Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Давідяна Давида Армаісовича*

академічної групи *125-17-1*

спеціальності *6.170103 Управління інформаційною безпекою*

спеціалізації[1]

за освітньо-професійною програмою

на тему *Захист інформаційних ресурсів бездротової мережі товариства з обмеженою відповідальністю «Рубін»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Конограй Н.О			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Давідяну Давиду Армаісовичу*** **академічної групи** ***125-17-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***6.170103 Управління інформаційною безпекою***
(код і назва спеціальності)

на тему ***Захист інформаційних ресурсів бездротової мережі товариства з обмеженою відповідальністю «Рубін»***

затверджену наказом ректора НТУ «Дніпровська політехніка» 317-с від 07.06.2021р

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи ТОВ «Рубін". Аналіз технології WiMAX Розробка моделі загроз.*	20.03.2021
Розділ 2	*Аналіз стану захищеності інформаційно-телекомунікаційної системи ТОВ «Рубін». Розробка політики безпеки інформації.*	30.05.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	11.06.2021

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 21.06.2019р.

Прийнято до виконання _____ Давідян Д.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 125 с., 28 рис., 13 табл., 4 додатка, 9 джерел.

Об'єкт розробки: Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ "Рубін".

Мета проекту: Розробка захищеної клієнтської частини для обробки та передачі інформації на основі технології WiMAX

У першому розділі описаний об'єкт: рід діяльності, інформаційна система, устаткування, програмне забезпечення, інформаційні потоки. Також виконана: аналіз технології WiMax, класифікація інформації, що обробляється в ІТС, визначений перелік джерел загроз, перелік вразливостей та перелік актуальних для ІТС загроз.

У другому розділі описано існуючий профіль захищеності та виконано вибір нового профілю захищеності підприємства, також були розроблені рекомендації, щодо забезпечення інформаційної безпеки ОІД.

В третьому розділі були розраховані витрати на впровадження та щорічну підтримку політики безпеки. Окрім цього, була доведена економічна доцільність введення в експлуатацію рекомендацій щодо політики безпеки, розроблених в другому розділі.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки ТОВ "Рубін"

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ.

РЕФЕРАТ

Пояснительная записка: 125 с., 28 рис., 13 табл., 4 приложения, 9 источников.

Объект разработки: Разработка политики безопасности информации информационно-телекоммуникационной системы ООО "Рубин".

Цель проекта: Разработка защищенной клиентской части для обработки и передачи информации на основе технологии WiMax

В первом разделе описан объект: род деятельности, информационная система, оборудование, программное обеспечение, информационные потоки. Также выполнен анализ технологии WiMax классификация информации, которая обрабатывается в ИТС, определён перечень источников угроз, перечень уязвимостей и перечень актуальных для ИТС угроз.

Во втором разделе описано существующий профиль защищенности и выполнен выбор нового профиля защищенности предприятия, также были разработаны рекомендации, касательно обеспечения информационной безопасности ОІД.

В третьем разделе были рассчитаны затраты на введение и ежегодную эксплуатацию политики безопасности. Кроме того, была доказана целесообразность введения в эксплуатацию рекомендаций касательно политики безопасности, разработанных во втором разделе.

Практическое значение проекта состоит в повышении уровня информационной безопасности ООО "Рубин"

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ.

THE ABSTRACT

Explanatory note: 125 p., 28 fig., 13 tables, 4 applications, 9 sources.

Object of elaboration: Information Security Policy for information and telecommunication system of "Rubin" LLC.

Project Objective: create a security policy for object of information activities.

The first section describes the object: type of activity, information system, equipment, software, information flows. Also, the information that is processed in the ITS has been classified, list of the threat sources, list of vulnerabilities and list of threats that are relevant for ITS have been created and analysis of WiMAX technology. WiMax technology analysis has also been performed

In the second section has been described an existing security profile and selected the new security profile for the company, also have been developed recommendations for ensuring information security of the object of information activity.

In the third section, the costs for implementation and annual support of the security policy have been calculated. In addition, the economic feasibility of commissioning the security policy guidelines, developed in the second section, has been calculated.

The practical significance of the project is to increase the level of information security of "Rubin" LLC.

SECURITY POLICY, MODEL OF THREATS, INFORMATION SECURITY, VULNERABILITIES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ТОВ – товариство з обмеженою відповідальністю;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

ОІД – об'єкт інформаційної діяльності;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

WiMAX – (рису) — телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях

ЗМІСТ

ВСТУП

З розвитком технологій дротяні комп'ютерні мережі стали менш зручні по ряду багатьох чинників, основним з яких є мобільність. На зміну їм прийшов розвиток безпровідних мереж.

Першими кроками по створенню безпровідних мереж стало виникнення окремих точок доступу Wi-Fi з підключенням до потужних магістральних "дротяних" мереж, наприклад, до оптоволоконних. Надалі з'явився новий клас провайдерів, що розвернули множинні комерційні мережі, внаслідок чого всього лише за декілька років мережі Wi-Fi виросли в серйозні інфраструктури - корпоративні і прилюдні. До справжнього моменту багато готелів, аеропорти і вокзали світу володіють покриттям Wi-Fi мережами, а в деяких країнах таким чином забезпечується покриття цілих мікрорайонів.

Безумовно, впровадження безпровідних мереж Wi-Fi мереж стало революційним вирішенням "зв'язку останньої милі". Проте обмеження за швидкістю обміну, що спочатку були в стандарті, даними, радіусу дії, кількості каналів і дорожнечі інфраструктури доки не дозволили стати мережам Wi-Fi тотальною загрозою стільниковим мережам з одного боку і дротяним мережам з іншою. Навіть не дивлячись на значні переваги і введення нових, сучасніших версій стандарту "природні обмеження" Wi-Fi будуть зняті лише за допомогою нових магістральних стандартів обміну даними. Таким як WIMAX.

WiMax (Worldwide Interoperability for Microwave Access) — комерційна назва міжнародного стандарту безпровідної широкосмугової передачі даних 802.16, розробленого Інститутом інженерів в області електроніки і електротехніки (IEEE). Головна мета організації — сприяти розробці безпровідного устаткування для доступу до широкосмугових мереж, швидкий розвиток мереж у всьому світі і сертифікація устаткування стандарту 802.16. Мережі WiMAX схожі з мережами для стільникових телефонів, але на відміну від їх базові станції WiMax можуть

забезпечувати широкосмуговий зв'язок в радіусі більш ніж 30 км., а пропускна спроможність може складати до 75 Мбіт/с, практично як і мережа на кабельній основі. З'єднання працює стабільно навіть за відсутності прямої видимості базової станції за рахунок використання відбитого сигналу. Це унікальна властивість дає можливість підтримувати стабільний високошвидкісний канал в умовах щільної міської забудови. По використанню частотного ресурсу WiMAX випереджає конкурентів в 1,5 разу, тобто стабільна одночасна робота, що гарантується, для великої кількості користувачів, що не заважають один одному. Що стосується шифрування, то тут використовується алгоритм AES з довжиною ключа 128, 192 та 256 біт або RSA з довжиною ключа 1024 біта, які забезпечують відмінне протистояння спробам злому. WiMax базується на алгоритмі планерування, який полягає в тому, що клієнт, що звертається до базової станції, одного разу отримує власний тимчасовий слот, що залишається за ним, навіть якщо обмін даними не відбувається. Це забезпечує можливість гарантувати пропускну спроможність каналу шляхом автоматичного управління параметром QOS (Quality of Service). WiMax дозволяє здійснювати передачу різних даних, у тому числі голоси, відео і іншого, тим самим забезпечуючи можливість швидко організувати корпоративні мережі, якісні відеотрансляції і IP-телефонію. Технологія WiMax дає можливість вирішити, одну з найсерйозніших проблем доступу до Інтернету — проблему «останньої милі».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд розвитку безпровідних систем

По радіусу дії і призначенню сучасні безпровідні мережі можна розділити на персональних (Wireless Personal Area Network, WPAN), локальних (Wireless Local Area Network, WLAN), міських (Wireless Metropolitan Area Network, WMAN) і глобальних (Wireless Wide Area Network, WWAN)

Персональні мережі (WPAN) служать, перш за все для зв'язування між собою компонентів комп'ютера в межах малого радіусу дії — в так званій персональній зоні. Проте WPAN-сети потрібні не лише для підключення комп'ютерної периферії: у міру того як зростає кількість пристроїв, що підключаються до мережі, все актуальніше стає проблема їх безпровідного з'єднання в персональній зоні.

До категорії WPAN відноситься цілий ряд технологій. Найстарішої з технологій передачі даних в межах малого радіусу дії є IRDA — технологія передачі даних в інфрачервоному діапазоні, яка просувається на ринку асоціацією Infrared Data Association, а стандарт IRDA був розроблений ще в 1993 році. Ця технологія дозволяє передавати дані в межах вільного від перешкод простору невеликого радіусу. Найбільш сучасною (і в даний час масовою) є технологія Bluetooth. Для встановлення безпровідного з'єднання Bluetooth пряма видимість між пристроями не потрібна, на відміну від інфрачервоного зв'язку.

Історія Bluetooth почалася в 1994 році з проекту шведської компанії Ericsson по розробці системи локального безпровідного зв'язку радіотелефону з різними аксесуарами типу телефонної гарнітури. У травні 1998 року Ericsson, IBM, Intel,

Toshiba і Nokia оголосили про створення спеціальної робочої групи Bluetooth SIG (Bluetooth Special Interest Group) з метою просування і розвитку цієї технології. Радіозв'язок Bluetooth здійснюється в діапазоні 2,4-

2,48 ГГц. Спектр сигналу формується по методу FHSS (Frequency Hopping Spread Spectrum — широкосмуговий сигнал по методу частотних стрибків), згідно з яким частота сигналу, що несе, стрибкоподібно міняється 1600 разів в секунду. Послідовність перемикання між частотами для кожного з'єднання відома лише передавачу і приймачу, що дозволяє забезпечити конфіденційність передачі даних і виключити перешкоди, якщо поруч працюють декілька пар «приймач — передатчик». Bluetooth забезпечує обмін інформацією між такими пристроями, як ПК, ноутбуки, PDA, мобільні телефони, принтери і цифрові фотоапарати, в радіусі від 10 до 100 м один від одного і навіть в різних приміщеннях.

ZigBee — безпровідна мережна технологія короткого радіусу дії, що базується на стандарті IEEE 802.15.4. Дана технологія була розроблена з метою забезпечення дешевшого і менш енергоємного рішення в порівнянні з іншими WPAN-технологиями, зокрема з Bluetooth. Для забезпечення сумісності пристроїв даного класу в 2002 році за ініціативою компанії Philips був утворений Альянс ZigBee (ZigBee Alliance), в який сьогодні входять компанії з 22 країн. Протоколи ZigBee розроблені з врахуванням максимального енергозбереження: велику частину часу пристрою знаходяться в сплячому режимі і лише зрідка перевіряють, чи поступили до них звернення. Дальність зв'язку між двома апаратами — до 75 м.

Ultrawideband (UWB) — надширокосмуговий зв'язок — отримала таку назву завдяки тому, що в цьому стандарті використовується найширший з поширених сьогодні технологій діапазон частот. Ця безпровідна технологія призначена для передачі даних на короткі (до 10 м) відстані з високою пропускною спроможністю (до 480 Мбіт/с) і низькою споживаною потужністю. UWB забезпечує передачу відео між пристроями побутової електроніки і периферійними пристроями ПК. Одна з основних переваг цієї технології полягає в тому, що вона не створює перешкод для інших безпровідних технологій, використовуваних в даний час, — таких як Wi-Fi, WIMAX і стільниковий зв'язок.

Технології WLAN базуються на сімействі стандартів 802.11. Багато організацій і домашні користувачі використовують Wi-Fi (Технології WLAN, що базуються на сімействі стандартів 802.11, часто позначають терміном Wi-Fi. Спочатку даний термін був введений організацією Wi-Fi Alliance, для позначення продуктів серії стандарту 802.11b, однак сьогодні цей термін застосуються для продуктів, відповідних будь-якому стандарту з сімейства 802.11) як альтернативу дротяним локальним мережам . Окрім безпровідних домашніх і офісних мереж технологія Wi-Fi знайшла широке застосування у сфері організації публічного доступу в Інтернет. Залежно від конкретного стандарту мережі Wi-Fi працюють на частотах 2,4 або 5 ГГц і забезпечують швидкість передачі даних до 54 Мбіт/с. Зону безпровідного доступу на базі декількох хот-спотов називають хот-зоной. Радикальне збільшення пропускної спроможності дає стандарт 802.11n, з появою якого пропускна спроможність WLAN буде збільшена відразу у декілька разів.

Для організації єдиної широкосмугової безпровідної мережі (міські безпровідні мережі (WMAN)), що працює на великих відстанях, був розроблений і запропонований стандарт IEEE 802.16, названий WIMAX-Worldwide Interoperability for Wicrowave Access (міжнародна взаємодія для мікрохвильового доступу).

WIMAX відноситься до технології Wireless MAN, яка може з'єднуватися з точками доступу стандарту IEEE 802.11 (Wi-Fi). WIMAX є альтернативою прокладенню кабелю або лінії DSL при організації останньої милі.

