, то можна умовно виділити три періоди розвитку засобів захисту інформації (ЗІ):

– перший ми відносимо до того часу, коли обробка інформації здійснювалася за традиційними (ручними, паперовими) технологіями;

– другий – коли для обробки інформації на регулярній основі застосовувалися засоби електронної обчислювальної техніки перших поколінь;

– третій – коли використання засобів електронно-обчислювальної техніки набрало масового і повсюдного характеру (поява персональних комп'ютерів).

У 60–70 рр. XX ст. проблема захисту інформації вирішувалася досить ефективно застосуванням, в основному, організаційних заходів. До них належали: режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання цих засобів досягалася за рахунок концентрації інформації в певних місцях (спец. сховища, обчислювальні центри), що сприяло забезпеченню захисту відносно малими силами.

«Розподілення» інформації по місцях зберігання і обробки загострило ситуацію з її захистом. З'явилися дешеві персональні комп'ютери. Це дало можливість побудови мереж ЕОМ (локальних, глобальних, національних і транснаціональних), які можуть використовувати різні канали зв'язку. Ці чинники сприяють створенню високоефективних систем розвідки і отримання інформації. Вони знайшли відображення і на сучасних підприємствах [2].

Сучасне підприємство являє собою складну систему, в рамках якої здійснюється захист інформації. Розглянемо основні особливості сучасного підприємства:

– складна організаційна структура;

– багатоаспектність функціонування;

– висока технічна оснащеність;

– широкі зв'язки з кооперації;

– необхідність розширення доступу до інформації;

– зростаюча питома вага цифрової технології обробки інформації;

− зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;

− важливість і відповідальність рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації;

− висока концентрація в автоматизованих системах інформаційних ресурсів;

− велике територіальне розподілення компонентів автоматизованих систем;

− накопичення на технічних носіях величезних обсягів інформації;

− інтеграція в єдиних базах даних інформації різного призначення і різної належності;

− довгострокове зберігання великих обсягів інформації на машинних носіях;

− безпосередній і одночасний доступ до ресурсів (також і до інформації) автоматизованих систем великого числа користувачів різних категорій і різних установ;

− інтенсивна циркуляція інформації між компонентами автоматизованих систем, також і віддалених один від одного.

Таким чином, створення індустрії переробки інформації, з одного боку, формує об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, а з іншого – породжує цілий ряд складних і великомасштабних проблем. Однією з них є забезпечення збереження встановленого статусу інформації, що циркулює і обробляється на підприємстві, в організації.

1.2.2 Поняття комплексної системи захисту інформації

Роботи з захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не вважає, що досить

провести на підприємстві ряд організаційних заходів, ввести до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговувального персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних, організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ.

На основі теоретичних досліджень і практичних робіт у сфері ЗІ сформульований системно-концептуальний підхід до захисту інформації.

Під системністю як основною частиною системно-концептуального підходу розуміється:

– системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт із ЗІ і управління ними [2].

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінювання економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід – це принцип розгляду проєкту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені такі її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті;

2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри

і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі сфер інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій із захисту інформації, переданої сигналами в кабельній лінії, що проходить територіями різних об'єктів. Як би не встановлювались межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними;

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декілька варіантів побудови системи, що забезпечують задані цілі функціонування. Для того, щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати

ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісне оцінювання на всіх етапах створення системи.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу [3].

Концептуальна модель інформаційної безпеки

Мета моделі:

- модель показує як проєктувати комплексну систему захисту інформації;
- модель розкриває основні напрямки захисту інформації;

Рисунок 1.1 Концептуальна модель інформаційної безпеки

1.2.3 Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації – забезпечення надійності ЗІ. Система ЗІ – це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого – самі організовують систему, здійснюючи захисні заходи.

Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами та пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальні СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правовий, організаційний, інженерно-технічний).

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які забезпечують або можуть впливати на якість захисту. Наприклад, система охоплює якісь об'єкти захисту, а всі вони внесені до неї чи ні – це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності (рисунок 1.2).

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися все, виходячи з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, в усіх місцях її збирання, зберігання, передачі і використання, весь час і при всіх режимах функціонування систем обробки інформації.

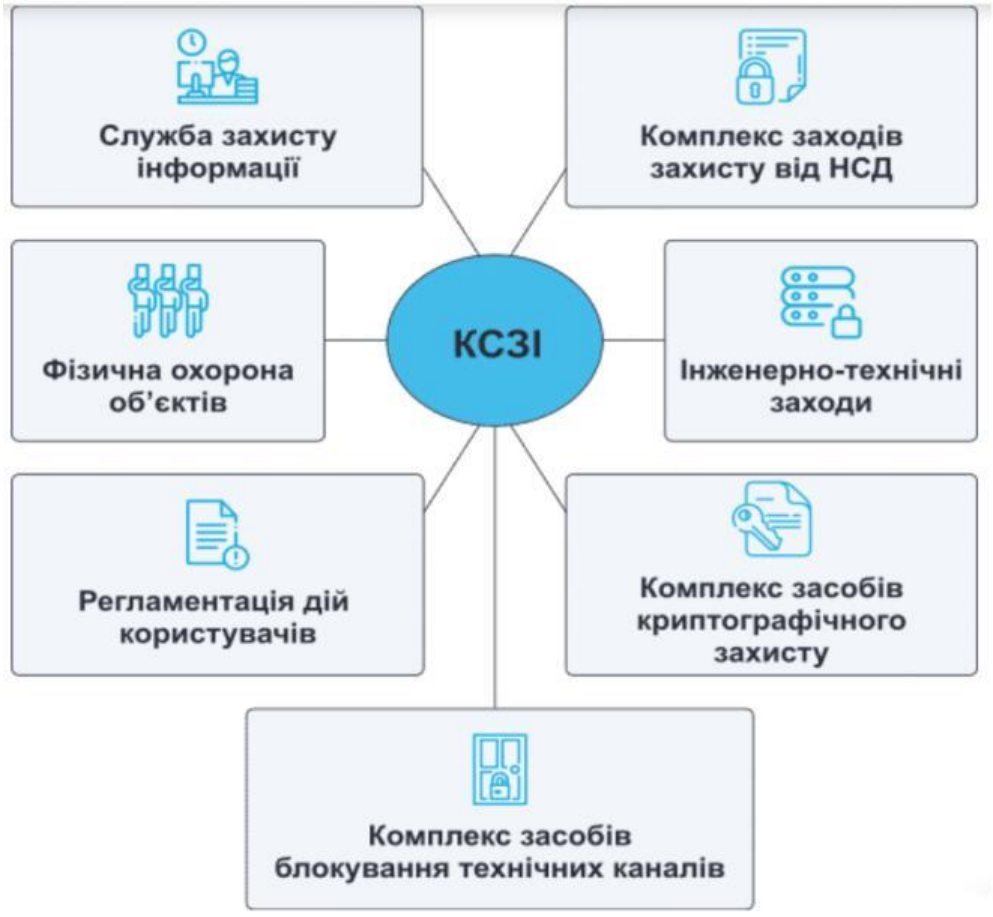

Рисунок 1.2 Модель комплексної системи захисту інформації

У той же час комплексність не усуває, а, навпаки, передбачає диференційований підхід до захисту інформації, залежно від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності,

засобів зберігання і обробки, форм і умов прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації полягає у:

– інтеграції локальних систем захисту;

– забезпеченні повноти всіх складових системи захисту;

– забезпеченні всеосяжності захисту інформації.

Виходячи з цього, можна сформулювати нижченаведене означення. «Комплексна система захисту інформації – система, що повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї захищуваної інформації».

1.3 Основні стратегії захисту інформації

Усвідомлення необхідності розробки стратегічних підходів до захисту формувалося в міру усвідомлення важливості, натхнення і проблеми захисту, а також неможливості ефективного її здійснення простим використанням деякого набору засобів захисту.

Під стратегією взагалі розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації.

Відомий канадський фахівець у сфері стратегічного управління Г. Мінцберг запропонував визначення стратегії в рамках системи «5-Р». На його думку, вона містить:

1) план (Plan) – заздалегідь намічені в деталях і контрольовані дії на певний термін, що переслідують конкретні цілі;

2) прийом, або тактичний хід (Ploy), що є короткочасною стратегією, яка має обмежені цілі, спроможна змінюватися та маневрувати з метою використати їх проти противника;

3) модель поведінки (Patten of behaviour) – часто спонтанну, неусвідомлену, що не має конкретних цілей;

4) позицію щодо до інших (Position in respect to others);

5) перспективу (Perspective).

Завдання стратегії полягає у створенні конкурентної переваги, усуненні негативного ефекту нестабільності навколишнього середовища, забезпеченні прибутковості, врівноваженні зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими організація стикається в повсякденному житті.

Здатність компанії, організації проводити самостійну стратегію в усіх сферах робить її більш гнучкою, стійкою, дозволяє адаптуватися до вимог часу і обставин.

Стратегія формується під впливом внутрішнього і зовнішнього середовищ, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати.

Фактори, які можуть мати для фірми вирішальне значення в майбутньому, називаються стратегічними. На думку одного з провідних західних фахівців Б. Карлофа, вони, впливаючи на стратегію будь-якої організації, надають і специфічні властивості. До таких факторів належать:

1) мета, яка відображає філософію фірми, організації, її призначення;

2) конкурентні переваги, які організація має в своїй сфері діяльності порівняно з суперниками або до яких прагне (вважається, що вони найбільше впливають на стратегію). Конкурентні переваги будь-якого типу забезпечують більш високу ефективність використання ресурсів підприємства;

3) характер продукції, що випускається, особливості її збуту, післяпродажного обслуговування, ринки та їх межі;

4) організаційні чинники, серед яких виділяється внутрішня структура компанії та її очікувані зміни, система управління, ступінь інтеграції і диференціації внутрішніх процесів;

5) наявні ресурси (матеріальні, фінансові, інформаційні, кадрові та ін.). Чим вони більші, тим масштабнішими можуть бути інвестиції в майбутні

проєкти. Сьогодні для розробки і реалізації стратегії велике значення мають, перш за все, структурні, інформаційні та інтелектуальні ресурси. Порівнюючи значення параметрів готівки і потрібних ресурсів, можна визначити ступінь їх відповідності стратегії;

6) потенціал розвитку організації, вдосконалення діяльності, розширення масштабів, зростання ділової активності, інновацій;

7) культура, філософія, етичні погляди і компетентність управлінців, рівень їх домагань і підприємливості, здатність до лідерства, внутрішній клімат в колективі.

На стратегічний вибір впливають: ризик, на який готова йти фірма; досвід реалізації чинних стратегій, позиції власників, наявність часу. Розглянемо особливості стратегічних рішень. За ступенем регламентованості вони належать до контурних (надають широку свободу виконавцям стосовно тактики), а за ступенем обов'язковості проходження головних установок – директивним [4, 5].

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими способами здійснення в певних ситуаціях тих чи інших дій. З точки зору визначеності, ці рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати. З точки зору важливості, стратегічні рішення кардинальні: стосуються основних проблем і напрямків діяльності фірми, визначають основні шляхи розвитку її в цілому, окремих підрозділів або видів діяльності на тривалу перспективу (не менше 5–10 років). Вони випливають, насамперед, із зовнішніх, а не з внутрішніх умов, повинні враховувати тенденції розвитку ситуації та інтереси безлічі суб'єктів. Практична незворотність стратегічних рішень обумовлює необхідність їх ретельної та всебічної підготовки. Стратегічним рішенням притаманна комплексність. Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами. Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу,

ринків, способи реакції на непередбачені події. Практика сформувала нижченаведені вимоги до стратегічних рішень:

1. Реальність, що передбачає її відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду й навичкам працівників і менеджерів, культурі, існуючій системі управління;

2. Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасність (реалізація рішення повинна встигнути призупинити негативний розвиток ситуації або не дозволити упустити вигоду);

4. Сумісність із середовищем, що забезпечує можливість взаємодії з ним (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

5. Спрямованість на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткий розподіл за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Облік прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути при реалізації стратегії або при відмові від неї для фірми, її партнерів в зв’язку з існуючим законодавством, етичною стороною права, допустимим рівнем ризику та інше.

Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

– виділяти, відстежувати і оцінювати ключові проблеми;

– адекватно і оперативно реагувати на зміни всередині і в оточенні організації;

– вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;

– створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Вихідний момент формування стратегії – постановка глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінювання яких дозволяє вибрати кращу стратегію.

Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено три стратегії захисту:

– оборонна – захист від вже відомих загроз, здійснюваний автономно, тобто без надання істотного впливу на інформаційно-керувальну систему;

– наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно-керувальної системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

– упереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для прояву.

1.4 Розробка політики безпеки

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі

особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, що виражається через сукупність факторів або критеріїв, які уточнюють мету. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки знати відповідні стандарти і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але й, наприклад, проявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів з організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити такі процеси, пов'язані з розробкою і реалізацією політики безпеки:

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінювання відповідності заходів забезпечення захисту інформації системи деякого еталонного зразка: стандарт, профіль захисту тощо.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту заданої безпеки.

4. Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій безпеки для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше, некоректно. Відзначимо лише, що для розробки моделей застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі. Слід відзначити, що засоби

захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки дають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, яке має на увазі, що

• всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

• права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу [6].

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі, що

– всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність, яка міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру, і, таким чином, в системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вища його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт, крім рівня прозорості, має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала ряду вимог, які будуть розглянуті в наступному розділі.

1.5 Основні напрямки захисту інформаційних ресурсів

Правові заходи

- Виконання норм і положень держполітики в сфері захисту.
- Контроль за захищеністю інформації, що є власністю держави.

Організаційні заходи

- Політика безпеки
- Режимні заходи
- Створення структури, відповідальної за безпеку інформації
- Контроль за виконанням та ефективністю заходів по захисту інформації

Програмно-апаратні засоби захисту

- Технічний захист інформації
  - Захист від витоків технічними каналами
  - Захист від несанкціонованого доступу
- Антивірусний захист
  - Аутентифікація і авторизація користувачів
  - Розмежування доступу до інформаційних ресурсів
  - Аудит
- Криптографічний захист інформації

Інженерні засоби захисту

- Створення системи гарантованого електропостачання
- Обладнання приміщень системою контролю доступу
- Створення екрануючих споруд

1.6 Виклики та можливості сучасності: комплексна система захисту інформації

У сучасному цифровому віці, де інформаційні технології переплітаються з усіма аспектами життя, захист інформації стає надзвичайно актуальною та критичною задачею. З ростом кількості зв’язаних пристроїв, масштабуванням хмарних сервісів та зростанням кількості кіберзагроз, традиційні методи захисту стають недостатніми для забезпечення стійкої інформаційної безпеки.

Основним шляхом пошуку захисту інформації в складних інформаційних системах є вдосконалення системного підходу до самої проблеми захисту. Під системністю розуміється, що захист інформації передбачає не лише створення

відповідних захисних механізмів, але також включає регулярний процес, який застосовується на всіх етапах життєвого циклу інформаційної системи та використовує всі наявні засоби захисту. Це означає, що захист інформації повинен бути розглянутий як невід'ємна частина всієї інформаційної системи, а не просто як окремий компонент.

У сучасних умовах глобалізації та зростаючої конкуренції, захист інформації стає надзвичайно важливим аспектом як для організацій, так і для державних підприємств та корпорацій України. Створення надійних систем захисту і збереження інформаційних ресурсів на рівні всієї організації і її окремих підрозділів стає все більш актуальним, а успішність таких заходів безпосередньо впливає на конкурентоспроможність організації в цілому.

На сьогоднішній день, існують два основних підходи до визначення оптимальної стратегії побудови систем захисту інформації організацій.

Перший підхід базується на перевірці відповідності рівня захищеності інформації в організації вимогам законодавчих актів або стандартів в галузі інформаційної безпеки. Однак цей підхід має свої недоліки, зокрема, коли рівень захисту інформації не визначений чітко, ускладняється вибір оптимального варіанту системи захисту.

Другий підхід використовує методи та моделі оптимізації складних систем для визначення найкращого варіанту побудови систем захисту інформації. Цей підхід дозволяє більш ефективно враховувати особливості конкретної організації та знаходити оптимальні рішення з урахуванням різноманітних факторів.

Стрімкий розвиток інформаційних технологій привів до проблем захисту інформації або забезпечення безпеки інформації. Комплексні системи захисту інформації (КСЗІ) допомагають у вирішенні цих проблем. Дослідження та огляд методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих системах (АС) є актуальними в цей час.

Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [3].

Українське законодавство по своєму захищає інформацію, відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» «Умови обробки інформації в системі Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.» [4].

Також законодавець визначає низку нормативно-правових документів у сфері комплексної системи захисту інформації:

- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Закон України «Про захист персональних даних»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;
- «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» (затверджені ПКМУ від 29.03.2006 №373).

До процесу створення КСЗІ залучаються наступні зацікавлені сторони:
– організація, для якої здійснюється побудова КСЗІ (Замовник);
– організація, що здійснює заходи з побудови КСЗІ (Виконавець);
– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (орган контролю);
– організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);
– організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник) [10].

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи. Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних, організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ [10].

Ефективність функціонування комплексних систем захисту інформації (КСЗІ) залежить від багатьох взаємопов’язаних елементів, які взаємодіють між собою. Зазвичай, оцінка ефективності КСЗІ здійснюється шляхом аналізу різноманітних критеріїв. Відсутність єдиного підходу до розв’язання таких завдань призводить до застосування різних, незалежних один від одного, методів оцінки рівня захисту інформації.

Процес визначення ефективності систем захисту розпочинається з вибору та обґрунтування показників або критеріїв, які використовуються для оцінки ефективності КСЗІ. Після цього переходять до розробки або вибору методик розрахунку цих показників, що дозволяють оцінити рівень захисту системи.

Істотна частина проблем забезпечення захисту такої інформації може бути вирішена відомими правовими та організаційними заходами, однак, враховуючи розвиток інформаційних технологій, наявна тенденція зростання необхідності застосування технічних заходів і засобів її захисту. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів [15].

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінювання економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця [17].

