Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення)

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

бакалавр
(ступінь вищої освіти)

на тему **«Забезпечення конфіденційності інформації в телекомунікаційній мережі електронної торгівельної площадки»**

Виконав: студент 4 курсу, групи 401-ТТ
спеціальності 172 «Електронні комунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)
Гонтар М. Ю.
(прізвище та ініціали)
Керівник Косенко В. В.
(прізвище та ініціали)
Рецензент _____ ____
(прізвище та ініціали)

Полтава - 2025 рік

РЕФЕРАТ

У бакалаврській роботі розглянуто проблематику забезпечення конфіденційності інформації в телекомунікаційній мережі електронної торгівельної площадки. Актуальність дослідження зумовлена зростанням обсягів електронної комерції та необхідністю захисту персональних і комерційних даних від несанкціонованого доступу, витоку або підміни.

У роботі проаналізовано сучасні загрози інформаційній безпеці у сфері електронної торгівлі, досліджено архітектуру телекомунікаційних мереж таких платформ і визначено вразливі точки, через які може бути порушено конфіденційність. Розглянуто теоретичні засади криптографічного захисту, протоколи шифрування, механізми автентифікації та безпечного обміну даними. Особливу увагу приділено впровадженню стандартів інформаційної безпеки.

У практичній частині роботи здійснено моделювання базової архітектури захищеної телекомунікаційної мережі для електронної торгової платформи з урахуванням вимог до конфіденційності. Також запропоновано рекомендації щодо посилення політики безпеки та впровадження засобів моніторингу та контролю доступу.

Результати дослідження можуть бути використані для підвищення рівня інформаційної безпеки в системах електронної торгівлі та зниження ризиків, пов’язаних з обробкою конфіденційних даних.

Ключові слова: інформаційна безпека, конфіденційність, електронна торгівля, телекомунікаційна мережа, криптографія, шифрування, автентифікація.

ABSTRACT

The bachelor's thesis examines the issue of ensuring the confidentiality of information in the telecommunications network of an electronic trading platform. The relevance of the study is due to the growth of e-commerce and the need to protect personal and commercial data from unauthorized access, leakage or substitution.

The paper analyzes modern threats to information security in the field of e-commerce, examines the architecture of telecommunications networks of such platforms and identifies vulnerabilities through which confidentiality can be violated. The theoretical principles of cryptographic protection, encryption protocols, authentication mechanisms and secure data exchange are considered. Special attention is paid to the implementation of information security standards.

In the practical part of the work, the basic architecture of a secure telecommunications network for an electronic trading platform is simulated, taking into account confidentiality requirements. Recommendations are also proposed for strengthening security policies and implementing monitoring and access control tools.

The results of the study can be used to increase the level of information security in electronic commerce systems and reduce the risks associated with the processing of confidential data.

Keywords: information security, confidentiality, electronic commerce, telecommunications network, cryptography, encryption, authentication.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій
_____О.В. Шефер
«01» квітня 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ
Гонтару Миколі Юрійовичу

1. Тема проекту (роботи) «Забезпечення конфіденційності інформації в телекомунікаційній мережі електронної торгівельної площадки»
керівник проекту (роботи) Косенко Віктор Васильович, д.т.н., професор
затверджена наказом вищого навчального закладу від 03. 03. 2025 року
№ 306/1– ф,а .

2. Строк подання студентом проєкту (роботи) 10.06.2025 р.

3. Вихідні дані до проекту (роботи) Вихідними даними є матеріали зібрані під час проходження практики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз критеріїв оцінки якості телекомунікаційних мереж. Особливості використання телекомунікаційних мереж у електронній комерції. Аналіз автоматизованих системи електронних торгів. Забезпечення надійності функціонування телекомунікаційних систем електронних торгів. Аналіз методів та засобів забезпечення апаратурної надійності та інформаційної безпеки. Дослідження методів та моделей оцінки надійності корпоративних телекомунікаційних мереж. Аналіз сучасних систем оцінки надійності та захисту інформації. Побудова графової моделі оцінки апаратурної надійності телекомунікаційної мережі. Засоби захисту інформації електронного торгового майданчика телекомунікаційних мереж. Застосування принципів управління криптографічними ключами. Розроблення процедури прийняття рішення щодо участі користувача в електронних торгах. Результати експериментального дослідження розробленого математичного апарату. Висновки по роботі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
Мета, обєкт та предмет роботи. Класифікація систем за рівнем надійності. Результати аналізу сучасних програмно-технічних методів підвищення безпеки

інформації телекомунікаційних мереж електронної комерції. Алгоритм апаратно-програмного захисту комерційної інформації. Графова модель розрахунку апаратурної надійності корпоративної телекомунікаційної мережі. Структурна схема підграфа графа. Можливість безвідмовної роботи мережі до та після резервування пристроїв. Імовірність безвідмовної роботи елемента мережі. Значення параметрів QoS під час передачі трафік. Середній показник безвідмовної передачі даних. Аналіз результатів підвищення ефективності функціонування мережі. Висновки.

6. Дата видачі завдання 01.04.2025 р.

Пор. №	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів роботи			Примітка (плакати)
1	Аналіз критеріїв оцінки якості телекомунікаційних мереж. Особливості використання телекомунікаційних мереж у електронній комерції.	22.04.25	I	20%	Пл. 1,2
2	Аналіз методів та засобів забезпечення апаратурної надійності та інформаційної безпеки. Дослідження методів та моделей оцінки надійності корпоративних телекомунікаційних мереж.	08.05.25		40%	Пл. 3,4
3	Аналіз сучасних систем оцінки надійності та захисту інформації. Побудова графової моделі оцінки апаратурної надійності телекомунікаційної мережі.	22.05.25	II	60%	Пл. 5,6
4	Засоби захисту інформації електронного торгового майданчика телекомунікаційних мереж. Результати експериментального дослідження розробленого математичного апарату.	30.05.25		80 %	Пл. 7-9
5	Робота над висновками та оформлення кваліфікаційної роботи.	10.06.25	III	100%	Пл. 10-11

Студент _____ Гонтар М.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи_____ Косенко В. В.
(підпис) (прізвище та ініціали)

ЗМІСТ

Вступ

У XXI столітті цифрова трансформація охопила практично всі сфери людської діяльності, зокрема й комерцію. Електронна торгівля, яка ще декілька десятиліть тому була лише перспективним напрямом, сьогодні стала повноцінним і надзвичайно потужним сегментом світової економіки. Онлайн-платформи для купівлі та продажу товарів і послуг забезпечують зручність, доступність і швидкість здійснення комерційних операцій, як для підприємців, так і для споживачів. У центрі цього процесу знаходяться електронні торгівельні площадки (ЕТП), які використовують телекомунікаційні мережі для взаємодії з користувачами, банками, постачальниками та іншими сервісами.

Однак активне використання інформаційних технологій супроводжується і значними викликами, головним серед яких є питання забезпечення інформаційної безпеки. З кожним роком зростає кількість кіберінцидентів, пов’язаних із витоком конфіденційної інформації, зломами облікових записів, підробками транзакцій і викраденням персональних та фінансових даних. Така ситуація зумовлює необхідність розробки комплексних заходів захисту інформації, зокрема конфіденційності даних, які передаються через телекомунікаційні мережі.

Конфіденційність є одним із ключових компонентів інформаційної безпеки. У контексті електронної торгівлі вона передбачає захист персональної, платіжної та комерційної інформації від несанкціонованого доступу, перехоплення або розголошення під час передавання даних між користувачами та серверами платформи. Враховуючи динаміку розвитку кібератак, все більше уваги приділяється впровадженню сучасних криптографічних засобів, протоколів безпечного обміну даними, систем автентифікації та моніторингу.

Особливу увагу в цьому аспекті заслуговує аналіз вразливостей телекомунікаційної інфраструктури, яку використовують ЕТП. Наприклад, використання застарілих протоколів передачі даних, недостатньо захищених API-інтерфейсів або ненадійних хмарних сервісів може призвести до

компрометації системи загалом. Тому на сучасному етапі важливо не лише впроваджувати окремі засоби захисту, а й будувати цілісні архітектурні рішення, орієнтовані на забезпечення конфіденційності «від кінця до кінця».

Метою даної бакалаврської роботи є дослідження принципів, методів і засобів забезпечення конфіденційності інформації в телекомунікаційній мережі електронної торгівельної площадки. Для досягнення поставленої мети передбачається виконання таких завдань:

- проаналізувати сучасні загрози, пов’язані з порушенням конфіденційності в електронній торгівлі;
- дослідити основні методи та протоколи захисту інформації в телекомунікаційних мережах;
- вивчити архітектуру типової ЕТП з позиції інформаційної безпеки;
- запропонувати практичні рекомендації або модель підвищення рівня конфіденційності інформації в рамках конкретної телекомунікаційної системи.

Об’єктом дослідження в цій роботі є процес побудови телекомунікаційної мережі електронної торгівельної площадки, яка функціонує в умовах сучасного інформаційного середовища. Предметом дослідження є методи забезпечення конфіденційності інформації, що передається в межах цієї мережі.

Актуальність теми зумовлена постійним зростанням обсягів електронної комерції, збільшенням кількості кіберзагроз, що впливають на довіру користувачів до онлайн-сервісів, а також потребою у відповідності до міжнародних та національних стандартів з інформаційної безпеки (таких як ISO/IEC 27001, GDPR, ЗУ «Про захист персональних даних» тощо).

Таким чином, дана робота має практичне значення для фахівців з кібербезпеки, адміністраторів інформаційних систем, а також для розробників ЕТП, які прагнуть забезпечити захищене функціонування своїх сервісів у цифровому середовищі.

У сучасному світі стрімкого розвитку інформаційних технологій електронна торгівля стала невід’ємною складовою економіки та повсякденного

життя. Зростання кількості електронних торгівельних площадок (ЕТП) і широке використання телекомунікаційних мереж для передачі чутливої інформації — особистих даних, платіжних реквізитів, комерційної та конфіденційної інформації — зумовлюють підвищені вимоги до безпеки інформаційних систем. Одним із найважливіших аспектів захисту є забезпечення конфіденційності переданої інформації.

Конфіденційність інформації в телекомунікаційних мережах ЕТП є критично важливою для довіри користувачів, захисту бізнес-інтересів та відповідності чинному законодавству у сфері інформаційної безпеки. Порушення конфіденційності може призвести до витоку персональних даних, фінансових втрат, репутаційних ризиків та юридичної відповідальності. Тому розробка та впровадження ефективних засобів забезпечення конфіденційності інформації є актуальним завданням у сфері кібербезпеки.

1. АНАЛІТИЧНА ЧАСТИНА

1.1. Надійність – як один із критеріїв оцінки якості телекомунікаційних мереж

До телекомунікаційних мереж відносяться [1]: комп'ютерні та телефонні мережі, радіомережі, телевізійні мережі. Аналіз теоретичних та експериментальних досліджень [2] дозволяє виділити основні критерії оцінки якості (критерії ефективності роботи) телекомунікаційних мереж – це продуктивність, надійність, безпека, розширюваність, масштабованість, прозорість, підтримка різних видів трафіку, керованість, сумісність. Іноді у поняття "якість обслуговування" мережі включають лише дві важливі характеристики - це продуктивність та надійність. На рис. 1.1 представлений приклад телекомунікаційної мережі

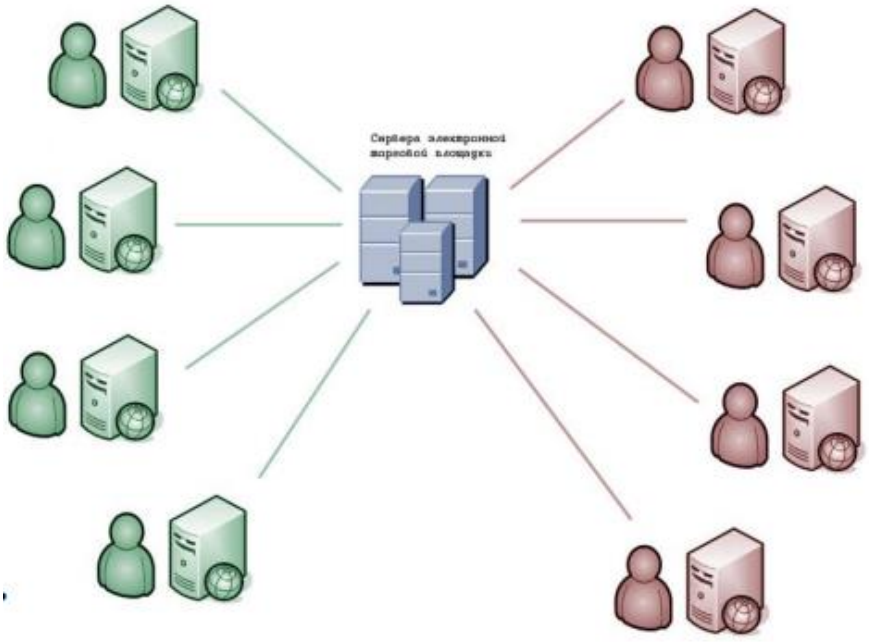


Рисунок 1.1 – Телекомунікаційна мережа

При аналізі надійності та безпеки мереж слід виділяти такі показники як: ймовірність відмови, середній час напрацювання на відмову, інтенсивність відмов, коефіцієнт готовності, збереження даних та захист їх від спотворень,

узгодженість (несуперечність) даних, можливість доставки пакета вузлу призначення без спотворень, можливість втрати пакета, ймовірність спотворення окремого біта даних, що передаються, ставлення втрачених пакетів до доставлених, безпека або здатність системи захистити дані від несанкціонованого доступу, відмовостійкість.

Для оцінки надійності мереж необхідно виділити окремі аспекти – апаратурну (елементарну) та функціональну (структурну) надійність, відповідні методи їх оцінки, та розглянути методичні питання надійності з урахуванням QoS.

Елементарна надійність – це властивість, властиве елементу мережі зв'язку, зберігати працездатність з якістю не гірше заданого на певному інтервалі часу.

Структурна надійність – властивість мережі забезпечувати зв'язність користувачів з якістю не гірша заданого на певному інтервалі часу.

Для оцінки надійності застосовуються такі основні характеристики: готовність, безпека та відмовостійкість. Надійність телекомунікаційних мереж багато в чому визначається надійністю сегментів фізичного середовища передачі для каналів зв'язку та надійністю мережевого обладнання. За допомогою одного показника надійність такого складного та багатогранного об'єкта, як телекомунікаційні мережі, повністю охарактеризувати неможливо, тому для повнішої характеристики необхідно визначення цілого набору параметрів надійності [3]. Як відомо, недостатньо визначити надійність на якісному рівні, необхідно оцінювати надійність кількісно та порівнювати різні об'єкти з їхньої надійності. З цією метою вводяться показники та критерії надійності Показник надійності – кількісна характеристика однієї чи кількох одиничних властивостей, визначальних надійність об'єкта. Розрізняють поодинокі та комплексні показники надійності [4]. Комплексні показники характеризують декілька одиничних властивостей.

Для характеристики якості функціонування мереж та пристроїв теорії надійності розроблено набір інтервальних, інтегральних та точкових показників надійності, і навіть методи їх розрахунку.

Кожен об'єкт характеризується вектором одиничних та комплексних показників. Оскільки при порівнянні варіантів один із них може бути краще альтернативного варіанта за одним показником і гірше за іншим, то серед показників обирають той, який у конкретних умовах найкращим чином відображає властивість надійності, і саме його вибирають як критерію надійності.

Існують такі критерії оцінки надійності пристроїв телекомунікаційних мереж: ремонтопридатність, гарантійний термін експлуатації, коефіцієнт готовності, коефіцієнт простою тощо. Вибір показника диктується або прийнятим у галузі стандартом, або безпосередньо споживачем.

У таблиці 1.1 представлено класифікацію систем за рівнем надійності

Таблиця 1.1

Класифікація систем за рівнем надійності

Коефіцієнт готовності	Типи систем	
0,99	Звичайна	Conventional
0,999	Висока надійність	Highavailability
0,9999	Відмовостійка	Faultresilient
0,99999	Безвідмовна	Faulttolerant

1.2 Особливості використання телекомунікаційних мереж у електронній комерції

Для телекомунікаційних мереж корпорацій, що займаються електронною комерцією (корпоративних телекомунікаційних мереж) характерні особливості. Організаційна структура такої корпорації така, що окремі функції розподіляються горизонтально між ним підрозділами, а ієрархічні взаємини

ослаблені. У сучасних західних дослідженнях, присвячених інформаційному суспільству, мережеві корпорації називаються також «організація з модульною структурою» чи «динамічна мережева організація» [5].