У 2001 році Міжнародним інститутом електроніки і електротехніки (IEEE- Institute of Electrical and Electronics Engineers) була прийнята перша версія стандарту IEEE 802.16, в якому були описані лише загальні принципи мережі

і робочий діапазон 10-66 ГГц. Потім в 2002 і 2003 роках були прийняті доповнення в особі стандартів IEEE 802.16c (робочий діапазон 10-66 ГГц) і IEEE 802.16a (2-11 ГГц) .У вересні 2003 року була створена робоча група, яка приступила до створення стандарту IEEE 802.16d. І 24 червня 2004 року

новий стандарт був затверджений, а був опублікований 1 жовтня 2004 року. Він передбачає вживання частотного діапазону 2-11 ГГц. Максимальна швидкість передачі інформації при цьому може досягати 70 Мбіт/с при ширині каналу в 20 Мгц, а радіус дії - 50 кілометрів у відсутності прямої видимості. Правда, це теоретичні значення, які можуть бути отримані за ідеальних умов, і на практиці пропускна спроможність мереж WIMAX і зона покриття будуть менші.

У 2005 році була розроблена специфікація мобільної версії WIMAX для пристроїв, що переміщаються з швидкістю до 120 км/ч. Портативне обладнання WIMAX використовує частотний діапазон від 2 до 6 ГГц, проте швидкість передачі даних (20 Мбіт/с) і радіус дії будуть менші, ніж в апаратури стандарту IEEE 802.16d. Зв'язано це з обмеженнями, що накладаються на потужність передавачів, габарити мобільних пристроїв і їх енергоспоживання.

Новий стандарт отримав кодове найменування IEEE 802.16e і поповнив серію технологій для побудови безпровідних широкосмугових мереж.

Завдяки своїм перевагам (можливість забезпечення широкосмугового зв'язку в умовах відсутності прямої видимості, велика зона покриття, висока якість послуг, що надаються, простота побудови мережі, а отже менші витрати) технологія WIMAX вважається найбільш перспективною при переході до мереж четвертого покоління (4G).

1.2 Технологія WIMAX

WIMAX (Worldwide Interoperability for Microwave Access) - це некомерційне об'єднання, створене при активній участі Intel, а також близько 30 провідних виробників телекомунікаційного обладнання. Діяльність WIMAX спрямована на усунення несумісності розгортаних мереж стандартів 802.11. При цьому члени ініціативної групи бачать вирішення багатьох проблем в просуванні і популяризації нового стандарту

802.16, який, на їх думку, повинен органічно доповнити собою сімейство Wi-Fi.

Спочатку IEEE 802.16 розроблявся для організації безпровідних мереж в умовах неосяжних просторів мегаполісів. Багато хто плутав найменування WIMAX, Wi-Fi, об'єднання групи розробників і самого стандарту, а тому для сімейства 802.16 було вигадано спеціальну назву, що запам'ятовується, - WMAN (Wireless Metropolitan Area Network - мережа для міських регіонів). WMAN - порівняно нова розробка 2001 року.

Переваги стандарту 802.16:

1 Мережа стандарту 802.16 проста в розгортанні і нарощуванні площі покриття.
2 Базові станції мережі діють в радіусі до 50 кілометрів, не вимагаючи зведення спеціальних веж для установки (підходять дахи будинків або інші існуючі висотні споруди, оскільки приймаючий і передавальний пристрої доки функціонують не лише в зоні прямої видимості).
3 Безперечною перевагою широкосмугового доступу перед DSL є можливість швидко придбати і налагодити все необхідне обладнання, а також оперативно розвернути зону безпровідного доступу.
4 Смуга пропускання стандарту досягає 70 Мбіт/секунду.
5 Одна базова станція WMAN здібна обслуговувати велике число користувачів, надаючи більш ніж прийнятну якість і швидкість з'єднання (60 чоловік - 2 Мб/с).
6 Робоча смуга частот стандарту складає 2-11 ГГц, дозволяючи застосовувати зв'язок на великих відстанях.
7 Можливість організації роумінгу між різними мережами 802.16, а також Wi-Fi і іншими безпровідними стандартами (по аналогії із стільниковим мобільним зв'язком).

Головне, що необхідно мати на увазі, - WMAN як стандарт не є заміною або аналогом Wi-Fi. Корпорація Intel позиціонує його як доповнення 802.11 для вирішення проблеми "останньої милі" в містах між провайдерами і

користувачами. Wi-Fi де виступатиме в ролі ланки єдиного ланцюга, що зв'язує абонентів 802.16 з мережами інших стандартів по всьому світу.

1.3 Особливості структури мереж WIMAX

Локальні мережі Wi-Fi можуть обслуговувати клієнтів в окремому приміщенні і як максимум – в окремій будівлі середніх габаритів, а локальні мережі WiMax можуть обслуговувати клієнтів декількох десятків будівель в радіусі від 1 до 5 кілометрів.

Радіус дії мережі WiMax залежить від:

— Швидкості передачі даних, тобто чим вище швидкість передачі, тим менше радіус дії.
— Архітектурно-географічних особливостей місцевості (наприклад, ступінь радіо прозорості будівель).
— Умови розміщення антен – приймачів.
— Від кількості частот, використовуваних даною конкретною технологічною системою WiMax (наприклад, в системі Expidience мережі Synterra WiMax використовується 1024 піднесущих частоти, тоді як базова система має лише 256 частот).

Стандарт 802.16e передбачає мобільність, тобто він підтримуватиме такі пристрої, як ноутбуки, КПК, а також стільникові телефони. Компанії такі як Accton, Gemtek, Zyxel та інші, з третього кварталу 2007 року виробляють WiMax-оборудование для мобільного застосування.

1.4 Принцип роботи WIMAX

Система WIMAX складається з двох основних частин.

— Базова станція WIMAX, може розміщуватися на висотному об'єкті: будівлі або вишці.
— Приймач WIMAX: антена з приймачем, у форм-факторі карти PC Card, карти розширення ПК або зовнішньої карти.

Для з'єднання базової станції і клієнтського устаткування використовується високочастотний діапазон від 2 до 11 ГГц. У ідеальних умовах швидкість обміну даними може досягати 70 Мбіт/с, при цьому не вимагається забезпечення прямої видимості між базовою станцією і приймачем.

Як вже говорилося вище, WIMAX застосовується як для вирішення проблеми «останньої милі», так і для надання доступу в мережу офісним і районним мережам.

Між базовими станціями встановлюється з'єднання (прямій видимості), що використовують діапазон частот від 10 до 66 ГГЦ, швидкість обміну даними може досягати 120 Мбіт/с. При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних провідних з'єднань. Фактично, ніж більше число БС підключене до мереж провайдера, тим вище швидкість передачі даних і надійність мережі в цілому.

По структурі мережі стандарту IEEE 802.16 дуже схожі на традиційні мережі мобільного зв'язку: тут теж є базові станції, які діють в радіусі до 50 км., при цьому їх також не обов'язково встановлювати на вишках - для них цілком підходять дахи будинків, потрібне лише дотримання умови прямої видимості між станціями. Для з'єднання базової станції з користувачем необхідна наявність абонентського устаткування. Далі сигнал може поступати по стандартному Ethernet-кабелю, як безпосередньо на конкретний комп'ютер, так і на точку доступу стандарту 802.11 Wi-Fi або в локальну провідну мережу стандарту Ethernet.

Це дозволяє зберегти існуючу інфраструктуру районних або офісних локальних мереж при переході з кабельного доступу на WIMAX. Це дозволяє також максимально спростити розгортання мереж, дозволяючи використовувати знайомі технології для підключення комп'ютерів.

1.5 Режими роботи мереж WiMAX

Стандарт 802.16e увібрав в себе всі версії, що раніше виходили, і на даний момент надає наступні режими.

— Fixed WIMAX - фіксований доступ;

— Nomadic WIMAX - сеансовий доступ;

— Portable WIMAX - доступ в режимі переміщення;

— Mobile WIMAX - мобільний доступ.

***Fixed** WIMAX*. Фіксований доступ є альтернативою широкосмуговим провідним технологіям (xDSL, T1, и т.п.). Стандарт використовує діапазон частот 3-66 ГГц. Цей частотний діапазон із-за сильного загасання коротких хвиль вимагає прямої видимості між передавачем і приймачем сигналу. З іншого боку, даний частотний діапазон дозволяє уникнути однієї з головних проблем радіозв'язку - багатопроменевого поширення сигналу. При цьому ширина каналів зв'язку в цьому частотному діапазоні досить велика (типове значення - 25 або 28 Мгц), що дозволяє досягати швидкостей передачі до 120 Мбіт/с. Фіксований режим включався у версію стандарту 802.16d і вже використовується у ряді країн. Проте більшість компаній, що пропонують послуги Fixed WIMAX, чекають швидкого переходу на портативний і надалі мобільний WIMAX.

***Nomadic** WIMAX*. Сеансовий (кочівний) доступ додав поняття сесій до вже існуючому Fixed WIMAX. Наявність сесій дозволяє вільно переміщати клієнтське устаткування між сесіями і відновлювати з'єднання вже за допомогою інших веж WIMAX, ніж тих, що були використані під час попередньої сесії. Такий режим розроблений в основному для портативних пристроїв, таких, як ноутбуки, КПК.

***Portable** WIMAX*. Для режиму Portable WIMAX додана можливість автоматичного перемикання клієнта від однієї базової станції WIMAX до іншої без втрати з'єднання. Проте для даного режиму все ще обмежена швидкість пересування клієнтського устаткування - 40 км/ч. Втім, вже у такому вигляді можна використовувати клієнтські пристрої в дорозі (у

автомобілі при русі по житлових районах міста, де швидкість обмежена, на велосипеді, рухаючись пішки, т.д.). Введення даного режиму зробило доцільним використання технології WIMAX для смартфонів і КПК. У 2006 році початий випуск пристроїв, що працюють в портативному режимі WIMAX.

Mobile *WIMAX* був розроблений в стандарті 802.16e і дозволив збільшити швидкість переміщення клієнтського устаткування більше 120 км/ч. Також реалізована можливість безшовного переходу між базовими станціями.

Основними досягненнями мобільного режиму вважається нижчеприведені чинники.

1 Стійкість до багатопроменевого розповсюдження сигналу і власних перешкод.

2 Масштабована пропускна спроможність каналу.

3 Технологія Time Division Duplex (TDD), яка дозволяє ефективно обробляти ассиметричний трафік і спрощує управління складними системами антен за рахунок естафетної передачі сесії між каналами.

4 Технологія Hybrid-Automatic Repeat Request (H-ARQ), яка дозволяє зберігати стійке з'єднання при різкій зміні напряму руху клієнтського обладнання.

5 Розподіл частот, що виділяються, і використання субканалів при високому завантаженні дозволяє оптимізувати передачу даних з врахуванням сили сигналу клієнтського обладнання.

6 Управління енергозбереженням дозволяє оптимізувати витрати енергії на підтримку зв'язку портативних пристроїв в режимі очікування або простою.

7 Технологія Network-Optimized Hard Handoff (HHO), яка дозволяє до 50 мілісекунд і менш скоротити час на перемикання клієнта між каналами.

8 Технологія Multicast and Broadcast Service (MBS), яка об'єднує функції DVB-H, MEDIAFLO і 3GPP E-UTRA для:

— досягнення високої швидкості передачі даних з використанням одночастотної мережі;

— гнучкого розподілу радіочастот;

— низького споживання енергії портативними пристроями:

— швидкого перемикання між каналами.

9 Технологія Smart Antenna, що підтримує субканали і естафетну передачу сесії між каналами, що дозволяє використовувати складні системи антен, включаючи формування діаграми спрямованості, простанственно-часову маркіровку, просторове мультиплексування (ущільнення).

10 Технологія Fractional Frequency Reuse, яка дозволяє контролювати наложение/пересечение каналів для повторного задіювання частот з мінімальними втратами.

11 Розмір фрейма в 5 мілісекунд створює оптимальний компроміс між надійністю передачі даних за рахунок використання малих пакетів і накладними витратами за рахунок збільшення числа пакетів (і як наслідок, заголовків).

1.6 Порівняння WiFi і WiMAX

Відмінності закладені в групі стандартів 802.16, на основі яких створюється обладнання і будуються мережі WIMAX. Розробники вказали на декілька принципових рис, що відрізняють 802.16 від 802.11, на якому працює Wi-Fi .

По-перше, з точки зору протоколу зв'язку група стандартів 802.16 — операторського класу, вона генерує послугу з гарантованою якістю обслуговування в залежності, природно, від товщини гаманця клієнта.

По-друге, стандарт WIMAX забезпечує високу перешкодостійкість, дальність і надійність передачі за рахунок OFDM — ортогональній частотній модуляції (або мультиплексування). Це дозволяє з будь-якого каналу здобувати велику пропускну спроможність на межі Шенона. Розробники роз'яснили механізм роботи OFDM. При її використанні канал оцінюється і ортогональними перетвореннями на передавальному і приймальному кінцях віртуально розбивається на паралельні канали. У них

«завантажується» такий потік даних, який вони спроможні передати. Причому ця здібність каналу до передачі оцінюється в кожен момент часу. Такий підхід приводить до серйозного виграшу в швидкості передачі інформації на межі Шенона, в 10 і більше разів.