Основні завдання, які повинна вирішувати комплексна система захисту інформації включають:

- Управління доступом користувачів до ресурсів інформаційної системи, забезпечення захисту від несанкціонованого доступу та втручання з боку сторонніх осіб, а також з обмеженням повноважень персоналу організації та користувачів.
- Захист даних, які передаються по каналах зв'язку, щоб забезпечити конфіденційність і цілісність інформації.
- Реєстрація, збір, зберігання, обробка і видача інформації про всі події, пов'язані з безпекою системи, для забезпечення контролю та аналізу потенційних загроз.
- Контроль діяльності користувачів системи з боку адміністрації, а також оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу.

- Забезпечення цілісності критичних ресурсів системи та перевірка середовища виконання прикладних програм з метою попередження можливих загроз безпеці.
- Створення замкнутого середовища для перевіреного програмного забезпечення з метою захисту від шкідливих програм, вірусів та засобів обходу системи захисту.
- Управління засобами комплексної системи захисту, що включає їх конфігурацію, моніторинг та аналіз ефективності.

Основні принципи організації КСЗІ:

• системність;

• комплексність;

• безперервність захисту;

• розумна достатність;

• гнучкість управління і застосування;

• відкритість алгоритмів і механізмів захисту;

• простота застосування захисних заходів і засобів [13].

Висновки до розділу 1

Забезпечення безпеки і захисту інформації стає надзвичайно важливим у сучасних умовах глобалізації та зростаючої конкуренції для організацій і державних підприємств України. Підхід до захисту інформації повинен бути системним і охоплювати всі аспекти процесу, від початкового проєктування та розробки системи до експлуатації, підтримки та оновлення.

На сьогоднішній день, існують два основних підходи до визначення оптимальної стратегії побудови систем захисту інформації організацій.

Перший підхід базується на перевірці відповідності рівня захищеності інформації в організації вимогам законодавчих актів або стандартів в галузі інформаційної безпеки. Однак цей підхід має свої недоліки, зокрема, коли рівень захисту інформації не визначений чітко, ускладняється вибір оптимального варіанту системи захисту.

Другий підхід використовує методи та моделі оптимізації складних систем для визначення найкращого варіанту побудови систем захисту інформації. Цей підхід дозволяє більш ефективно враховувати особливості конкретної організації та знаходити оптимальні рішення з урахуванням різноманітних факторів.

Стрімкий розвиток інформаційних технологій привів до проблем захисту інформації або забезпечення безпеки інформації. Комплексні системи захисту інформації (КСЗІ) допомагають у вирішенні цих проблем. Дослідження та огляд методів і засобів, об’єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих системах (АС) є актуальними в цей час.

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних

заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Законодавство України також регулює питання захисту інформації, вимагаючи застосування комплексної системи захисту з підтвердженою відповідністю для інформації з обмеженим доступом.

Загалом, ефективність систем захисту інформації визначається ретельним аналізом, плануванням та впровадженням комплексу організаційних, технологічних і технічних заходів, які забезпечують надійний захист інформації в умовах зростаючих загроз та вимог сучасного світу.

РОЗДІЛ 2 ПОБУДОВА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Побудова комплексної системи захисту інформації для туристичної фірми

Даний розділ атестаційної роботи присвячений розробці комплексної системи захисту інформації для туристичної фірми «Мандри світом».

2.1.1 Опис діяльності туристичної фірми

Туристична фірма «Мандри світом» була заснована в 2007 році в м. Чернігові.

В 2018 році проведений ребрендинг, оптимізовані напрямки діяльності, покращений сайт і з'явилась можливість замовлення турів через онлайн з будь-якої точки світу.

Основні напрямки діяльності турфірми:

Екскурсії по Україні: великий вибір різноманітних турів, індивідуальні та групові поїздки, тури вихідного дня. Транспортне обслуговування, поселення в хостели, готелі, екскурсійне обслуговування, харчування. Турфірма співпрацює з організаціями та підприємствами.

Екскурсії до Європи: величезний вибір екскурсій Європою, авіа-, автобусні, групові, індивідуальні тури, відразу ж онлайн бронювання, професійне обслуговування та великий досвід роботи в цьому напрямку менеджерів.

В'їзний туризм: турфірма здійснює комплексне обслуговування туристів по Чернігову та області (прийом туристів, зустріч, транспортне обслуговування, поселення в готель, харчування, екскурсійне обслуговування). Менеджери

турфірми пропонують більш доступне та якісне обслуговування клієнтів (пасажирів) за вибраними маршрутами.

Відпочинок на морі, «гарячі» тури, пляжний відпочинок, екзотика: Туреччина, Єгипет, Домінікана, Іспанія, Чорногорія, Грузія, Болгарія, Греція, Мальдіви, Тайланд та ін.

Доступний індивідуальний та сімейний відпочинок, допомога при здійснені поїздки власним та орендованим транспортом, автобусами, мікроавтобусами, групові тури (Болгарія, Чорногорія, Греція, Італія, пропонуються для проживання бази відпочинку та готелі.

Дитячий відпочинок у таборах України та Європи, групові пізнавальні тури, екскурсії у зоопарк, парки відпочинку, морські тури та гірськолижні курорти.

Круїзні тури по Європі, Індійський океан, Австралія, Середиземне, Красне море, Кариби, Егейське море, тихоокеанські та трансатлантичні круїзи, кругосвітні подорожі та інші.

Є можливість онлайн-бронювання та відправки заявок і замовлень із сайту турфірми. Візи, готелі, залізничні квитки та авіабронювання.

Довіра клієнтів і хороші рекомендації є основою у співпраці та швидкому проведенні угоди від початку до кінця.

Освіта за кордоном: пропонуються й інші види туризму, розраховані на різні вікові категорії людей та за індивідуальними вимогами.

Переваги звернення до туристичної фірми:

- Економія часу: Професіонали підберуть оптимальний варіант відпочинку з урахуванням побажань клієнтів.
- Гарантія якості: отримання якісних послуг від перевірених партнерів.
- Комплексне обслуговування: Всі питання, пов'язані з поїздкою, будуть вирішені за клієнтів.
- Безпека: Туристична фірма несе відповідальність за безпеку своїх клієнтів.

2.1.2 Етапи створення КСЗІ

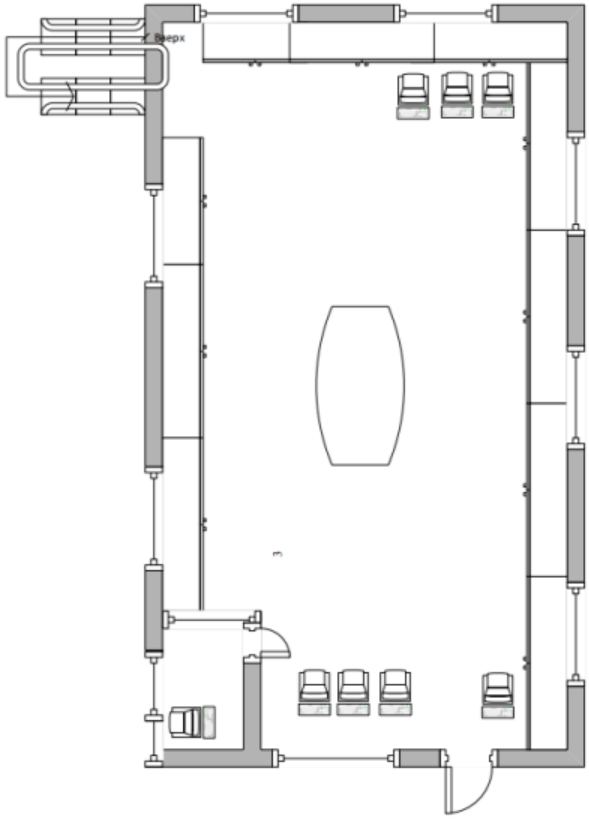

Рисунок 2.1 Ситуаційний план (1 поверх)

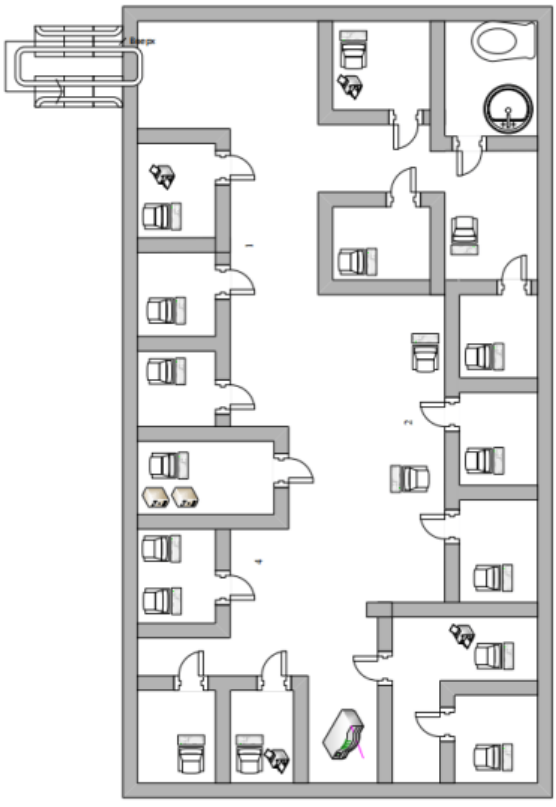

Рисунок 2.2 Ситуаційний план (2 поверх)

Етап 1. Обґрунтування необхідності створення КСЗІ

Основою для визначення необхідності створення КСЗІ являються норми та вимоги діючого законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації чи забезпечення її цілісності, доступності, чи прийнято власником інформації рішення тому, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ в загальному випадку отримуються по результатам:

1. Аналізу нормативно-правових актів (державних, відомчих і таких, які діють в межах установи, організації, підприємства), на основі яких можуть встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, чи визначення необхідності забезпечення захисту інформації у відповідності з іншими критеріями;
2. Визначення наявності у складі інформації, що належить автоматизованій обробці, таких її видів, які вимагають обмеження доступу до неї чи забезпечення цілісності і доступності у відповідності з вимогами нормативно- правових актів;
3. Оцінки можливості переваг (фінансово-економічних, соціальних і т.д.) експлуатація ІТС у випадку створення КСЗІ.

На основі проведеного аналізу приймається рішення про необхідність створення КСЗІ на підприємстві.

КСЗІ направлена на забезпечення захисту інформації та нерозголошення, витоку, несанкціонованого доступу та модифікації даних в системі, охорону продукції та персонал.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Документи:

1. Наказ «Про затвердження Переліку відомостей, що відносяться до конфіденційної інформації».
2. Перелік відомостей, що відносяться до конфіденційної інформації.
3. Акт визначення вищого ступеню обмеження доступу інформації.

Етап 2. Обстеження середовищ функціонування АС

Автоматизована система представляю собою сукупність інформації, персоналу та комплексу засобів автоматизації діяльності, які реалізуються процеси, або його частин. Таке розуміння добре гармонізує з сучасним підходом до обробки інформації в документованій формі, де документом вважається зафіксованим на матеріальному носії інформації з реквізитами, які дозволяють ідентифікувати її. Таким чином, документом являється не тільки текст, але й зображення на листах, і файл на матеріальному носії, та стрічка запису в базі даних.

Тому, для більш точного визначення інформаційної системи туристичної фірми як сукупності інформації, персоналу, матеріальних носіїв, засобів автоматизації, технічних та технологічних рішень обробки інформації.

В туристичній фірмі «Мандри світом» застосовують 1 тип автоматизованої системи – 2 класу (у вигляді мережі окремих робочих станцій, які не мають вихід до мережі Інтернет).

Інформація загальнодоступної інформації:

1. Інформація щодо статуту організації, правил внутрішнього трудового розпорядку дня та правил техніки безпеки при роботі з технікою.
2. Інформація щодо посад працівників, прізвище, ім’я та по батькові та їх робочі телефони.
3. Інформація про графіки роботи організації.
4. Клієнтські бази даних;
5. Інформація про списки підприємств по регіону та їх керівників.

Перелік інформації обмеженого доступу:

1. Особиста інформація про працівників та їх посадові інструкції.
2. Інформація про поставки техніки та обладнання для підприємства.
3. Інформація щодо фінансової діяльності організації (бухгалтерський облік та заробітна плата працівників та обслуговуючого персоналу).
4. Інформація про мережеві налаштування комп’ютерів та серверів.
5. Інформація щодо документації організації.

Документи: Акт обстеження.

Етап 3. Визначення потенційних загроз для інформації, яка буде циркулювати в АС

В процесі проведення обстеження туристичної фірми «Мандри світом», були визначені потенційні загрози для інформації, таким чином було створено модель загроз та модель порушника, дані вимоги створюються відповідно нормативно-правових документів, такі як:

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22);
2. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» (Затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53);
3. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р. №125).

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Варіантами моделі загроз визначені властивості захищеності інформаційних об'єктів, які можуть бути порушеними – конфіденційність (К), 17 цілісність (Ц), доступність (Д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків (шкоди) по кожному з видів порушень.

Документи: Модель загроз.

Етап 4. Розробка політики безпеки інформації в АС

Даний етап комплексної системи захисту інформації передбачає вивчення об'єкта, на якому створюється КСЗІ, при цьому уточнює модуль загроз, модель

потенційного порушника та аналіз ризиків, що виконуються на основі попередніх етапів.

Розробляючи політику безпеки, треба враховувати специфіку порівняно з іншими інформаційними системами. Особливості інформаційної системи туристичної фірми зумовлені специфікою тих завдань, які виконують за її допомогою, а саме:

1. Уся інформація, яка обробляється, накопичується і зберігається в системі, є конфіденційною, тому значну увагу доводиться приділяти криптографічному захисту за допомогою шифрування, розподілу доступу й автентифікації в мережі, захисту місць підключення до мереж зв'язку тощо;

2. Інформація, яка циркулює в такій системі, не може бути втрачена, дубльована або модифікована. У зв'язку з цим посилюються вимоги до надійності апаратного і програмного забезпечення, оперативного і повного (за можливостями) відновлення інформації після аварій та збоїв у роботі;

Основними принципами створення системи захисту:

1. Конфіденційність, тобто гарантія, що інформація дається тільки авторизованим користувачам;

2. Цілісність, тобто гарантія, що інформація не може бути несанкціонованого змінена;

3. Доступність і безперервність роботи системи, тобто гарантія, що достовірна інформація буде доступна, коли це потрібно.

Загроза неавторизованого проникнення до системи охоплює всі типи несанкціонованого доступу, у тому числі такі: фальсифікація санкції на доступ, неправомірне використання паролів, спроби працювати від імені іншої особи, несанкціоноване використання носіїв даних, перехоплення повідомлень у каналах зв'язку, вірусні атаки тощо. Загроза ненавмисної модифікації виникає унаслідок помилок у програмному забезпеченні, апаратних збоїв, помилок персоналу та користувачів і т. ін. Затримка або погіршення обслуговування можуть призвести до втрати коштів унаслідок штрафних санкцій і, що найважливіше, до втрати довіри.

Документи: Політика безпеки.

Етап 5. Розробка плану захисту інформації в АС

Для забезпечення ефективного захисту автоматизованої системи розробляють план захисту інформації для підприємства. План захисту представляє собою набір документів, згідно до яких здійснюється організація захисту інформації на всіх етапах життєвого циклу автоматизованої системи, а саме:

1. Класифікація інформації автоматизованої системи;
2. Загальний опис компонентів автоматизованої системи;
3. Технології розробки інформації в автоматизованої системи;
4. Модель загроз автоматизованої системи.

Документи: План захисту інформації.

Етап 6. Розробка технічного завдання на створення КСЗІ в АС

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є основним організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється відповідно до вимог функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброки в автоматизованій системі. Додатково необхідно також викласти вимоги до організаційних, фізичних та інших заходів захисту (комплекс програмно-технічних заходів захисту інформації).

Дане технічне завдання є обов’язковим документом під час проведення експертизи автоматизованої системи на відповідність вимог.

Роботу з погодження проєкту проводить технічного завдання на КСЗІ в АС здійснюють спільно Розробник ТЗ та Замовник.

В свою чергу Розробник за домовленістю із Замовником відправляє ТЗ на КСЗІ в АС на затвердження в Адміністрацію Держспецзв’язку України.

Документи: Технічне завдання.

Етап 7. Складання технороботочого проєкту створення КСЗІ

Техноробочий проєкт комплексної системи захисту інформації в АС розробляється на підставі та у відповідності до технічного завдання на створення КСЗІ в АС. На цьому етапі розробляється перелік документів, в якому описується, як саме створюється система, її експлуатація, а також модернізація КСЗІ в АС.

Техноробочий проєкт включає такі етапи:

Розробка технічного проєкту. На етапі розробки технічного проєкту. Необхідно розробити загальні проєкті рішення, для реалізації вимог ТЗ на КСЗІ, рішення щодо структури КСЗІ, її алгоритмів функціонування та умов використання засобів захисту, рішень щодо архітектури КЗЗ та механізмів реалізації, визначення профілем послуг безпеки інформації. Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до рівня гарантій реалізації послуг безпеки згідно зі специфікаціями НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 3.7-003-05. Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

Розробка робочого проєкту. На етапі створення робочого проєкту виконується опис порядку функціонування АС та настанови (інструкція) щодо забезпечення цього порядку обслуговуючим персонал і користувачами, порядку супроводження КСЗІ впродовж життєвого АС.

Документи: Техноробочий проєкт.

Етап 8. Підготовка КСЗІ до введення в дію

Проводиться робота з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в АС. Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах. В основному має бути завершені робота і затверджені документи, що входять до

Плану захисту (за виключенням тих, для розробки яких необхідні результати етапів робіт).

Проєкт КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС (доповнення до нього, окремого ТЗ на створення КСЗІ). Під час розробки проєкту КСЗІ обґрунтовуються і приймаються проєктні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. Проєкт КСЗІ виконується на таких стадіях створення ІТС: ескізний проєкт, технічний проєкт, робочий проєкт.

Для всіх стадій розробки проєкту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5 – 004. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЕСКД.

Документи: Паспорт-формуляр.

Етап 9. Попередні випробування КСЗІ в АС

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатності КСЗІ та відповідність її вимогам ТЗ. Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50 – 34.698. Попередні випробування організовує замовник ІТС, а проводять розробник КСЗІ спільно із замовником.

Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представником замовника. Результати попередніх випробувань оформлюються «Протоколом випробувань», де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

Після усунення недоліків у випадку їх наявності та коригування проєктної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

Документи:

1. Протокол попередніх випробувань комплексної системи захисту інформації.
2. Акт приймання комплексної системи захисту інформації.

Етап 10. Дослідна експлуатація КСЗІ

Дослідну експлуатацію організовує та проводить Замовник.

Під час дослідної експлуатації КСЗІ:

1. Відпрацьовування технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;
2. Співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;
3. Здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування КЗЗ;
4. Здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державно експертизу.

Документи: Акт завершення дослідної експлуатації.

Етап 11. Експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань АС. Для проведення експертизи КСЗІ або засобу безпеки (далі – засіб ТЗІ) Замовник надсилає заяву встановленої форми на ім’я Голови (заступника голови) Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку) за адресою: 03680, м. Чернігів, вул. Солом’янська, 13.

За результатами розгляду заяви у місячний термін приймається рішення про можливість й доцільність проведення експертизи та визначення підрозділу Держспецзв'язку підприємства, установи або в організації, які проводитимуть експертизу (далі – Організатор експертизи).

Відносини між Замовником і Організатором експертизи регламентується укладеним між ними договором про проведення експертизи. Термін проведення експертизи визначається договором і не повинен перевищувати 6 місяців. У разі значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації Держспецзв'язку та Замовника.

Замовник надає Організатору експертизи комплект організаційно-технічної документації на КСЗІ в АС або засіб ТЗІ, необхідний для проведення експертних випробувань.

Організатор експертизи, за результатами аналізу наданих Замовником документів і з урахуванням загальних методик оцінювання задекларованих характеристик об'єкта експертизи, формує програму і окремі методики проведення експертизи та розробляє , у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань відповідне програмно-технічне забезпечення.

Програма проведення експертизи узгоджується із замовником та Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Держспецзв'язку, а окремі методики – з зазначеним департаментом.

Терміни розробки окремих методик та необхідного програмно-технічного забезпечення залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

Результати експертних робіт за окремими методиками оформлюються у вигляді протоколу виконання робіт, затвердженого Організатором експертизи.

У разі виявлення невідповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, Організатор експертизи може запропонувати Замовнику виконати доробку КСЗІ в ІТС або засобу ТЗІ. Терміни доробки

визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором експертизи.

Відомості щодо всіх доробок, а також додаткових експертних робіт оформлюються окремими протоколами.

За результатами проведених робіт Організатор експертизи складає експертний висновок щодо відповідності КСЗІ в ІТС або засобу ТЗІ вимоги нормативних документів з ТЗІ і разом з протоколом виконаних робіт подається до Адміністрації Держспецзв'язку.

У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи, він може звернутися до Адміністрації Держспецзв'язку з пропозицією щодо здійснення контролю за проведенням Організатором експертизи експертних робіт. Мета проведення Експертизи КСЗІ в АС полягає у дослідженні, перевірці, аналізі та оцінці КСЗІ в АС щодо можливості її використання для забезпечення безпеки в АС.

Суб'єктами, що приймають участь в Державній експертизі КСЗІ в АС є:

1. Замовник (організація – власник КСЗІ та АС);
2. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку – контролюючий орган);
3. Організатор (організація-виконавець Державної експертизи);
4. Експерти.

Відповідно до 1.4 «Положення про Державну експертизу в сфері технічного захисту інформації» (Затвердженого наказом Адміністрації Держспецзв'язку України №93 від 16.05.07), КСЗІ підлягає обов'язковій перевірці на відповідність вимогам нормативних документів з безпеки (НД ТЗІ). НД ТЗІ та технічного завдання на КСЗІ в АС і містить наступні етапи:

1. Аналіз документації на КСЗІ в АС;
2. Розробка програми та методики проведення Експертизи КСЗІ в АС;
3. Узгодження програми і методики з Державною службою спеціального зв'язку та захисту інформації України (Програма також погоджується із замовником);
4. Обстеження об'єкта і проведення випробувань;

5. Оформлення протоколів проведення випробувань;

6. Оформлення Експертного висновку.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань.

Якщо в силу якихось причини усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проєктування. В першу чергу такий порядок рекомендується застосувати для складних з точки зору архітектури, складу та обсягів робіт КСЗІ. При цьому експертами послідовно здійснюється оцінка технічних та організаційних рішень на всіх етапах робіт. Це дає змогу оперативно усувати недоліки проєктування та скоротити час проведення державної експертизи, яка може бути в основаному завершена до етапу приймальний випробувань АС.

Необхідно звернути увагу, що державну експертизу КСЗІ не може проводити організація, яка розробляє КСЗІ. Організація, що проводить Державну експертизу визначається ДССЗЗІ України.

Етап 12. Супроводження КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації. Підготовка організаційно-розпорядчої документації.

2.2 Статут проєкту створення КСЗІ

Замовник: Туристична фірма «Мандри світом»

Класифікаційні ознаки:

Тип проєкту – інтелектуальний;

За складністю – середньої складності;

По термінах реалізації – короткостроковий;

За складом, структурою проєкту та його предметної області – невеликий;

За вимогами до якості – високі вимоги якості.

1. Мета проєкту і продукту.

Проєкт: Створення комплексної системи захисту інформації для туристичної фірми "Мандри світом"

Мета проєкту: забезпечення високого рівня безпеки інформації, яка обробляється туристичною фірмою "Мандри світом". Це включає в себе захист конфіденційних даних клієнтів, фінансової інформації, а також внутрішньої інформації компанії від несанкціонованого доступу, розкриття, зміни або знищення.

Тривалість проєкту: 80 робочих днів.

Продукт: Продуктом цього проєкту є комплексна система захисту інформації, яка забезпечує безпеку даних компанії та її клієнтів. Ця система є набором взаємопов'язаних технологічних рішень, політик і процедур, спрямованих на захист інформації від несанкціонованого доступу, розкриття, зміни або знищення.

Основні компоненти цього продукту можуть включати:

- Системи виявлення вторгнень: Проактивно виявляють і попереджають про спроби несанкціонованого доступу до системи.
- Захищені мережі: Ізолюють внутрішню мережу від зовнішніх загроз, забезпечуючи безпечний обмін даними.
- Системи автентифікації та авторизації: Контролюють доступ до інформаційних ресурсів, дозволяючи лише авторизованим користувачам виконувати певні дії.
- Зашифрування даних: Забезпечує конфіденційність даних, перетворюючи їх на незрозумілий для сторонніх осіб код.
- Системи резервного копіювання: Забезпечують збереження даних і дозволяють відновити їх у разі втрати.

- Мобільні рішення: Забезпечують безпечний доступ до корпоративних даних з мобільних пристроїв.
- Політики безпеки: Визначають правила поведінки персоналу щодо захисту інформації.
- Процедури реагування на інциденти: Визначають порядок дій у разі виявлення інцидентів інформаційної безпеки.

Мета продукту:

- Збільшення рівня безпеки інформації: Зменшення ризику втрати даних, фінансових втрат і пошкодження репутації компанії.
- Забезпечення відповідності законодавству: Дотримання вимог законодавства щодо захисту персональних даних та інших видів інформації.
- Підвищення довіри клієнтів: Забезпечення безпеки персональних даних клієнтів є важливим фактором для їхньої лояльності.
- Створення безпечного робочого середовища: Співробітники отримують надійні інструменти для роботи з інформацією.

2. Вимоги до продукту і його характеристики:

- доступність;
- узгодженість;
- актуальність;

3. Критерії до приймання:

- ✓ Відповідність стандартам безпеки: Система повинна відповідати загальноприйнятим стандартам безпеки (наприклад, ISO 27001).
- ✓ Надійність: Система повинна бути стійкою до збоїв і відмов.
- ✓ Масштабованість: Система повинна мати можливість масштабуватися відповідно до зростання компанії.
- ✓ Документація: Повинна бути розроблена повна технічна документація на систему, включаючи інструкції з експлуатації та обслуговування.
- ✓ Виконання робіт в обумовлений термін.

4. Гарантії проєкту: страхування даного проєкту не передбачено. Виконавець

проєкту гарантує, що розроблена система захисту інформації буде функціонувати без збоїв протягом 12 місяців з моменту введення в експлуатацію. У разі виявлення будь-яких дефектів виконавець зобов'язується усунути їх протягом 5 робочих днів з моменту отримання письмового повідомлення від замовника.

5. Вимоги до постачання устаткування і матеріалів:

Для виконання проєкту необхідні наступні матеріали:

- державні стандарти;
- повний доступ до інформації щодо діяльності підприємства;
- носії інформації.

Устаткування і забезпечення:

- Апаратне забезпечення (сервери, мережеве обладнання, системи зберігання даних, системи відеоспостереження, сенсори).
- Програмне забезпечення (операційні системи, системи виявлення вторгнень, брандмауери, системи шифрування, системи управління доступом, системи резервного копіювання, системи моніторингу, антивіруси).
- Інше забезпечення (канали зв’язку, електроенергія, охоронна сигналізація).

6. Обмеження проєкту:

Проєкт слід реалізувати протягом 4х місяців. Завдання проєкту повинні бути виконані у встановлений термін, подальше впровадження повинно бути проконтрольовано.

7. Припущення проєкту:

Проєкт допускається до реалізації без урахування вартості всіх статей витрат.

8. Характеристики вихідної організації, що здійснює проєкт:

Вихідна організація, яка здійснює проєкт – міжнародна IT компанія «H-X Technologies», а також співробітники турфірми «Мандри світом».

9. Початковий опис робіт за проєктом:

1. Аудит

- Аналіз поточного стану інформаційної безпеки туристичної фірми

2. Розробка технічного завдання
    - Аналіз вразливості інформаційної системи
    - Визначення вимог до системи захисту
    - Розробка інформаційної моделі КСЗІ
3. Визначення технічного рішення
    - Визначення детального переліку обладнання, програмного забезпечення та змісту робіт
    - Опис технічного рішення (робочий проєкт)
    - Визначення вартості
4. Реалізація КСЗІ
    - Побудова повного комплексу засобів захисту
    - Тестування КСЗІ
5. Експертиза
    - Отримання експертного висновку (атестата)
6. Експлуатація
    - Підтримка актуальності КСЗІ протягом життєвого циклу

Висновки до розділу 2

У даному розділі було проведено детальний аналіз діяльності туристичної фірми "Мандри світом" з метою виявлення потенційних загроз інформаційній безпеці та визначення вимог до комплексної системи захисту інформації (КСЗІ).

На основі проведеного аналізу було описано основні етапи створення КСЗІ, включаючи:

- Оцінку ризиків: Визначення найбільш ймовірних загроз для інформаційної безпеки компанії.
- Розробку політики безпеки: Створення набору правил та процедур, що регулюють взаємодію з інформаційними ресурсами.

- Вибір технологічних рішень: Підбір програмного та апаратного забезпечення, необхідного для забезпечення безпеки.
- Розробку технічної документації: Створення детального опису структури та функціоналу КСЗІ.
- Впровадження системи: Реалізація розроблених рішень та інтеграція їх з існуючою ІТ-інфраструктурою компанії.

Для ефективного управління проєктом створення КСЗІ було розроблено детальний статут проєкту, який визначає цілі, завдання, ресурси, відповідальних осіб та терміни виконання робіт.

За результатами проведеної роботи було розроблено проєкт КСЗІ, який забезпечить:

- Захист конфіденційності персональних даних клієнтів: Запобігання несанкціонованому доступу до інформації про клієнтів.
- Цілісність інформаційних ресурсів: Захист від випадкового або навмисного зміни даних.
- Доступність інформаційних ресурсів: Гарантування безперебійної роботи систем та швидкого відновлення даних у разі інцидентів.
- Відповідність законодавству: Дотримання вимог чинного законодавства у сфері захисту інформації.

Впровадження розробленої КСЗІ дозволить компанії "Мандри світом" підвищити рівень захисту інформації, знизити ризики кібератак та забезпечити безперебійну роботу бізнес-процесів.

РОЗДІЛ 3 МОДЕЛЬ УПРАВЛІННЯ ПРОЄКТОМ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.

3.1 Управління змістом проєкту

Відповідно до PMBOK [6], процес управління змістом проєкту включає в себе процеси, які забезпечують виконання в ході проєкту всіх робіт, необхідних для його успішного виконання. Це такі процеси: планування та визначення змісту; створення ІСР; підтвердження змісту; контроль змін змісту. Ці процеси взаємодіють один із одним, а також з процесами інших груп управління проєктом. Перші два процеси відносяться до групи процесів планування, два інших - до групи процесів моніторингу та управління.

На вхід процесу "Планування змісту" надходять результати виконання процесів групи ініціації - Статут проєкту, попередній зміст опису проєкту та план УП. Процес "Визначення змісту" пов'язаний з процесом "Планування змісту" та з процесами групи моніторингу та контролю, отримуючи від них на вхід План управління змістом проєкту та схвалені запити на зміну.

Процес "Створення ІСР" пов'язаний із процесом "Визначення змісту". Входами процесу "Підтвердження змісту" є виходи процесу "Створення ІСР" та процесу "Керівництво та управління виконанням проєкту" групи процесів моніторингу та контролю. Процес "Управління змістом" пов'язаний з процесом "Підтвердження змісту" та процесами групи моніторингу та управління документами "Звітність щодо виконання" та "Керівництво та управління виконанням проєкту".

Управління змістом проєкту має бути так інтегровано в інші процеси та галузі знань, щоб результатом проєктної роботи стало створення ІС необхідного змісту. Розглянемо процеси управління змістом:

1. Планування змісту. Процес "Планування змісту" виконує розробку та документування плану управління змістом проєкту. Вхідними даними для процесу планування є Статут, Попередній зміст опису проєкту та План УП, а також фактори довкілля та організаційні активи. За допомогою експертної

оцінки та досвіду аналогічних проєктів, а також шаблонів планів управління змістом та шаблонів ІСР формується План управління змістом.

Згідно з PMBOK [6], План управління змістом - це документ, що описує, як будуть визначатися, розроблятися і перевірятися роботи, які необхідно виконати для отримання результату із зазначеними характеристиками, і задає дії з управління змістом проєкту. План управління змістом є інструментом планування, що описує, як проєктна команда формулюватиме зміст проєкту, розроблятиме докладний опис змісту, визначатиме і розроблятиме ІСР, перевірятиме і контролюватиме зміст проєкту.

Розробка плану управління змістом та деталізація змісту проєкту починаються з аналізу інформації, що міститься у Статуті, попередньому описі змісту, останньої схваленої редакції плану УП та інформації, що перебуває в активах організаційного процесу та факторів зовнішнього середовища підприємства.

План управління змістом має містити опис таких процесів:

- підготовка докладного опису змісту на основі попереднього опису змісту,

- створення ІСР на основі докладного опису змісту та визначення способів підтримки та схвалення ІСР,

- визначення формальної процедури верифікації та приймання завершених результатів постачання проєкту,

- контроль обробки запитів на зміни докладного опису змісту проєкту. (цей процес безпосередньо пов'язаний із процесом загального управління змінами).

2. Уточнення (визначення) змісту. Процес уточнення (визначення) змісту виконує розробку докладного опису змісту, який буде основою прийняття майбутніх рішень щодо проєкту. Команда проєкту аналізує потреби, побажання та очікування учасників проєкту, проводить коригування вимог до ІС, що розробляється. Допущення та обмеження аналізуються на повноту, і при необхідності додаються додаткові припущення та обмеження. Вхідними документами процесу визначення змісту є План управління змістом та схвалені запити на зміни. Як інструменти для уточнення вимог можуть бути використані

такі методи, як ієрархічна структура продукту, системний аналіз, системний інжиніринг, метод оптимізації вигод, аналіз вартості та функціональний аналіз, метод "мозкового штурму". Для розробки докладного опису змісту проєкту залучаються експерти.

Аналіз учасників проєкту – це нструмент, який виявляє вплив та інтереси різних учасників проєкту та документує їх потреби, побажання та очікування, здійснює відбір потреб, побажань та очікувань, визначає їх пріоритети та кількісну оцінку. Рекомендується використовувати мережевий графік Замовника – інструмент розробки системного підходу для врахування вимог Замовника. Мережеві графіки розробляють для великих проєктів.

Мережевий графік забезпечує прозорість процесу роботи із клієнтом. Результат процесу визначення змісту:

1) опис змісту проєкту,

2) оновлений докладний план управління змістом,

3) запит на зміни.

3. Створення ієрархічної структури робіт. Процес створення ІСР виконує розбиття укрупненої структури робіт, поданої в документі "Попередній опис змісту", на більш дрібні та керовані елементи. В ІСР включаються роботи, зазначені у поточному схваленому описі змісту проєкту. У процесі створення ІСР структурується та визначається зміст всього проєкту. Вхідною інформацією для процесу створення ІСР є опис змісту проєкту, план управління змістом, активи організаційного процесу, схвалені запити на зміни. Для розробки ІСР PMBOK рекомендує використовувати шаблони ІСР, декомпозицію, системний підхід до складання ІСР.

Шаблони ієрархічної структури робіт. Незважаючи на унікальність кожного проєкту, ІСР попереднього проєкту часто може бути шаблоном нового проєкту. Наприклад, більшість проєктів впровадження ІС у конкретній організації матиме однакові життєві цикли, тому й однакові чи схожі результати кожної фази. Стандарт Інституту управління проєктами (PMI) для ієрархічної структури робіт містить посібник зі створення, доопрацювання та застосування

ICP. У цьому посібнику включені приклади шаблонів ICP, які можна адаптувати під конкретні проєкти в конкретній області програми.

Декомпозиція. Декомпозиція - це інструмент, що дозволяє виконати поділ результатів поставки проєкту на дрібні, більш керовані елементи. Кожен наступний рівень ієрархії детальніше відбиває елементи проєкту. Декомпозиція виконується до тих пір, поки робота та результати постачання не визначаються на рівні пакетів робіт.