Погодження дій підрозділів у корпораціях даного типу здійснюється головним офісом через Інтернет, але при цьому відмінними особливостями є процеси, що самоорганізуються і децентралізоване керування; кількість внутрішніх ієрархічних рівнів у мережевих корпораціях невелика. Процес створення мережі у цьому випадку істотно спрощується, оскільки відпадає потреба у розробці інтеграційного проекту, оскільки окремі підрозділи можуть створювати власні підсистеми, використовуючи свої локальні мережі та сервери, не пов'язуючи їх з іншими підрозділами, а потім можуть підключатися до єдиної системі корпорації. Особливості побудови таких мереж [6]:

- вдосконалення методів доступу до Інтернету;

- перенесення інтернет-сервісів на мобільні термінали (у тому числі на стільникові телефони), багато зарубіжних банків активно впроваджують мобільні торгові платформи, оптимізовані для iPad, iPhone та інших пристроїв, перспективний розвиток аналогічних мобільних банківських платформ;

- створення та розповсюдження зручніших інтернет-стандартів;

- використовуються високошвидкісні технології передачі інформації та різні комбінації каналів зв'язку;

- передбачається інтеграція мережі з іншими телекомунікаційними системами, а також створення резервних каналів зв'язку та дублювання всіх основних компонентів систем, що забезпечує високу продуктивність, надійність та відмовостійкість мережі, а також здатність до подальшого розвитку;

- об'єднання десятків тисяч комп'ютерів, розміщених у різних країнах та містах;

- підвищені вимоги до надійності передачі та захисту інформації у таких мережах.

Серед вимог до проведення комерційних операцій слід виділити: аутентифікація, конфіденційність, цілісність, авторизація, гарантії та збереження таємниці. Перші 4 вимоги можна забезпечити технічними засобами, виконання останніх 2-х залежить від технічних коштів та від відповідальності окремих осіб та організацій, а також від дотримання законів.

1.3 Аналіз автоматизованих системи електронних торгів

Апаратно-програмною основою електронної комерції є телекомунікаційні системи та мережі, глобальна мережа Інтернет, комерційні та корпоративні мережі, інформаційні та телекомунікаційні технології [7].

Системи електронних торгів являють собою програмні та технологічні рішення, призначені для автоматизації процедур підготовки та проведення електронних аукціонів та інших видів конкурентних закупівель. Найпоширенішою, найпростішою та зручнішою формою застосування систем електронної торгівлі є електронні торгові майданчики (ЕТП). Велике значення у розвитку електронних торгових майданчиків має формування законодавчої державної бази закупівель. Системи електронних торгів поступово переходитимуть із рівня ЕТП на рівень повномасштабних систем управління торговельно-закупівельною.

ЕТП – це комплекс інформаційних та технічних засобів, що забезпечує взаємодія замовника з постачальником через телекомунікаційні канали всіх етапах під час укладання угоди [8].

Функції ЕТП включають: інформаційну функцію, що забезпечує доступ до переліку організацій на ЕТП та отримати інформацію щодо цікавить організації; функцію маркетингу; рекламну функцію; торгову функцію; аналітичну функцію, що дозволяє проводити порівняльний аналіз різних показників діяльності організацій; функцію захисту інформації, що забезпечує безпечний електронний документообіг, збудований з використанням сертифікованих коштів криптографічного захисту інформації.

Переваги роботи на ЕТП для замовника та для компанії полягають у наступному:

велика економія робочого дня;

економія грошей для організації та проведення закупівель;

прозорість процесу закупівель;

чесна конкуренція; участь у торгах можлива «з будь-якої точки світу, не виходячи з офісу»; доступність для представників будь-якого бізнесу - ціна та

умови лоту нічим не обмежені.

Для роботи на електронному торговому майданчику Організація – учасник розміщення замовлення повинен мати кошти електронного підпису (ЕП), видані посвідчувальним центром, що пройшов авторизацію та уклавши угоду з оператором електронного майданчика, відібраним для проведення аукціонів під час розміщення державного замовлення [8].

Існують такі ЕТП призначені:

1) для розміщення державного замовлення;

2) для комерційних замовників – спеціалізовані та багатопрофільні.

1.4 Забезпечення надійності функціонування телекомунікаційних систем електронних торгів

Для побудови надійних телекомунікаційних мереж (ТКС) та систем можна використовувати різноманітні види забезпечення:

a) економічне;
b) тимчасове;
c) організаційне;
d) структурне;
e) технологічне;
f) експлуатаційне;
g) соціальне;
h) алгоритмічне.

Для забезпечення надійності технічних засобів найчастіше виробляється:

● резервування (дублювання) технічних засобів (комп'ютерів та їх компонентів, сегментів мереж тощо);

● використання стандартних протоколів роботи пристроїв ТКС;

● застосування спеціалізованих технічних засобів захисту інформації.

Засобами захисту інформації телекомунікаційних систем стем, у тому серед систем електронних торгів є технічні, криптографічні, програмні та інші засоби, призначені для захисту інформації, кошти, в якому воно реалізовано, а також засіб контролю ефективності захисту інформації Засоби захисту інформації діляться на: фізичні, апаратні, програмні, криптографічні, та комбіновані.

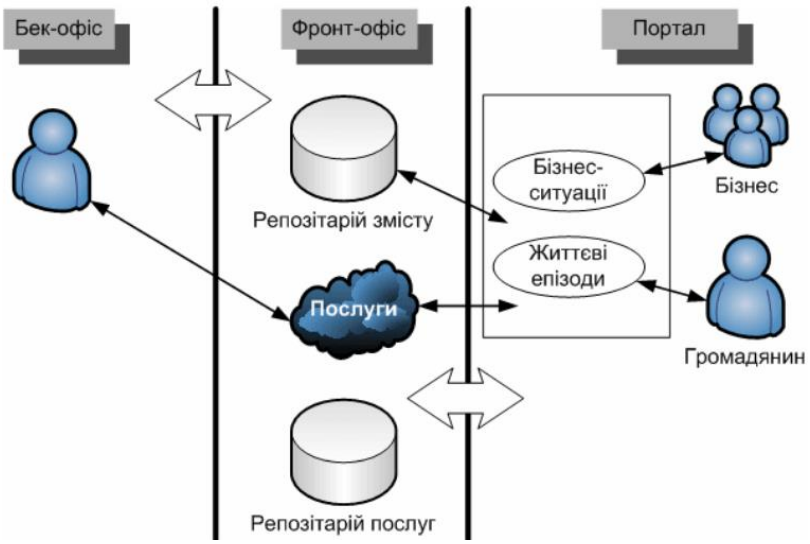


Рисунок 1.2 – Архітектура електронних регламентів

1.5 Аналіз методів та засобів забезпечення апаратурної надійності та інформаційної безпеки в телекомунікаційних мережах електронної комерції

Підвищення надійності полягає у запобіганні несправностям, відмов та збоїв. Основним способом підвищення готовності є надмірність, на основі якої реалізуються різні варіанти відмовостійких архітектур.

Для комерційних підприємств безпека є економічною категорією. В даний час розробляються комплексні підходи до інформаційну безпеку підприємства, особливо під час агресії рф проти України. Створюються концепції (політики) безпеки підприємства. У мережі вразливим є мережеві протоколи та пристрої, що утворюють мережу, бази даних та програми. Методи та засоби забезпечення надійності та інформаційної безпеки у телекомунікаційних мережах поділяються на організаційні та програмно-технічні.

1. Організаційні методи: управління персоналом, фізичний захист, підтримка працездатності, планування відновлювальних робіт.

2. Програмнотехнічні методи.

Серед сучасних програмно-технічних методів підвищення безпеки інформації телекомунікаційних мереж електронної комерції можна виділити:

a. правильна конфігурація вузлів мережі;

b. раціональне застосування методів резервування;

c. при проектуванні мережі потрібно використовувати елементи, що забезпечують безпеку; використання відмовостійких комп'ютерів з відмовостійкими апаратними компонентами;

d. кластеризація комп'ютерів (забезпечують коефіцієнт готовності до 0,999-high availability);

e. дуплексування та дзеркальне відображення дисків (Diskmirroring); автоматичне підключення (auto-reconnection);

f. дублювання файлової системи; відстеження транзакцій (transactiontracking);

g. використання міжмережевих екранів та брандмауерів;

h. ідентифікація та автентифікація;

i. розмежування доступу;

j. протоколювання та аудит;

k. криптографічне перетворення даних.

Рисунок 1.3 – Архітектура порталу надання електронних послуг

1.6 Висновки за розділом

1. В ході роботи над першим розділом кваліфікаційної роботи бакалавра, встановлено, що електронна комерція поєднує безліч комунікаційних технологій. Найпоширенішою, найпростішою та зручнішою формою застосуваннясистем електронної торгівлі є електронні торгові майданчики (ЕТП).

2. Розглянуто функції, можливості та переваги роботи на ЕТП для замовника та для компанії, представлені приклади комерційних торгівельних майданчиків.

3. Проаналізовано існуючі способи забезпечення надійності функціонування телекомунікаційних систем електронних торгів. Показано, що системи електронних торгів переходять з рівня електронних торгових майданчиків на рівень повномасштабних систем управління торгово-закупівельною детальністю з використанням телекомунікаційних мереж, отже, основою електронної комерції є телекомунікаційні мережі.

4. Проаналізовано особливості використання телекомунікаційних мереж в електронній комерції. Наведено основні критерії ефективності роботи мереж

Показано, що до таких мереж пред'являються підвищені вимоги до надійності передачі та захисту інформації.

5. Проведено аналіз методів та засобів забезпечення інформаційної безпеки у телекомунікаційних мережах електронної комерції. Досліджено методи та моделі оцінки надійності таких мереж. Визначено вимоги до моделей – це універсальність, точність, адекватність, економічність, економічність, наочність, обчислюваність, алгоритмізованість. Проведене дослідження показало, що методи та моделі мають свої переваги та недоліки, що викликає певні обмеження на їхнє застосування при проектуванні спеціалізованих корпоративних телекомунікаційних мереж. Отже, розробка нових моделей та алгоритмів розрахунку апаратурної надійності пристроїв таких мереж, з урахуванням наявних напрацювань у цій галузі, є актуальним науковим завданням.

6. Проаналізовано та досліджено сучасні системи оцінки надійності та захисту інформації, як вітчизняні, так і зарубіжні. Як показало дослідження, більшість таких систем є складними та дорогими.

2. ДОСЛІДНИЦЬКА ЧАСТИНА

2.1 Дослідження методів та моделей оцінки надійності корпоративних телекомунікаційних мереж

Проблема мережевої надійності досліджується досить давно. Точного рішення навіть для мереж обмеженого розміру це завдання не має, але можна зробити оцінку надійності зверху та знизу, але навіть це вимагає достатньо складних розрахунків. Тому через складність прямих обчислень багато дослідники обмежуються лише оцінкою можливих меж надійності [9, 10].

Оскільки мережі є дуже зв'язковими структурами, то їх розрахунок надійності суворо аналітичними методами утруднений [11].

Єдиним чисельним методом розрахунку надійності сильно пов'язаних мереж є метод повного перебору, який, навіть із залученням швидкодіючих ЕОМ, не дозволяє аналізувати мережі, що містять більше 50 випадкових компонентів, тому часто застосовують метод часткового перебору [12].

Іноді на практиці надійність та розподіл надійності визначаються емпірично [13].

Серед методів ймовірнісного аналізу мереж використовуються алгоритмічні та логіко-імовірнісні методи [14].

Через відсутність прийнятної моделі механізму втрат у мережі та властивої складності розрахунку використовуються час-залежні моделі з дискретною ймовірністю.

Можна виділити такі алгоритми точного обчислення заходів надійності: точні алгоритми з експоненційним часом для загальних мереж та точні алгоритми з поліноміальним часом обмеженого класу мереж.

Методи структурної надійності мереж. При дослідженні структурної надійності мереж застосовуються такі методи [14]:

Точний метод аналізу структурної надійності; наближені методи - статистичної оцінки, розкладання, двосторонньої оцінки, метод перерізів або сукупності шляхів.

Моделі безвідмовності елемента. Експонентне (Показовий) розподіл. Розподіл Вейбулла.

Простим і легко реалізованим методом підвищення апаратури надійності корпоративних телекомунікаційних мереж є резервування. Резервування - це підвищення надійності системи з допомогою застосування додаткових засобів. Існують такі види резервування: структурне, функціональне, тимчасове, інформаційне.

Існують і інші методи та моделі, що використовуються при вирішенні задач забезпечення апаратурної надійності мереж. Всі ці методи та моделі мають свої переваг а й недоліки, що викликає певні обмеження на їхнє застосування при проектуванні спеціалізованих корпоративних телекомунікаційних мереж. Отже, розробка нових моделей та алгоритмів розрахунку апаратурної надійності пристроїв таких мереж, з урахуванням наявних напрацювань у цій галузі, є актуальним науковим завданням.

До моделей мереж висуваються такі основні вимоги – це універсальність, точність, адекватність та економічність.

При розрахунку апаратурної надійності корпоративних телекомунікаційних мереж слід враховувати і низку вимог до моделей таких мереж та їх елементів: економічність, наочність; обчислюваністю, тобто можливістю дослідження якісних та кількісних закономірностей функціонування мережі.

2.2 Аналіз сучасних систем оцінки надійності та захисту інформації

Сучасною проблемою оцінки надійності систем, мереж та засобів обчислювальної техніки займалася значна кількість науково-технологічних

центрів та організацій, результатом їх діяльності стало створення програмно-інструментальних комплексів.

Серед сучасних програмних засобів, призначені для аналізу та розрахунку надійності, готовності та ремонтопридатності можна виділити такі системи:

AnyGraph, CRISS, AggreGateNetworkManager, BlockSim, ITEMSoftware, ReliabilityWorkbench, Windchill.

Наприклад, AnyGraph створена для спрощення розробки системних моделей, що використовуються при розрахунку надійності складних технічних систем та їх аналізі. Теоретичною основою програмного забезпечення (ПЗ) є логіко-імовірнісні методи (ЛВМ) моделювання.

Концепцією ПЗ є представлення моделі як набору взаємодіючих між собою вузлів (технічних елементів) та логічних зв'язків між ними.

AnyGraph модель має високу наочність.

Система AggreGateNetworkManager здійснює моніторинг елементів мережі. Перевіряється показник доступності, що характеризує стан контрольованого елемента мережі за допомогою стандартних процедур, таких як пінг мережевого пристрою або з'єднання з сервісом через вказаний порт. Моніторинг працездатності мережного елемента полягає в комплексній перевірці, що гарантує, що керований елемент не "працює належним чином".

На ринку захисту інформації пропонується багато окремих інженерно-технічних, програмно-апаратних, криптографічних засобів захисту інформації [15].