Таблиця 1.1 – Порівняння від WiFi з WiMAX

	802.11	802.16a	802.16e
Сфера застосування	Локальні мережі	Міські мережі	Міські мережі
Дальність дії	До 100 м; оптимальний для локальної мережі всередині будівлі	До 50 км.	До 8 км.
Умови зв'язку	Поза приміщеннями –в межах прямої видимості	Поза межами прямої видимості	Поза межами прямої видимості
Діапазон	2,4 і 5 ГГц	від 2до 11 ГГц	від 2 до 6 ГГц
Підтримка мобільності	Локальний роумінг для переносних пристроїв	Стаціонарний	Регіональний роумінг –мобильность при пересуванні до 120км/г.
Поділ по каналах	20 Мгц	Що налаштовується від 1,5 до 20 Мгц	Що налаштовується від 1,5 до 5 Мгц з підканалами
Спектральна ефективність	до 2,7 (біт/с) /Гц	до 3,75 (біт/с)/Гц	до 3 (біт/с) /Гц
Швидкість передачі даних	54 Мбіт/с(смуга 20 Мгц)	до 75 Мбіт/с (смуга 20 Мгц)	до 15 Мбіт/с(смуга 5МГц)

По-третє, в WIMAX використані технології «розумних антен», що дають великий виграш по перешкодостійкості завдяки можливості стеження антеною за абонентом і концентрації енергії у напрямі руху абонента.

Розробники підкреслили незмінність наступного принципу: будь-яка передача інформації влаштована так, що відбувається обмін швидкості на перешкодостійкість. Принцип Шенона свідчить: підвищуємо швидкість — зменшуємо дальність. Простіше кажучи, щоб передавати по каналу більше

інформації, потрібно збільшувати відношення сигнал/шум в точці прийому. Наскільки підвищили перешкодостійкість і швидкість, настільки ж слід збільшити відношення сигнал/шум. Принцип OFDM, що полягає в розбитті на постійні паралельні віртуальні канали будь-якого каналу, що змінюється, і в потужному перешкодостійкому кодуванні, дозволяє досягти цієї пропускної спроможності на межі Шенона. Причому йде постійне підстроювання під характеристики каналу. У стандартах 802.11a і 802.11g в мережах Wi-Fi немає такої динамічної оцінки параметрів каналу, а саме вона і дає основний ефект. Поважно відзначити, що в стандарті WiMAX досягаються теоретичні межі Шенона за швидкостями передачі даних.

В результаті технологія WiMAX і стандарт 802.16 дозволяють передавати інформацію на пристрої, по габаритах такі ж, як і пристрої Wi-Fi, але тільки із швидкістю на два-три порядки вище. Треба сказати, що стандарт 802.16 також еволюціонує. Спочатку був просто 802.16, потім з'явилися 802.16a і 802.16b, потім випущений 802.16d для фіксованого доступу. І нарешті виник стандарт 802.16e для мобільного доступу, так званий мобільний WIMAX.

У фіксованого і мобільного WIMAX багато спільного, але є і відмінності. У них різна довжина кадрів (пакетів) OFDM, різні діапазони частот: у фіксованого — 3,5, а деколи і 5,8 ГГц, в мобільного — 2 ГГц.

802.11 — стандарт класу LAN, локальних мереж з демократичною процедурою розподілу доступу. І тут діє принцип «хто перший встав, того і тапки». Сама ідеологія побудови Wi-Fi-сетей — не операторська. Дійсно, процедура заняття каналу в мережах Wi-Fi така ж, як і в звичайних стандартах локальної мережі. Не можна розділити користувачів на групи по рівню надання гарантованої якості послуги (тобто Quality-of-Service), що зроблене в мережах WIMAX: більше заплатив — гарантовано отримаєш більший ресурс, менше заплатив — менший. У мережі Wi-Fi робота йде, як і в звичайній локальній, як правило, при великому запасі пропускної спроможності, коли мережа далека від пікового навантаження, тобто коли число одночасно працюючих абонентів невелике. Якщо m — загальне число

абонентів, а M — число активних, то ці мережі ефективно працюють при малій величині відношення M/m. Але так буває не завжди, особливо в місцях колективного доступу в Мережу. І якщо в місцях де є наплив любителів безпровідного зв'язку з ноутбуками, мережа, виражаючись мовою зв'язківців, «ляже». Тому мережі Wi-Fi завжди мають бути розраховані з серйозним запасом, аби зберігати працездатність в умовах пікового навантаження.

Wi-Fi мають досить обмежену площу покриття базової станції Wi-Fi|. Фахівці WiMAX провели нескладний розрахунок. Припускатимемо, є рішення|вирішення| покривати територію міста базовими станціями Wi-Fi|. При цьому слід врахувати, що зазвичай|звично| одна станція Wi-Fi| забезпечує дальність зв'язку 50—100 м. Якщо приблизно представити| уявляти| площу покриття у вигляді квадрата 20х20 км., а радіус соти Wi-Fi| прийняти 50х50 м, то для забезпечення зв'язку по Wi-Fi| буде потрібно 160 тис. базових станцій.

1.7 Технічна характеристика стандарту IEEE802.16

Зі всього різноманіття стандартів сімейства IEEE 802.16 ми зупинимося на двох: IEEE 802.16-2004 і IEEE 802.16e .

Перший стандарт описує фізичний рівень і MAC- (Media Access Control- управління доступом до середовища передачі) рівень для фіксованих мереж високошвидкісного безпровідного доступу FBWA (Fixed Broadband Wireless Access). Другий стандарт є доповненням до першого для забезпечення мобільності.

Фізичний рівень

Основними вузлами мережі за стандартом IEEE 802.16 є базова станція (Base Station) і призначена для користувача станція (Subscriber Station).

Передбачено дві топології взаємодії між вузлами мережі : «крапка-багатокрапка» PMP (Point-to-MultiPoint), при якій кожна призначена для користувача станція взаємодіє зі своєю базовою станцією і комірчаста

(Mesh), при якій призначені для користувача станції можуть взаємодіяти між собою. Перша топологія має на увазі стільникову структуру організації зони покриття мережі. При цьому не виключений простіший спосіб організації зв'язку - "крапка-крапка".

Стандарт IEEE 802.16 описує чотири фізичні рівні:

— Single Carrier (WIRELESSMAN-SC) - символи модуляції передаються на частоті -, що несе, орієнтований на роботу в умовах прямого поширення сигналу на частоті що несе в діапазоні 10-66 ГГц;

— Single Carriera (WirelessMAN-SCa) - модифікація WIRELESSMAN-SC- для роботи в умовах непрямого поширення сигналу на частоті до 11 ГГц;

— Orthogonal Frequency Division Multiplexing (WIRELESSMAN-OFDM) – символи модуляції передаються на безлічі тих, що піднесуть з використанням технології OFDM – призначений для роботи в умовах непрямого розповсюдження сигналу на частоті до 11 ГГц;

— Orthogonal Frequency Division Multiple Access (WIRELESSMAN-OFDMA) - численний доступ з частотно-тимчасовим розділенням з використанням технології OFDM- призначений для роботи в умовах непрямого розповсюдження сигналу на частоті до 11 ГГц.

Таблиця 1.2 – Основні режими в стандарті IEEE 802.16-2004

Режим	Частотний	Опції	Метод
WirelessMAN-SC	10–66		TDD / FDD
WirelessMAN-SCa	< 11	AAS / ARQ / STC /	TDD / FDD
WirelessMAN-OFDM	< 11	AAS / ARQ / STC / Mesh	TDD / FDD
WirelessMAN-OFDMA	< 11	AAS / ARQ / STC /	TDD / FDD
WirelessHUMAN	<11	DFS / AAS /ARQ / Mesh /STC	TDD

Де - ARQ (automatic repeat request) – автоматичний запит повторної передачі;

- AAS (adaptive antenna system) – робота з адаптивними антенними системами;

- STC (space time coding) – просторово-часове кодування;

- MESH – режим взаємодії АС один з одним;

- DFS (dynamic frequency selection) – режим динамічного розподілу частот.

WIRELESSMAN-SC

Фізичний рівень WIRELESSMAN-SC призначений для роботи в умовах прямого поширення сигналу на частоті що несе в діапазоні 10-66 ГГц.

Стандарт IEEE 802.16 жорстко не регламентує смугу частот для WIRELESSMAN-SC. Замість цього наведено три найбільш типових значення - 20, 25 і 28 Мгц.

Фізичний рівень WIRELESSMAN-SC підтримує два види дуплексу: частотний FDD (Frequency Division Duplex) і тимчасовою TDD (Time Division Duplex). В разі частотного дуплексу стандарт підтримує як повнодуплексні призначені для користувача станції: які можуть приймати і передавати одночасно, так і напівдуплексні призначені для користувача станції, які одночасно можуть або передавати, або приймати. Передача даних в прямому каналі (від базової станції до призначеної для користувача) і у зворотному напрямі має кадрову структуру. Стандарт регламентує три розміри кадру: 0.5, 1 і 2 мс.

Розглянемо детальніше структуру кадру. Він містить кадр прямого каналу, і кадр зворотного каналу. В разі частотного дуплексу кадри прямого і зворотного каналів передаються одночасно на різних частотах (рисунок.1.1).

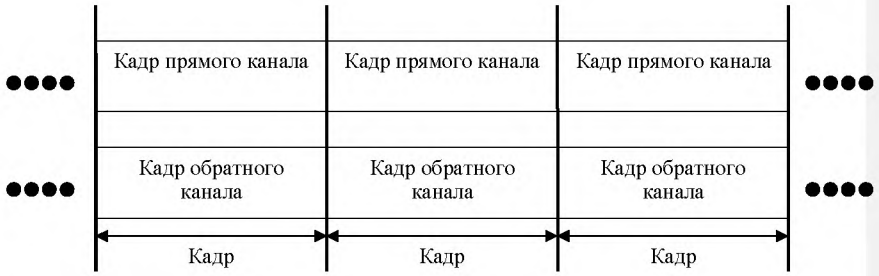

Рисунок 1.1 - Кадри прямого і зворотного каналів в разі частотного дуплексу

При використанні тимчасового дуплексу в кадрі спочатку передають кадр прямого каналу, а за ним кадр зворотного каналу (Рисунок 1.2.). При цьому кадр має фіксований розмір, а долі кадру, займані кадрами прямого і зворотного каналів, можуть адаптивний мінятися від кадру до кадру.

Рисунок 1.2 - Кадри прямого і зворотного каналів в разі тимчасового дуплексу

В разі частотного дуплексу кадр прямого каналу має структуру, показану на рисунку 1.3.

Кадр прямого каналу при використанні частотного дуплексу включає наступні основні елементи: преамбулу кадру прямого каналу; DL-MAP (Dowlink Map) - розклад кадру прямого каналу; UL-MAP (Uplink Map) - розклад кадру зворотного каналу; TDM-частина; TDM-пакети з призначеними для користувача даними; TDMA-частина; TDMA-пакети з

призначеними для користувача даними, перед кожним з яких передається преамбула.

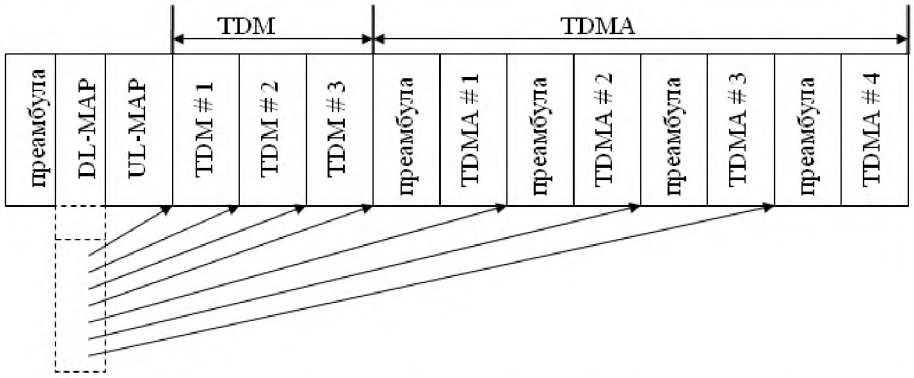

Рисунок 1.3 - Структура кадру прямого каналу в разі частотного дуплексу

Дані різних призначених для користувача станцій в прямому каналі розділяються за часом. При цьому передбачено два підходи: TDM (Time Division Multiplexing) - тимчасове мультиплексування; TDMA (Time Division Multiple Access) - множинний доступ з тимчасовим розділенням. Останній підхід передбачений для підтримки напівдуплексних станцій.

Повідомлення DL-MAP задає розклад пакетів різних користувачів всередині кадру прямого каналу, а повідомлення UL-MAP- всередині кадру зворотного каналу.

Преамбули служать для вимірювань, частотно-тимчасової синхронізації і оцінки каналу.

В разі тимчасового дуплексу кадр прямого каналу має структуру, показану на малюнку. Вона простіша, оскільки відсутня TDMA-частина. Доданий часовий інтервал TTG (Transmit/Receive Transition Gap) - захисний інтервал, призначений для перебудови від передачі до прийому (на базовій станції) і від прийому до передачі (на призначеній для користувача станції).