Пакети робіт – це найнижчий рівень деталізації, який менеджер проєкту має тримати під своїм безпосереднім контролем. Далі пакети робіт можуть розбиватися на операції, які потім можуть бути розбиті на завдання. Рівень деталізації варіюватиметься в залежності від розміру та складності проєкту. У різних результатів постачання можуть бути різні рівні декомпозиції. Надмірна декомпозиція може призвести до непродуктивної управлінської трудомісткості, неефективного використання ресурсів та зниження ефективності під час виконання роботи. Команда проєкту має знайти баланс між надто малою та надто великою деталізацією планування ICP.

Декомпозиція всієї сукупності проєктних робіт включає такі операції:

1. Визначення результатів поставки та робіт для їх досягнення, одержуваних шляхом аналізу детального опису робіт за проєктом. Список робіт визначається шляхом експертної оцінки результатів постачання.

2. Структурування та організація ICP - метод аналізу, який використовує шаблони ICP, структурує результати поставки та відповідні проєктні роботи та представляє їх у вигляді ієрархічної структури. Залежно від вибраного шаблону може вийти кілька різних видів структури. У шаблонах як перший рівень декомпозиції можуть бути використані підпроєкти та основні результати поставки або фази життєвого циклу проєкту.

Структура декомпозиції робіт по проєкту створення комплексної системи захисту інформації на підприємстві (туристичної фірми «Мандри світом») представлена на рисунку 3.1.

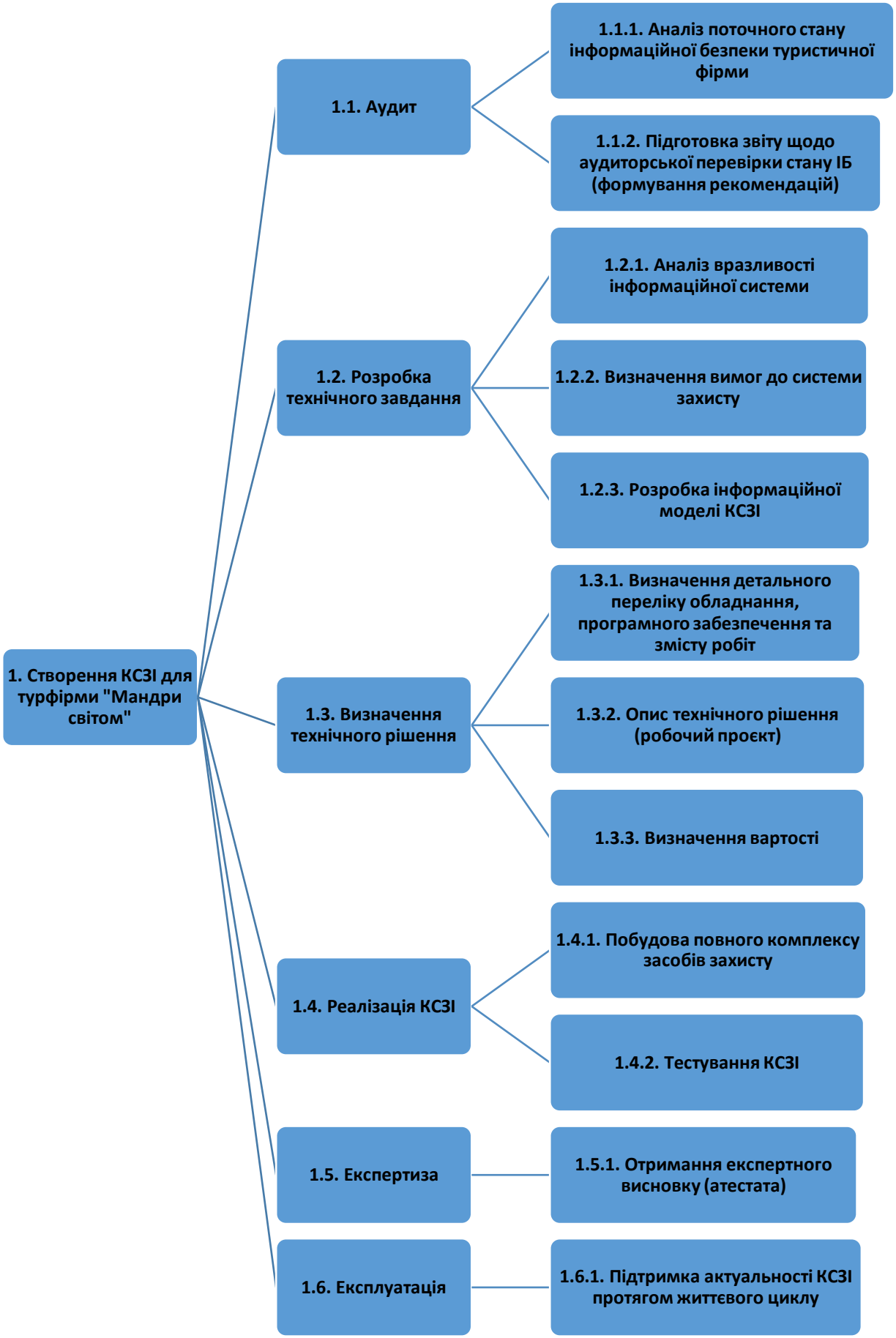

Рисунок 3.1 Структура декомпозиції робіт проєкту створення КСЗІ для туристичної фірми «Мандри світом»

3.2 Організаційна структура проєкту

Залежно від визначення мети проєкту, запасу часу для вирішення завдання і мети (очікуваного результату) проєкту можна вибирати організаційний тип для реалізації проєкту (тобто тип організації проєктного менеджменту). Існують два класичні типи проєктної організації:

– Лінійний тип (тип А – рисунок 3.2)

– Матричний тип (тип Б – рисунок 3.4).

Щоб уникнути помилок цих двох типів проєктного менеджменту, використовують два проміжні типи:

– Функціонально-впливовий тип (У)

– Тип періодичного переходу (Г).

Лінійний тип характерний для великих проєктів із швидким темпом здійснення. Проєктна група працює винятково для виконання проєктних завдань.

Рисунок 3.2 Лінійний тип (тип А) – чистий проєктний менеджмент

До переваг цього типу належать: чітко розподілена відповідальність, компетентність керівника (проєктного менеджера), хороші можливості контролю проєктного процесу керівником і членами групи, висока мотивація, швидке прийняття рішень, дух колективу. Помилками можна вважати: ускладнений відбір співробітників для проєктної групи, робота тільки із завданнями даного проєкту, оскільки після виконання проєкту важко повернутися на попереднє робоче місце.

Лінійний тип проєктного менеджменту використовують як самостійну проєктну групу з підпорядкуванням головному менеджеру фірми (рис. 3.3). У США застосовують схему лінійного підпорядкування проєктної групи головному менеджеру фірми в літакобудуванні й деяких галузях будівництва.

Рисунок 3.3 Місце лінійного проєктного менеджменту в компанії

Матричний тип організації проєктного менеджменту (рис. 3.4) прийнятий у фірмах і об'єднаннях, коли реалізація проєкту потребує комплексного вирішення із застосуванням знань з різних галузей і різних відділ фірми чи об'єднання.

У матричному типі організації члени проєктної групи мають подвійне підпорядкування – через лінійного менеджера і через проєктного менеджера. Автономні або цілком самостійні проєктні групи не створюються.

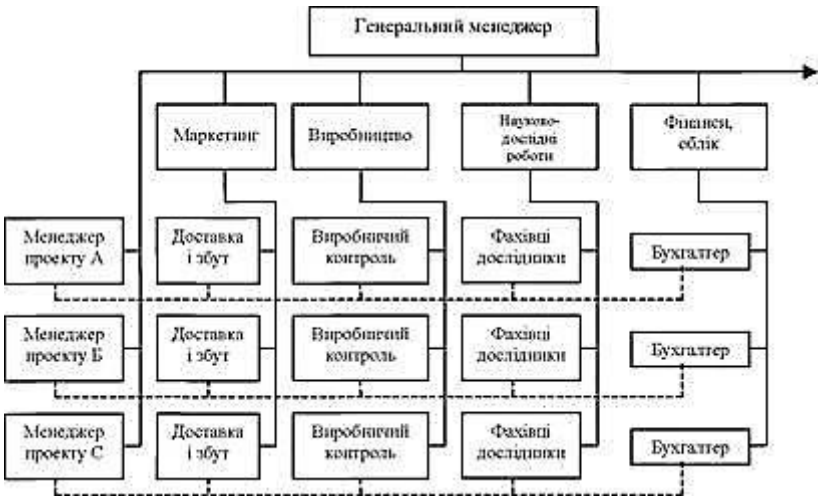

Рисунок 3.4 Матрична система проєктної організації в рамках компанії

Перевага цього типу полягає у тому, що члени проєктної групи можуть ефективно працювати як на звичайному робочому місці, так і над виконанням проєктного завдання. Такому співробітнику (і керівнику проєкту) не варто шукати собі нове робоче місце після завершення проєкту. До недоліків можна віднести те, що складно швидко знаходити рішення, постійно потрібно узгоджувати діяльність співробітників, можливість виникнення конфліктів у різних інтересах між лінійними і проєктними менеджерами, досить великий обсяг адміністративної діяльності. велике навантаження всіх учасників проєкту.

Функціонально-впливовий тип проєктного менеджменту застосовують для вирішення невеликих проєктів, які не потребують особливого темпу реалізації проєктних завдань. Місце проєктного менеджера знаходитися поза лінійною структурою фірми. Хоча всі рішення приймаються лінійні менеджери, проєктний менеджер може скористатись своєю наближеністю до генерального менеджера. Проєктний менеджер повинен підготувати прийняття рішень і є консультантом без права прийняття рішень. Автономні або самостійні проєктні групи не створюються.

Перевага цього типу у тому, що члени проєктної групи не втрачають контакти із звичайною діяльністю. Цей факт може значно підвищити мотивацію до проєктної роботи. До недоліків можна віднести те, що складно знайти оптимальне рішення, багато залежить від особливості менеджера проєкту фірми. Часто керівник проєктної групи не має права давати членам групи вказівки щодо виконання будь-яких завдань. Він повинен керувати узгоджено з лінійним менеджером шляхом переконання. Рисунок 3.5 показує можливий варіант функціонально- впливового типу (типу У) проєктного менеджменту.

Рисунок 3.5 Місце функціонально-впливового виду проєктного менеджменту

Щоб уникнути недоліків типів А, Б і В проєктного менеджменту застосовують схему тимчасового переходу з звичайного робочого режиму в режим проєктної діяльності – тип періодичного переходу (Г) (Time-Sharing). Періодичний заміняє спеціалісту участь у виконанні звичайних завдань на виконання проєктних завдань. За визначеною календарною схемою спеціаліст працює домовлену кількість днів звичайно і домовлену кількість днів "проєктно". Залежно від обсягу проєктного завдання цей режим періодично повторюється.

Перевага цього типу полягає у тому, що спеціаліст завжди має тільки одного начальника – лінійного або проєктного менеджера. Через цей тип менеджменту компанія може ефективно використовувати власні ресурси персоналу і устаткування.

Для забезпечення ефективності управління проєктом необхідно:

– врахувати всі розділи, етапи і роботи проєкту;

– визначити коло організацій, що беруть участь у проєкті;

– забезпечити дієвість управління шляхом розподілу відповідальності.

Проєкт має ряд властивостей, які допомагають методично правильно організувати роботу з його реалізації: він виникає, існує і розвивається у певному оточенні, яке називають зовнішнім середовищем; склад учасників не залишається незмінним у процесі його реалізації та розвитку; як і будь-яка система, проєкт може бути поділений на елементи, що потребують певних зв'язків.

Організаційна структура проєкту створення комплексної системи захисту інформації для туристичної фірми «Мандри світом»:

1. **Проєктний офіс**
    - Керівник проєкту
    - Менеджер з безпеки інформації
    - Технічний директор
    - Менеджер з персоналу
2. **Робочі групи**

- Аналітики
  - Збір інформації
  - Аналіз ризиків
  - Розробка політики безпеки
- Розробники
  - Вибір технологій
  - Розробка програмного забезпечення
  - Налаштування системи
- Тестувальники
  - Функціональне тестування
  - Тестування на проникнення
  - Тестування продуктивності

3. **Зацікавлені сторони**
   - Керівництво компанії
   - Відділи компанії (маркетинг, бронювання, бухгалтерія тощо)
   - Постачальники (обладнання, ПО, послуги)

3.2.1 Формування команди проєкту

Важливим завданням управління проєктом є формування команди. Керівникам проєкту і функціональних підрозділів, які беруть участь у створенні проєкту, на цій стадії доводиться розв'язувати ряд специфічних задач, пов'язаних із мотивацією праці, конфліктами, виконанням, контролем, відповідальністю, комунікаціями, владою, лідерством і т. п. Це створює сприятливі умови для роботи, допомагає перебороти величезні психічні навантаження, що виникають у процесі пошуку, узгодження і реалізації проєктних рішень, дозволяє уникнути конфліктів і стресів, що в кінцевому рахунку позначаться на науково-технічному рівні та якості проєкту.

Багато дослідників підтверджують, що близько 80% опитаних висувають фактор людських відносин на перше місце з усіх факторів, що впливають на успішне здійснення проєкту, тому пріоритетність цієї сфери діяльності не викликає сумнівів.

Створення професіональної команди для нового проєкту — один із основних обов'язків проєкт-менеджера на першому етапі його роботи. Цей процес вимагає ряду навиків управління у визначенні, відборі й об'єднанні в команду спеціалістів із різних відділів і організацій.

Команда проєкту — сукупність працівників, які здійснюють функції управління проєктом і персоналом проєкту. Формуючи команду, проєкт-менеджер збирає разом групу людей, намагаючись об'єднати їх загальною ціллю і єдиними задачами. Новизна, унікальність, ризик і швидкоплинність — всі ці риси притаманні новому проєкту, вони ж і визначають труднощі при формуванні команди. Створення команди для нового проєкту ускладнено ще й тим, що ці люди не працювали разом, не мають загальних цінностей і норм, але повинні працювати ефективно і синхронно. Потрібен тривалий час, щоб всередині групи виникло командне почуття, щоб встановилися загальні норми, стандарти і цінності. Щоб проєкт був успішним, згрупування людей повинно відбутися до того, як команда почне працювати "на повну потужність".

За формою команда проєкту відображає існуючу організаційну структуру управління проєктом, розділення функцій, обов'язків і відповідальності за рішення, що приймаються в процесі його реалізації. На верхньому рівні структури знаходиться менеджер проєкту, а на нижніх — виконавці, відділи і фахівці, що відповідають за окремі функціональні сфери.

За змістом команда проєкту є групою фахівців високої кваліфікації, які володіють знаннями і навичками, необхідними для ефективного досягнення цілей проєкту.

Основним інтегруючим чинником створення і діяльності команди виступає стратегічна мета реалізації проєкту. У процесі досягнення цілей проєкту команда набуває своїх меж, використовує організаційні можливості учасників і ресурси проєкту. Команда проєкту виступає як соціальний організм, що має свій початок, здійснює процес життєдіяльності (управління проєктом) і завершує своє існування розформуванням або трансформацією в іншу управлінську команду. З одного боку, команда проєкту впливає на створення

певного організаційного середовища проєкту, формуючи цінності, принципи і норми поведінки персоналу. З іншого боку, діє в ній, підкоряючись єдиній меті та філософії управління проєктом. Тому проблеми формування і діяльність команди проєкту доцільно розглядати в логічній послідовності: мета проєкту - система управління - команда проєкту.

При організації роботи над проєктом необхідно вирішити два завдання:

1. формування команди проєкту;
2. організація ефективної роботи команди.

Залежно від специфіки, розміру та типу проєкту в його реалізації можуть брати участь від однієї до кількох десятків (іноді сотень) організацій та окремих фахівців. У кожної з них свої функції, ступінь участі в проєкті й міра відповідальності за його реалізацію. Фахівців та організації, залежно від виконуваних ними функцій, прийнято об'єднувати в абсолютно конкретні групи (категорії) учасників проєкту, до складу яких входять: замовники, інвестори, проєктувальники, постачальники ресурсів, підрядники, консультанти, ліцензіари, фінансові інститути – банки.

Нарешті, існує команда проєкту, очолювана керівником проєкту – менеджером проєкту (проєкт-менеджер), а також, залежно від специфіки проєкту, в проєкті можуть бути й інші учасники. Слід зазначити, що учасники проєкту – категорія більш широка, ніж команда проєкту.

Команда проєкту – одне з головних понять управління проєктами. Це група співробітників, які безпосередньо працюють над здійсненням проєкту і підлеглих керівникові останнього; основний елемент його структури, оскільки саме команда проєкту забезпечує реалізацію його задуму. Ця група створюється на період реалізації проєкту і після його завершення розпускається. Кількість людей в команді визначається обсягом робіт, передбачених проєктом. Як правило, лідери (менеджери) функціонально і (або) предметно орієнтованих груп фахівців і складають команду управління проєктом. Лідери груп – це керівники, координатори зусиль всіх членів групи; члени групи – безпосередні виконавці, які мають можливість зосереджуватися на конкретній роботі. При необхідності

деякі ролі членів команди можуть поєднуватися.

Основу проєктної команди складають постійні члени:

- Генеральний директор;
- Головний бухгалтер;
- Системний адміністратор;
- Адміністратор баз даних.

Вони очолюють функціональні відділи команди і відповідають за прийняття рішень з управління проєктом в межах своєї компетенції.

Команда проєкту має усі притаманні соціальні групі якості та характеристики. Як формальна група вона займає певне місце в структурі організації, має закріплені функції та обов'язки, користується формальними каналами інформації. Як неформальна група, вона досить стійка до криз і конфліктів, користується різними неформальними зв'язками і інформаційними каналами.

Для успішного створення комплексної системи захисту інформації (КСЗІ) для туристичної фірми "Мандри світом" необхідно сформувати команду проєкту, яка об’єднає експертів з різних галузей, що відповідають за розробку, впровадження та підтримку системи безпеки.