Програмний продукт дозволяє запобігти витоку конфіденційних даних з інформаційної системи організації. Результат:

– виявлення фактів порушення конфіденційності;

– інформації у централізованому сховищі даних;

– статистичної звітності з можливістю угруповання з різних параметрам, виявлення випадків порушення встановлених правил роботи у мережі організації;

– виявлення випадків нецільового використання, фактів;

– зміни користувачами, встановлення або видалення ними програмного забезпечення

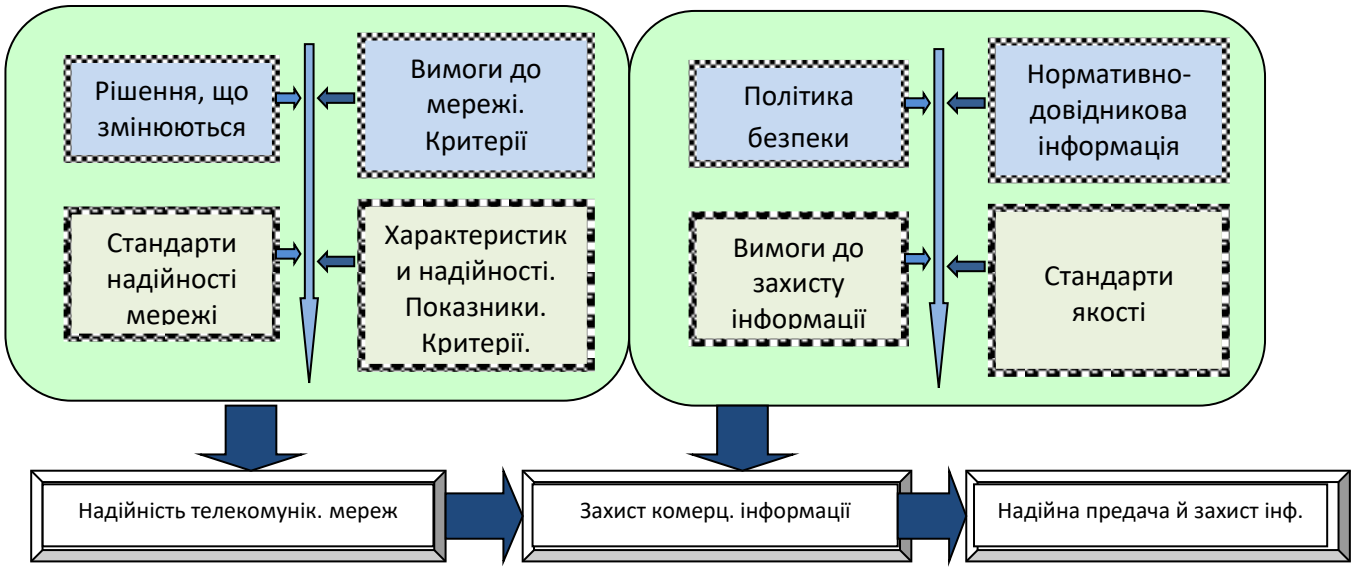


Рисунок 2.1 – Алгоритм апаратно-програмного захисту комерційної інформації

2.3 Графова модель оцінки апаратурної надійності телекомунікаційної мережі

2.3.1 Розроблення графової моделі

Математичну модель для розрахунку апаратурної (фізичної) надійності корпоративної телекомунікаційної мережі електронної комерції можна розглянути, як орієнтований граф. Граф G=(E,L) (рисунок 2.2), де вершини графа це фізичні елементи мережі – вузли та канали зв'язку (обладнання), а дуги – це ієрархічні зв'язки цих елементів.

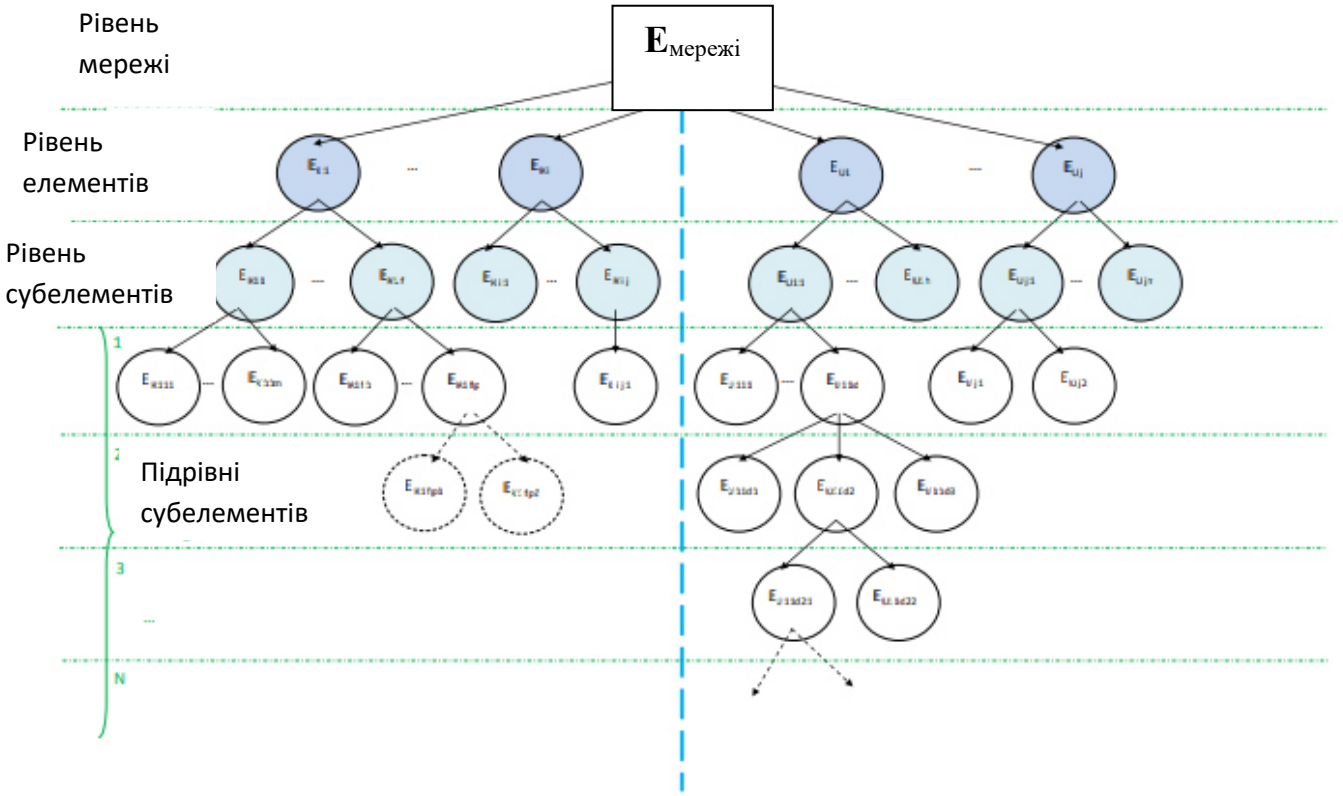


Рисунок 2.2 - Графова модель розрахунку апаратурної надійності корпоративної телекомунікаційної мережі

Графова модель має три основні рівні:

1 – рівень мережі (всі пристрої мережі). Апаратурна надійність мережі, як і будь-якої системи, визначається надійністю складових її елементів.

2 – рівень елементів мережі (вузли – пристрої та фізичні канали зв'язку). Тут елементом є сервер, робоча станція, термінал, канал зв'язку тощо, наприклад, це робоча стація.

3 – рівень субелементів. Так, при розгляді функціонування робочої станції можна виділити процесор, пристрої вводу/виводу і т.д.

Рівень субелементів містить безліч підрівнів 1, 2, …, N, на яких детальніше аналізується апаратурна надійність складових елементів. Для робочої станції це може бути, наприклад, пристрої введення/виводу. Далі на наступному підрівні відбувається подальша деталізація елемента та його складових частин. Як показано в розділі 1, ступінь деталізації елемента мережі

в кожному конкретному випадку визначається метою дослідження та характером обраного показника надійність.

Наприклад: безліч елементів мережі ECETI ={EK1,…, EKi; EU1,…, EUj}, т.е. {EK1,…, EKi } ⊆ ECETI и{EU1,…, EUj} ⊆ ECETI В свою чергу EK1 = {EK11,…,EK1f},…, EKi= {EKi,…,EKi}, причому EK11 = {EK111,…,EK11m}, …, EK1f={ EK1f1,…, EK1fp},…, EKi={EKi1}, і т.д. EU1={EU11,…, EU1h},…, EUj={EUj1,…, EUjn}, причому EU11={EU111,…, EU11d}, …, далі EU11d={EU11d1,EU11d2, EU11d3},… На наступному підрівні EU11d2 = {EU11d21, EU11d22} і так далі.

Таким чином, розрахунок апаратурної надійності корпоративної телекомунікаційної мережі проводиться за допомогою процедури декомпозиції.

2.3.2 Алгоритм аналізу графової моделі

Алгоритм аналізу графової моделі телекомунікаційної мережі включає наступні основні кроки.

1 крок. Введення даних (види обладнання, кількість пристроїв, види пристроїв (з урахуванням ступеня деталізації), Т - аналізований період;

завдання показника надійності для елементів мережі, де РЕ – значення ймовірності;)

2 крок. Аналіз даних, що вводяться.

3 крок. Формування графової моделі мережі G=(E,L) виходячи з даних, що вводяться.

3.1. Визначення безлічі вершин та дуг графа G=(E,L).

3.2. Вибір рівнів та підрівнів графової моделі мережі:

1 – рівень мережі.

2 – рівень елементів мережі.

3 – рівень субелементів: підрівні 1, 2, …, N.

3.3. Формування безлічі вершин ЕСЕТИ графа G = (E, L), причому, Еєk ∪ Еєu ∪ Есєk ∪ Есєu ∪ Епсєk ∪ Епсєu=Емереж. - у початковому стані множини

вершин Еєk=∅, Еєu=∅, Есєk=∅, Есєu=∅, Епсєk=∅, Епсєu=∅ - вибір невідміченої вершини;

- на 1-му рівні: вершина Eki відзначається і включається до множини вершин Еє K, вершина EUj відзначається і включається до множини Eeu;

- на 2-му рівні: вершина EKif відзначається і включається до безлічі вершин Ecek, вершина EUjm відзначається і включається до безлічі Eceu;

- на 3-му рівні для кожного з підрівнів: вершини Ekifn та Eujmn відзначаються та включаються до відповідних множин Е псе K та Eупсє. - Формування завершується після перегляду всіх необхідних вершин графа G.

3.4. Визначення вершини входу Еевх та вершини виходу Еевых графа G=(E,L).

3.5. Побудова шляху між Евх та вершини виходу Евих графа G=(E,L).

4 крок. Виділення підграфів Gk (Ek, Lk) і Gu (Eu, Lu) графа G = (E, L), де k = 1,2, ..., і u = 1,2, ... На рис.2.3 представлений приклад підграф графа G = (E, L).

4.1. Визначення безлічі необхідних елементів мережі, на підставі якого здійснюється виділення підграфа Gk (Ek, Lk) і Gu (Eu, Lu).

4.2. Формування підмножин вершин Eeki та E e Uj – елементів, Eseki, Ece Uj – субелементів, Епсeki, Епсeuj – підрівень субелементів для підграфів Gk ε (Ek, Lk) та Gu ε (Eu, Lu).

4.3. Визначення вершин входу Еквх ε Еквих і Екних ε Е для підграфу Gk ε (Ek, Lk).

4.4. Визначення вершин входу Euвх ε Евих та Euвих ε Е для підграфа Gu ε (Eu, Lu).

4.5. Побудова шляху між вершинами Евх та Екних, а також між вершинами Еввх та Euвих.

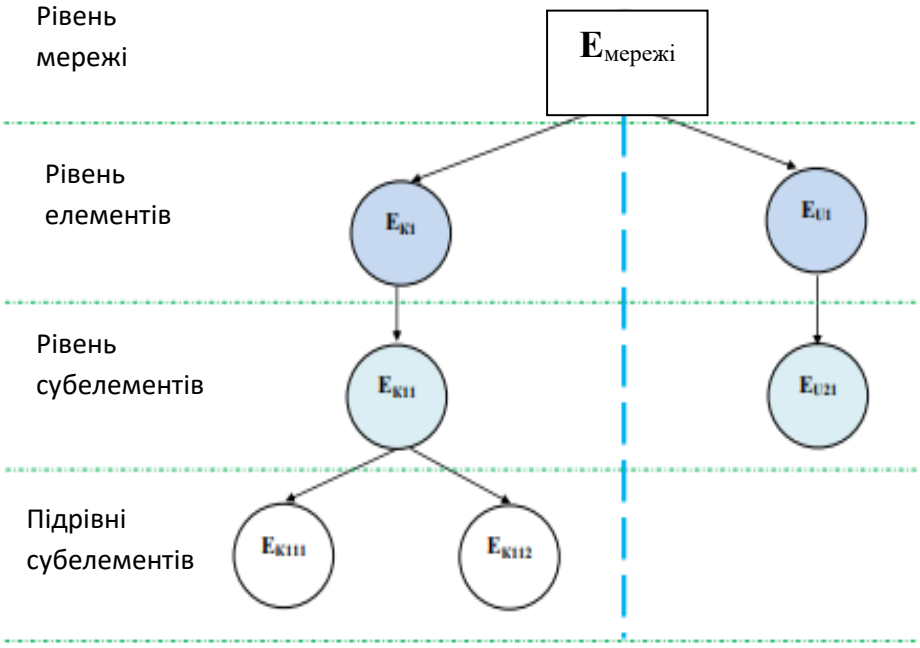


Рисунок 2.3 – Підграф графа G = (E, L)

5 крок. Аналіз підграфів Gk = (Ek, Lk) та Gu = (Eu, Lu).

5.1. Для графа G = (E, L) кожен з виділених підграф складається з K і U елементів мережі, кожен з елементів виконує функції Fi = {f1, f2, ..., fn} і може знаходитися в одному зі станів: -

- s1 – повної працездатності (з можливістю виконання всіх функцій {f1, f2, ..., fn}),

- s2 – функцій, що реалізуються),

- s3 – повної відмови.

5.2. З метою скорочення обсягу пам'яті доцільно подати підграфи таблицями, де номер рядка таблиці – це номер вершини, а вміст рядка визначає зв'язок цієї вершини з іншими вершинами.

5.3. Розрахунок ймовірності безвідмовної роботи пристроїв мережі:

- розрахунок ймовірності безвідмовної роботи пристроїв мережі за формулами (2.1)-(2.5).

Імовірність безвідмовної роботи будь-якого елемента телекомунікаційної мережі можна записати як

$$P_T(x) = P_1(y_1)P_1(y_2 \mid y_1)...P_m(y_m,...,y_{m-1}), \quad (2.1)$$

де $P_1(y_1)$- безумовна ймовірність виконання j-го умови працездатності; x – вхідні параметри; y – вихідні параметри елемента мережі;

$P_T(y_k \mid y_1,...,y_{k-1})$ – умовна ймовірність виконання до і-ої умови працездатності.

Імовірність $P_T(X)$ також можна представити як математичне очікування деякого функціоналу для вихідних параметрів Y(X) на заданому інтервалі часу функціонування елемента T з урахуванням Y(x(t)) - номінальних значень його вихідних параметрів.

Позначимо через Y_{jmin} мінімальне значення j-го вихідного параметра елемента на інтервалі часу [0, T]:

$$Y_{jmin} = \min_{t\in[0,T]} Y_j(x(t)), \quad j = 1,...,n \quad (2.2)$$

Величина Y_{jmin} є випадковою із щільністю розподілу, яка в загальному випадку визначається номінальними значеннями параметрів елементів, законами розподілу цих параметрів у часі, видом функціональної залежності $Y_j(x(t))$ та величиною інтервалу часу.

Сукупність номінальних значень параметрів елементів мережі представляє припустиме рішення, якщо відповідний вектор належить до області допустимої варіації його параметрів. Внаслідок дії різних факторів, що дестабілізують (знос, температура, вологість і т.д.) реальні значення параметрів мережевих елементів відрізняються від номінальних (розрахункових).

Під час експлуатації ці відхилення визначаються умовами роботи. Оскільки значення параметрів елементів мережі є випадковими, то умови їхньої працездатності можуть виконуватися не абсолютно, а з тією чи іншою ймовірністю.

Тоді можливість виконання j-го умови працездатності елемента мережі можна записати у вигляді:

$$P_j(y_j(x)) = \int_{a_m}^{} \Phi_j(y)dy, \tag{2.3}$$

де $\Phi_j(y)$ - щільність розподілу величини Y_j;

(a, am, ..., 1) область працездатності.

Імовірність безвідмовної роботи і-го елемента мережі

$$P_{Ti} = \prod_{j=1}^{H} P_j(y_j(x)) \tag{2.4}$$

Для локальних критеріїв апаратурної надійності телекомунікаційної мережі, серед яких існують суперечливі та незведені один до одного, умови працездатності елементів визначаються за допомогою нерівності:

$$y_j(x+\Delta x) \geq y_j(x), \qquad j = 1,..., m\,. \tag{2.5}$$

Випадкові величини Y_j можуть бути значеннями вихідних параметрів елементів в момент часу t=0. Введення випадкових величин щодо параметричної надійності (це ймовірність безвідмовної роботи елемента по поступовим відмовам на заданому інтервалі часу [0,T]) дає можливість перейти від розгляду випадкових функцій (процесів) до розгляду випадкових величинY_j і істотно спростити проблему оптимізації параметричної надійності та її рішення, за рахунок можливості уніфікувати.

- Розрахунок надійності пристроїв мережі, критичних для затримки результатів обчислень.

- Оцінка відмови пристрою у вільному стані.

Для кожної таблиці будується матриця $\|\varphi_{ij}\|_{n*m}$, елемент якої – це елемент облпднання: у вихідному стані все $\varphi_{ij} = 1$, якщо j-й здатний виконати функцію f_i, то $\varphi_{ij} = 1$, інакше $\varphi_{ij} = 0$, тобто. Таблиці характеризуються матрицями станів елементів мережі.