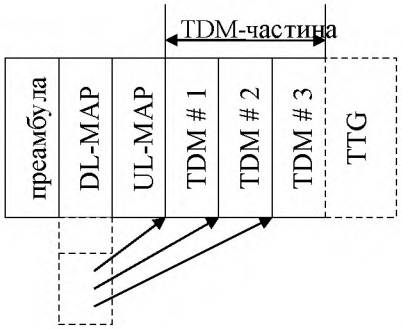

Рисунок 1.4 - Структура кадру прямого каналу в разі тимчасового дуплексу

Структура кадру зворотного каналу показана на малюнку.. Вона практично однакова для частотного і тимчасового дуплексу. Відмінність полягає в наявності тимчасового інтервалу RTG (Receive/Transmit Transition Gap) - захисного інтервалу, призначеного для перебудови від прийому до передачі (на базовій станції) і від передачі до прийому (на призначеній для користувача станції).

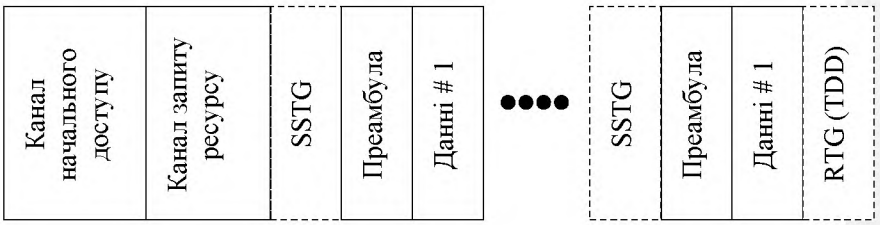

Рисунок 1.5 - Структура кадру зворотного каналу

Кадр зворотного каналу включає наступні основні елементи: канал початкового доступу; канал запиту частотно-тимчасового ресурсу; пакети з призначеними для користувача даними . Останні складаються з SSTG (Subscriber Station Transition Gap) - захисного тимчасового інтервалу між пакетами різних призначених для користувача станцій;

преамбули; призначених для користувача даних; тимчасового інтервалу RTG (лише в разі тимчасового дуплексу).

Тривалість каналу початкового доступу м каналу запиту частотно-тимчасового ресурсу, а так само розклад пакетів з призначеними для користувача даними задає повідомлення UL-MAP поточного або одного з попередніх кадрів прямого каналу.

Фізичний рівень WIRELESSMAN-SC стандарту IEEE 802.16 визначає чотири схеми кодування: код Рида-Соломона (Reed-Solomon Code);код Рида-Соломона і блоковий згортальний код (Block Convolutional Code); код Рида-Соломона і перевірка парності (Parity Check); блоковий турбокод (Block Turbo Code). Передбачено три види модуляції: QPSK; 16-QAM; 64-QAM. Декілька схем кодування і видів модуляції дозволяють здійснювати адаптивне кодування і модуляцію.

Канальні швидкості передачі для розміру кадру 1мс і трьох рекомендованих смуг частот для фізичного рівня WIRELESSMAN-SC приведені в таблиці 1.3.

Таблиця 1.3 Канальні швидкості передачі для WIRELESSMAN-SC

Смуга частот, Мгц	Швидкість передачі, QPSK, Мбіт/с	Швидкість передачі 16-QAM, Мбіт/с	Швидкість передачи,64-QAM, Мбіт/с
20	32	64	96
25	40	80	120
28	44.8	89.6	134.4

Для роботи стандарт передбачає початкову і періодичну частотно-тимчасову синхронізацію. Передбачається, що вона здійснюється по сигналу базової станції.

Також передбачено регулювання потужності призначеної для користувача станції .

Для адаптивного кодування і модуляції, а також для регулювання потужності стандарт IEEE 802.16 передбачає періодичні виміри рівня сигналу, що приймається, а також стосунки сигнал/(шум + перешкоди).

WIrelessMAN-SCA

Фізичний рівень WirelessMAN-SCa призначений для роботи в умовах не прямого розповсюдження сигналу на частоті до 11 ГГц.

Передбачені наступні схеми кодування : код Ріда-Соломона + перемежитель + спільне кодування і модуляція із змінною швидкістю на основі згортальної коди (rate-compatible TCM from K=7, R=1/2 CC); кодування відсутнє; блоковий турбокод; згортальний код.

Передбачені наступні види модуляції: BPSK з розширенням спектру; BPSK;QPSK; 16-QAM; 64-QAM; 256-QAM.

У структуру кадру додані пілотні символи для оцінки каналу; є можливість повторної передачі (ARQ); передбачена рознесена передача на основі просторово-часових код; існує підтримка адаптивних антенних систем.

WIRELESSMAN-OFDM

Фізичний рівень WIRELESSMAN-OFDM призначений для роботи в умовах не прямого поширення сигналу на частоті до 11 ГГц і заснований на технології OFDM.

OFDM-символ містить 256 піднесущих, з яких використовуються тільки 200 піднесущих. З них на 8 піднесущих передають пілот - сигнали, а останні використовують для передачі даних.

Стандарт IEEE 802.16 жорстко не регламентує смугу частот для WIRELESSMAN-OFDM. Замість цього приведені значення, одному з яких має бути кратна смуга частот: 1,25; 1,5; 1,75; 2 і 2,75 Мгц.

Фізичний рівень WIRELESSMAN-OFDM підтримує два види дуплексу: частотний і часовий. В разі частотного дуплексу стандарт підтримує як повнодуплексні призначені для користувача станції, так і напівдуплексні призначені для користувача станції.

Стандарт регламентує наступні розміри кадру для WIRELESSMAN-OFDM: 2,5; 4; 5; 8; 10; 12,5 і 20 мс.

Розглянемо детальніше структуру кадрів прямого і зворотного каналів для режиму «крапка-багатокрапка».

Кадр прямого каналу має структуру, показану на рисунку 1.6.

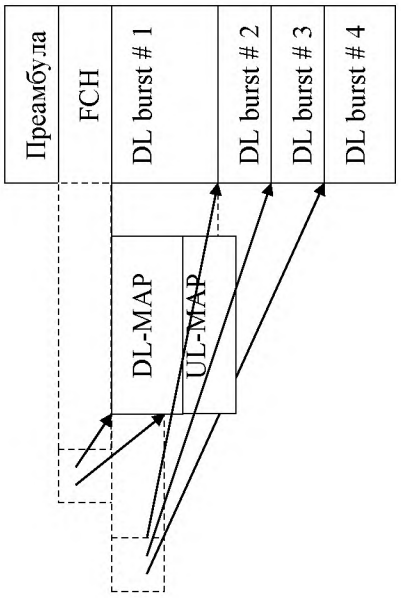

Рисунок 1.6 - Структура кадру прямого каналу

Кадр прямого каналу включає наступні основні елементи: преамбулу кадру прямого каналу; FCH(Frame Control Header) - заголовок кадру, вказуючий на місце розташування і вигляд кодування і модуляції повідомлень DL-MAP і UL-MAP; DL burst #1- перший пакет прямого каналу. Останній містить DL-MAP-розклад кадру прямого каналу; UL-MAP-розклад кадру зворотного каналу. DL burst #n- останні пакети прямого каналу.

Вигляд кодування і модуляції - однаковий всередині пакета прямого каналу і може мінятися від пакети до пакету. Пакет може містити дані, призначені як для одного, так і для різних користувачів.

Повідомлення DL-MAP задає розклад пакетів різних користувачів всередині кадру прямого каналу, а повідомлення UL-MAP- всередині кадру зворотного каналу.

Преамбула служить для вимірювань, частотно-тимчасової синхронізації і оцінки каналу.

Кадр зворотного каналу має структуру, показану на малюнку 1.7

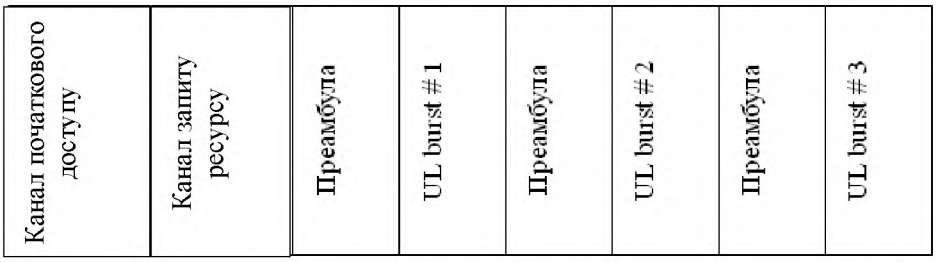

Рисунок 1.7 - Структури кадру прямого каналу

Кадр зворотного каналу включає наступні основні елементи: канал початкового доступу; канал запиту частотно-тимчасового ресурсу; пакети з призначеними для користувача даними. Останні включають: преамбулу, призначені для користувача дані.

Як і в попередніх фізичних рівнях, передбачені захисні інтервали для розділення кадрів прямого і зворотного каналів при використанні тимчасового дуплексу і для розділення пакетів зворотного каналу різних призначених для користувача станцій.

Тривалість каналу початкового доступу і каналу запиту частотно-тимчасового ресурсу, а так само розклад пакетів з призначеними для користувача даними задає повідомлення UL-MAP поточного або одного з попередніх кадрів прямого каналу.

Фізичний рівень стандарту IEEE 802.16 визначає три схеми кодування: код Ріда Соломона і блоковий згортальний код; блоковий

турбокод; згортальний турбокод (Convolutional Turbo Code). Передбачено чотири види модуляції: BPSK; QPSK; 16-QAM; 64-QAM. Декілька схем кодування і видів модуляції дозволяють здійснювати адаптивне кодування і модуляцію.

Канальні швидкості передачі для смуг 6, 7 і 20 Мгц для фізичного рівня WIRELESSMAN-OFDM, для циклічного префікса і для різних видів кодування і модуляції приведені в таблиці 1.4

Таблиця 1.4 – Канальні швидкості передачі для WIRELESSMAN-OFDM

Смуга частот, Мгц	BPSK 1/2	QPSK 1/2	QPSK 3/4	16-QAM 1/2	16-QAM 3/4	64-QAM 2/3	64-QAM 3/4
6	2,43	4,86	7,28	9,71	14,57	19,43	21,85
7	2,82	5,65	8,47	11,29	16,94	22,59	25,41
20	8,13	16,26	24,40	32,53	48,79	65,05	73,19

Стандарт передбачає початкову і періодичну частотно-тимчасову синхронізацію. Передбачається, що вона здійснюється по сигналу базової станції. Також є регулювання потужності призначеної для користувача станції.

Для адаптивного кодування, модуляції і для регулювання потужності стандарт IEEE 802.16 передбачає періодичні виміри рівня сигналу, що приймається, а також стосунки сигнал/(шум + перешкоди).

Існує можливість повторної передачі (ARQ), а також рознесена передача і підтримка адаптивних антенних систем.

WIRELESSMAN-OFDMA

Фізичний рівень WIRELESSMAN-OFDMA призначений для роботи в умовах не прямого розповсюдження сигналу на частоті до 11 ГГц.

Як численний доступ в прямому і зворотному каналах даний фізичний рівень використовує OFDMA (Orthogonal Frequency Division Multiple Access) - численний доступ з частотно-тимчасовим розділенням з використання технології OFDM.

OFDM-символ містить 2048 піднесущих, з яких для передачі використовується лише частина. З них що на частини піднесуть передають пілот-сигнали, а останні використовують для передачі даних.

Стандарт IEEE 802.16 жорстко не регламентує смугу частот для WIRELESSMAN-OFDMA. Замість цього приведені значення, одному з яких має бути кратна смуга частот: 1,25; 1,5; 1,75; 2 і 2,75 Мгц.

Фізичний рівень WIRELESSMAN-OFDMA підтримує два види дуплексу: частотний і часовий. В разі частотного дуплексу стандарт підтримує як повнодуплексні призначені для користувача станції, так і напівдуплексні.

Стандарт регламентує наступні розміри кадру для WIRELESSMAN-OFDMA: 2,5; 4; 5; 8; 10; 12,5 і 20 мс.

Кадри прямого і зворотного каналів можуть містити одну або більш зони (рисунок 1.8). Зони в основному відрізняються кількістю пілот-сигналів і схемами перемеження піднесущих.

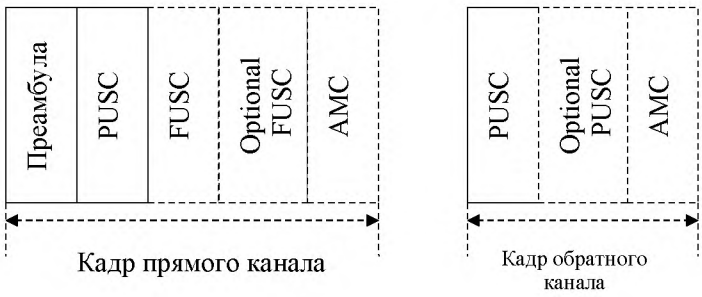

Рисунок 1.8 - Структура кадрів прямого і зворотного каналу

У прямому каналі можливі наступні зони:

— PUSC (Partial Usage of Subcarriers) - зона, що використовує те, що частотне розноситься при передачі і передбачає три частотні сегменти, при цьому базова станція може використовувати 1/3, 2/3 або всю смугу частот;

— FUSC (Full Usage of Subcarriers) - зона, що використовує те, що частотне розноситься при передачі і передбачає лише один частотний сегмент;
— Optional FUSC- відрізняється від зони FUSC лише кількістю пілот-сигналів;
— AMC (Adaptive Modulation and Coding) - зона, що не використовує того, що частотного розноситься (передбачається використання того, що розрахованого на багато користувачів розноситься).
— У зворотному каналі можливі наступні зони:
— PUSC- зона, що використовує те, що частотне розноситься при передачі і передбачає три частотні сегменти, при цьому базова станція може використовувати 1/3, 2/3 або всю смугу частот (для зворотного каналу);
— Optional PUSC- відрізняється від зони PUSC лише кількістю пілот-сигналів;
— AMC - зона, що не використовує того, що частотного розноситься (передбачається використання того, що розрахованого на багато користувачів розноситься).