Склад команди з описом ролей:

1. Керівник проєкту
   - Задачі: загальне управління проєктом, планування ресурсів, контроль за виконанням завдань, комунікація з керівництвом фірми.
   - Вимоги: досвід в управлінні IT-проєктами, базові знання з інформаційної безпеки.
2. Аналітик з інформаційної безпеки
   - Задачі: аналіз поточних загроз, виявлення ризиків, проведення оцінки вразливостей.
   - Вимоги: знання в області інформаційної безпеки, навички проведення аудиту, знання стандартів (ISO/IEC 27001, ДСТУ).
3. Інженер із захисту інформації

- Задачі: розробка технічних засобів захисту, вибір і налаштування систем, таких як міжмережеві екрани, системи виявлення вторгнень, антивірусне ПЗ.
- Вимоги: технічні знання з налаштування IT-безпеки, розуміння технологій VPN, шифрування, аутентифікації.

4. Адміністратор безпеки мережі
   - Задачі: управління мережевою інфраструктурою, моніторинг мережевих загроз, забезпечення безпечного доступу до мережевих ресурсів.
   - Вимоги: досвід адміністрування мереж, знання протоколів безпеки, навички в налаштуванні міжмережевих екранів.
5. Фахівець з криптографічного захисту
   - Задачі: розробка та впровадження криптографічних методів захисту інформації (шифрування даних, електронний цифровий підпис).
   - Вимоги: досвід у криптографії, знання сучасних алгоритмів шифрування та стандартів.
6. Спеціаліст з програмної безпеки
   - Задачі: аналіз вразливостей ПЗ, захист програмного забезпечення, проведення тестування на проникнення (пентестинг).
   - Вимоги: знання мов програмування, досвід тестування ПЗ на безпеку.
7. Консультант із правових питань
   - Задачі: аналіз відповідності законодавчим нормам, підготовка документації з захисту персональних даних відповідно до законів.
   - Вимоги: юридичні знання в галузі захисту даних, досвід роботи з нормативними актами.
8. Фахівець із захисту персональних даних
   - Задачі: контроль за дотриманням політик захисту персональних даних, впровадження методик захисту конфіденційної інформації клієнтів.
   - Вимоги: знання стандартів захисту даних, досвід впровадження політик GDPR (або національних стандартів).
9. Технічний письменник

- Задачі: розробка та оформлення документів, політик, інструкцій з безпеки для співробітників.
- Вимоги: вміння створювати технічну документацію, знання базових принципів інформаційної безпеки.

10. Тренер із кібербезпеки
    - Задачі: навчання співробітників безпечному використанню систем, проведення тренінгів з кібербезпеки.
    - Вимоги: досвід проведення тренінгів, знання основних загроз кібербезпеки.
11. Спеціаліст з моніторингу та реагування на інциденти
    - Задачі: моніторинг безпеки, реагування на інциденти, ведення журналів аудиту та інцидентів.
    - Вимоги: досвід у сфері інформаційної безпеки, вміння працювати з інструментами моніторингу.

Ця команда забезпечить всебічний підхід до захисту інформації в туристичній фірмі "Мандри світом", включаючи технічні, організаційні та правові аспекти захисту даних.

На рисунку 3.6 представлена організаційна структура проєкту створення комплексної системи захисту інформації для туристичної фірми «Мандри світом»

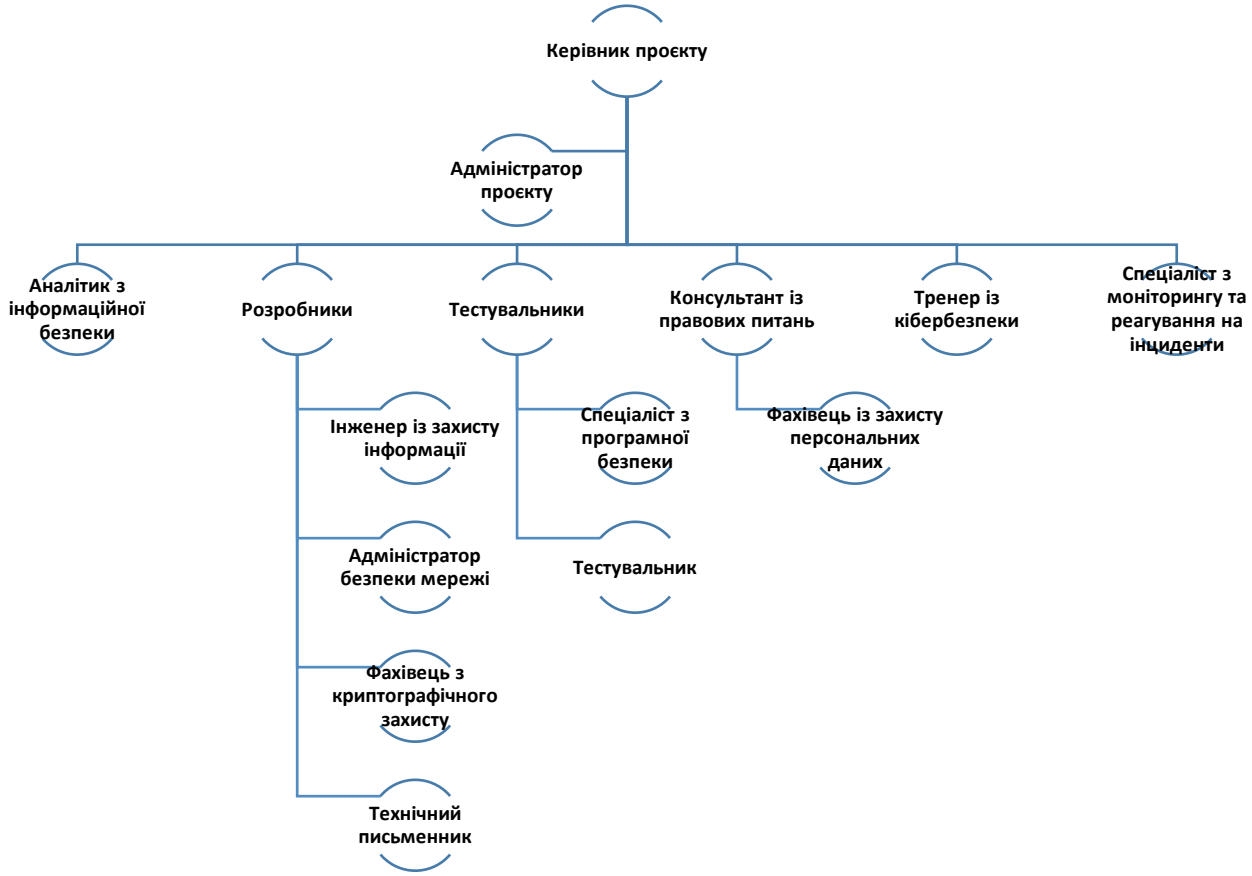

Рисунок 3.6 Організаційна структура проєкту створення КСЗІ для туристичної фірми «Мандри світом»

3.3 Управління термінами проєкту

Початковим кроком у плануванні проєкту є структуризація, яка передбачає планування обсягів робіт. Проте етап структуризації не дає змоги відповісти на запитання: скільки часу потрібно, щоб виконати всі роботи за проєктом, якими є календарні терміни виконання окремих робіт, субпроєктів, як розподіляється у часі потреба у різних ресурсах упродовж виконання проєкту? Тобто постає потреба планування ще однієї головної мети проєкту — виконання його у часі.

Для вирішення цього завдання у проєктному менеджменті застосовується сіткове і календарне планування. Враховуючи, що для успішної роботи над проєктом менеджеру треба швидко опрацьовувати значний масив інформації, життєво необхідними стають такі спеціальні інструменти, як сітковий і календарний графіки. Їхня роль посилюється ще й тим, що вони поєднують у собі параметри часу, вартості й ресурсів.

Використання цих інструментів у плануванні проєкту дає низку переваг, до яких належать можливості:

- визначити і наочно представити повний обсяг робіт у вигляді графіка;
- встановити такі цілі проєкту щодо часу виконання робіт, вартості й обсягів ресурсів, що їх реально можна досягнути;
- оцінити бюджет проєкту;
- за ходом здійснення проєкту контролювати виконання робіт і передбачати подальший перебіг подій;
- ефективно розподілити відповідальність за проєктні роботи між членами команди;
- визначивши критичні роботи, переміщувати ресурси, зменшувати ризики і невизначеність.

Перед тим як розміщувати роботу на діаграмі, потрібно розглянути, чи існує логічний зв'язок між роботами, тривалість робіт, залежно від забезпечення необхідними ресурсами, розподіл ресурсів між роботами. Діаграма Ганта дає можливість наочно визначити, які роботи є критичними, а які — некритичними, який запас часу мають некритичні роботи, резерв часу, логічний зв'язок між роботами.

Тривалість роботи — це головний параметр планування. Вона залежить від сумарної трудомісткості, що витрачається на виконання елементів роботи, і числа працюючих, які можуть її виконати. Звичайно, що тривалість роботи залежить від обсягу, який потрібно виконати, та інтенсивності виконання роботи.

При оцінці реальної тривалості потрібно врахувати різні фактори, а саме: втрачений час на непроєктні роботи (святкові, вихідні, лікарняні тощо), робота у

неповний день, перешкоди. Тривалість деяких робіт може залежати від вчасності постачання матеріалів. Крім того, при призначенні базових або поточних планових дат необхідно враховувати ресурсні обмеження.

Задачі планування мають, як правило, два типи постановки:

1. Облік потреб в окремих видах ресурсів та їх згладжування.
2. Розподіл ресурсів.

Обов'язково потрібно зробити аналіз спроможності реалізації проєкту. Він проводиться у дві стадії. На першій — аналізується наявність ресурсів по всіх роботах, на другій — проводиться згладжування ресурсів.

У цілому, аналіз можливості реалізації проєкту проводиться на основі вхідної інформації з врахуванням технічного проєкту календарного плану, оцінки витрат за додатковими критеріями таким чином:

- проводиться інтегральна оцінка надійності проєкту, а саме: ресурсні можливості реалізації; економічні можливості реалізації (мінімальні витрати за даним варіантом); фінансові можливості реалізації (чи буде план забезпечений фінансовими ресурсами);
- на основі проведеної оцінки проводяться коригування, оптимізація проєкту (чи задовольняє проєкт плану плановим критеріям) і приймається робочий проєкт календарного плану.

На рис. 3.7. представлено календарно-мережевий графік робіт по проєкту створення комплексної системи захисту інформації для туристичної фірми «Мандри світом».

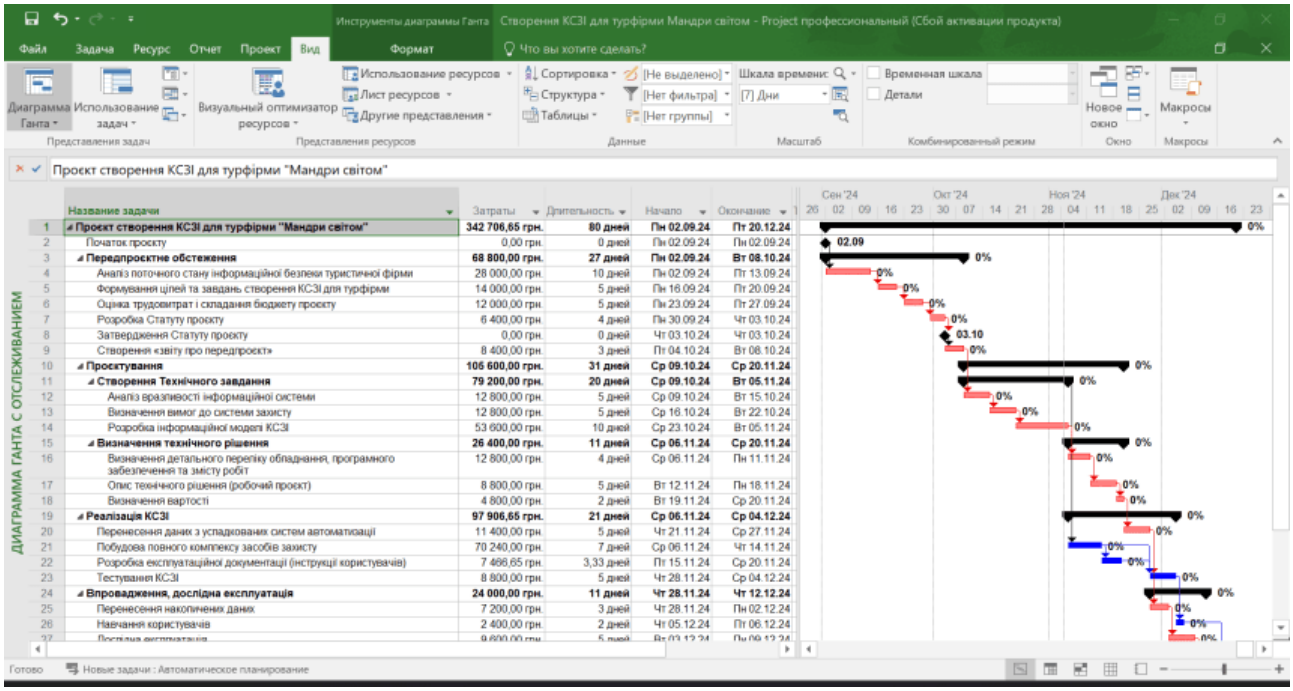

Рисунок 3.7 Календарно-мережевий графік робіт по проєкту

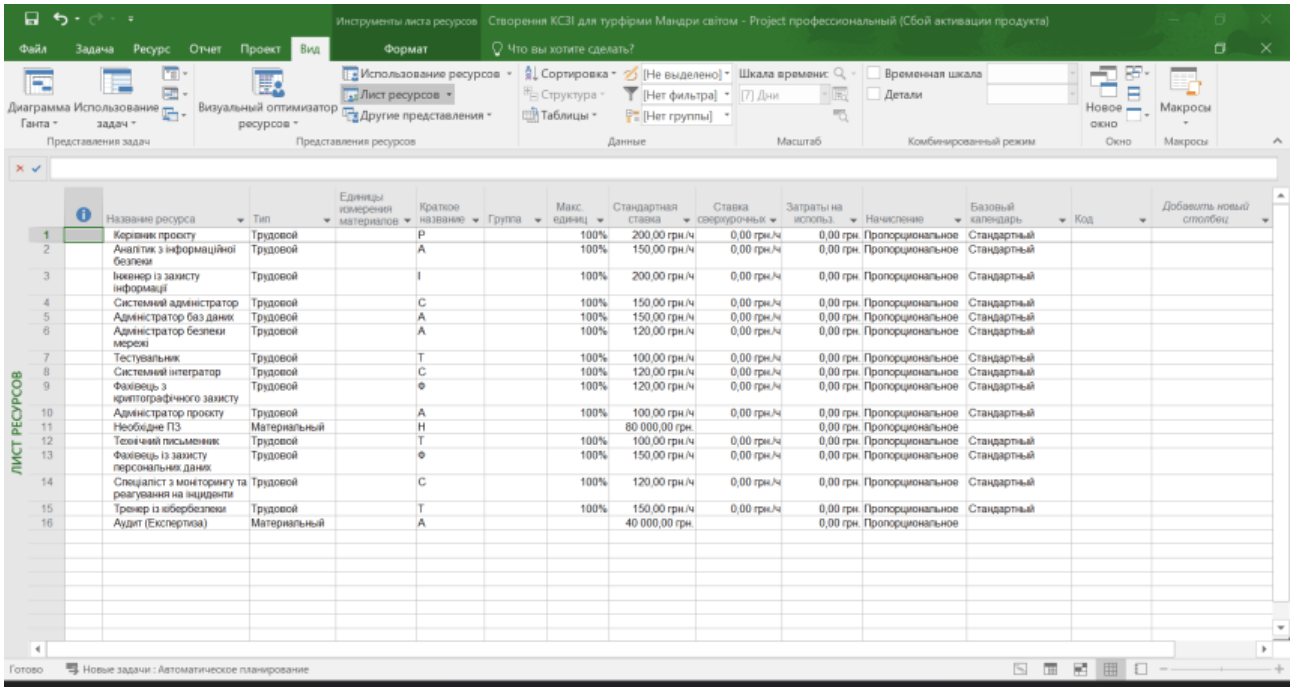

Рисунок 3.8. Лист ресурсів проєкту

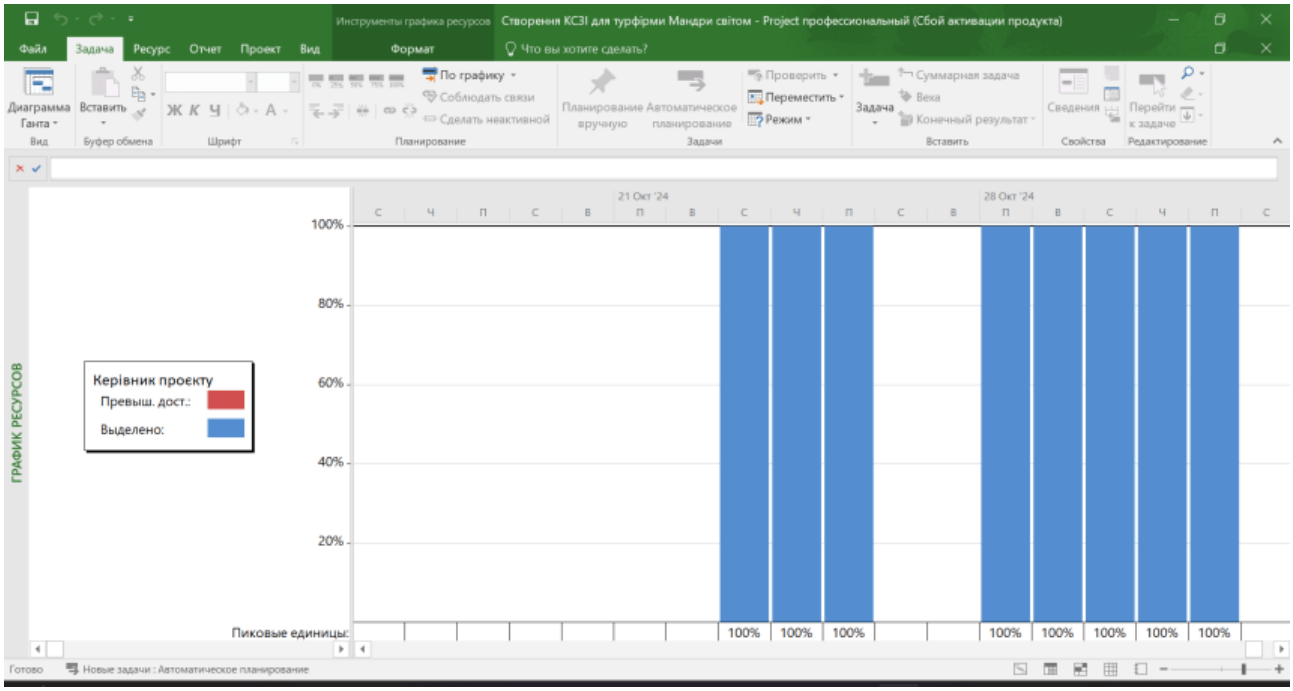

Рисунок 3.9 Завантаження ресурсу «Керівник проєкту»