5.4. Виділення σ-ї вибірки елементів та визначення l-діагоналі матриці n $\|\varphi_{ij}\|$: - вибір послідовності з l елементів і-го рядка матриці $\|\varphi_{ij}\|_{n*m}$ відповідає σ-ї вибірці включає n елементів по l з кожного рядка, без повторення стовпців розташування обраних елементів

$$\varphi(1,\sigma), \varphi(2,\sigma), \ldots,\varphi(n,\sigma), \tag{2.6}$$

σ-а вибірка включає n елементів по lс кожного рядка, без повторення стовпців розташування обраних елементів (послідовність (2.6) є l-діагоналлю матриці $\|\varphi_{ij}\|_{n*m}$;

- підсумовування по всіх вибірках послідовностей елементів (2.6) матриці:

$$\sum \sigma \varphi *(1,\sigma),(2,\sigma),..., (n,\sigma), \tag{2.7}$$

де $\varphi *(1,\sigma)$ - добуток l елементів і-n рядка матриць, що відповідають $\|\varphi_{ij}\|_{n*m}$, котра відповідає в свою чергу σ-й вибірці.

5.5. Аналіз умов працездатності елементів мережі. l-діагональ матриці n $\|\varphi_{ij}\|_{n*m}$ позитивна, якщо відповідний їй l-діагональний добуток дорівнює одиниці.

Елементи мережі працездатні, якщо є позитивна l-діагональ матриці $\|\varphi_{ij}\|_{n*m}$ (для бінарної матриці дорівнює 1).

- Якщо

$$\sum \sigma \varphi *(1,\sigma),(2,\sigma),..., (n,\sigma) =1, \tag{2.8}$$

то мережа працездатна (забезпечує необхідну якість обслуговування).

- Якщо

$$\sum \sigma \varphi^{*}(1,\sigma),(2,\sigma),\ldots,(n,\sigma)=0, \qquad (2.9)$$

то мережа не працездатна.

- Перехід елемента підматриці з 1 в 0 відображає відмову відповідних елементів мережі, перехід елемента підматриці з 0 в 1 показує можливість відновлення працездатності (перетин, що розглядається, є мінімальним).

- При оцінці надійності обладнання досліджуваних підмереж (ділянок мережі) необхідно враховувати перетин обладнання задіяного при виконанні функцій Fi={f1, f2,…,fn}. Для цього виділяється деяке загальне обладнання, відмова якого пов'язаний з виходом з ладу всієї ділянки, та обладнання, відмова якого призводить до втрати лише відповідних функцій Fi.

Припустимо, що втрата різних функцій рівноймовірна.

Умови (2.7 і 2.9) дозволяють оцінити число працездатних станів частини (або всієї) мережі залежно від сумарного числа 0<k<n функцій Fi={f1, f2,…,fn}.

Умови (2.7 і 2.9) дозволяють оцінити кількість працездатних станів частини (або всієї) мережі залежно від сумарного числа 0<k< n функцій {f1,f2,…,fn}. Кожний стан відповідає варіанту розташування (комбінації) k нулів у матриці $\|\varphi_{ij}\|_{n*m}$, а з урахуванням перетину обладнання може складатися з kd,…,kg,…,km.

- При k ≥ n всі елементи мережі не працездатні, при 0<k<n відмова всіх елементів мінімального перерізу, що відображається в матриці $\|\varphi_{ij}\|_{n*m}$ неможливий, отже, всі Cnk станів системи (для кожного k) можуть бути працездатними.

- визначення числа працездатних станів:

$$N_k = C_n^k - \sum_{s=1}^{n} b(s_i, k_g), \qquad (2.10)$$

де b(si,kg) - кількість комбінацій, що відповідають відмові елементів мінімального перерізу, що відображається в матриці $\|\varphi_{ij}\|_{n*m.}$ Формула (2.10) дає нижню оцінку числа працездатних станів системи, оскільки при підсумовуванні (2.10) можливий багаторазовий облік станів із відмовою елементів двох або більшої кількості мінімальних перерізів. Похибка наближення (2.10) зростає при великих k (введення та порівняння з допустимим значенням похибки).

5.6. Для елементів мережі більшість умов працездатності мають конфліктний характер - збільшення значень одних запасів працездатності спричиняє зменшення інших та знаходиться на вершині конфліктних запасів працездатності.

Отже, ймовірність безвідмовної роботи будь-якого пристрою мережі, насамперед, визначатиметься найменшою з ймовірностей задоволення окремих умов працездатності.

По заданим значенням P_E (а також при обчисленні $K_{готз}$) оцінюється можливість забезпечення апаратурної надійності:

- якщо

$$P_{Ti} < P_E \text{ та } K_{гот} < K_{готз}, \tag{2.11}$$

то необхідна ймовірність неприпустима, це обладнання для мережі обрано невдало з погляду апаратурної надійності всієї мережі, та потрібні заходи для досягнення необхідної ймовірності, наприклад такі як заміна обладнання, дублювання тощо, перехід до кроку 6.

Якщо

$$P_{Ti} <= P_E \text{ та } K_{готз} <= K_{гот}, \tag{2.12}$$

то обладнання вибрано вдало, і можна (якщо це необхідно) провести оптимізацію за критерієм вартості, перехід до кроку 7.6 крок.

Резервування пристроїв мережі за допомогою розробленого алгоритму,. Перехід до кроку 3.

6.1. Виконуються розрахунок надійності та оцінка отриманих результатів обчислень із заданими (необхідними).

6.2. Перевірка умов (2.11) та (2.12): - якщо виконуються умови (2.11), то перехід до кроку 3; - якщо виконуються умови (2.12), перехід до кроку 7.

7 крок. Закінчення роботи алгоритму. Слід зазначити, що при вирішенні завдань оптимізації апаратурної надійності мережі можна використовувати як цільову функцію ймовірність безвідмовної роботи пристроїв, мінімальний запас працездатності пристроїв і критерій гарантованого запасу працездатності, так як саме ці критерії надійності найкращим чином дозволяють проводити ефективну оптимізацію параметричної надійності мережі і забезпечують задану.

Розроблена графова модель оцінки апаратурної надійності корпоративної телекомунікаційной мережі та алгоритм аналізу графової моделі забезпечують багаторівневе моделювання та дозволяють враховувати специфіку роботи пристроїв різних рівнів.

З їхньою допомогою можна обґрунтовано прогнозувати стратегію модернізації та розвитку мережі. Проведена експериментальна перевірка показала, що точність результатів є достатньою для оцінки надійності мережі, а показники надійності відповідають міжнародним стандартам [69].

Рисунок 2.4 – Технологія формування документа про проведення електронних торгів

2.4 Висновки за розділом

1. Досліджено джерела ненадійності мереж. Визначено характеристики, показники та критерії апаратурної надійності. телекомунікаційних мереж електронної комерції Показано, що для оцінки надійності мереж необхідно вибрати окремі аспекти – апаратурну (елементарну) та функціональну (структурну) надійності.

2. Розроблено графову модель оцінки апаратурної надійності телекомунікаційної електронної комерції мережі та алгоритм її аналізу, що дозволяють:

- перевіряти правильність проектних рішень, знаходити «слабкі місця» та застосовувати суттєві заходи щодо підвищення надійності мереж, а також ефективності їх функціонування, забезпечуючи необхідну надійність передачі комерційної інформації ЕТП з телекомунікаційних мереж,
- проводити оптимізацію апаратурної надійності для широкого спектру мереж
- проводити багаторівневе моделювання з урахуванням специфіки роботи мережевих пристроїв різних рівнів,
- прогнозувати стратегію модернізації та розвитку корпоративної мережі електронної комерції.

3 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

3.1 Засоби захисту інформації електронного торгового майданчика телекомунікаційних мережах

У телекомунікаційних мережах електронної комерції системи електронної торгівлі повинні гарантувати юридично значущий документообіг, тобто. забезпечити: аутентифікацію, цілісність інформації та невідмовність. Задля більшої юридично значимого документообігу використовується Електронний Підпис (ЕП).

3.2 Управління криптографічними ключами

Управління ключами – це інформаційний процес, що реалізує такі три основні функції: генерацію, зберігання та розподіл ключів.

Для отримання ключів використовуються апаратні та програмні засоби генерації випадкових значень ключів [15]. Закритий ключ відомий лише клієнту електронного торгового майданчика. ЕТП має лише публічний ключ, що дозволяє йому визначити правильність ЕП, створюваної за допомогою закритого ключа. Без закритого ключа ніхто не може створити документ з підписом клієнта. Закритий ключ є вразливим компонентом усієї криптосистеми ЕП.

В даний час використовуються такі пристрої зберігання закритого ключа: смарт-карти, USB-носії, таблетки Touch-Memory та інші [16]. Існують криптопроцесори, необхідні для захищеного зберігання та використання криптографічних ключів, сертифікатів, файлів та для роботи з ЕП. Розроблено специфікацію TrustedPlatformModule (TPM), що описує криптопроцесор, у якому зберігаються криптографічні ключі [17].

Розподіл ключів - найвідповідальніший процес управління ключами, реалізується двома способами: використанням однієї чи кількох центрів

розподілу ключів; прямий обмін сеансовими ключами між користувачами мережі. Важливою проблемою всієї криптографії з відкритим ключем, у тому числі систем ЕТП, є управління відкритими ключами. Завдання захисту ключів від заміни вирішується за допомогою сертифікатів. Сертифікат відкритого ключа – це електронний документ, який засвідчує власника пари ключів. Сертифікат публічного ключа реєструється в Центрі Сертифікації (державному, приватному чи банківському), що забезпечує визначення належності даної пари ключів конкретній юридичній або фізичній особі та терміну дії цієї пари ключів. Зазвичай, виходячи з безпекової політики, бажано перестворення пари ключів щороку. Для використання ЕП необхідний центр посвідчення (ЦП), який підтвердить, що сертифікат виданий саме тій особі, яка його застосовує.

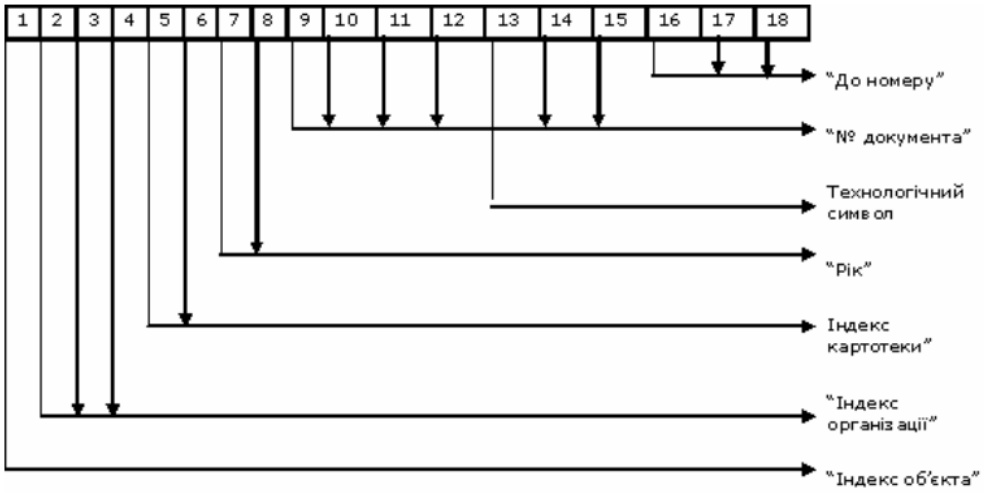


Рисунок 3.1 – Структура штрих-коду документа щодо проведення електронних торгів

3.3 Використання електронного підпису для конфіденційності інформації

Електронний підпис (ЕП) або електронний цифровий підпис (ЕЦП) – це рядок біт, отриманий в результаті процесу формування підпису, який може мати внутрішню структуру, яка залежить від конкретного механізму формування підпису. ЕП є реквізитом електронного документа, який дозволяє встановити належність підпису власнику сертифіката ключа ЕП та визначити відсутність спотворення електронної інформації в документі з моменту

формування ЕП. Значення цього реквізиту утворюється після криптографічного перетворення інформації з використанням закритого ключа ЕП.

При організації захищеного каналу зв'язку з власником ЕП використовують відкритий ключ. Захист ключів від заміни здійснюється за допомогою сертифікатів. Сертифікат відкритого ключа – це цифровий або паперовий документ, що підтверджує відповідність між відкритим ключем та інформацією, що ідентифікує власника ключа. Сертифікат містить інформацію про власника, відомості про відкритий ключ, його призначення та застосування, назву центру сертифікації тощо.

Моделі організації сертифікатів:

1) централізована, що реалізується на основі «мереж довіри» (тут шляхом перехресного підписання сертифікатів знайомих та довірених людей кожним користувачем будується так звана «мережа довіри»);

2) децентралізована (тут використовуються центри сертифікації, що підтримуються довіреними організаціями).

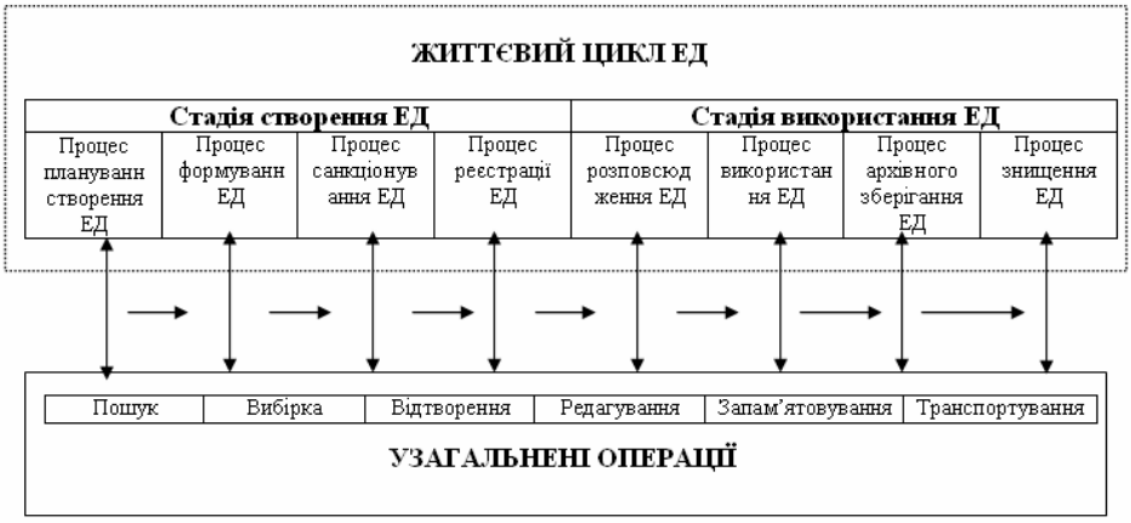


Рисунок 3.2 – Життєвий цикл електронного документа торгівельної площадки

Центр сертифікації формує закритий ключ, власний сертифікат, сертифікати кінцевих користувачів та засвідчує їхню автентичність своєї ЕП, проводить відкликання сертифікатів, що минув, і веде бази виданих та

відкликаних сертифікатів. Застосування ЕП має сенс, якщо під час обчислення легітимного підпису без знання закритого ключа процес стає обчислювально складним. Таким чином, при формуванні політики безпеки та системи оцінок ефективності, а також при проведенні комплексних випробувань захищеності слід користуватися положеннями ISO 15408 (CommonCriteria).

Якщо потрібно захистити канал обміну довільною інформацією, доцільно використовувати протокол TLS. При необхідності забезпечення безпеки фінансових транзакцій можна використовувати стандарт SET (Secure Electronic Transaction), що включає протоколи захисту каналів як один зі стандартів нижчого рівня.

3.4 Процедура прийняття рішення щодо участі користувача в електронних торгах

Процедура прийняття рішення щодо участі користувача в електронних торгах на ЕТП проводиться особою, яка приймає рішення - цеспівробітники електронного торгового майданчика. Тут вибір рішення можездійснюватись як в умовах визначеності, так і в умовах невизначеності вихідної інформації. Для цього необхідно провести аналіз методів оцінки альтернативних варіантів рішень, що дозволяють кількісно оцінити їхню ефективність. При виборі рішення працівниками ЕТП потрібне застосування специфічних прийомів та методів, що передбачають використання їх інтуїції та досвіду роботи. Отримані альтернативні варіанти рішень допускають упорядкування щодо деяких аспектів. Тут важливим є отримання оцінок аналізованих альтернатив, при якому кожному рішенню ставиться у відповідність сукупність чисел (вектор значень критеріїв якості розв'язків).