Всі зони мають приблизно однакові логічні структури. Для прикладу розглянемо зону PUSC прямого каналу і зону PUSC зворотного каналу. При цьому передбачатимемо, що базова станція (сектор) використовує всю смугу частот. На рисунку 1.9. показана структура цих зон.

Зона PUSC прямого каналу включає наступні основні елементи:
— Преамбулу(оскільки це перша зона в кадрі прямого каналу);
— FCH- заголовок кадру, вказуючий на місце розташування і вигляд кодування і модуляції повідомлення DL-MAP;
— DL-MAP- розклад кадру прямого каналу;
— UL-MAP- розклад кадру зворотного каналу;
— DL burst #n- пакети прямого каналу.

Зона PUSC зворотного каналу містить пакети зворотного каналу.

DL-MAP задає розклад зон усередині кадру прямого каналу, а так само розклад пакетів даних усередині кожної зони прямого каналу. UL-MAP задає розклад зон усередині кадру зворотного каналу, а так само розклад пакетів даних усередині кожної зони зворотного каналу.

Зони PUSC і Optional PUSC зворотного каналу можуть містити канали початкового доступу і запиту частотно – часового ресурсу.

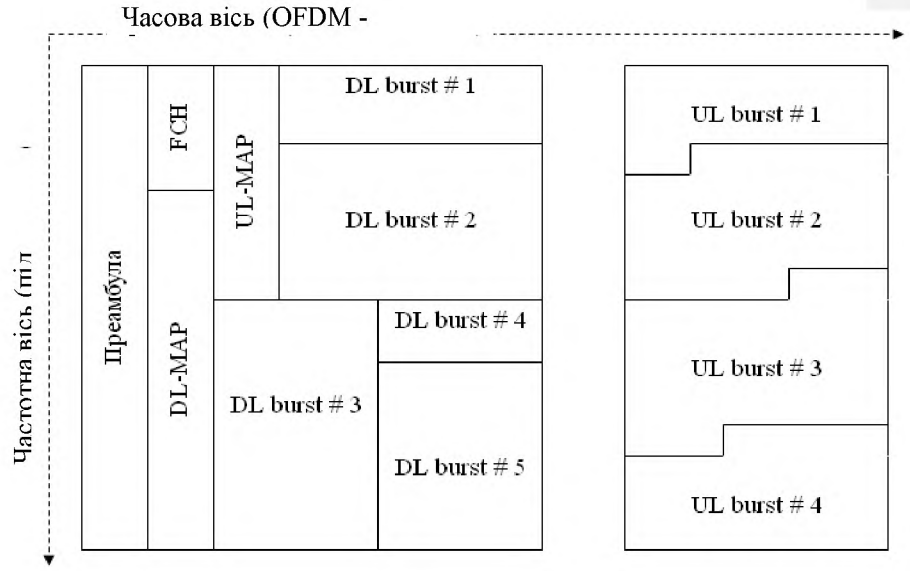

Рисунок. 1.9 структура зони PUSC прямого і зворотного каналів

Фізичний рівень WIRELESSMAN-OFDMA стандарту IEEE 802.16 визначає три схеми кодування: блоковий згортальний код; блоковий турбокод; згортальний турбокод.

Передбачено три види модуляції: QPSK; 16-QAM; 64-QAM.

Декілька схем кодування і вдів модуляції дозволяють здійснювати адаптивне кодування і модуляцію.

Канальні швидкості передачі для смуг частот 6 і 7 МГц- для фізичного рівня WIRELESSMAN-OFDMA, для циклічного префікса і для різних видів кодування і модуляції приведені в таблиці 1.5.

Стандарт передбачає початкову і періодичну частотно-тимчасову синхронізацію. Передбачається, що вона здійснюється по сигналу базової станції. Є регулювання потужності призначеної для користувача станції. Для адаптивного кодування і модуляції, а так само для регулювання потужності стандарт IEEE 802.16 передбачає періодичні виміри рівня сигналу, що приймається, а також стосунки сигнал/(шум + перешкоди).

Передбачена можливість повторної передачі (ARQ) і гібридної повторної передачі (H-ARQ), а також рознесена передача і підтримка адаптивних антенних систем.

Табл 1.5 – Канальні швидкості передачі для WIRELESSMAN-OFDMA

Смуга частот, Мгц	QPSK 1/2	QPSK 3/4	16-QAM 1/2	16-QAM 3/4	64-QAM 2/3	64-QAM 3/4
6	4,99	7,48	9,97	14,96	19,95	22,44
7	5,82	8,73	11,64	17,45	23,27	26,18

MAC-рівень

Рівень MAC здійснює управління доступом до середовища передачі різних призначених для користувача станцій, а також управління параметрами передачі.

Основні функції рівня MAC базової станції і призначеної для користувача станції показані на малюнках 1.10, 1.11 і 1.12.

У стандарті IEEE 802.16 реалізований рівень MAC з централізованим управлінням. Управління передачею даних в прямому і зворотному каналі здійснюється на базовій станції. Рівні MAC призначених для користувача станцій при передачі даних в зворотному каналі виконують рішення, прийняті на базовій станції.

На базову станцію і на призначені для користувача станції поступають пакети даних SDU (Service Data Unit) з верхніх рівнів. При

цьому пакети даних йдуть від різних джерел або застосувань. Потік даних від одного джерела (застосування) називають сервісним потоком (Service Fow). Він характеризується своїм набором вимог за якістю обслуговування QOS (Quality of Service). На рівні MAC кожен сервісний потік обробляється окремо.

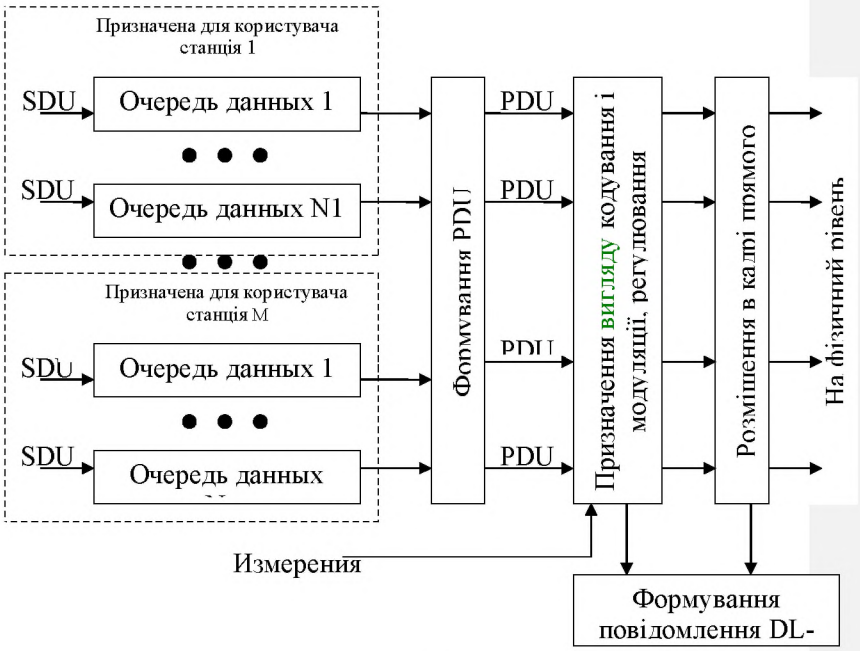

Рисунок1.10. - Основні функції рівня MAC базової станції при управлінні передачею в прямому каналі

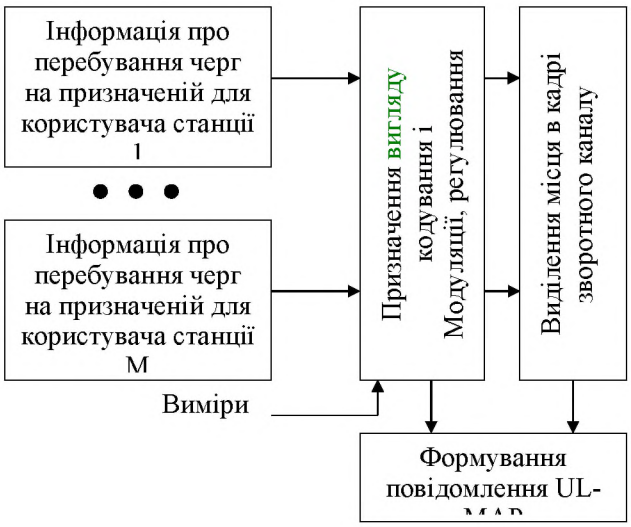

Рисунок 1.11 - Основні функції рівня MAC базової станції при управлінні передачею в зворотному каналі

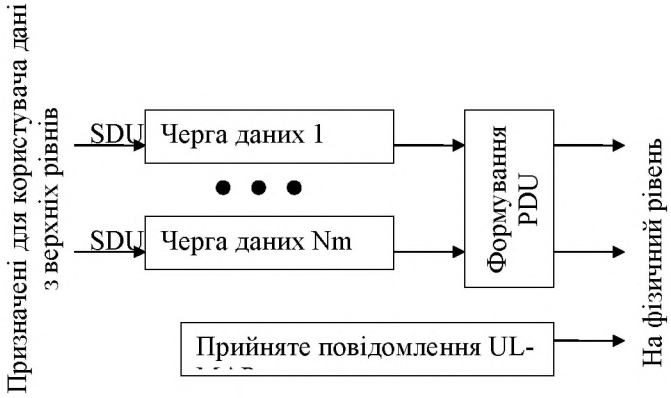

Рисунок 1.12 - Основні функції рівня MAC призначеної для користувача станції при управлінні передачею

Рівень MAC базової станції при управлінні передачею в прямому каналі виконує наступні основні функції:

— Зберігання пакетів даних SDU, що поступили з верхніх рівнів, в чергах (окрема черга для кожного сервісного потоку);
— Ухвалення рішення про те, скільки даних і з яких черг буде передано в поточному кадрі;
— Перетворення пакетів даних SDU в пакети даних PDU (Protocol Data Unit);
— Окреме призначення кожному набору пакетів даних PDU одного сервісного потоку вигляду кодування і модуляції, а також випромінюваній потужності (при цьому використовується інформація про вимоги QOS цього сервісного потоку, кількість і структуру сформованих пакетів даних PDU, а також результати вимірів стану каналу передачі);
— Логічне розміщення сформованих наборів пакетів даних PDU сервісних потоків в кадрі прямого каналу.

Формування повідомлення DL-MAP, що містить для поточного кадру прямого каналу наступну інформацію: кількість наборів пакетів даних PDU; використовувані при їх передачі види кодування і модуляції; їх положення в кадрі прямого каналу; передача сформованих наборів пакетів даних PDU на фізично рівень.

Рівень MAC базової станції при управлінні передачею в зворотному каналі виконує наступні основні функції:

— Ухвалення рішення про те, скільки даних і з яких черг буде передано в поточному кадрі (при цьому використовується інформація про розмір черг на призначених для користувача станціях);
— Призначення окремо кожному сервісному потоку вигляду кодування і модуляції, а також випромінюваній потужності (при цьому використовується інформація про вимоги QOS цього сервісного потоку, розмір його черги на призначеній для користувача станції, а також результатах вимірів стану каналу передачі);

— Виділення місця для передачі сервісних потоків в кадрі зворотного каналу.

Формування повідомлення UL-MAP, що містить для поточного кадру зворотного каналу наступну інформацію: кількість виділених місць; призначені види кодування і модуляції; положення виділених місць в кадрі зворотного каналу.

Рівень MAC призначеної для користувача станції при управлінні передачею в зворотному каналі виконує наступні основні функції:

— Зберігання пакетів даних SDU, що поступили з верхніх рівнів, в чергах (окрема черга для кожного сервісного потоку);
— Прийом інформації, що міститься в повідомленні UL-MAP;
— Ухвалення рішення про те, скільки даних буде узято з черг, під які виділено місце для передачі в поточному кадрі зворотного каналу;
— Перетворення пакетів даних SDU в пакети даних PDU;
— Передача сформованих наборів пакетів даних PDU, а також інформації з повідомлення UL-MAP на фізичний рівень.

Розглянемо детальніше механізми рівня MAC стандарту IEEE 802.16, що дозволяють здійснювати описані функції.