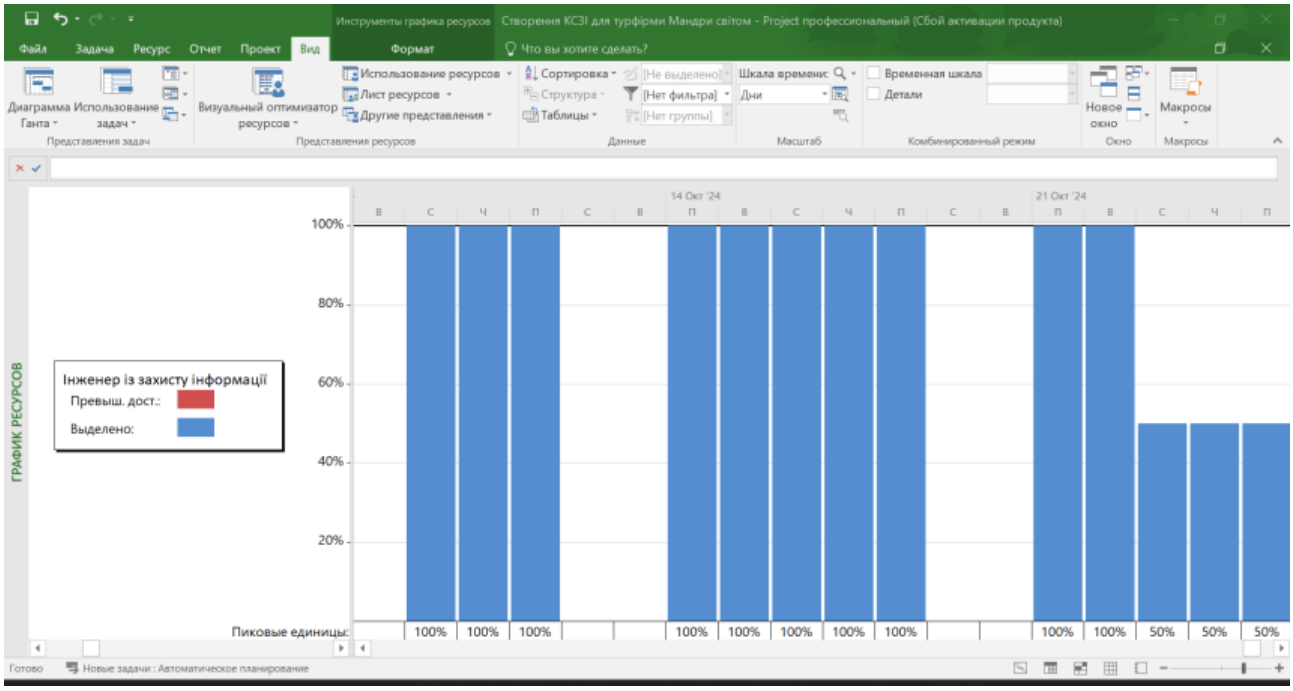

Рисунок 3.10 Завантаження ресурсу «Інженер із захисту інформації»

Проведене автоматичне вирівнювання в MS Project виявилося ефективним інструментом для балансування робочого навантаження між різними ресурсами проєкту, шляхом перерозподілу завдань та усунення конфліктів у графіку. Хоча цей процес міг призвести до деяких змін у загальній тривалості проєкту, загалом він сприяв підвищенню ефективності використання ресурсів та покращенню якості планування.

3.4 Управління вартістю проєкту

Управління вартістю є одним з найважливіших аспектів успішної реалізації проєктів розробки інформаційних систем. Воно включає в себе комплекс заходів, спрямованих на планування, оцінку, контроль та оптимізацію витрат протягом усього життєвого циклу проєкту.

Оцінка вартості включає розробку приблизної оцінки вартості ресурсів, необхідних для виконання робіт проєкту. Оцінка вартості проєкту по суті є оцінкою усіх витрат, необхідних для успішної і повної реалізації проєкту.

Планування витрат проєкту має здійснюватися для:

- визначення економічної ефективності проєкту порівнянням проєктних витрат і доходів;
- забезпечення фінансування проєкту;
- розподілу ресурсів проєкту відповідно до обсягів і змісту робіт;
- оцінювання тривалості робіт, оскільки визначення затрат необхідне для оцінювання часу, і навпаки – оцінювання часу дає змогу підрахувати витрати;
- забезпечення контролю проєкту (порівняння планових витрат із фактичними, визначення відхилень і прийняття відповідних коригувальних дій);
- підготовки участі компанії в тендерах (фірми, які беруть участь у тендерах з виконання проєктів, мають підрахувати витрати з метою визначення ціни своєї пропозиції, та прогнозування своїх прибутків від виконання проєкту).

Якщо проєкт виконується за контрактом, увага має бути приділена відмінності між оцінкою вартості та ціновою політикою. Оцінка вартості включає отримання оцінки ймовірних кількісних результатів – скільки коштуватиме для організації, що виконує проєкт, розробка конкретного продукту чи послуги. Цінова політика – це комерційне рішення, скільки коштів може заплатити організація-користувач проєкту за виробництво нового продукту чи послуги; тут використовується як один з безлічі чинників і оцінка вартості.

Методи та засоби оцінки вартості

1. *Оцінка на основі аналогів.* Оцінка на основі аналогів, або оцінка "зверху – вниз", означає використання фактичної вартості попередньої аналогічної роботи як оцінки вартості майбутньої роботи. Вона часто використовується для оцінки загальної вартості проєкту, коли про нього є небагато детальної інформації (наприклад, на його ранніх фазах). Оцінка на основі аналогів є однією з форм висновку експерта. Оцінка на основі аналогів дешевша за інші методи. Вона найбільш надійна, коли (a) попередні проєкти схожі не тільки за формою, а й за змістом, і коли (b) особи (група осіб), що виконують цю роботу, мають необхідний досвід.
2. *Параметричне моделювання.* Параметричне моделювання включає використання властивостей (параметрів) математичної моделі для прогнозу вартості проєкту. Моделі можуть бути простими (при зведенні житлового будинку квадратний метр житлової площі коштуватиме певну суму грошей) або складними (одна модель вартості розробки програмного забезпечення використовує 13 різних змінних чинників, по кожному з яких є 5-7 значень). Як вартість, так і точність параметричних моделей варіюється у великих межах. Найбільш імовірно надійними вони будуть, коли (a) інформація з архіву, що використовується для розробки моделі, була достатньо точною, (b) використовувані в моделі параметри є такими, що чітко вимірюються кількісно, і коли (c) модель масштабується – працює однаково добре як для дуже великого проєкту, так і для дуже малого.
3. Оцінка "знизу – *вверх".* Метод полягає в оцінці вартості окремих елементів робіт і подальшому підсумовуванні їх для отримання результату по проєкту. Вартість і точність оцінки "знизу вверх" залежать від розміру окремих елементів робіт: чим дрібніші елементи робіт, тим вищі вартість і точність. Команда управління проєктом має оцінити, що важливіше: підвищена точність або підвищена вартість.

Витрати, пов'язані з реалізацією проєкту, можуть бути різними, тому їх визначають за низкою ознак.

За методом віднесення на проєктні роботи розрізняють витрати:

– *прямі* – витрати за робочими пакетами відповідно до структури робіт проєкту (наприклад, заробітна плата виконавців роботи, оплата роботи субпідрядників);

– *непрямі* – накладні витрати, пов'язані з процесом управління проєктом та обслуговуванням виробництва продукту проєкту (наприклад, заробітна плата адміністративного персоналу проєкту, орендна плата за офіс, у якому працює проєктна команда).

За залежністю від зміни обсягів проєктних робіт витрати поділяють на:

– *постійні* – витрати, величина яких залишається незмінною у разі зміни обсягу виконання проєктних робіт (наприклад, витрати, пов'язані з управлінням, організацією та обслуговуванням проєкту);

– *змінні* – витрати, величина яких залежить від зміни обсягу виконання проєктних робіт (наприклад, матеріальні витрати, витрати на оплату роботи консультантів у проєкті).

За призначенням проєктні витрати групують на:

– *інвестиційні* – витрати на придбання основного і оборотного капіталу проєкту (наприклад, витрати на придбання землі, купівлю або оренду технологій та обладнання);

– *поточні* – витрати на випуск продукції проєкту та виконання інших проєктних робіт (наприклад, амортизаційні відрахування, витрати на оплату праці і соціальні нарахування).

За економічним змістом розрізняють такі елементи витрат:

– *трудові витрати* – це витрати на оплату праці людей, залучених до виконання проєкту. У грошовій формі вони обчислюються множенням кількості запланованих людино-годин на вартість однієї людино- години по кожному виду трудового ресурсу;

– *матеріальні витрати* – це вартість матеріалів або сировини, закуплених для створення кінцевого продукту проєкту. Наприклад, для проєкту проведення навчання персоналу це будуть втрати на придбання навчальної літератури та канцелярського приладдя;

– *витрати на придбання, оренду або лізинг обладнання і придбання або оренду виробничих приміщень.* Ці витрати враховують частину вартості устаткування (через амортизаційні відрахування) та приміщень у межах часу їх використання в проєкті;

– *субконтракта* – це витрати, які відображають вартість виконання частини проєктних робіт зовнішніми організаціями. До них відносять оплату праці зовнішніх учасників та матеріалів, які постачаються зовнішніми підрядниками;

– *витрати на управління проєктом* – це виграти на здійснення процесів управління проєктом. До них можуть відноситися трудові або матеріальні виграти, але які не прямо пов'язані з виконанням конкретних проєктних робіт, а стосуються всього проєкту. Наприклад, оплата праці менеджера проєкту, витрати на утримання управлінських структур проєкту (проєктного офісу) та проєктних інформаційних систем;

– *інші витрати* – це витрати, які за своїм економічним змістом не увійшли до названих вище груп. До цієї категорії можуть відноситися різні наладні та адміністративні витрата, такі як транспортні, складські витрати, страхові або ліцензійні виплата по проєкту [10].

Структура вартості проєкту в розрізі статей витрат звичайно базується на структурі плану рахунків проєкту, що представляє собою декомпозицію витрат від самого верхнього рівня вартості всього проєкту до нижнього рівня вартості однієї одиниці ресурсів. Для конкретного проєкту вибирається свій план рахунків або їх сімейство. Як базові варіанти можуть використовуватися бухгалтерські плани рахунків, плани рахунків управлінського обліку.

Витрати по проєкту створення комплексної системи захисту інформації для туристичної фірми «Мандри світом» представлені в таблиці 3.1.

Таблиця 3.1

Витрати по проєкту

Назва задачі	Витрати
Проєкт створення КСЗІ для турфірми "Мандри світом"	**342 706,65 грн.**
Передпроєктне обстеження	**68 800,00 грн.**
Аналіз поточного стану інформаційної безпеки туристичної фірми	28 000,00 грн.
Формування цілей та завдань створення КСЗІ для турфірми	14 000,00 грн.
Оцінка трудовитрат і складання бюджету проєкту	12 000,00 грн.
Розробка Статуту проєкту	6 400,00 грн.
Створення «звіту про передпроєкт»	8 400,00 грн.
Проєктування	**105 600,00 грн.**
Створення Технічного завдання	**79 200,00 грн.**
Аналіз вразливості інформаційної системи	12 800,00 грн.
Визначення вимог до системи захисту	12 800,00 грн.
Розробка інформаційної моделі КСЗІ	53 600,00 грн.
Визначення технічного рішення	**26 400,00 грн.**
Визначення детального переліку обладнання, програмного забезпечення та змісту робіт	12 800,00 грн.
Опис технічного рішення (робочий проєкт)	8 800,00 грн.
Реалізація КСЗІ	**97 906,65 грн.**
Перенесення даних з успадкованих систем автоматизації	11 400,00 грн.
Побудова повного комплексу засобів захисту	70 240,00 грн.
Розробка експлуатаційної документації (інструкції користувачів)	7 466,65 грн.
Тестування КСЗІ	8 800,00 грн.
Впровадження, дослідна експлуатація	**24 000,00 грн.**
Перенесення накопичених даних	7 200,00 грн.
Навчання користувачів	2 400,00 грн.
Дослідна експлуатація	9 600,00 грн.
Здача в промислову експлуатацію	4 800,00 грн.
Аудит проєкту (експертиза)	**46 400,00 грн.**
Проведення аудиту проєкту	23 200,00 грн.
Формування рекомендацій щодо коригувальних дій	23 200,00 грн.
Отримання експертного висновку (атестату відповідності)	0,00 грн.

Згідно з даними таблиці витрат, загальна сума, витрачена на проєкт «Створення КСЗІ для турфірми "Мандри світом"», склала 342 706,65 грн.
Найбільшу частку витрат склали:

- Придбання програмного забезпечення (80 000 грн.): Ця стаття витрат включає в себе створення та налаштування програмних засобів, необхідних для забезпечення безпеки інформаційних систем компанії, таких як системи виявлення вторгнень, антивіруси, засоби шифрування даних тощо.
- Аудит та експертиза (40 000 грн.): Ці витрати пов'язані з проведенням комплексної оцінки рівня захищеності інформаційних систем компанії, виявленням вразливостей та розробкою рекомендацій щодо їх усунення.

Проведені аудити та експертизи підтвердили, що розроблена КСЗІ повністю відповідає сучасним вимогам до систем захисту інформації. Впровадження системи дозволило турфірмі "Мандри світом" досягти високого рівня захисту персональних даних клієнтів, що є обов'язковою умовою для роботи в туристичній індустрії.

Інвестиції в створення КСЗІ є виправданими, оскільки забезпечують високий рівень захисту інформації та сприяють стабільному розвитку бізнесу турфірми "Мандри світом". Впровадження КСЗІ дозволить компанії підвищити свою конкурентоспроможність та забезпечити довгострокову стабільність.

3.5 Управління ризиками проєкту

Одним з основних завдань, які розв’язують у межах управління ІТ-проєктами, є управління ризиками проєктної діяльності, або управління ризиками проєкту. Це завдання не відокремлюється від більшості інших функцій управління ІТ-проєктами. Під час визначення фінансових потреб, обчислення кошторису й бюджету, підготовки й укладення контрактів, під час контролю за реалізацією проєкту постає завдання захисту учасників проєктної діяльності від

різних видів ризиків. Саме тому проблеми дослідження та управління ризиками в проєктній діяльності є важливими і актуальними з погляду як теорії, так і застосувань на практиці.

У межах теорії та практики управління проєктними ризиками найважливішими є, зокрема, методи оцінки, моніторингу та прогнозування ризиків, інформаційного забезпечення управління ризиками. Діяльність з управління ризиками охоплює такі основні етапи: виявлення ризику, його оцінювання, вибір методу та засобів управління ризиком, запобігання, контролювання, фінансування ризику, оцінювання результатів. Проєкт функціонує у визначеному оточенні, що містить внутрішні і зовнішні компоненти, які, своєю чергою, враховують економічні, політичні, соціальні, технологічні, нормативні, культурні й інші фактори.

Основними елементами системи управління в ситуаціях невизначеності є: виявлення в альтернативах ризику та утримання його в межах прийнятного рівня; розроблення конкретних рекомендацій, орієнтованих на усунення або мінімізацію можливих негативних наслідків ризику. Задача управління ризиками IT-проєктів полягає у зменшенні впливу небажаних факторів на життєвий цикл проєкту для отримання результатів, найближчих до бажаних.

Поняття ризику визначається залежно від сфери застосування по-різному, і саме в проєктній діяльності (стратегічне планування, управління проєктом та оперативне корегування перебігу його виконання) виникають найрізноманітніші види ризиків.

Під оперативним управлінням проєктом розумітимемо управління проєктом в процесі його реалізації з урахуванням досягнутих результатів і зміни зовнішніх і внутрішніх умов. Під зовнішніми умовами розумітимемо сукупність істотних з погляду проєкту параметрів, які описують навколишнє середовище. Під внутрішніми умовами розумітимемо сукупність істотних з погляду проєкту параметрів, що описують його учасників (центр, виконавців тощо). Основною метою оперативного управління проєктами є забезпечення виконання планових

показників і підвищення загальної ефективності функцій планування і контролю проєкту.

Нехай відомі обмеження на значення управляючих параметрів і заданий критерій ефективності управління, що залежить як від управляючих, так і від залежних параметрів. Тоді на якісному рівні задача управління сформулюється так: вибрати такі допустимі значення управляючих параметрів, які приводили б критерій ефективності управління в екстремум. Якщо в ході реалізації проєкту виявляється відхилення фактичних значень показників від планових, то задачу планування необхідно розв'язувати «наново» з урахуванням наявної інформації. Техніка розв'язання не змінюється, змінюються лише початкові умови («початкове» значення часу дорівнюватиме не нульовому, а поточному тощо) і параметри, скореговані з урахуванням інформації, що надійшла. Якщо на етапі планування була невизначеність щодо стану природи, то в ході реалізації проєкту під час розв'язання задач оперативного управління ця невизначеність буде зменшуватися за рахунок наявної інформації про історію реалізації проєкту. Зміст оперативного управління проєктами полягає у визначенні результатів діяльності на основі оцінки і документування фактичних показників виконання і порівняння їх з плановими показниками.