Завдання оцінювання найчастіше вирішуються експертними методами. Методи експертних оцінок докладно представлені у таких роботах як [18-20]. Серед існуючих методів можна виділити метод шкалювання, методи

ранжирування альтернатив, метод мінімальної відстані та ін. Слід зазначити, що методи безпосереднього ранжування досить важкі для експертів, оскільки їм доводиться одночасно оцінювати ряд альтернатив, присвоюючи кожній певне місце (ранг) в ряду ранжування. Більш прийнятним є використання експертами механізму попарних порівнянь. При попарному порівнянні альтернатив використовується апарат бінарних відносин.

Метод аналізу ієрархій є систематичною процедурою для ієрархічного представлення елементів, що визначають суть будь-якої проблеми, і зокрема проблеми вибору рішення співробітником ЕТП про допуску до участі користувачів в електронних торгах на ЕТП.

Використання методу аналізу ієрархій у розглянутій задачі має наступні переваги:

- метод дає можливість провести декомпозицію та аналіз проблеми оцінювання альтернативних рішень у конкретній ситуації;

- дозволяє враховувати переваги ЛПР на безлічі критеріїв та потрібно лише визначити важливість критерію шляхом попарного порівняння;

- ієрархічне уявлення дає ЛПР просту для розуміння картину впливу зміни пріоритетів на верхніх рівнях на пріоритети елементів нижніх рівнів;

- метод досить добре автоматизується.

Існує кілька видів ієрархій. Для процедури прийняття рішення щодо участі користувача в електронних торгах на ЕТП найбільш прийнятними є домінантні ієрархії.

У розв'язуваній задачі є набір альтернатив A1, A2, …, An та безліч критеріїв оцінки альтернатив К1, К2, ..., Кm. Завдання полягає в тому, щоб вибрати найбільш раціональне рішення в конкретній ситуації.

Альтернативні дії:

- А1 – допустити до торгів,

- А2 – не допустити,

- А3 – ще раз перевірити надійність мережі, каналу зв'язку, обладнання ЕТП.

Безліч критеріїв оцінки альтернатив К = {К1, К2, ..., Кm} включає: сертифікати, позиції сертифікатів, інформація про користувача, списокдокументів, хеш-суму документів.

Процедура прийняття рішення щодо участі користувача в електронних торгах на ЕТП включає 8 кроків.

1. Методом попарних порівнянь необхідно оцінити важливість критеріїв. На цьому кроці потрібна участь ЛПР: використовуючи задану шкалу градації якості, він має порівняти попарно всі критерії.

Якщо критерій Кі краще Кj, то Кij = 1, інакше Кij = -1, при еквівалентності Кij =0.

2. Порівняння критеріїв попарно та отримання матриці:

	K_1	…	K_i	…	K_m
K_1	K_{11}	…	K_{1i}	…	K_1 m
…	…	…	…	…	…
K_j	K_{j1}	…	K_{ji}	…	K_{jm}
…	…	…	…	…	…
K_k	K_{k1}	…	K_{ki}	…	K_{lm}

3.Обчислення ваг критеріїв:

$$W_i = \sqrt[m]{K_{i1} \ldots K_{im}}$$

$$|W_i| = \sqrt[m]{\prod_{i=1}^{m} K_{im}}$$

$$\overline{W_i} = \frac{W_i}{\sum_{i=1}^{m} W_i}$$

4. Порівняння важливості альтернатив за критеріями, що проводиться при фіксації кожного з критеріїв

K_i	A_i		A_3
A_1	y_{11}	...	y_{13}
...	...	...	...
A_3	y_{31}	...	y_{33}

5. Обчислення ваг альтернатив за кожним критерієм:

$$V_i(K_i) = \sqrt[n]{\prod_{r=1}^{n} y_{i'r}} ,$$

$$\overline{V}_i(K_i) = \frac{V_i(K_i)}{\sum_{i=1}^{n} V_i(K_i)} .$$

6. Отримання матриці ваг альтернатив за кожним критерієм.

	A_1	A_2	A_3
K_1	$\overline{V_1(K_1)}$	$\overline{V_2(K_1)}$	$\overline{V_3(K_1)}$
...	...	...	...
K_m	$\overline{V_1(K_m)}$	$\overline{V_2(K_m)}$	$\overline{V_n(K_m)}$

7. Обчислення функції цінності кожної альтернативы.

$$F_i = \sum_{i=1}^{m} \overline{V_i}(K_i)\overline{W_i} .$$

8. Вибір альтернативи Ai (дії) за функцією цінності.

У разі використання методу попарних порівнянь кожному експерту доводиться виконувати число порівнянь альтернатив, що визначається числом поєднань з n по 2: 2C n, тобто. порівнювати альтернативи між собою.

Отримана при цьому матриця відбиває його систему переваг. У окремих випадках переваги експерта можуть містити циклічні ділянки, коли переваги

експерта не визначаються однозначно. Якщо матрицю переваг експерта зобразити графом, то у графі при обході по орієнтованим дугам у разі виникають замкнуті контури. У такій ситуації метод ранжування не дає можливості визначення рангів, що відбивають систему переваг експерта. Тому, перед обчисленням сумарної матриці переваг експертів її перевіряють на відсутність циклів, тобто. на ациклічність.

3.5 Результати експериментального дослідження розробленого математичного апарату

Метою цього дослідженняє експериментальне підтвердження розробленого математичного апарату.

На рис. 3.3 представлена можливість безвідмовної роботи елементів телекомунікаційної мережі електронної комерції за період часу Т, що вимірюється в роках:

- графік 1 відповідає етапу проектування мережі без попереднього розрахунку апаратурної надійності та використання оптимального (Раціонального) резервування мережевих пристроїв;

- графік 2 - та ж функція за аналогічний період часу, але після попереднього розрахунку надійності із застосуванням розробленого алгоритм резервування пристроїв мережі;

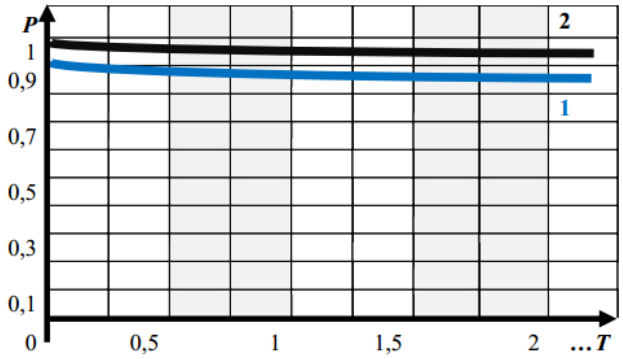


Рисунок 3.3 - Можливість безвідмовної роботи мережі до та після резервування пристроїв

Наведені результати показують, що можливість безвідмовної роботи корпоративної телекомунікаційної мережі електронної комерції в результаті використання резервування пристроїв, заснованого на розробленому алгоритмі підвищилася до 0,9998, тобто мережа перейшла з розряду.

Таблиця 3.1

Середній показник безвідмовної передачі даних

t_1	99,965
t_2	99,974
t_3	99,967
t_4	99,976
t_5	99,968
t_6	99,978
t_7	99,969
t_8	99,967
t_9	99,963
t_{10}	99,971
t_{11}	99,977
t_{12}	99,978
t_{13}	99,981
t_{14}	99,982
t_{15}	99,973
t_{16}	99,971
t_{17}	99,969
t_{18}	99,972
...	...
t_L	99,975

У таблиці 3.1 подано значення середнього показника безвідмовної передачі даних по фізичному каналу зв'язку для доступу до мережі Інтернет при швидкості 1 Гбіт/с протягом інтервалу часу T, поділеного на періоди по 24 годин.

Як видно з таблиці, канал зв'язку фізично забезпечує середній показник безвідмовної передачі даних від 99,965% до 99,991% протягом безперервного 24-годинного періоду при швидкості передачі 1 Гбіт/с.

На фізичному рівні цей показник повинен бути не менше 99,95% протягом 24-ї години.

У таблиці 3.2 представлено порівняння експериментальних та розрахункових даних в оцінці апаратурної надійності мережі. Дані представлені за період спостереження t, що складається з часових інтервалів t1<ti<<tN.

Таблиця 3.2

Імовірність безвідмовної роботи елемента

	Експериментальні дані	Розрахункові дані
t_1	0,99984	0,99984
t_2	0,99981	0,99980
t_3	0,99982	0,99981
t_4	0,99981	0,99980
t_5	0,99984	0,99984
t_6	0,99983	0,99982
t_7	0,99980	0,99981
...	…	…
t_i	0,99982	0,99981

З таблиці 3.2 випливає, що різниця між експериментальними та розрахунковими даними становить трохи більше $\Delta P(t_j) = 0{,}00001$.

У таблиці 3.3 наведено значення параметрів якості обслуговування під час передачі мультимедійного трафіку АКД, отримані під час використання розроблених методів та моделей для розрахунку надійності.

Таблиця 3.3

Значення параметрів QoS під час передачі трафіку

Тип сервісу	Параметри якості обслуговування			
	Допустимі значення		Отримані значення	
	Ймовірність відмови елемента	Ймовірність втрати даних	Ймовірність відмови елемента	Ймовірність втрати даних
IP-телефонія	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$
Відеоконференція	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$
Цифрове відео на запит	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-4}$
Передача даних	10^{-6}	10^{-6}	$1x10^{-6}$	$1x10^{-6}$
Телевізійне мовлення	10^{-8}	10^{-8}	$0{,}5x10^{-8}$	$0{,}2x10^{-8}$

Отримані значення для ймовірності відмови елемента та ймовірності втрати даних відповідають допустимим значенням, згідно існуючим стандартам.

На рис. 3.4 схематично представлено підвищення ефективності функціонування мережі та ЕТП за рахунок застосування запропонованого теоретичного апарату, де графік 1 – це ефективність функціонування до застосування розроблених методів, алгоритмів та моделей; графік 2 – результат їхнього застосування.

Тут слід зазначити, що ефективність функціонування є інтегральним критерієм:

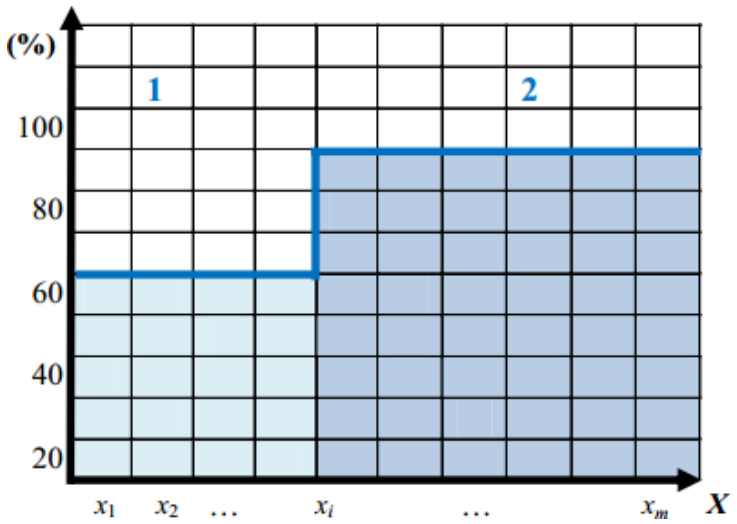


Рисунок 3.4 - Підвищення ефективності функціонування мережі

Критерій включає (крім показників надійності та безпеки) і такий приватний критерій як – «темп подвоєння капіталу», який виражається скалярною функцією часу і може бути як прогнозним (обчислюється шляхом математичного моделювання), так і оперативним (безпосередньо вимірюється). На підставі цього критерію оцінюють стратегічні та оперативні рішення, наприклад: чи варто розробляти свою систему або краще закупити пропоновану на ринку; як формувати тарифи; у напрямі розвивати склад послуг; чи доцільно інтегруватися із відомчими мережами телекомунікації тощо.

Як видно з рис.3.4, ефективність функціонування мережі та ЕТП за рахунок застосування запропонованого теоретичного апарату можна підвищити більш ніж 30%.

3.6 Висновки за розділом

1. Проведено аналіз та дослідження засобу та методів захисту інформації ЕТП у телекомунікаційних мережах електронної комерції Показано, що у таких мережах системи електронної торгівлі мають гарантувати юридично значимий документообіг, тобто. забезпечити: автентифікацію, цілісність інформації та невідмовність.

2. Розроблено ефективний метод поетапного підписання документів ЕП для електронного торгового майданчика, що містить 8 основних етапів: підготовка даних; одержання комплекту ЕП; ЕП;перевірка даних; ЕП; перевірка ЕП, прийняття рішення про участь користувача в електронних торгах.

3. Розроблено процедуру прийняття рішення щодо участі користувача у електронних торгах. Аналіз існуючих підходів до вирішенню цього завдання показав доцільність ухвалення рішення на базі експертних процедур, де найефективнішим є метод аналізу ієрархій, оскільки:

- метод дає можливість провести декомпозицію та аналіз проблеми оцінювання альтернативних рішень у конкретній ситуації;

- дозволяє враховувати переваги ЛПР на безлічі критеріїв та потрібно лише визначити важливість критерію шляхом попарного порівняння;

- ієрархічне уявлення дає ЛПР просту для розуміння картину впливу зміни.

4. Проведена експериментальна перевірка розроблених методів, моделей та алгоритмів розрахунку апаратурної надійності корпоративних телекомунікаційних мереж електронної комерції показала, що точність результатів є достатньою для оцінки надійності мереж та їх елементів, а показники надійності відповідають міжнародним стандартам, визначеним у рекомендаціях МСЕ-Т G.602, G.821 ITU-T.

Отримані значення для ймовірності відмови елемента та ймовірності втрати даних під час передачі мультимедійного трафіку мережі відповідають допустимим значенням, згідно з існуючими стандартами. Різниця між

експериментальними та розрахунковими даними при оцінці ймовірності безвідмовної роботи елементів мережі не перевищує $\Delta P(t_j) = 0{,}00001$.

Експерименти показали, що ймовірність безвідмовної роботи корпоративної телекомунікаційної мережі електронної комерції у результаті використання резервування пристроїв, заснованого на розробленому алгоритмі підвищилася до 0,9998. Канал зв'язку на фізичному рівні забезпечує середній показник безвідмовної передачі даних від 99,965% до 99,991% протягом безперервного 24-х годинного періоду при швидкості передачі 1 Гбіт/с, при вимогі не гірше за 99,95%.

5. Показано, що ефективність функціонування мережі та ЕТП за рахунок застосування запропонованого теоретичного апарату можна підвищити що на 30%.

ВИСНОВКИ

1. У даній кваліфікаційній роботі бакалавра встановлено, що електронна комерція поєднує безліч комунікаційних технологій. Найпоширенішою, найпростішою та зручнішою формою застосуваннясистем електронної торгівлі є електронні торгові майданчики (ЕТП).

2. Розглянуто функції, можливості та переваги роботи на ЕТП для замовника та для компанії, представлені приклади комерційних торгівельних майданчиків.

3. Проаналізовано існуючі способи забезпечення надійності функціонування телекомунікаційних систем електронних торгів. Показано, що системи електронних торгів переходять з рівня електронних торгових майданчиків на рівень повномасштабних систем управління торгово-закупівельною детальністю з використанням телекомунікаційних мереж, отже, основою електронної комерції є телекомунікаційні мережі.

4. Проаналізовано особливості використання телекомунікаційних мереж в електронній комерції. Наведено основні критерії ефективності роботи мереж Показано, що до таких мереж пред'являються підвищені вимоги до надійності передачі та захисту інформації.

5. Проведено аналіз методів та засобів забезпечення інформаційної безпеки у телекомунікаційних мережах електронної комерції. Досліджено методи та моделі оцінки надійності таких мереж. Визначено вимоги до моделей – це універсальність, точність, адекватність, економічність, наочність, обчислюваність, алгоритмізованість. Проведене дослідження показало, що методи та моделі мають свої переваги та недоліки, що викликає певні обмеження на їхнє застосування при проектуванні спеціалізованих корпоративних телекомунікаційних мереж.

6. Проаналізовано та досліджено сучасні системи оцінки надійності та захисту інформації, як вітчизняні, так і зарубіжні. Як показало дослідження, більшість таких систем є складними та дорогими.

7. Досліджено джерела ненадійності мереж. Визначено характеристики, показники та критерії апаратурної надійності. телекомунікаційних мереж електронної комерції Показано, що для оцінки надійності мереж необхідно вибрати окремі аспекти – апаратурну (елементарну) та функціональну (структурну) надійності.