Формування пакетів даних PDU

Пакети даних SDU, що приходять з верхніх рівнів, мають в загальному випадку довільний розмір. Для збільшення ефективності їх передачі на фізичному рівні, на рівні MAC, вони заздалегідь перетворяться в пакети даних PDU.

Для цього в стандарті IEEE 802.16 передбачені наступні операції:

— Фрагментація (Fragmentation) - розбиття пакету даних SDU на декілька фрагментів, кожен з яких включається в свій пакет даних PDU;

— Упаковка (Packing) - об'єднання декількох пакетів даних SDU або їх фрагментів для включення в один пакет даних PDU;

— Об'єднання(Concatenation) - об'єднання декількох формованих пакетів даних PDU в один набір.

Сформований пакет даних PDU включає заголовок (MAC Header) і може включати тіло (Payload) і контрольну суму (CRC). Якщо при формуванні пакету даних PDU використовуються операції фрагментації або упаковки, той тіло містить також підзаголовки фрагментації (Fragmentation Subheader) і підзаголовки упаковки (Packing Subheader).

Стандарт IEEE 802.16 передбачає використання повторної передачі ARQ помилково прийнятих пакетів даних SDU.

Для цього кожному сервісному потоку, що використовує повторну передачу ARQ, призначається розмір блоку ARQ. Всі пакети даних сервісного потоку логічно діляться на блоки ARQ заданого розміру. Фрагментація здійснюється по кордону блоків ARQ. Передані блоки ARQ віддаляються з черги на передачу, лише якщо прийшло підтвердження на їх успішний прийом. Очевидно, що при використанні повторної передачі ARQ пакет даних PDU повинен включати суму для контролю правильності прийому блоків ARQ, що містяться в нім.

Окрім механізму повторної передачі ARQ, деякі схеми кодування частини фізичних рівнів стандарту IEEE 802.16 дозволяють використовувати механізм гібридної повторної передачі H- ARQ, який відрізняється вищою складністю реалізації і вищою ефективністю.

Засоби запиту і виділення частотно-тимчасового ресурсу

Як наголошувалося раніше, управління передачею в стандарті IEEE 802.16 здійснюється на рівні MAC базової станції. Для управління передачею в зворотному каналі в стандарті передбачені наступні засоби запиту і виділення частотно-тимчасового ресурсу:

— Запити (Request);

— Виділення ресурсу для передачі даних (Grant);

— Виділення ресурсу для передачі запиту (Poll);

— Канал запиту ресурсу (Bandwidth Request Subchannel).

— Ці засоби використовуються відповідно до однієї з передбачених в стандарті процедур (Scheduling Service). У стандарті IEEE 802.16 передбачено чотири процедури:

— Виділення ресурсу без попереднього запиту UGS (Unsolicited Grant Service);

— Виділення ресурсу під запит з високою частотою rtPS (Real Time Polling Service);

— Виділення ресурсу під запит з середньою частотою nrtPS (non real time Polling Service);

— Запити з випадковим доступом BE (Best Effort).

Кожному сервісному потоку в зворотному каналі призначається одна з чотирьох процедур виходячи з вимог QOS і інших параметрів цього сервісного потоку.

Процедура UGS призначена для передачі сервісного потоку з постійною швидкістю вступу призначених для користувача даних і постійним розміром пакетів даних SDU. Вона полягає в тому, що сервісному потоку на періодичній основі виділяється ресурс в кадрі зворотного каналу під передачу даних.

Процедури rtPS і nrtPS дуже схожі між собою. Відповідно до їх сервісному потоку на періодичній основі виділяють в кадрі зворотного каналу ресурс під передачу запиту, який тримає інформацію про розмір черги цього сервісного потоку на призначеній для користувача станції. Після прийому цього запиту рівень MAC базової станції виділяє ресурс в кадрі зворотного каналу під передачу даних з черги цього сервісного потоку.

Відмінності процедур rtPS і nrtPS.

Як випливає з назви, передбачається, що при використанні процедури rtPS ресурс під запит виділяється частішим, ніж при використанні процедури nrtPS.

Сервісним потокам, що використовують процедуру nrtPS, додатково дозволяється передавати повідомлення в каналі запиту ресурсу.

Процедура BE призначена для передачі сервісних потоків, практично не чутливих до затримки. При цьому мінімальна швидкість передачі також не гарантується. Відповідно до процедури BE рівень MAC призначеної для користувача станції передає повідомлення в каналі запиту ресурсу. Цей канал використовує випадковий доступ. В разі успішного прийому повідомлення на базовій станції вона виділяє ресурс для передачі запиту в кадрі зворотного каналу. Запит містить інформацію про розмір черги сервісного потоку. Після прийому запиту рівень MAC базової станції виділяє ресурс для передачі даних цього сервісного потоку.

Вхід в мережу і синхронізація

Для входу в мережу призначеної для користувача станції передбачений канал початкового доступу. Він ідентичний каналу запиту ресурсу за виключення того, що використовує інший набір повідомлень. Під час процедури входу в мережу призначена для користувача станція здійснює початкову частотно-тимчасову синхронізацію і регулювання потужності (Initial Ranging). Також призначена для користувача і базова станції обмінюються інформацією про сервісні потоки, які треба буде підтримувати в прямому і зворотному каналах.

При вході в мережу відбувається аутентифікація призначеної для користувача станції. Стандарт IEEE 802.16 підтримує шифрування зраджених даних для забезпечення безпеки.

В процесі роботи призначена для користувача станція здійснює періодичну частотно-тимчасову синхронізацію (Periodic Ranging).

Стандарт IEEE 802.16e є доповнення до стандарту IEEE 802.16 для забезпечення мобільності. Розглянемо основні додаткові механізми стандарту IEEE 802.16e.

Фізичний рівень

Стандарт IEEE 802.16e підтримує роботу мобільних користувачів з наступними фізичними рівнями стандарту IEEE 802.16: WirelessMAN-SCa; WIRELESSMAN-OFDM; WIRELESSMAN-OFDMA.

Основні доповнення торкнулися фізичного рівня WIRELESSMAN-OFDMA. З них можна виділити два основні доповнення. По-перше, окрім OFDM- символу з тими, що 2048 піднесуть, в стандарті IEEE 802.16e передбачені OFDM- символи з 1024, 512 і що 128 піднесуть. По-друге, передбачений новий вигляд кодування - код з низькою надмірністю і перевіркою парності LDPC (LowDensity Parity Check).

MAC-рівень

Рівень MAC стандарту IEEE 802.16e містить ряд істотних доповнень для підтримки мобільних призначених для користувача станцій.

Для економії витрати батареї мобільних призначених для користувача станцій передбачений сплячий режим (Sleep Mode). У цьому режимі мобільна призначена для користувача станція здійснює прийом і передачу лише в наперед узгоджені інтервали часу, а в останній час відключається.

У стандарті IEEE 802.16e передбачені різні види Handover (передача обслуговування мобільної призначеної для користувача станції між базовими станціями) для підтримки безперервності з'єднань при русі мобільної призначеної для користувача станції. Передбачені наступні види Handover: жорсткий (Hard); швидка зміна обслуговуючої базової станції (FBSS- Fast Base Station Switching); м'який (Soft).

У стандарті IEEE 802.16e передбачений режим очікування (Idle Mode). У випадку якщо в мобільної призначеної для користувача станції немає активних з'єднань, то вона може перейти в режим очікування. Це суттєво зменшує навантаження на мережу як в прямому, так і в зворотному каналах, а також економить ресурс батареї мобільної

призначеної для користувача станції. У цьому режимі передбачений пошук мобільної призначеної для користувача станції (Paging).

1.8 Ключові технологи стандарту

У стандарті IEEE 802.16 b IEEE 802.16e закладені технології, які є обов'язковими для сучасних безпровідних мереж передачі даних. Немає сумнівів, що всі ці технології будуть використані в мережах стільникового зв'язку четвертого покоління і включають: забезпечення вимог QOS; адаптивне кодування і модуляцію; підтримку адаптивних антенних систем; підтримку мобільних користувачів.

Забезпечення вимог QOS

При передачі даних і мультимедійної інформації потоки призначених для користувача даних характеризуються різними вимогами за якістю сервісу (вимоги QOS). На відміну від стільникових мереж другого покоління, орієнтованих на передачу голосу, забезпечення вимог QOS є обов'язковою властивістю безпровідних мереж передачі даних.

Для забезпечення вимог QOS в стандарті передбачено поняття сервісного потоку (Service Flow) . Сервісний потік - потік призначених для користувача даних від одного джерела або застосування, що характеризується набором вимог QOS, і інших параметрів. Стандарт IEEE 802.16 дозволяє на кожній призначеній для користувача станції забезпечувати підтримку декількох різних сервісних потоків в прямому і зворотному каналах.

Окрім цього, стандарт передбачає ряд механізмів: запити (Request), виділення ресурсу для передачі даних (Grant) і для передачі запиту (Poll) - і ряд процедур їх використання - UGS, rtPS, nrtPS, BE- для забезпечення найрізноманітніших наборів вимог QOS.

Адаптивне кодування і модуляція.

Стандарт підтримує механізм адаптивного кодування і модуляції, а також механізм регулювання потужності. Це дозволяє адаптивний

підстроювати параметри передачі під умови прийому, що змінюються, для самих різних наборів вимог QOS.

Адаптивне кодування і модуляція є найефективнішою технологією підвищення пропускної спроможності при передачі даних. Механізм регулювання потужності в прямому і зворотному каналах дозволяє у ряді випадків додатково збільшити ефективність передачі.

Підтримка адаптивних антенних систем.

У безпровідних стільникових мережах передачі даних основним чинником, що обмежує пропускну спроможність, є наявність внутрісистемних перешкод. Використання адаптивних антенних систем, рознесеної передачі і прийому є одним із способів боротьби з внутрісистемними перешкодами.

Стандарт IEEE 802.16 забезпечує підтримку широкого класу методів просторово-часової обробки при передачі і прийомі.

Підтримка мобільних користувачів

Стандарт IEEE 802.16e забезпечує підтримку мобільності. При цьому він передбачає всі ключові механізми, такі як: механізм пошуку мобільної призначеної для користувача станції (Paging); жорсткий Handover; швидка зміна обслуговуючої базової станції (швидкий жорсткий Handover); м'який Handover; режим енергозбереження (Sleep Mode).

Все це говорить про те, що сімейство стандартів IEEE 802.16, поза сумнівом, є ключовим кандидатом на роль базису для створення безпровідних мереж передачі даних четвертого покоління.

Технології і рішення, закладені в поточну версію стандарту, дозволяють забезпечити ефективну мобільну безпровідну передачу даних, мультимедійної інформації, голосу, відео і Інтернету.

1.9 Висновок

1. Технологія WI-MAX доповнює Wi-Fi.
2. Стандарт IEEE 802.16 – альтернатива дротяним лініям і DSL.

3. Дозволяє провайдерам широкосмугового доступу розширити існуючу зону дії своєї мережі, охоплюючи райони, що не мають інфраструктури провідного зв'язку.
4. Стандарт 802.16 забезпечує ефективну роботу поза межами видимості, що значно полегшує планування і установку обладнання в умовах міської забудови.
5. Стандарт 802.16 забезпечує прискорене зростання ринку безпровідного широкосмугового доступу завдяки:
6. меншій вартості
7. сумісності обладнання
8. відповідності існуючим стандартам безпровідного широкосмугового з'єднання, що з'являються
9. WIMAX забезпечує сумісність обладнання стандарту 802.16 завдяки стандартизації тестів сумісності.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна характеристика підприємства і умови функціонування мережі.

Підприємство ТОВ «Рубін» займається розробкою програмного забезпечення для платформ Windows. Підприємство розташовується в місті Каменське, головний офіс розташований в центрі міста, працівники і віддалені користувачі а так само другий офіс розташовується на периферії міста, в приватному секторі а так само в місті Дніпро.

2.2 Вимоги до системи

Об'єкти інформаційної діяльності перебувають на відстані до 12 км.

Швидкість каналу повинна забезпечувати:

— телефонію Voip (256 Кбіт\с)

— відео конференцію (512 Кбіт\с)

— файл-сервер (1 Мбіт\с)

— поштовий сервер (64 Кбіт\с)

— інтернет сервер (512 Кбит\с)

Система повинна забезпечувати:

— для відкритої інформації

а) цілісність;

б) доступність;

— для інформації з обмеженим доступом

а) цілісність;

б) конфіденційність;

в) доступність;

г) спостережливість.

2.3 2.3 Опис корпоративної мережі підприємства ТОВ «Рубін»

Інформація обробляється за допомогою спеціального інструменту - програмного забезпечення. Тому базисом будь-якої корпоративної мережі є загальносистемне програмне забезпечення, яке може містити різні операційні системи, програмні оболонки, програми загального призначення, текстові процесори, редактори і інтегровані пакети програм, системи управління базами даних. Крім того, для обробки інформації використовується також прикладне програмне забезпечення.

В процесі обробки інформації використовуються різні технічні пристрої обробки, зберігання і передачі даних. Інформація може поступати з автоматизованого робочого місця по внутрішніх і по зовнішніх каналах зв'язку, при цьому інформація може вводитися як з клавіатури, так і із зовнішніх носіїв інформації

Під поняттям "Користувач корпоративної мережі" розуміється зареєстровані встановленим порядком персони, наділені певними повноваженнями доступу в мережі. В рамках своїх повноважень користувач може здійснювати лише дозволені йому дії з використанням загальносистемного і прикладного ПО.