Задача управління ризиками полягає у зменшенні впливу небажаних факторів на життєвий цикл інформаційно-технологічного проєкту для отримання результатів, найближчих до бажаних. Можливості маневрування при управлінні ризиками доволі різноманітні: запобігання ризику, відхилення від ризику, свідоме і неусвідомлене прийняття ризику, дублювання операцій, скорочення величини потенційних і фактичних утрат, розподілення ризику між учасниками, розукрупнення ризику, рознесення експозицій у просторі та у часі, ізоляція небезпечних синергетичних факторів один від одного, перенесення ризику (страховий та нестраховий трансфер) на інших агентів, аутсорсинг тощо.

Але яким би не був той чи інший метод управління ризиком, взагалі позбутись ризику не вдається. Це зумовлено тим, що в довільній динамічній системі завжди існує певний рівень залишкової ентропії. У випадку проєктної

діяльності, зокрема ІТ-проєктів, такою системою є, з одного боку, проєкт, а з іншого – зовнішнє середовище, що оточує його, як сукупність всього того, що взаємодіє з проєктом і впливає на нього.

Таблиця 3.2

Ризики проєкту створення КСЗІ

№	Ризик	Можливі наслідки	Ймовірність	Вплив	Заходи протидії
1	Недостатнє фінансування	Затримка або припинення проєкту, зниження якості системи	Середня	Високий	Складання детального бюджету, пошук додаткових джерел фінансування, гнучке планування витрат
2	Недостатня кваліфікація персоналу	Помилки при розробці та впровадженні системи, низька ефективність	Середня	Середній	Навчання персоналу, залучення зовнішніх експертів
3	Затримки у розробці	Збільшення витрат, зниження мотивації співробітників	Середня	Середній	Чіткий графік робіт, регулярні звіти про прогрес, резервування часу на непередбачені ситуації
4	Несумісність з існуючою ІТ-інфраструктурою	Додаткові витрати на модернізацію, затримки у впровадженні	Середня	Середній	Попередній аналіз існуючої інфраструктури, розробка плану міграції даних
5	Відсутність підтримки з боку керівництва	Недостатнє фінансування, відсутність мотивації співробітників	Висока	Високий	Залучення керівництва до процесу прийняття рішень, демонстрація переваг проєкту
6	Зміна вимог замовника	Збільшення витрат, затримки у розробці	Висока	Середній	Чітке формулювання вимог на початку проєкту, регулярні зустрічі з замовником для уточнення деталей
7	Кібератаки	Втрата даних, фінансові втрати, репутаційні ризики	Низька	Високий	Регулярне оновлення програмного забезпечення, навчання співробітників, інцидент-менеджмент
8	Внутрішні загрози	Несанкціонований доступ до даних, зловмисні дії співробітників	Середня	Високий	Система контролю доступу, навчання співробітників, політика безпеки
9	Технічні збої	Втрата даних, перебої в роботі системи	Середня	Середній	Резервне копіювання даних, моніторинг системи, швидке відновлення після збоїв
10	Недостатня ефективність системи	Відсутність очікуваного результату, незадоволеність замовника	Висока	Високий	Тестування системи, збір зворотного зв'язку від користувачів, постійна оптимізація

Звичайно, керованішим є проєкт, а на зовнішні невизначеності вплив є зазвичай меншим. Зважаючи на це, для зменшення ризиків ІТ-проєкту основну увагу необхідно зосередити на управлінні проєктом. Така система повинна реалізувати такі основні функції: виявлення ризиків, оцінювання ризиків, аналіз ризиків, управління ризиками. Чим триваліший горизонт планування проєкту, тим більше повинні використовуватися методи стратегічного планування, а на ближчих більшого значення набувають власне процеси координування, управління, і на коротких проміжках часу – диспетчерування, оперативне управління ресурсами.

Яким би не був той чи інший метод управління ризиком, взагалі позбутися ризику не вдасться, оскільки в довільній системі завжди існує певний рівень залишкової ентропії, а у випадку проєктної діяльності такою системою є, з одного боку, проєкт, а з іншого – зовнішнє середовище, що його оточує, як сукупність всього того, що взаємодіє з проєктом. Однак оперативне управління ризиками ІТ-проєкту та його надійністю дає змогу підвищити ефективність загального управління проєктом, особливо в умовах невизначеності.

Висновок до розділу 3

В даному розділі атестаційної роботи описано хід реалізації проєкту зі створення комплексної системи захисту інформації для турфірми "Мандри світом". Було успішно застосовано сучасні методи управління проєктами. Використання діаграм Ганта та мережевих графіків дозволило ефективно планувати та контролювати терміни виконання робіт.

Регулярний моніторинг витрат забезпечив дотримання бюджету проєкту. Згідно з даними таблиці витрат, загальна сума, витрачена на проєкт «Створення КСЗІ для турфірми "Мандри світом"», склала 342 706,65 грн.

Проведені аудити та експертизи підтвердили, що розроблена КСЗІ повністю відповідає сучасним вимогам до систем захисту інформації.

Впровадження системи дозволило турфірмі "Мандри світом" досягти високого рівня захисту персональних даних клієнтів, що є обов'язковою умовою для роботи в туристичній індустрії.

Інвестиції в створення КСЗІ є виправданими, оскільки забезпечують високий рівень захисту інформації та сприяють стабільному розвитку бізнесу турфірми "Мандри світом". Впровадження КСЗІ дозволить компанії підвищити свою конкурентоспроможність та забезпечити довгострокову стабільність.

Однак, виникли деякі труднощі, пов'язані з непередбаченими змінами вимог замовника. Для їх вирішення було розроблено додаткові заходи, що дозволило уникнути серйозних затримок. Загалом, проєкт був успішно завершений, і розроблена система відповідає всім поставленим вимогам. Основним уроком, винесеним з цього проєкту, є необхідність гнучкого підходу до управління змінами та постійної комунікації з замовником.

Яким би не був той чи інший метод управління ризиком, взагалі позбутися ризику не вдасться, оскільки в довільній системі завжди існує певний рівень залишкової ентропії, а у випадку проєктної діяльності такою системою є, з одного боку, проєкт, а з іншого – зовнішнє середовище, що його оточує, як сукупність всього того, що взаємодіє з проєктом. Однак оперативне управління ризиками ІТ-проєкту та його надійністю дає змогу підвищити ефективність загального управління проєктом, особливо в умовах невизначеності.

ЗАГАЛЬНІ ВИСНОВКИ

У результаті проведеного дослідження та практичної реалізації проєкту зі створення комплексної системи захисту інформації для туристичної фірми "Мандри світом" було доведено, що ефективне управління проєктом є ключовим фактором успішної реалізації складних ІТ-проєктів.

Основні висновки:

1. Важливість детального планування: Складання детального плану проєкту, включаючи розподіл завдань, визначення термінів та ресурсів, дозволяє забезпечити чітке розуміння цілей проєкту та контролювати його хід.
2. Значення гнучкого підходу: Здатність адаптуватися до змін вимог замовника та непередбачених обставин є критично важливою для успіху проєкту. Використання ітеративних методів розробки та гнучких методологій (наприклад, Agile) дозволяє знизити ризики та підвищити задоволеність замовника.
3. Роль комунікації: Ефективна комунікація між усіма учасниками проєкту є запорукою успішного виконання робіт. Регулярні звіти, зустрічі та використання інструментів для спільного доступу до інформації сприяють прозорості та координації дій.
4. Управління ризиками: Ідентифікація, оцінка та управління ризиками є невід'ємною частиною будь-якого проєкту. Розробка планів реагування на ризики дозволяє мінімізувати їх негативний вплив.
5. Значення людського фактора: Кваліфікація команди проєкту, її мотивація та ефективна співпраця мають вирішальне значення для успіху проєкту.
6. Важливість тестування та впровадження: Ретельне тестування системи перед впровадженням дозволяє виявити та усунути помилки. Розробка плану впровадження забезпечує плавний перехід до нової системи.

Рекомендації для майбутніх проєктів:

- Використання сучасних інструментів управління проєктами: Програмне забезпечення для управління проєктами (наприклад, MS Project, як

альтернатива Jira, Trello) може значно полегшити планування, контроль та комунікацію.

- Залучення досвідчених фахівців: Команда проєкту повинна складатися з досвідчених фахівців у різних областях (розробка, безпека, управління проєктами).
- Регулярна оцінка ефективності проєкту: Проведення регулярних оцінок дозволяє виявляти проблеми на ранніх стадіях і вносити необхідні корективи.
- Постійна підтримка замовника: Активна участь замовника у проєкті забезпечує чітке розуміння його потреб і очікувань.

Висновки щодо створеної системи захисту інформації:

- Система забезпечує високий рівень безпеки інформації та відповідає сучасним вимогам.
- Впровадження системи дозволило знизити ризики кібератак та захистити конфіденційні дані клієнтів.
- Система є гнучкою та може бути легко адаптована до зміни вимог бізнесу.

Загалом, результати проєкту свідчать про ефективність застосованих методів управління проєктом і високу якість створеної системи захисту інформації.

СПИСОК ДЖЕРЕЛ

1. Комплексні системи захисту інформації: навч. посіб. / Ю.Є. Яремчук та ін. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с.
2. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
3. Матеріали VI Міжнародної науково-практичної конференції “Інформаційна безпека та комп’ютерні технології”: тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.
4. Остапов С.Е. Технологія захисту інформації: навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.
5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР: станом на 1 лип. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 25.09.2024).
6. A Guide to the Project Management Body of Knowledge: Fifth Edition (PMBOK Guide). - 2013. - 616 p.
7. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
8. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.
9. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

11. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіонепрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. № 3 – С. 56–65.
12. Яремчук Ю. Є. Дослідження характеристик вітчизняних радіонепрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42–51.
13. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
14. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
15. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроєктні роботи.
16. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».
17. НД ТЗІ 2.7-011-2012 «Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв».
18. ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».
19. Проєктування комплексних систем захисту інформації: методичні вказівки, завдання на контрольну та курсову роботи / Уклад.: В. С. Орленко, В. О. Хорошко, Д. В. Чирков. – К. : ДУІКТ, 2005. – 14 с.

ДОДАТКИ

Додаток 1

Презентація роботи в MS PowerPoint

Рис. Д.1.1 Слайд 1

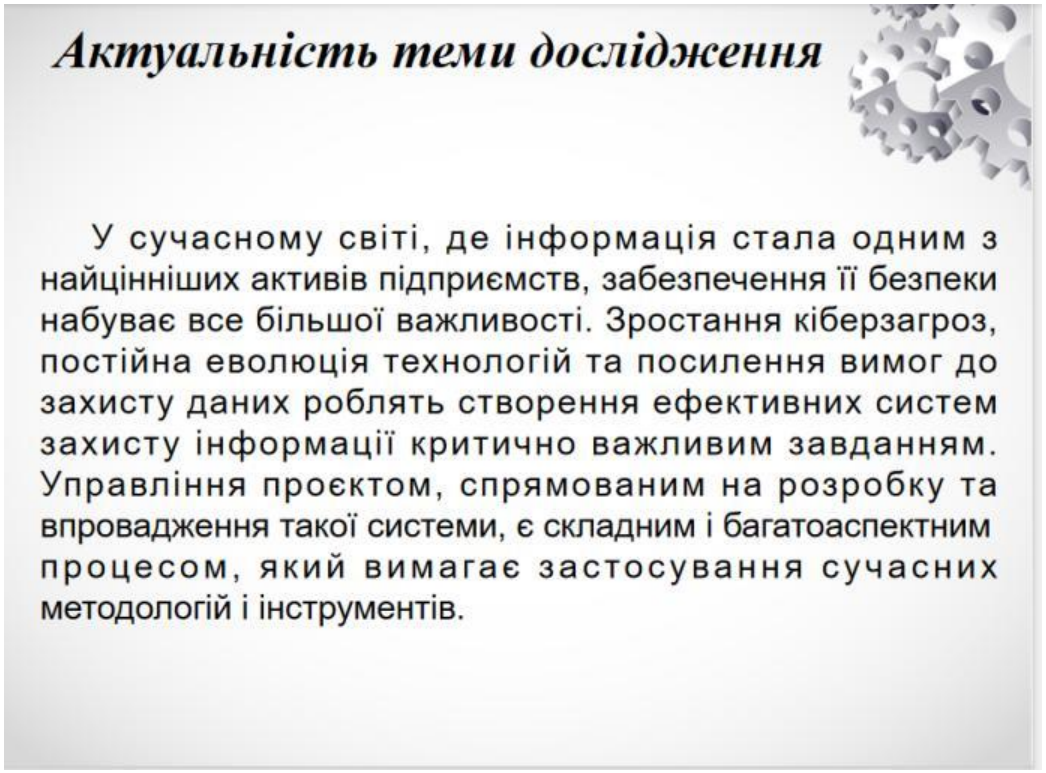

Рис. Д.1.2 Слайд 2

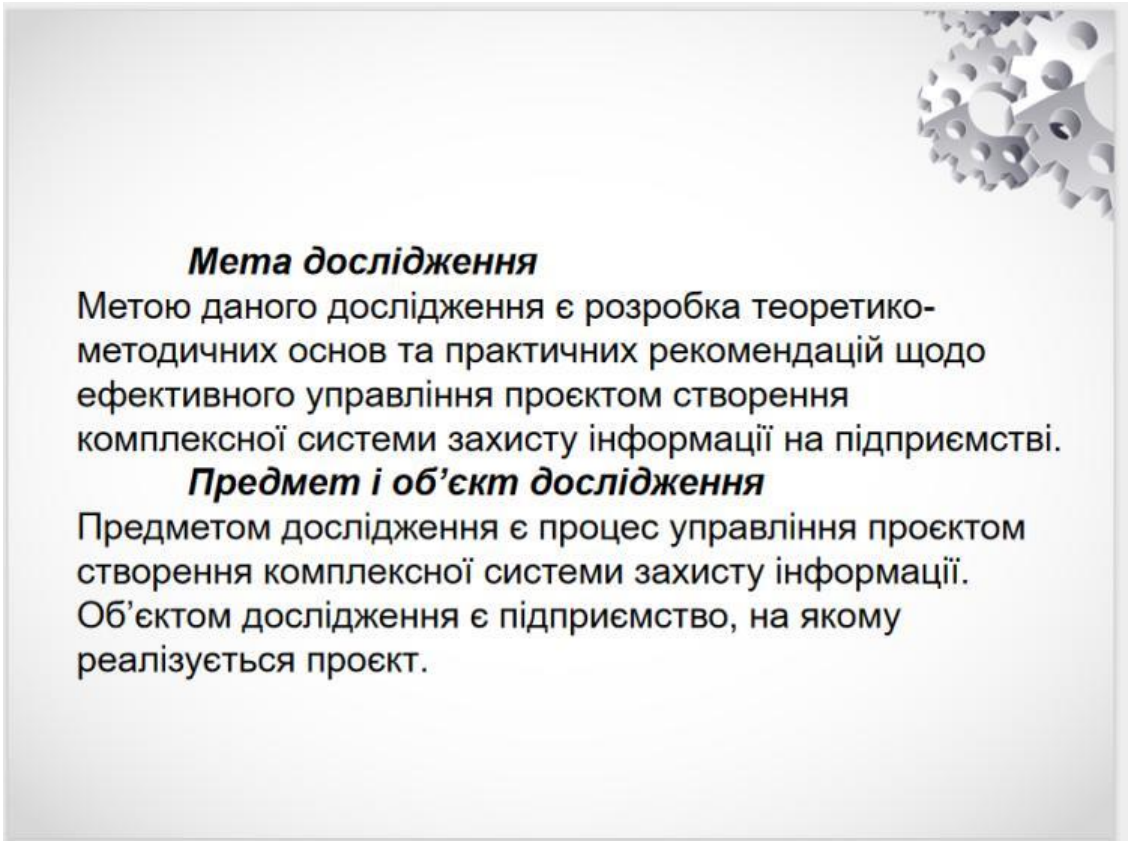

Рис. Д.1.3 Слайд 3

Рис. Д.1.4 Слайд 4

Концептуальна модель інформаційної безпеки

Мета моделі:

- модель показує як проєктувати комплексну систему захисту інформації;
- модель розкриває основні напрямки захисту інформації.

Рис. Д.1.5 Слайд 5

Призначення комплексної системи захисту інформації

- **Комплексна система захисту інформації** — це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.
- Головна мета КСЗІ полягає у забезпеченні конфіденційності, цілісності та доступності інформації, що обробляється в дата центрі чи хмарному середовищі.