8. Розроблено графову модель оцінки апаратурної надійності телекомунікаційної електронної комерції мережі та алгоритм її аналізу, що дозволяють:

- перевіряти правильність проектних рішень, знаходити «слабкі місця» та застосовувати суттєві заходи щодо підвищення надійності мереж, а також ефективності їх функціонування, забезпечуючи необхідну надійність передачі комерційної інформації ЕТП з телекомунікаційних мереж,
- проводити оптимізацію апаратурної надійності для широкого спектру мереж
- проводити багаторівневе моделювання з урахуванням специфіки роботи мережевих пристроїв різних рівнів,
- прогнозувати стратегію модернізації та розвитку корпоративної мережі електронної комерції.

9. Проведено аналіз та дослідження засобу та методів захисту інформації ЕТП у телекомунікаційних мережах електронної комерції Показано, що у таких мережах системи електронної торгівлі мають гарантувати юридично значимий документообіг, тобто. забезпечити: автентифікацію, цілісність інформації та невідмовність.

10. Розроблено ефективний метод поетапного підписання документів ЕП для електронного торгового майданчика, що містить 8 основних етапів: підготовка даних; одержання комплекту ЕП; ЕП;перевірка даних; ЕП; перевірка ЕП, прийняття рішення про участь користувача в електронних торгах.

11. Розроблено процедуру прийняття рішення щодо участі користувача у електронних торгах. Аналіз існуючих підходів до вирішенню цього завдання

показав доцільність ухвалення рішення на базі експертних процедур, де найефективнішим є метод аналізу ієрархій, оскільки:

- метод дає можливість провести декомпозицію та аналіз проблеми оцінювання альтернативних рішень у конкретній ситуації;
- дозволяє враховувати переваги ЛПР на безлічі критеріїв та потрібно лише визначити важливість критерію шляхом попарного порівняння;
- ієрархічне уявлення дає ЛПР просту для розуміння картину впливу зміни.

12. Проведена експериментальна перевірка розроблених методів, моделей та алгоритмів розрахунку апаратурної надійності корпоративних телекомунікаційних мереж електронної комерції показала, що точність результатів є достатньою для оцінки надійності мереж та їх елементів, а показники надійності відповідають міжнародним стандартам, визначеним у рекомендаціях МСЕ-Т G.602, G.821 ITU-T.

13. Отримані значення для ймовірності відмови елемента та ймовірності втрати даних під час передачі мультимедійного трафіку мережі відповідають допустимим значенням, згідно з існуючими стандартами. Різниця між експериментальними та розрахунковими даними при оцінці ймовірності безвідмовної роботи елементів мережі не перевищує $\Delta P(tj) = 0{,}00001$.

14. Експерименти показали, що ймовірність безвідмовної роботи корпоративної телекомунікаційної мережі електронної комерції у результаті використання резервування пристроїв, заснованого на розробленому алгоритмі підвищилася до 0,9998. Канал зв'язку на фізичному рівні забезпечує середній показник безвідмовної передачі даних від 99,965% до 99,991% протягом безперервного 24-х годинного періоду при швидкості передачі 1 Гбіт/с, при вимогі не гірше за 99,95%.

15. Показано, що ефективність функціонування мережі та ЕТП за рахунок застосування запропонованого теоретичного апарату можна підвищити що на 30%.

ЛІТЕРАТУРА

1. Білоус, О. І. Захист інформації в комп’ютерних системах і мережах: навчальний посібник. – Київ: Ліра-К, 2020. – 264 с.

2. Дьяконов, В. П. Інформаційна безпека в інформаційно-комунікаційних системах. – Харків: ХНУРЕ, 2019. – 220 с.

3. Козлов, Д. В., Кузнєцов, С. І. Методи захисту інформації в інформаційно-комунікаційних системах. – Львів: Видавництво Львівської політехніки, 2021. – 198 с.

4. Мазуренко, В. П. Організація захисту інформації в комп’ютерних системах. – К.: Академія, 2018. – 312 с.

5. Frederix, F. (2003). "The Dynamic Networked Organization: A New Paradigm that is Here to Stay". In *E-Business Applications*.

6. Stallings, W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Pearson Education, 2023. – 752 p.

7. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. Security in Computing. – 6th ed. – Pearson, 2015. – 864 p.

8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", Відомості Верховної Ради України, 2001, № 31, ст. 148.

9. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – International Organization for Standardization, 2022.

10. Kizza, J. M. Guide to Computer Network Security. – 5th ed. – Springer, 2020. – 560 p.

11. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – Wiley, 2020. – 1232 p.

12. Holló, Cs. A partial enumeration algorithm for solving PNS problems. Mathematical and Computer Modelling, 38(7-9), 855–864 (2003).

13. RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2. – Internet Engineering Task Force, 2008. https://tools.ietf.org/html/rfc5246

14. ENISA (European Union Agency for Cybersecurity). Cybersecurity Guidelines for eCommerce Platforms. – 2021. https://www.enisa.europa.eu

15. ISO/IEC 19790:2025. Security requirements for cryptographic modules. Міжнародний стандарт, аналог FIPS 140-2/3.

16. Гулак Г. М., Мухачов В. А., Хорошко В. О., Яремчук Ю. Є. Основи криптографічного захисту інформації: підручник. – Вінниця: ВНТУ, 2011. – 199 с.

17. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем: навчальний посібник. – Київ: ДТЕУ, 2023. – 312 с.

18. Козіна Г. Л., Романчук Т. В. Лабораторні роботи з дисципліни "Криптографічні засоби захисту інформації". – Запоріжжя: ЗНТУ, 2009. – 46 с.

19. Задірака В. К., Кудін А. М., Людвиченко В. О., Олексюк О. С. Комп’ютерні технології криптографічного захисту інформації на цифрових носіях. – Київ – Тернопіль: Підручники і посібники, 2007. – 272 с.

20. Войтусік С. С., Журавель І. М., Мороз Л. В. Апаратно-програмні засоби криптографічного захисту інформації: метод. вказівки до лаб. робіт. – Львів: ЛП, 2017. – Лаб. №1 – 32 с., Лаб. №3 – 17 с.

21. Goldreich O. Foundations of Cryptography: Vol. I & II. – Cambridge University Press, 2001/2004. – Vol. I: 410 pages, Vol. II: 423 pages.

ДОДАТКИ

1 ANALYTICAL PART

1.1. Reliability – as one of the criteria for assessing the quality of telecommunication networks

Telecommunications networks include [1]: computer and telephone networks, radio networks, television networks. Analysis of theoretical and experimental studies [2] allows us to identify the main criteria for assessing the quality (performance criteria) of telecommunication networks - these are productivity, reliability, security, expandability, scalability, transparency, support for various types of traffic, manageability, compatibility. Sometimes the concept of "quality of service" of a network includes only two important characteristics - productivity and reliability. Fig. 1.1 shows an example of a telecommunication network

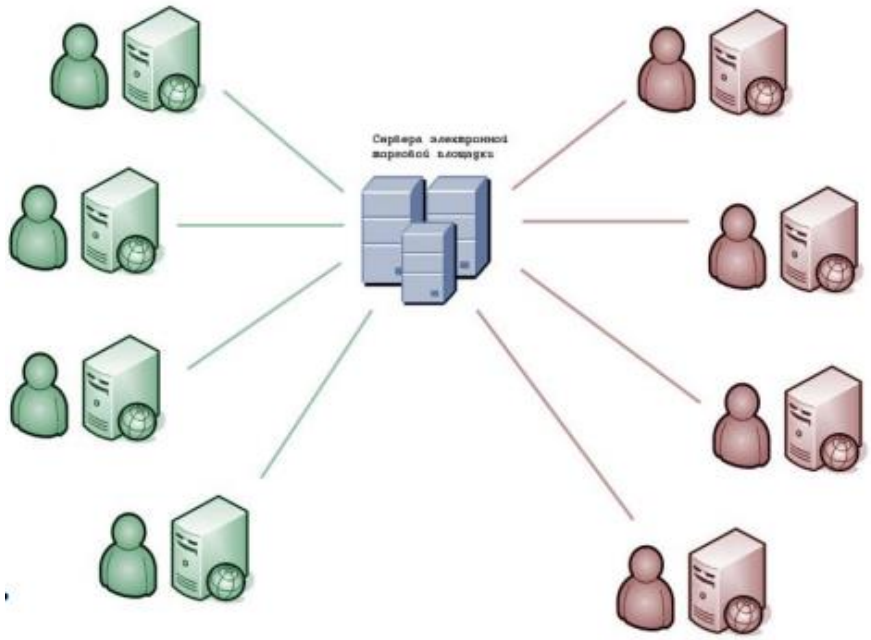


Figure 1.1 – Telecommunications network

When analyzing the reliability and security of networks, the following indicators should be highlighted: probability of failure, mean time to failure, failure rate, availability factor, data storage and protection from distortion, data consistency (consistency), the ability to deliver a packet to the destination node without

distortion, the possibility of packet loss, the probability of distortion of a single bit of transmitted data, the ratio of lost packets to delivered packets, security or the ability of the system to protect data from unauthorized access, fault tolerance.

To assess the reliability of networks, it is necessary to highlight separate aspects - hardware (elementary) and functional (structural) reliability, appropriate methods for their assessment, and consider methodological issues of reliability taking into account QoS.

Elementary reliability is the property inherent in an element of a communication network to maintain operability with a quality no worse than the specified one for a certain time interval.

Structural reliability is the property of a network to provide user connectivity with a quality not worse than the specified one for a certain time interval.

The following main characteristics are used to assess reliability: availability, security and fault tolerance. The reliability of telecommunication networks is largely determined by the reliability of segments of the physical transmission medium for communication channels and the reliability of network equipment. It is impossible to fully characterize the reliability of such a complex and multifaceted object as telecommunication networks using one indicator, therefore, for a more complete characteristic, it is necessary to determine a whole set of reliability parameters [3]. As is known, it is not enough to determine reliability at a qualitative level; it is necessary to assess reliability quantitatively and compare different objects in terms of their reliability. For this purpose, reliability indicators and criteria are introduced. Reliability indicator is a quantitative characteristic of one or more single properties that determine the reliability of an object. There are single and complex reliability indicators [4]. Complex indicators characterize several single properties.

To characterize the quality of functioning of networks and reliability theory devices, a set of interval, integral, and point reliability indicators, as well as methods for their calculation, has been developed.

Each object is characterized by a vector of single and complex indicators. Since when comparing options, one of them may be better than the alternative option

in one indicator and worse in another, among the indicators, the one that best reflects the reliability property in specific conditions is chosen, and it is chosen as the reliability criterion.

There are the following criteria for assessing the reliability of telecommunication network devices: maintainability, warranty period of operation, availability factor, downtime factor, etc. The choice of indicator is dictated either by the standard adopted in the industry, or directly by the consumer.

1.4. Features of the use of telecommunication networks in electronic commerce

Telecommunication networks of corporations engaged in electronic commerce (corporate telecommunication networks) have some characteristic features. The organizational structure of such a corporation is such that individual functions are distributed horizontally between its divisions, and hierarchical relationships are weakened. In modern Western studies devoted to the information society, network corporations are also called “organization with a modular structure” or “dynamic network organization” [5].

Coordination of the actions of divisions in corporations of this type is carried out by the head office via the Internet, but at the same time, distinctive features are self-organizing processes and decentralized management; the number of internal hierarchical levels in network corporations is small. The process of creating a network in this case is significantly simplified, since there is no need to develop an integration project, since individual units can create their own subsystems using their local networks and servers, without connecting them to other units, and then they can connect to a single corporate system. Features of building such networks [6]:

- improvement of Internet access methods;

- transfer of Internet services to mobile terminals (including cell phones), many foreign banks are actively implementing mobile trading platforms optimized for iPad,

iPhone and other devices, promising development of similar mobile banking platforms;

- creation and distribution of more convenient Internet standards;

- high-speed information transmission technologies and various combinations of communication channels are used;

- it is planned to integrate the network with other telecommunication systems, as well as create backup communication channels and duplicate all the main components of the systems, which ensures high performance, reliability and fault tolerance of the network, as well as the ability to further develop;

- combining tens of thousands of computers located in different countries and cities;

- increased requirements for the reliability of information transmission and protection in such networks.

Among the requirements for conducting commercial transactions, the following should be highlighted: authentication, confidentiality, integrity, authorization, guarantees and preservation of secrecy. The first 4 requirements can be ensured by technical means, the implementation of the last 2 depends on technical means and the responsibility of individual individuals and organizations, as well as compliance with laws.

1.4. Analysis of automated electronic trading systems

The hardware and software basis of electronic commerce are telecommunication systems and networks, the global Internet, commercial and corporate networks, information and telecommunication technologies [7].

Electronic trading systems are software and technological solutions designed to automate the procedures for preparing and conducting electronic auctions and other types of competitive procurement. The most common, simplest and most convenient form of application of electronic trading systems is electronic trading platforms (ETP). The formation of a legislative state procurement framework is of great importance in the development of electronic trading platforms. Electronic trading

systems will gradually move from the ETP level to the level of full-scale trade and procurement management systems.

ETP is a complex of information and technical means that ensures the interaction of the customer with the supplier through telecommunication channels at all stages during the conclusion of the agreement [8].

The functions of the ETP include: an information function that provides access to the list of organizations on the ETP and obtain information about the organization of interest; a marketing function; an advertising function; a trading function; an analytical function that allows for a comparative analysis of various indicators of the organizations' activities; an information protection function that provides secure electronic document flow built using certified cryptographic information protection tools.

The advantages of working on the ETP for the customer and for the company are as follows:

a significant saving of working hours;

saving money for organizing and conducting procurement;

transparency of the procurement process;

fair competition; participation in the auction is possible "from anywhere in the world, without leaving the office"; accessibility for representatives of any business - the price and

terms of the lot are not limited.

To work on an electronic trading platform, an organization that is a participant in placing an order must have electronic signature (ES) funds issued by a certification center that has been authorized and has concluded an agreement with the operator of the electronic platform selected to conduct auctions during the placement of a state order [9].

There are the following ETPs designed:

1) for placing a state order;

2) for commercial customers - specialized and multi-profile.

1.4 Ensuring the reliability of the functioning of telecommunication systems for electronic trading

To build reliable telecommunication networks (TCS) and systems, various types of support can be used:

i) economic;

j) temporary;

k) organizational;

l) structural;

m) technological;

n) operational;

o) social;

p) algorithmic.

To ensure the reliability of technical means, the following is most often done:

- backup (duplication) of technical means (computers and their components, network segments, etc.);
- use of standard protocols for the operation of TCS devices;
- use of specialized technical means of information protection.

Information protection means of telecommunication systems, including electronic trading systems, are technical, cryptographic, software and other means designed to protect information, the means in which it is implemented, as well as a means of monitoring the effectiveness of information protection. Information protection means are divided into: physical, hardware, software, cryptographic, and combined.

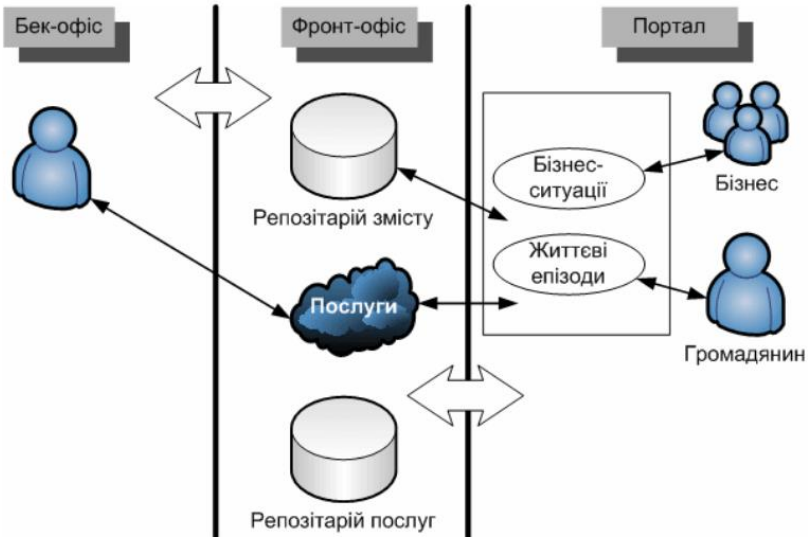


Figure 1.2 – Architecture of electronic regulations

1.5 Analysis of methods and means of ensuring hardware reliability and information security in telecommunication networks of e-commerce

Improving reliability consists in preventing malfunctions, failures and failures. The main way to increase readiness is redundancy, on the basis of which various variants of fault-tolerant architectures are implemented.

For commercial enterprises, security is an economic category. Currently, comprehensive approaches to enterprise information security are being developed, especially during the aggression of the Russian Federation against Ukraine. Concepts (policies) of enterprise security are being created. In the network, network protocols and devices that form the network, databases and programs are vulnerable. Methods and means of ensuring reliability and information security in telecommunication networks are divided into organizational and software-technical.