Обробка інформації в мережі здійснюється під контролем адміністраторів системи, а її захисту - адміністраторів безпеки, які виконують свої функції, маючи спеціалізовані робочі місця. Ці місця не

завжди дозволяють дістати доступ до оброблюваної інформації, але завжди дозволяють вплинути на процес її обробки, а також модернізацію інструменту обробки.

Для розробки прикладного ПЗ, адаптації загальносистемного ПЗ і підтримку мережі в працездатному стані є фахівці-програмісти і технічний персонал, які так само мають обмежені можливості по доступу до самої інформації, та необмежені можливості по зміні програмного забезпечення і процесів обробки інформації.

Дану корпоративну мережу можна представити у вигляді системи, що складається з ряду апаратно-програмних підсистем – окремих користувачів, користувачів одноранговой мережі і мережі з виділеним сервером

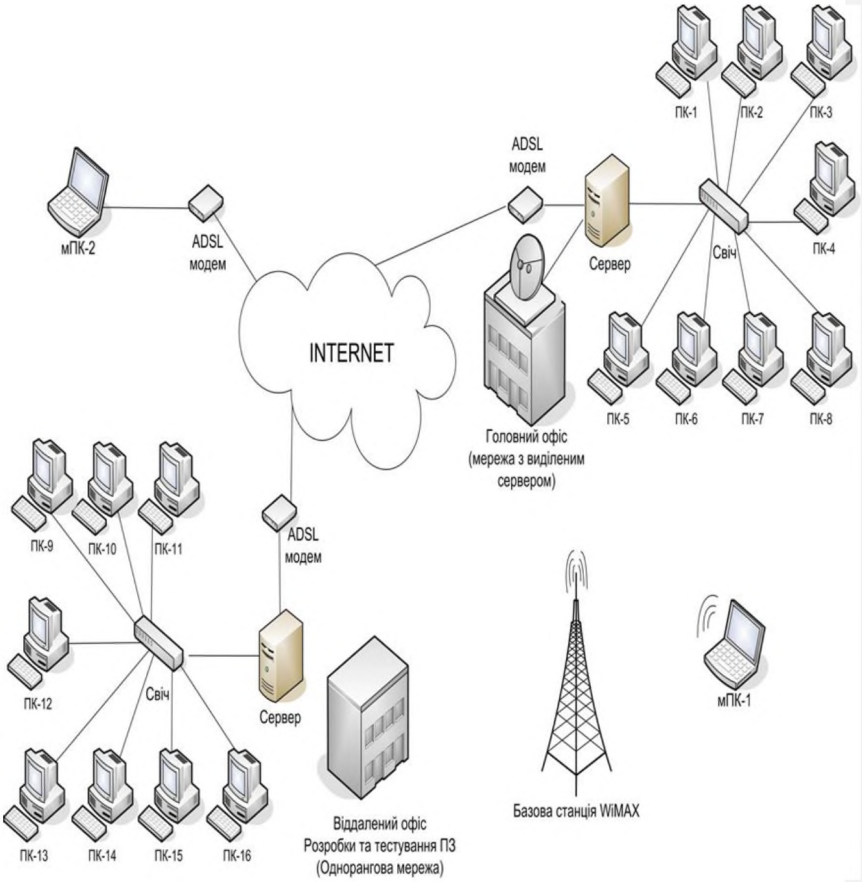

Рисунок. 2.1 - модель існуючої мережі підприємства ТОВ «Рубін»

Таблиця. 2.1 - характеристика існуючої мережі підприємства ТОВ «Рубін»

Тип мережі головного офісу		Мережа з виділеним сервером (8ПК +1сервер)
Тип мережі видаленого офісу		Мережа з виділеним сервером (8ПК +1сервер)
Відстань між офісами		12 км.
Тип з'єднання між офісами		VPN (Virtual Private Network) - віртуальна приватна мережа (через ADSL модем)
Кількість користувачів головного офісу		8
Кількість користувачів віддаленого офісу		8
Головний офіс	ПК-1	Генеральний директор
	ПК-2	Секретар
	ПК-3	Бухгалтер
	ПК-4	Системний адміністратор №1
	ПК-5	Менеджер №1
	ПК-6	Менеджер №2
	ПК-7	Розробник №1
	ПК-8	Розробник №2
Віддалений офіс	ПК-9	Начальник відділу
	ПК-10	Системний адміністратор №2
	ПК-11	Розробник №3
	ПК-12	Розробник №4
	ПК-13	Розробник №5
	ПК-14	Розробник №6
	ПК-15	Спеціаліст з тестування №1
	ПК-16	Спеціаліст з тестування №2

Віддалені користувачі	мПК-1	Ноутбук генерального директора
	мПК-2	Віддалений персонал підприємства

Вимоги до мережі:

— Масштабованість мережі

Розвиток організації, встановивши у себе обчислювальну мережу спричиняє за собою необхідність в розширенні мережі. Добре продумана масштабованість дозволяє збільшити кількість користувачів при найменших витратах.

— Керованість

Керованість мережі повинна дозволити швидко перенастроювати її під часто змінні потреби користувачів.

— Продуктивність

Висока продуктивність забезпечує працездатність сучасних мережевих застосувань і сервісів.

— Захищеність

Висока захищеність забезпечує конфіденційність комерційної таємниці та цілісність інформації при її обробці.

Недоліки існуючої мережі:

— обмежені можливості віддаленої роботи

— низька швидкість передачі інформації між клієнтами різних офісів

— невисока надійність каналу VPN

— низька захищеність клієнтського обладнання

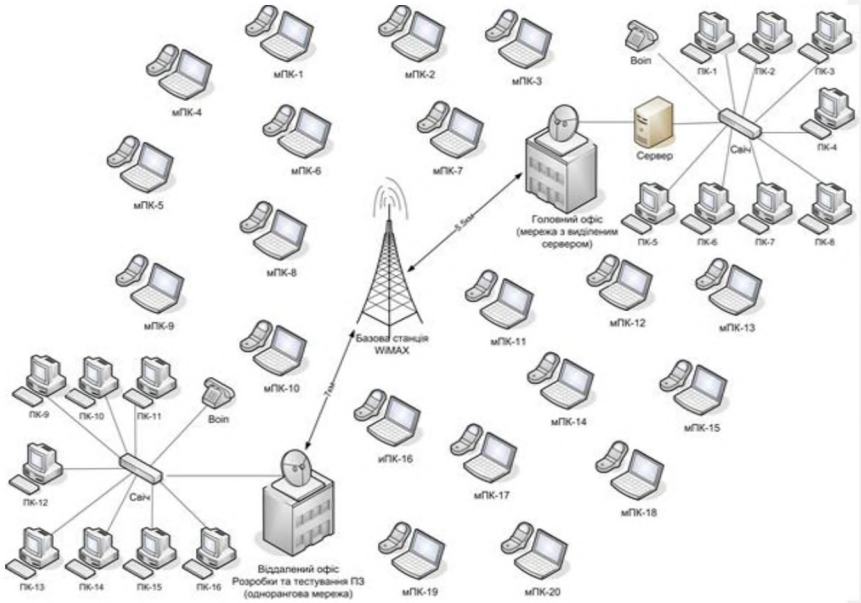

Рисунок. 2.2 - Корпоративної мережа підприємства ТОВ «Рубін» після введення системи WIMAX

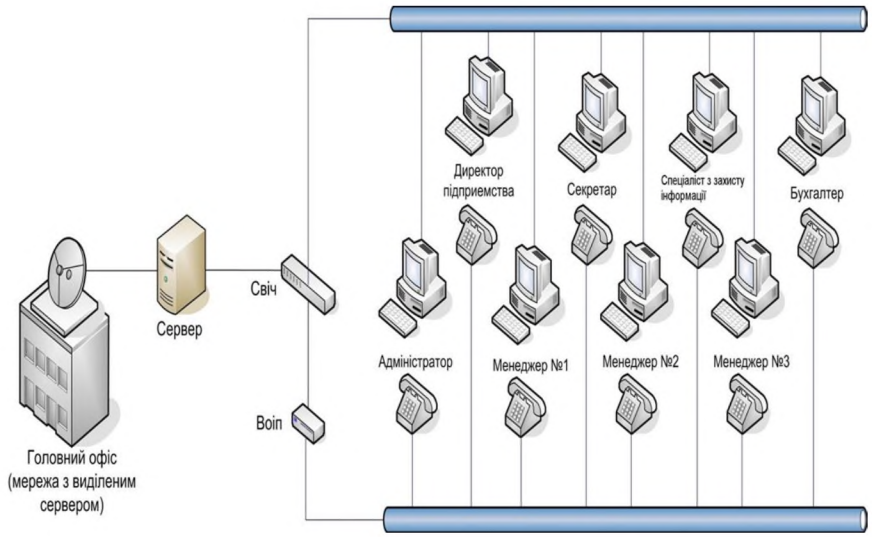

Рисунок 2.3 - Мережа головного офісу

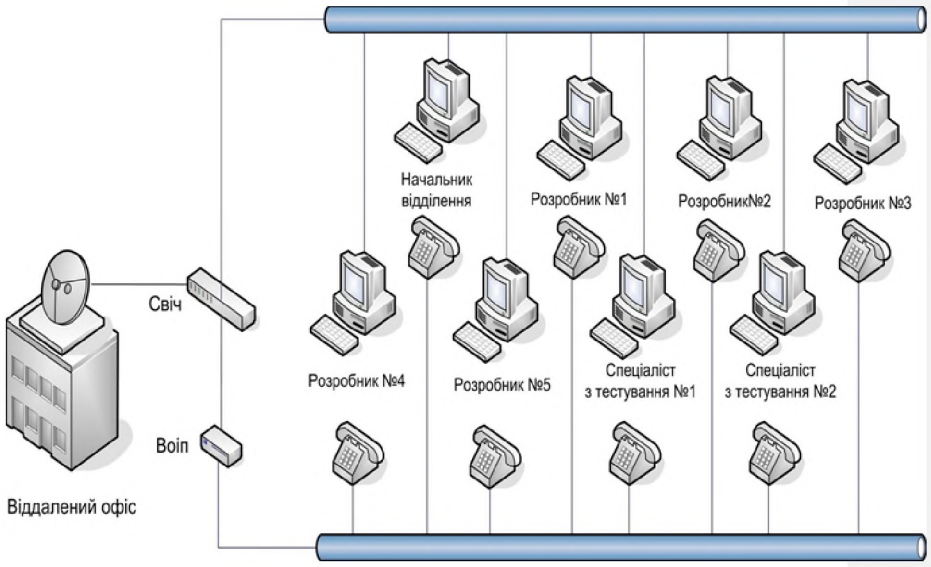

Рисунок 2.4 Мережа віддаленого офісу

Таблиця 2.2 - характеристика існуючої мережі підприємства ТОВ «Рубін»

Тип мережі головного офісу		Мережа з виділеним сервером (8ПК +1сервер)
Тип мережі видаленого офісу		Однорангова мережа (8ПК)
Відстань між офісами		12 км.
Тип з'єднання між офісами		WiMAX
Кількість користувачів головного офісу		8
Кількість користувачів віддаленого офісу		8
Головний офіс	ПК-1	Генеральний директор
	ПК-2	Секретар
	ПК-3	Бухгалтер
	ПК-4	Системний адміністратор
	ПК-5	Фахівець захисту інформації

	ПК-6	Менеджер №1
	ПК-7	Менеджер №2
	ПК-8	Менеджер №3
Віддалений офіс	ПК-9	Начальник відділу
	ПК-10	Розробник №1
	ПК-11	Розробник №2
	ПК-12	Розробник №3
	ПК-13	Розробник №4
	ПК-14	Розробник №5
	ПК-15	Спеціаліст з тестування №1
	ПК-16	Спеціаліст з тестування №2
Віддалені користувачі	мПК-1-15	Розробник №6-21
	мПК-16-20	Спеціаліст з тестування №3-8

Переваги:

— можливість віддаленої роботи;

— велика пропускна спроможність каналу між мобільними користувачами;

— велика пропускна спроможність каналу між офісами;

— забезпечення телефонним та відео зв'язком між персоналом та стаціонарними користувачами;

— забезпечення багато ступеневої системи аутентифікації персоналу;

— забезпечення шифрування WIMAX каналу;

— забезпечення захисту інформації на втрачених (вкрадених) носіях.

— забезпечення захисту від крадіжки клієнтського обладнання.

2.4 Категорії інформації

Інформація яка циркулює на підприємстві ділиться на відкриту та інформацію з обмеженим доступом.

Так як на підприємстві є інформація яка являється комерційною таємницею та інформація яка на думку керівника являється конфіденційною та власністю підприємства, цю інформацію треба віднести до інформації з обмеженим доступом.

Відкрита інформація:

— ціни;

— ринок послуг;

— замовлення на виконання послуг;

— проекти договорів;

— проекти накладних;

— оперативна інформація для співробітників підприємства, що стосується виконання ними своїх обов'язків.