Рис. Д.1.6 Слайд 6

Рис. Д.1.7 Слайд 7

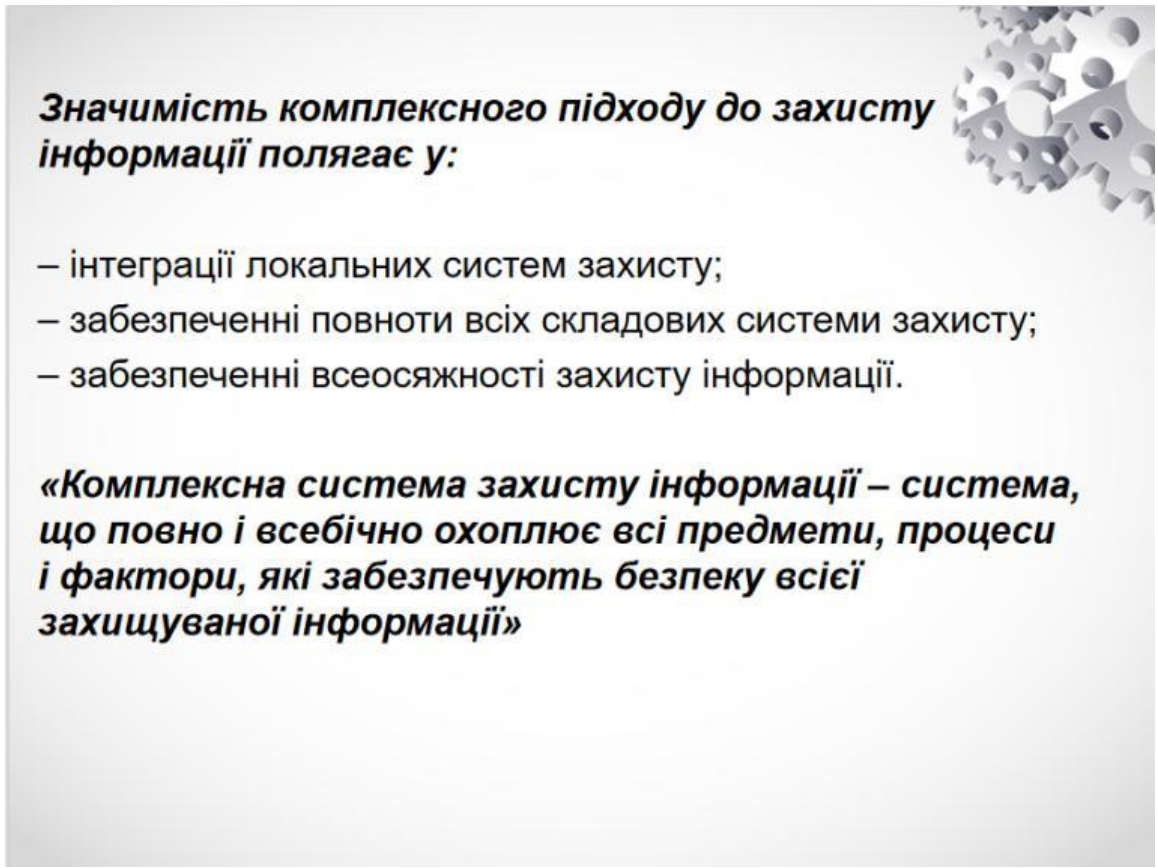

Рис. Д.1.8 Слайд 8

Рис. Д.1.9 Слайд 9

Рис. Д.1.10 Слайд 10

SWOT-аналіз проєкту створення КСЗІ для туристочної фірми

Фактор	Опис
Сильні сторони	* Захист конфіденційної інформації клієнтів * Підвищення довіри клієнтів * Спрощення внутрішніх процесів * Відповідність законодавству * Можливість отримання сертифікатів
Слабкі сторони	* Висока вартість впровадження * Складність технічної реалізації * Опір змін * Потреба в постійному оновленні
Можливості	* Поліпшення конкурентоспроможності * Розширення спектру послуг * Співпраця з іншими компаніями * Отримання державної підтримки
Загрози	* Кібератаки * Зміна законодавства * Вихід з ладу обладнання * Зміна поведінки споживачів

Рис. Д.1.11 Слайд 11

Статут проєкту створення КСЗІ

1. Мета проєкту і продукту.

Проєкт: Створення комплексної системи захисту інформації для туристичної фірми "Мандри світом"

Мета проєкту: забезпечення високого рівня безпеки інформації, яка обробляється туристичною фірмою "Мандри світом". Це включає в себе захист конфіденційних даних клієнтів, фінансової інформації, а також внутрішньої інформації компанії від несанкціонованого доступу, розкриття, зміни або знищення.

Тривалість проєкту: 80 робочих днів.

Продукт: Продуктом цього проєкту є комплексна система захисту інформації, яка забезпечує безпеку даних компанії та її клієнтів. Ця система є набором взаємопов'язаних технологічних рішень, політик і процедур, спрямованих на захист інформації від несанкціонованого доступу, розкриття, зміни або знищення.

Рис. Д.1.12 Слайд 12

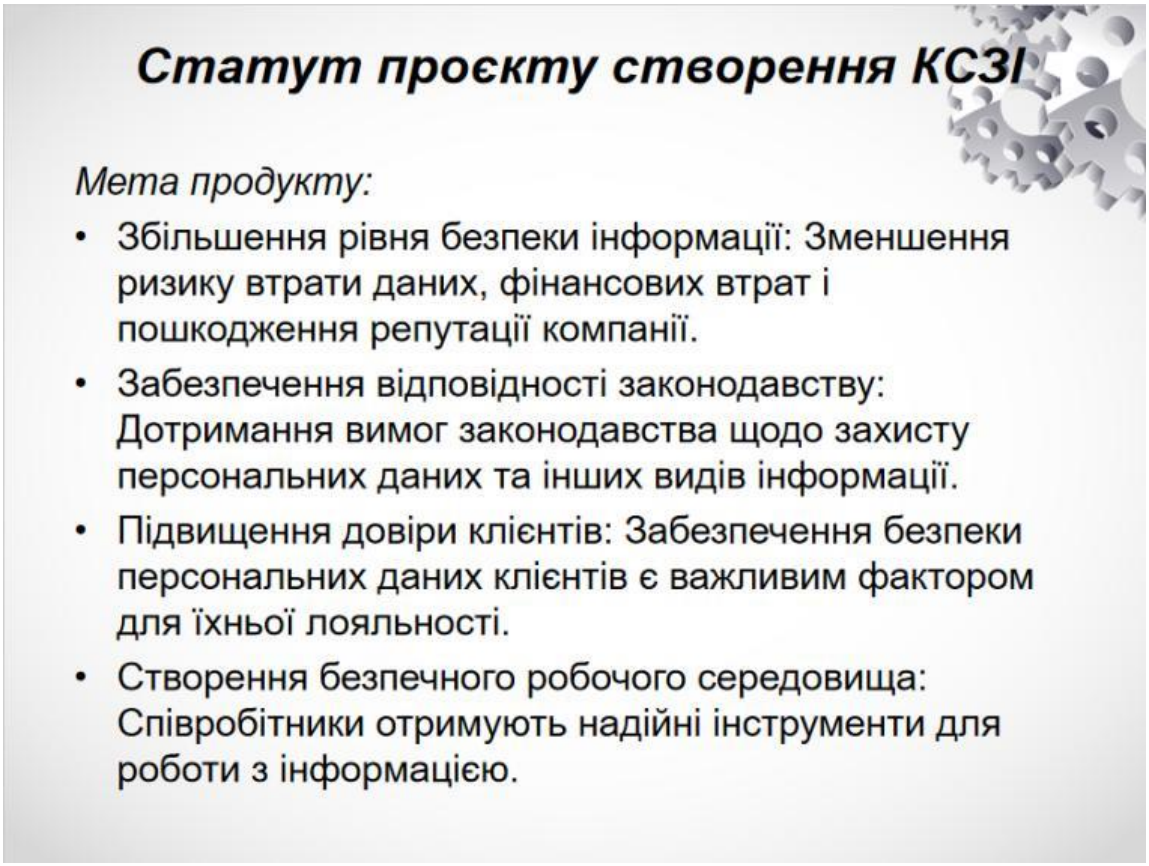

Рис. Д.1.13 Слайд 13

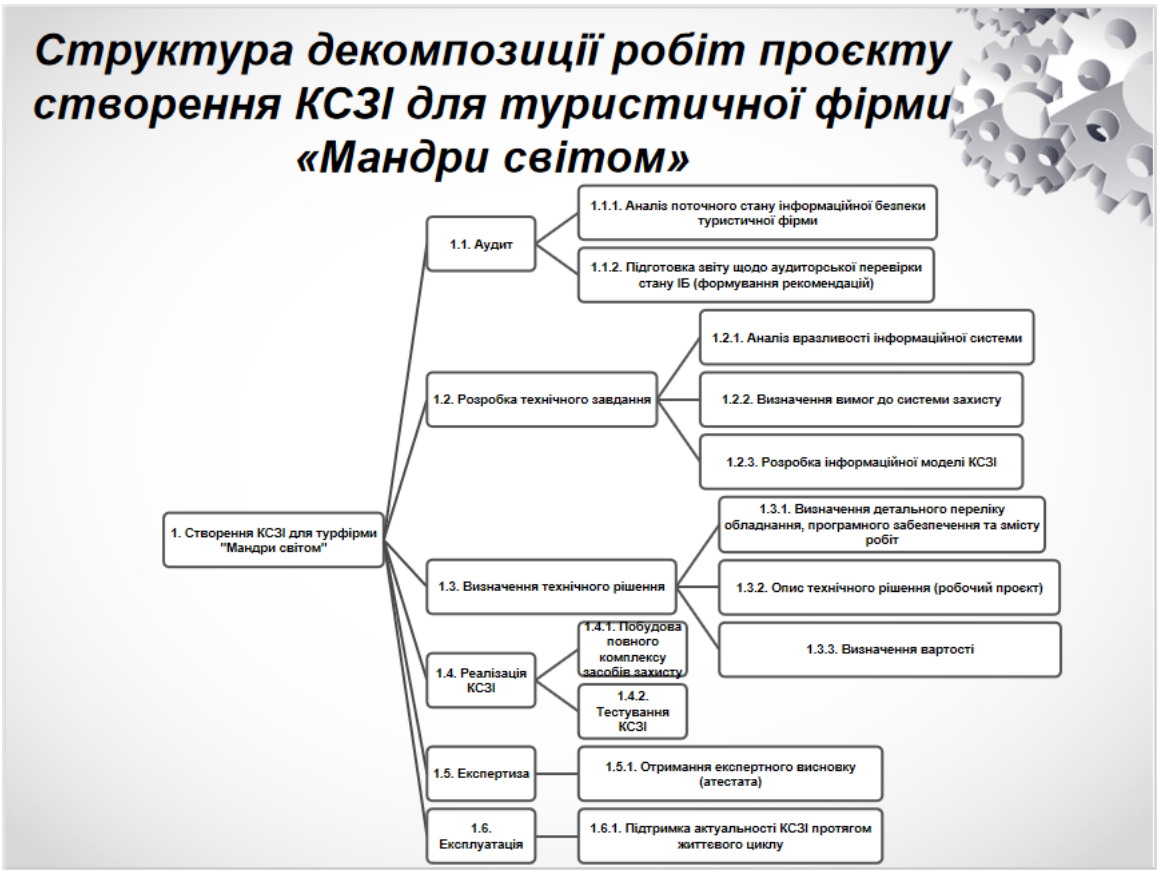

Рис. Д.1.14 Слайд 14

Рис. Д.1.15 Слайд 15

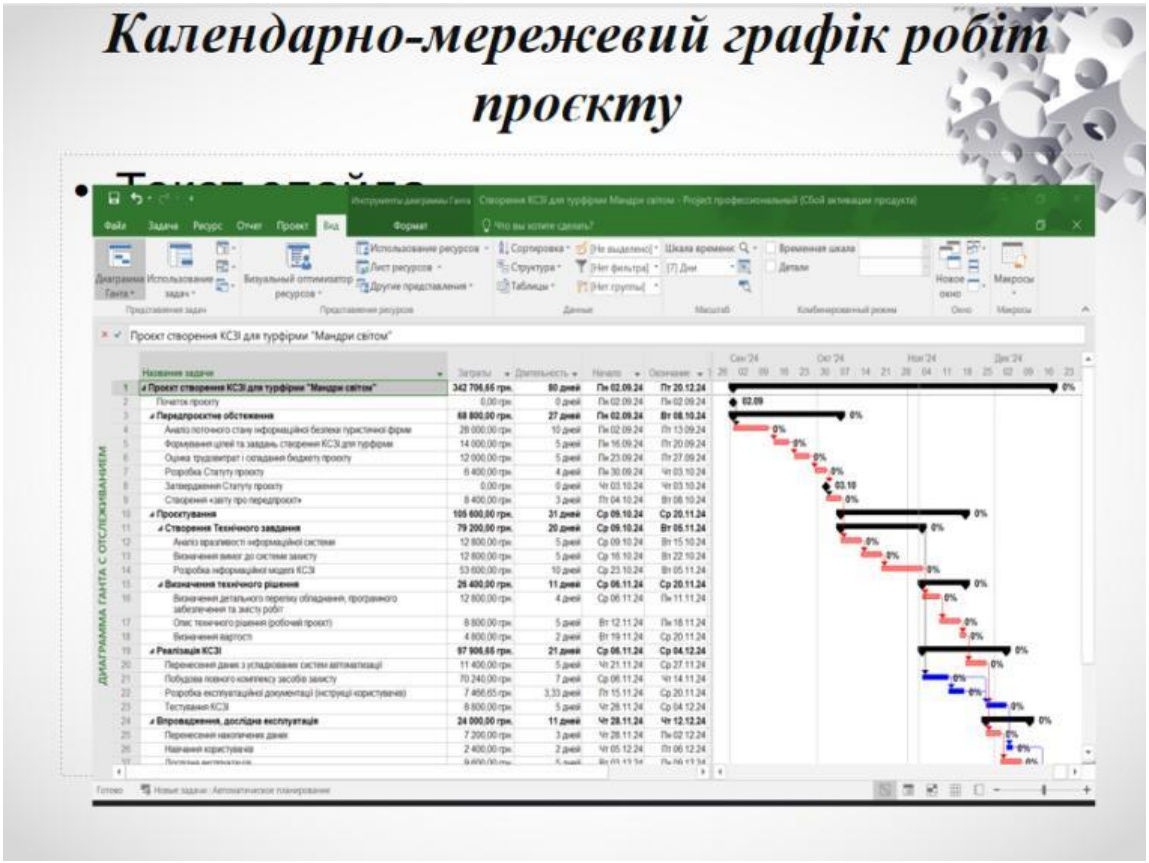

Рис. Д.1.16 Слайд 16

Витрати по проєкту

Назва задачі	Витрати
Проєкт створення КСЗІ для турфірми "Мандри світом"	342 706,65 грн.
Передпроєктне обстеження	68 800,00 грн.
Аналіз поточного стану інформаційної безпеки туристичної фірми	28 000,00 грн.
Формування цілей та завдань створення КСЗІ для турфірми	14 000,00 грн.
Оцінка трудовитрат і складання бюджету проєкту	12 000,00 грн.
Розробка Статуту проєкту	6 400,00 грн.
Створення «звіту про передпроєкт»	8 400,00 грн.
Проєктування	105 600,00 грн.
Створення Технічного завдання	79 200,00 грн.
Визначення технічного рішення	26 400,00 грн.
Реалізація КСЗІ	97 906,65 грн.
Впровадження, дослідна експлуатація	24 000,00 грн.
Аудит проєкту (експертиза)	46 400,00 грн.

Рис. Д.1.17 Слайд 17

Ризики проєкту створення КСЗІ

№	Ризик	Можливі наслідки	Ймовірність	Вплив	Заходи протидії
1	Недостатнє фінансування	Затримка або припинення проєкту, зниження якості системи	Середня	Високий	Складання детального бюджету, пошук додаткових джерел фінансування, гнучке планування витрат
2	Недостатня кваліфікація персоналу	Помилки при розробці та впровадженні системи, низька ефективність	Середня	Середній	Навчання персоналу, залучення зовнішніх експертів
3	Затримки у розробці	Збільшення витрат, зниження мотивації співробітників	Середня	Середній	Чіткий графік робіт, регулярні звіти про прогрес, резервування часу на непередбачені ситуації
4	Несумісність з існуючою IT-інфраструктурою	Додаткові витрати на модернізацію, затримки у впровадженні	Середня	Середній	Попередній аналіз існуючої інфраструктури розробка плану міграції даних
5	Відсутність підтримки з боку керівництва	Недостатнє фінансування, відсутність мотивації співробітників	Висока	Високий	Залучення керівництва до процесу прийняття рішень, демонстрація переваг проєкту

Рис. Д.1.18 Слайд 18

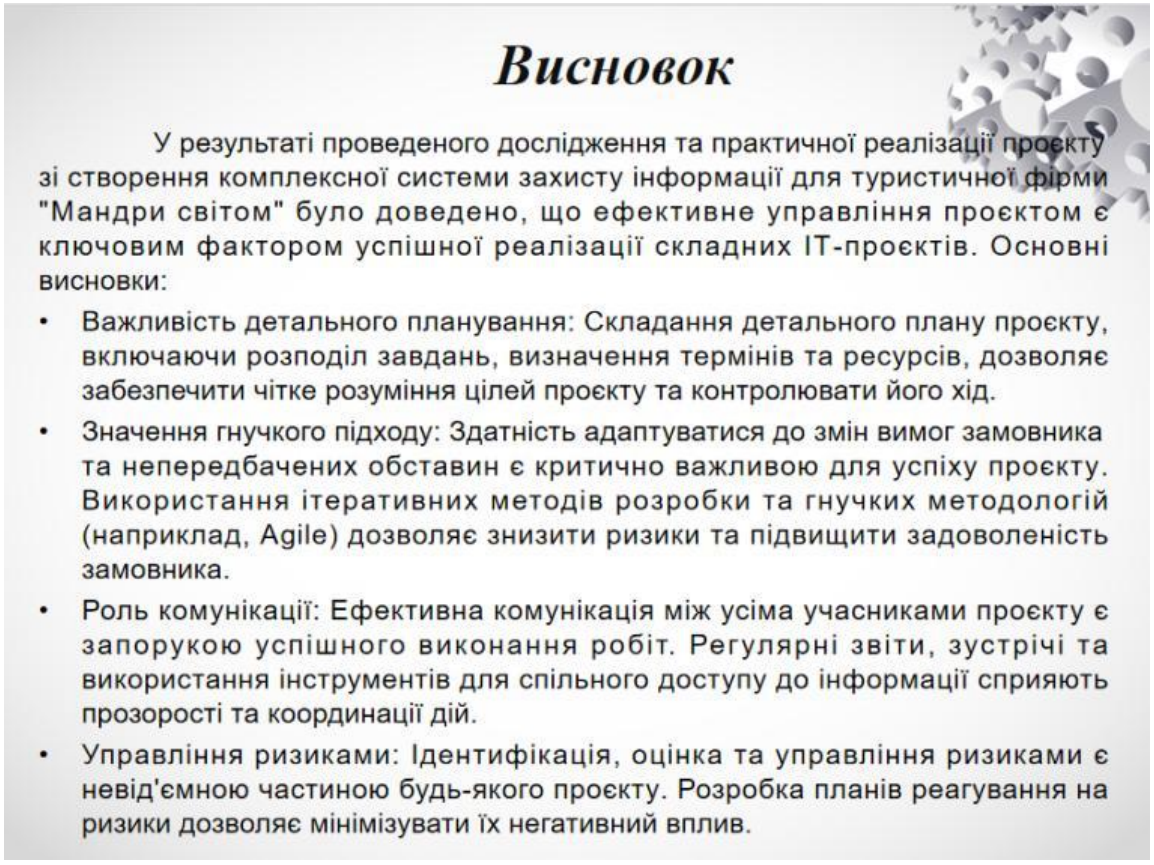

Рис. Д.1.19 Слайд 19

Рис. Д.1.20 Слайд 20