1. Organizational methods: personnel management, physical protection, maintenance of operability, planning of restoration work.

2. Software-technical methods.

Among the modern software and technical methods for increasing the security of information in telecommunication networks of e-commerce, the following can be distinguished:

correct configuration of network nodes;

rational use of redundancy methods;

when designing a network, it is necessary to use elements that ensure security; use of fault-tolerant computers with fault-tolerant hardware components;

clustering of computers (provide a readiness factor of 0.999-high availability);

duplexing and disk mirroring (Diskmirroring); automatic connection (auto-reconnection);

file system duplication; transaction tracking (transactiontracking);

use of firewalls and firewalls;

identification and authentication;

access delimitation;

logging and auditing;

cryptographic data conversion.

Figure 1.3 – Architecture of the portal for providing electronic services

1.6 Conclusions by section

1. During the work on the first section of the bachelor's qualification work, it was established that electronic commerce combines many communication technologies. The most common, simplest and most convenient form of application of electronic trading systems is electronic trading platforms (ETP).

2. The functions, capabilities and advantages of working on ETP for the customer and for the company are considered, examples of federal and commercial trading platforms are presented.

3. The existing methods of ensuring the reliability of the functioning of telecommunication systems for electronic trading are analyzed. It is shown that electronic trading systems are moving from the level of electronic trading platforms to the level of full-scale systems for managing trade and procurement details using telecommunication networks, therefore, the basis of electronic commerce is telecommunication networks.

4. The features of using telecommunication networks in electronic commerce are analyzed. The main criteria for the efficiency of networks are given. It is shown that such networks are subject to increased requirements for the reliability of information transmission and protection.

5. An analysis of methods and means of ensuring information security in telecommunication networks of e-commerce is carried out. Methods and models for assessing the reliability of such networks are studied. Requirements for models are determined - universality, accuracy, adequacy, economy, cost-effectiveness, clarity, computability, algorithmicity. The study showed that methods and models have their advantages and disadvantages, which causes certain restrictions on their application in the design of specialized corporate telecommunication networks. Therefore, the development of new models and algorithms for calculating the hardware reliability of devices of such networks, taking into account existing developments in this field, is an urgent scientific task.

6. Modern systems for assessing the reliability and protection of information, both domestic and foreign, are analyzed and investigated. As the study showed, most such systems are complex and expensive.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

КАФЕДРА АВТОМАТИКИ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЕЛЕКТРОННОЇ ТОРГІВЕЛЬНОЇ ПЛОЩАДКИ

Кваліфікаційна робота бакалавра

Виконав: **М. Ю. Гонтар**

Керівник:
д.т.н., професор **В. В. Косенко**

Полтава 2025

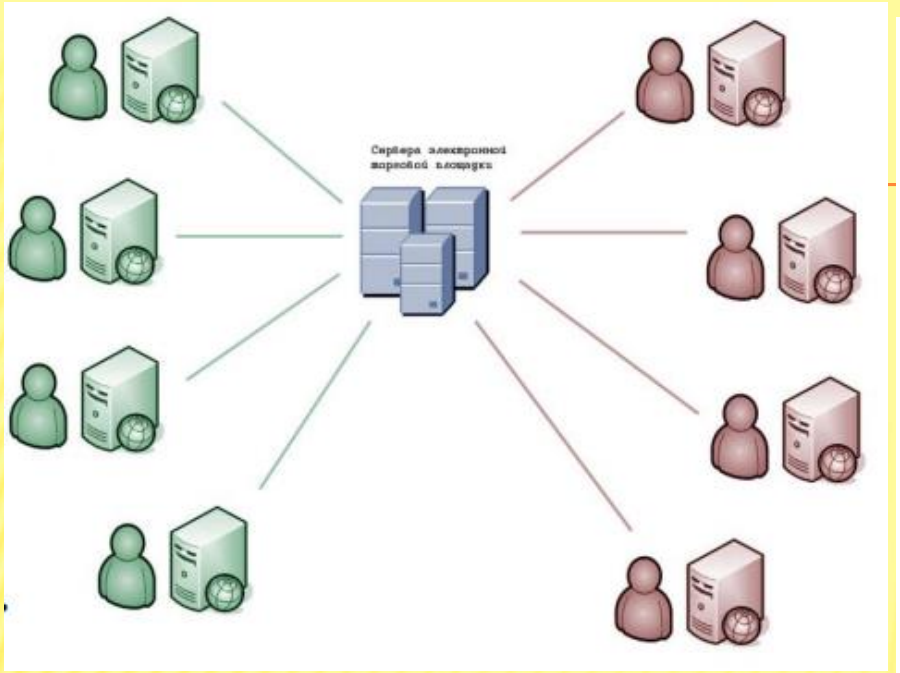
Метою даної бакалаврської роботи є дослідження принципів, методів і засобів забезпечення конфіденційності інформації в телекомунікаційній мережі електронної торгівельної площадки.

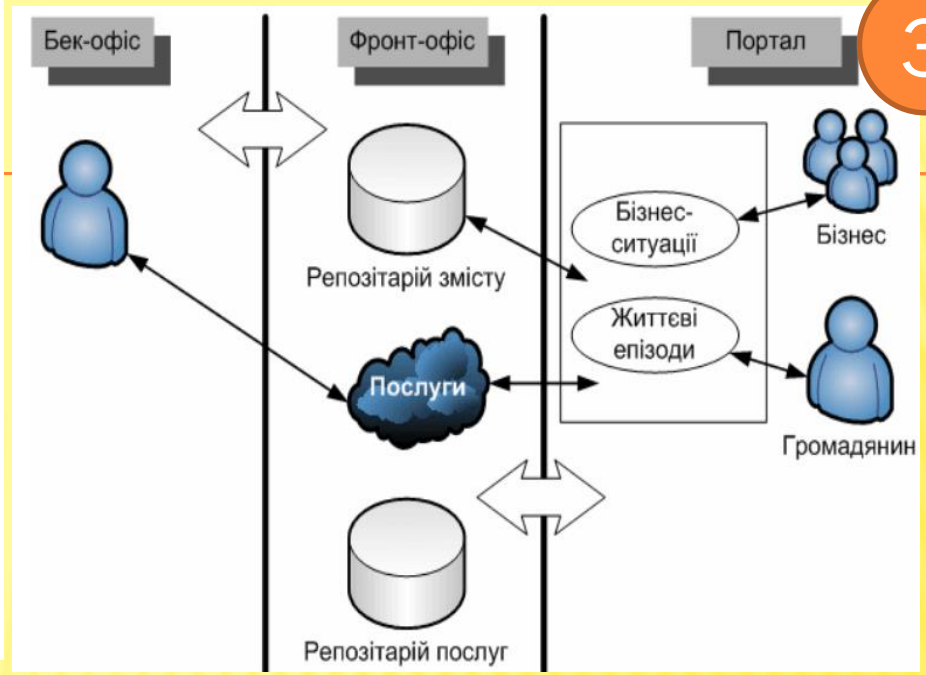
Для досягнення поставленої мети передбачається виконання таких завдань:

✓*проаналізувати сучасні загрози, пов'язані з порушенням конфіденційності в електронній торгівлі;*
✓*дослідити основні методи та протоколи захисту інформації в телекомунікаційних мережах;*
✓*запропонувати практичні рекомендації підвищення рівня конфіденційності інформації в рамках конкретної телекомунікаційної системи.*

Об'єктом роботи є процес побудови телекомунікаційної мережі електронної торгівельної площадки, яка функціонує в умовах сучасного інформаційного середовища.

Предметом є методи забезпечення конфіденційності інформації, що передається в межах цієї мережі.





Телекомунікаційна мережа

Коефіцієнт готовності	Типи систем	
0,99	Звичайна	Conventional
0,999	Висока надійність	Highavailability
0,9999	Відмовостійка	Faultresilient
0,99999	Безвідмовна	Faulttolerant

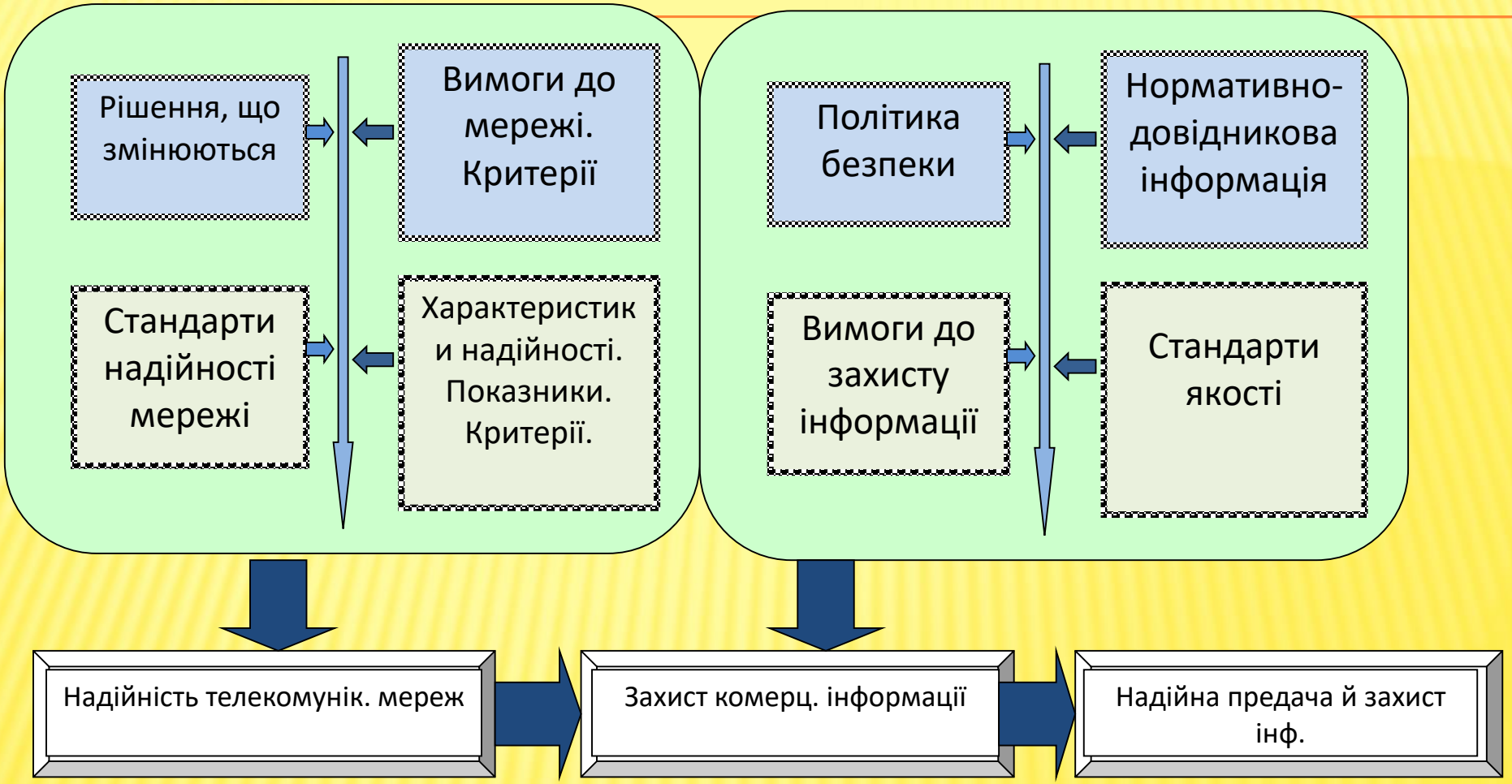
Класифікація систем за рівнем надійності

Засоби захисту інформації діляться на: фізичні, апаратні, програмні, криптографічні, та комбіновані.

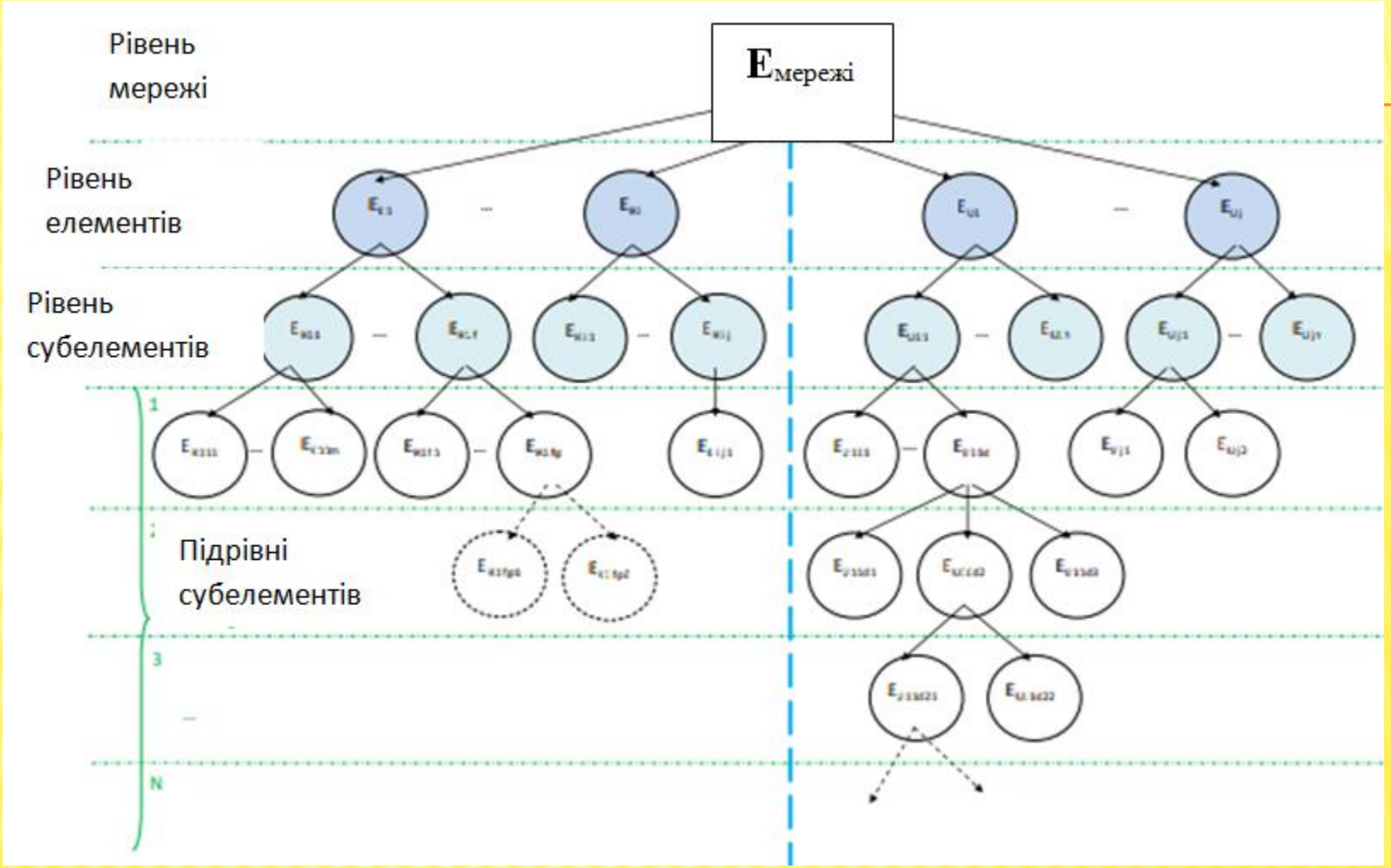
Серед сучасних програмно-технічних методів підвищення безпеки інформації телекомунікаційних мереж електронної комерції можна виділити:

- правильна конфігурація вузлів мережі;
- раціональне застосування методів резервування;
- при проектуванні мережі потрібно використовувати елементи, що забезпечують безпеку; використання відмовостійких комп'ютерів з відмовостійкими апаратними компонентами;
- кластеризація комп'ютерів (забезпечують коефіцієнт готовності до 0,999-high availability);
- дуплексування та дзеркальне відображення дисків (Diskmirroring); автоматичне підключення (auto-reconnection);

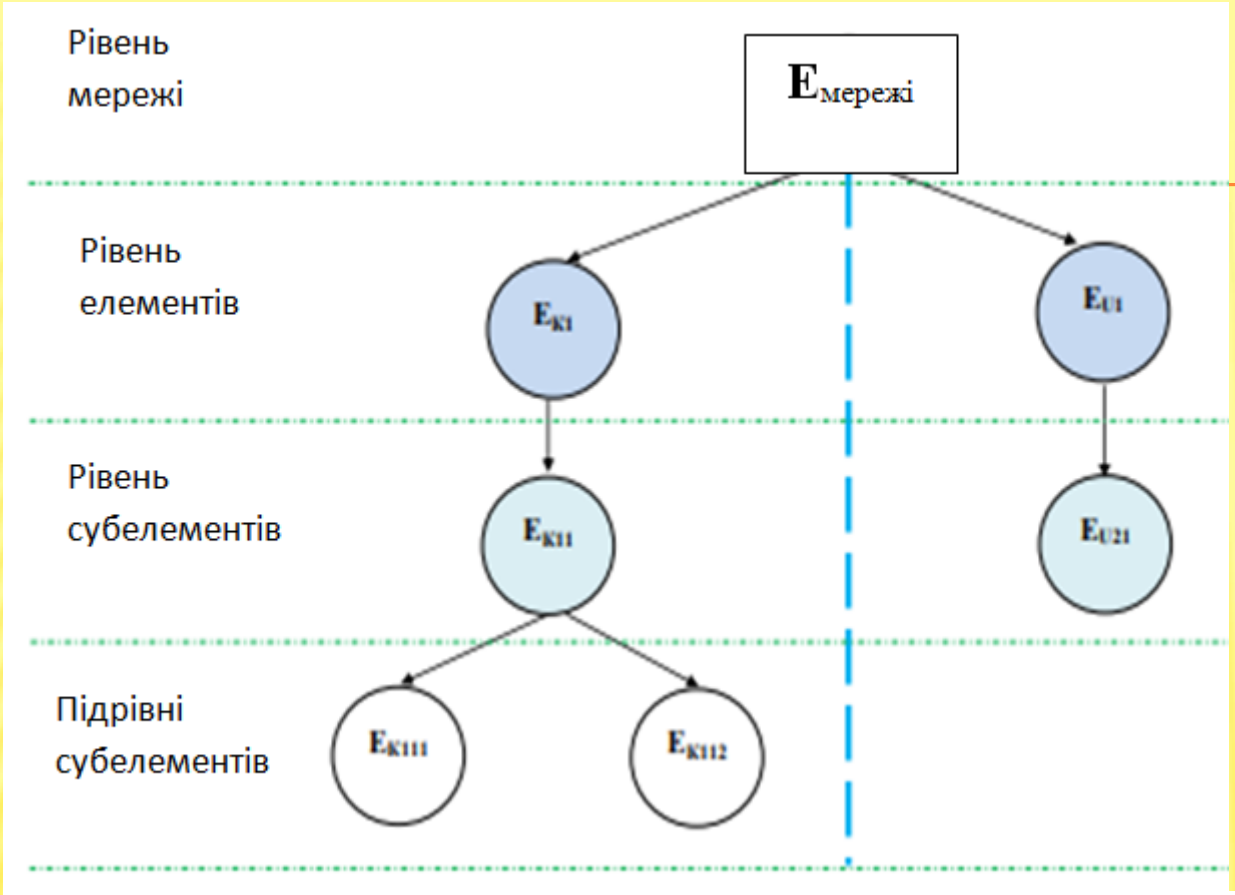
- дублювання файлової системи; відстеження транзакцій (transactiontracking);
- використання міжмережевих екранів та брандмауерів;
- ідентифікація та автентифікація;
- розмежування доступу;
- протоколювання та аудит;
- криптографічне перетворення даних.



Алгоритм апаратно-програмного захисту комерційної інформації

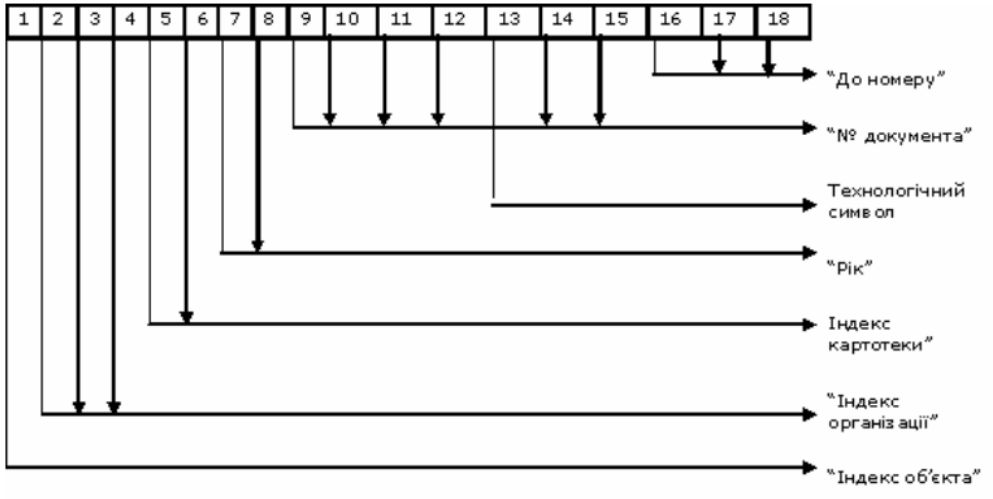


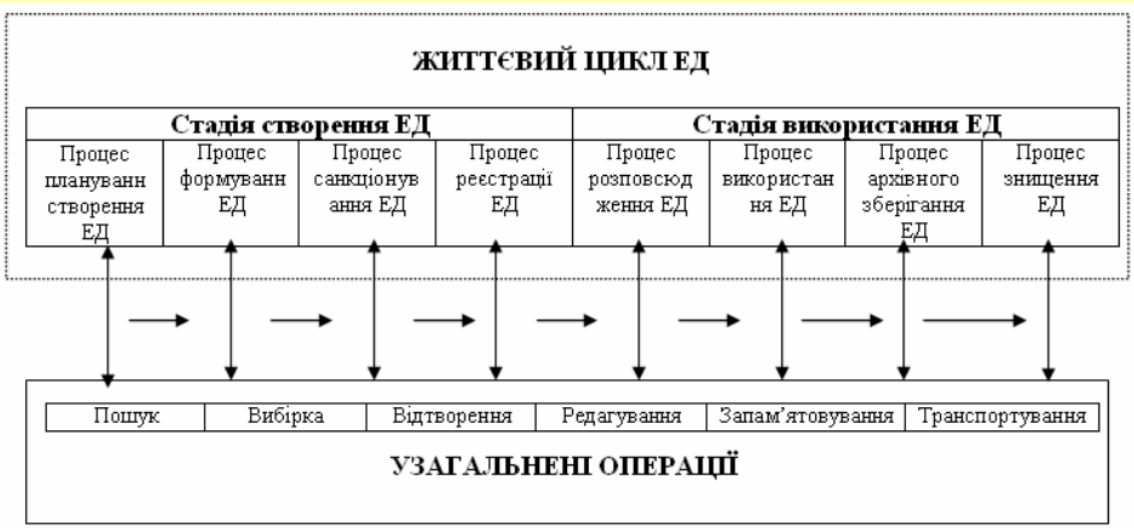
Графова модель розрахунку апаратурної надійності корпоративної телекомунікаційної мережі



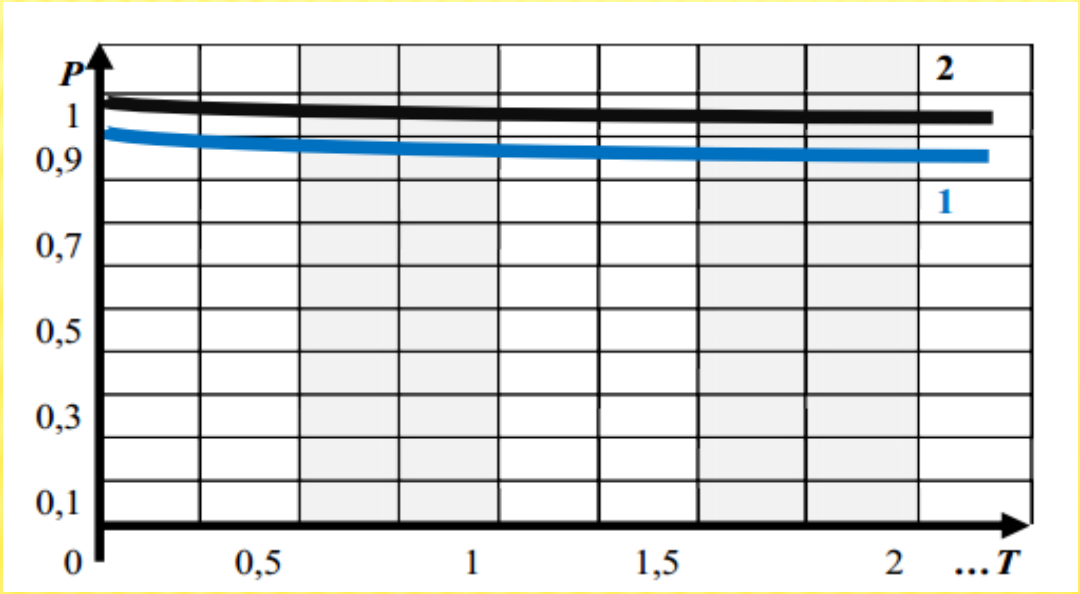
Підграф графа G = (E, L)

Структура штрих-коду документа щодо проведення електронних торгів





Життєвий цикл електронного документа торгівельної площадки



Можливість безвідмовної роботи мережі до та після резервування пристроїв

Можливість безвідмовної роботи елементів телекомунікаційної мережі електронної комерції за період часу Т, що вимірюється в роках:

- графік 1 відповідає етапу проектування мережі без попереднього розрахунку апаратурної надійності та використання оптимального (раціонального) резервування мережевих пристроїв;
- графік 2 - та ж функція за аналогічний період часу, але після попереднього розрахунку надійності із застосуванням розробленого алгоритму резервування пристроїв мережі.

Імовірність безвідмовної роботи елемента мережі

	Експериментальні дані	Розрахункові дані
	0,99984	0,99984
t_2	0,99981	0,99980
t_3	0,99982	0,99981
t_4	0,99981	0,99980
t_5	0,99984	0,99984
t_6	0,99983	0,99982
t_7	0,99980	0,99981
…	…	…
t_i	0,99982	0,99981

Значення параметрів QoS під час передачі трафіку

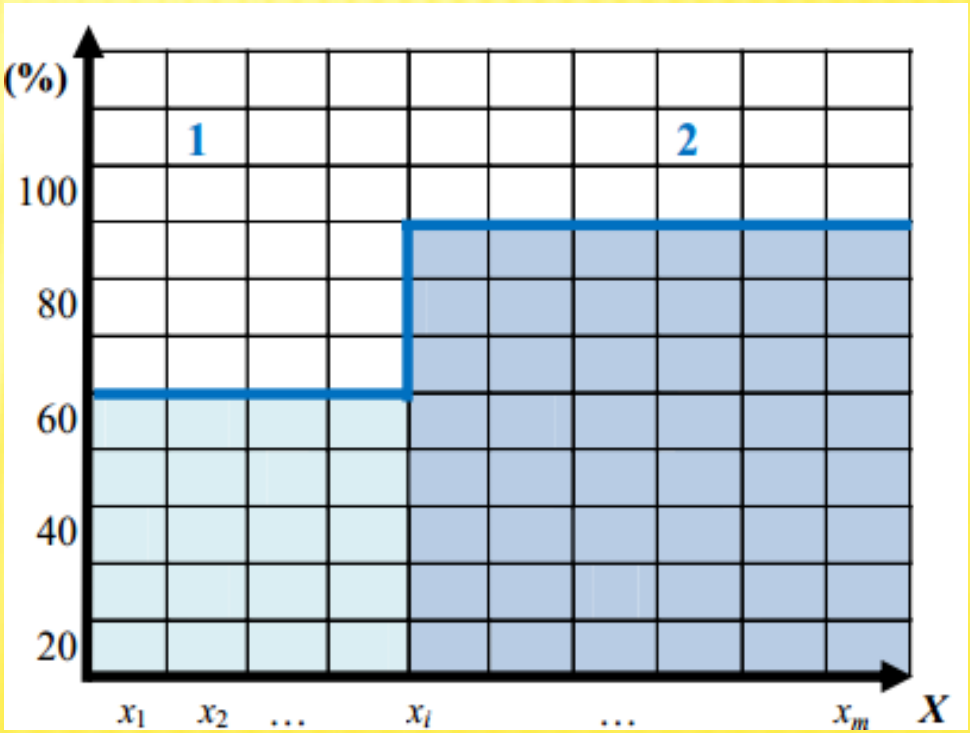
Тип сервісу	Параметри якості обслуговування			
	Допустимі значення		Отримані значення	
	Ймовірність відмови елемента	Ймовірність втрати даних	Ймовірність відмови елемента	Ймовірність втрати даних
IP-телефонія	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$
Відеоконференція	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$
Цифрове відео на запит	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-4}$
Передача даних	10^{-6}	10^{-6}	$1x10^{-6}$	$1x10^{-6}$
Телевізійне мовлення	10^{-8}	10^{-8}	$0,5x10^{-8}$	$0,2x10^{-8}$

t_1	99,965
t_2	99,974
t_3	99,967
t_4	99,976
t_5	99,968
t_6	99,978
t_7	99,969
t_8	99,967
t_9	99,963
t_{10}	99,971
t_{11}	99,977
t_{12}	99,978
t_{13}	99,981
t_{14}	99,982
t_{15}	99,973
t_{16}	99,971
t_{17}	99,969
t_{18}	99,972
...	...
t_L	99,975

Середній показник безвідмовної передачі даних

Як видно з графіків, ефективність функціонування мережі за рахунок застосування запропонованого технічного апарату можна підвищити більш ніж 30%.

Підвищення ефективності функціонування мережі



Висновки

Основні результати кваліфікаційної роботи бакалавра полягають у наступному:

1) Розглянуто функції, можливості та переваги роботи на ЕТП для замовника та для компанії, представлені приклади комерційних торгівельних майданчиків.
2) Проаналізовано існуючі способи забезпечення надійності функціонування телекомунікаційних систем електронних торгів.
3) Проведено аналіз методів та засобів забезпечення інформаційної безпеки у телекомунікаційних мережах електронної комерції. Досліджено методи та моделі оцінки надійності таких мереж. Визначено вимоги до моделей – це універсальність, точність, адекватність, економічність, наочність, обчислюваність, алгоритмізованість.
4) Досліджено джерела ненадійності мереж. Визначено характеристики, показники та критерії апаратурної надійності. телекомунікаційних мереж електронної комерції Показано, що для оцінки надійності мереж необхідно вибрати окремі аспекти – апаратурну (елементарну) та функціональну (структурну) надійності.
5) Розроблено графову модель оцінки апаратурної надійності телекомунікаційної електронної комерції мережі та алгоритм її аналізу.
6) Проведено аналіз та дослідження засобу та методів захисту інформації ЕТП у телекомунікаційних мережах електронної комерції Показано, що у таких мережах системи електронної торгівлі мають гарантувати юридично значимий документообіг, тобто. забезпечити: автентифікацію, цілісність інформації та невідмовність.
7) Розроблено ефективний метод поетапного підписання документів ЕП для електронного торгового майданчика, що містить 8 основних етапів: підготовка даних; одержання комплекту ЕП; ЕП;перевірка даних; ЕП; перевірка ЕП, прийняття рішення про участь користувача в електронних торгах.
8) Проведена експериментальна перевірка розроблених методів, моделей та алгоритмів розрахунку апаратурної надійності корпоративних телекомунікаційних мереж електронної комерції показала, що точність результатів є достатньою для оцінки надійності мереж та їх елементів, а показники надійності відповідають міжнародним стандартам, визначеним у рекомендаціях МСЕ-Т G.602, G.821 ITU-T.
9) Отримані значення для ймовірності відмови елемента та ймовірності втрати даних під час передачі мультимедійного трафіку мережі відповідають допустимим значенням, згідно з існуючими стандартами. Різниця між експериментальними та розрахунковими даними при оцінці ймовірності безвідмовної роботи елементів мережі не перевищує $\Delta P(tj) = 0{,}00001$.
10) Експерименти показали, що ймовірність безвідмовної роботи корпоративної телекомунікаційної мережі електронної комерції у результаті використання резервування пристроїв, заснованого на розробленому алгоритмі підвищилася до 0,9998. Канал зв'язку на фізичному рівні забезпечує середній показник безвідмовної передачі даних від 99,965% до 99,991% протягом безперервного 24-х годинного періоду при швидкості передачі 1 Гбіт/с, при вимогі не гірше за 99,95%.

ДЯКУЮ ЗА УВАГУ!