Інформація з обмеженим доступом:

— державна звітність;

— установчі документи;

2.5 Модель загроз

У літературі, присвяченій питанням захисту інформації можна знайти різні варіанти моделей загроз безпеці інформації. Це пояснюється прагненням точніше описати різноманітні ситуації дії на інформацію і визначити найбільш адекватні заходи захисту. Можна користуватися будь-якою вподобаною моделлю, необхідно лише переконатися, що вона описує максимально велике число чинників, що впливають на безпеку інформації.

Загроза безпеці інформації - дія, що спрямована проти об'єкту захисту, виявляється в небезпеці спотворень і втрат інформації. Треба обмовитися, що йдеться не про всю інформацію, а лише про ту її частину, яка на думку її власника (користувача) має комерційну цінність (інформація як товар) або підлягає захисту через закон (конфіденційна інформація).

Необхідно враховувати, що джерела загроз безпеці можуть знаходитися як всередині фірми - внутрішні джерела, так і поза нею - зовнішні джерела. Таке ділення виправдане тому, що для однієї і тієї ж

загрози (наприклад крадіжка) методи протидії для зовнішніх і внутрішніх джерел будуть різними.

Всі джерела погроз безпеці інформації, циркулюючої в корпоративній мережі можна розділити на три основні групи:

— Загрози, обумовлені діями суб'єкта (антропогенні загрози)

— Загрози, обумовлені технічними засобами (техногенні загрози)

— Загрози, обумовлені стихійними джерелами

Перша група найбільш обширна і представляє найбільший інтерес з точки зору організації парирування цим загрозам, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Методи протидії цим погрозам керовані і напряму залежать від волі організаторів захисту інформації.

Суб'єкти, дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішні:

— кримінальні структури;

— рецидивісти і потенційні злочинці;

— недобросовісні партнери;

— конкуренти;

— політичні супротивники;

так і внутрішні:

— персонал установи;

— персонал філій;

— обличчя з порушеною психікою;

— спеціально впроваджені агенти.

Ґрунтуючись на результатах міжнародного досвіду, дії суб'єктів можуть привести до ряду небажаних наслідків, серед яких стосовно корпоративної мережі, можна виділити наступні:

— Крадіжка

— Підміна (модифікація)

— Знищення (руйнування)

— Порушення нормальної роботи (переривання)

— Помилки

— Перехоплення інформації (несанкціонований)

II. Друга група містить погрози менш прогнозовані, напряму залежна від властивостей техніки і тому що вимагають особливої уваги. Технічні засоби, що містять потенційні погрози безпеці інформації так само можуть бути внутрішніми:

— неякісні технічні засоби обробки інформації;

— неякісні програмні засоби обробки інформації;

— допоміжні засоби (охорона, сигналізації, телефонії);

— інші технічні засоби, вживані в установі;

і зовнішніми:

— засоби зв'язку;

— близько розташовані небезпечні виробництва;

— мережі інженерних комунікації (енерго або водопостачання, каналізації);

— транспорт.

Наслідками застосування таких технічних засобів, напряму впливають на безпеку інформації можуть бути:

— Порушення нормальної роботи

— Знищення (руйнування)

— Модифікація (зміна)

Третю групу складають погрози які цілком не піддаються прогнозуванню і тому заходи їх парирування повинні застосовуватися завжди. Стихійні джерела, що становлять потенційні загрози інформаційній безпеці як правило є зовнішніми по відношенню до даного об'єкту і під ними розуміються перш за все природні катаклізми:

— пожежі;

— землетруси;

— повені;

— урагани;

— інші форс-мажорні обставини;

— різні непередбачені обставини;

— нез'ясовні явища.

Ці природні і нез'ясовні явища так само впливають на інформаційну безпеку, небезпечні для всіх елементів корпоративної мережі і можуть привести до наступних наслідків:

— Знищення (руйнування)

— Зникнення (пропажа)

Описавши склад загроз безпеці інформації, ми ще не вирішили проблеми моделювання їх дії. Всі ці загрози по-різному виявляються в кожній точці корпоративної мережі.

2.6 Модель загроз для підприємства ТОВ «Рубін»

2.6.1 Антропогенні загрози

1 Крадіжка

— технічних засобів (вінчестерів, ноутбуків, системних блоків);

— інформації (читання і несанкціоноване копіювання);

— засобів доступу (ключі, паролі, ключова документація і ін.).

3 Знищення (руйнування)

— технічних засобів (вінчестерів, ноутбуків, системних блоків);

— програмного забезпечення (ОС, СУБД, прикладного ПЗ)

— інформації (файлів, даних)

— паролів і ключової інформації.

4 Порушення нормальної роботи

— пропускній спроможності каналів зв'язку;

— електроживлення технічних засобів;

5. Помилки

— при інсталяції ПЗ, ОС, СУБД;

— при експлуатації ПЗ;

— при експлуатації технічних засобів.

6. Перехоплення інформації (несанкціонований)

Таблиця 2.3 - види атак на безпровідні мережі

Види атак	Склад атак	Цілі	Результат
Пасивна атака на протокол маршрутизації	прослухування пакетів, що посилаються відповідно до протоколу маршрутизації.	здобуття інформації про взаємодію між вузлами з виявленням їх адрес, про зразкове розташування вузлів, про мережеву топологію.	При пасивних атаках порушується конфіденційність, проте доступність і цілісність залишаються незайманими.
«Чорна діра»	використання протоколу маршрутизації для перенаправлення пакетів, що йдуть від	дана атака може використовуватися для проведення згодом інших атак, таких як: викидання	Чорна діра погіршує доступність, оскільки після неї починають використовуватися неоптимальні маршрути.

	або до цільового вузла, через певний вузол.	пакетів або чоловік посередині.	Конфіденційність порушується унаслідок того, що зловмисник має можливість прослухувати весь цільовий трафік. Також чорна діра дозволяє зловмисникові порушити цілісність передаваної інформації.
Переповнювання таблиці маршрутизації	створення маршрутів до неіснуючих вузлів.	переповнювання таблиці маршрутизації протоколу, яке б запобігло створенню нових маршрутів.	Дана атака може використовуватися у в'язці з іншими атаками для запобігання зміні маршрутів. Вона наносить утрату доступності через те, що маршрутні таблиці починають зберігати неактуальну інформацію. Але вона має силу лише над попереджуючими протоколами маршрутизації, які намагаються взнати маршрутну інформацію до того, як це необхідно, і те не над всіма.
«Егоїстичність»	схильність вузла не надавати послуги іншим, наприклад послугу маршрутизації.	зберегти власні ресурси, наприклад заряд батареї.	Проблема «егоїстичності» вузлів нова і особливо актуальна для динамічних мереж, оскільки вузли належать різним адміністративним доменам.

			Дана атака негативно впливає на доступність.
«Жадність»	схильність вузла використовувати ресурси, що розділяються, більше останніх, наприклад середовище передачі даних.	задовольнити власні потреби без врахування витікаючого з цього збиткового положення останніх вузлів.	По суті, «жадність» і «егоїстичність» — дві сторони однієї монети. Дана атака негативно впливає на доступність.
«Випробування безсонням»	підвищення потужності роботи цільового вузла дорогою змушення його проводити додаткові дії.	витратити енергію цільового вузла, запасену в його джерелі живлення.	Побічним ефектом випробування безсонням є порушення доступності. Для здійснення цієї атаки можуть бути використані інші, наприклад чорна діра, для напряму великого трафіку на цільовий вузол.
Виявлення місця розташування	посилка маршрутних повідомлень, які б наводили до здобуття деякої інформації про топологію мережі.	відновлення топології прилеглої мережі або відновлення ланцюжка вузлів, розташованих на маршруті до цільового вузла, шляхом аналізу отриманої інформації.	За наявності інформації про розташування деяких вузлів, можна обчислити зразкове розташування останніх. Дана атака порушує конфіденційність
Спуфінг	підробка ідентифікації.	змусити останні вузли рахувати вузол, провідний атаку, не тим, ким він є насправді.	Успішно провівши атаку, зловмисник дістає можливість проводити які-небудь дії від чужого імені, тим самим порушується конфіденційність.

Постановка перешкод	«засмічення» каналу передачі даних сторонніми шумами.	зробити неможливим передачу даних через цей канал.	Дана атака порушує доступність.

2.6.2 Техногенні загрози

1. Порушення нормальної роботи
   — порушення працездатності системи обробки інформації;
   — порушення працездатності зв'язку;
   — порушення встановлених правил доступу;
   — електромагнітна дія на технічні засоби.
2. Знищення (руйнування)
   — програмного забезпечення, ОС, СУБД;
   — засобів обробки інформації (кидки напруги, виток);
   — приміщень
   — інформації (розмагнічування, радіація, виток і ін.);
   — персоналу.
   —

2.6.3 Стихійні загрози

1. Знищення (руйнування)
   — технічних засобів обробки інформації;
   — носіїв інформації;
   — програмного забезпечення (ОС, СУБД, прикладного ПЗ);
   — інформації (файлів, даних);
   — приміщень;
   — персоналу.
2. Зникнення (пропажа)
   — інформації в засобах обробки;
   — інформації при передачі по телекомунікаційних каналах;
   — носіїв інформації;
   — персоналу.

На основі аналізу, що проводиться фахівцями в області комп'ютерних злочинів і спостереженнями, по частоті вияву загрози безпеці можна розставити так:

— крадіжка (копіювання) програмного забезпечення
— підміна (несанкціоноване введення) інформації
— знищення (руйнування) даних на носіях інформації
— порушення нормальної роботи (переривання) внаслідок вірусних атак
— модифікація (зміна) даних на носіях інформації
— перехоплення (несанкціоноване знімання) інформації
— крадіжка (несанкціоноване копіювання) ресурсів
— порушення нормальної роботи (перевантаження) каналів зв'язку
— непередбачувані втрати.

2.7 Модель порушника

Добавлено примечание ([ФСВ1]): 21_05_21

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

— перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
— другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
— третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
— четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних

компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

2.7.1 Модель порушника для підприємства ТОВ «Рубін»

У таблиці 2.4 наведено модель порушника для ТОВ «Рубін»

Таблиця 2.4 - модель порушника підприємства ТОВ «Рубін»

Групи	Назва групи	Опис
I	Зареєстровані користувачі	- Користувачі, здійснюють віддалений доступ до системи по каналау зв'язку WiMAX; - Користувачі, що здійснюють доступ до системи з локальної обчислювальної мережі, що знаходиться в межах контрольованої зони;
II	Технічний персонал	- Технічні спеціалісти з обслуговування технічних засобів ТОВ «Рубін» і супроводу використовуваного на них загальносистемного і прикладного програмного забезпечення; - Технічні спеціалісти, що здійснюють конфігурування та налагодження технічних засобів, що використовуються в ТОВ « Рубін »
III	Фізичні особи, які мають доступ до ТОВ « Рубін », але не є зареєстрованими	- Обслуговуючий персонал, що проводить роботи в приміщеннях, в яких розміщуються технічні засоби

	користувачами або технічним персоналом	підприємства; - Співробітники, що мають доступ до приміщення, в яких розміщуються технічні засоби підприємства
IV	Фізичні особи, що є користувачами зовнішніх по відношенню до ТОВ «Рубін» систем	- Користувачі зовнішніх по відношенню до інформаційних систем підприємства.
V	Фізичні особи, які не мають права доступу всередину контрольованої зони, в межах якої розташовані програмно-технічні засоби ТОВ « Рубін » , і які не є зареєстрованими користувачами або технічним персоналом підприємства	- всі сторонні особи

2.8 Впровадження розгортання системи

2.8.1 Реалізація конфіденційності

Ідентифікація суб'єкта полягає в тому, що суб'єкт повідомляє ідентифікуючу інформацію про себе. У нашому випадку ідентифікатором служить парольний доступ і біометричні дані.

Аутентифікація має на увазі перевірку достовірності суб'єкта, яким в принципі може бути не лише людина, але і програмний процес. Взагалі аутентифікація індивідів можлива при пред'явленні інформації, що зберігається в різній формі. Аутентифікація дозволяє обгрунтовано і достовірно розмежувати права доступу до інформації, що знаходиться в загальному користуванні. Однак, з іншого боку, виникає проблема забезпечення цілісності і достовірності цієї інформації. Користувач має

бути упевнений, що дістає доступ до інформації із заслуговуючої довіри джерела і що дана інформація не була змінена без відповідних санкцій. Пошук збігу "один до одного" (по одному атрибуту) зазвичай називають верифікацією. Вона відрізняється високою швидкістю і пред'являє мінімальні вимоги до обчислювальної потужності комп'ютера. Пошук же "один до багатьом" називається ідентифікацією.

Біометричні технології аутентифікації можна розділити на дві категорії - фізіологічні і психологічні. До першої відносяться методи, засновані на фізіологічній характеристиці людини, тобто невід'ємній, унікальній характеристиці, даній йому від народження. Тут аналізуються такі ознаки, як риси обличчя, структура ока (сітківки або веселкової оболонки), параметри пальців (папілярні лінії, рельєф, довжина суглобів і т. д.), долоня (її відбиток або топографія), форма руки, малюнок вен на зап'ясті або теплова картина.

До групи психологічних відносять так звані динамічні методи, які грунтуються на поведінковій (динамічною) характеристиці людини. Іншими словами, вони використовують особливості, характерні для підсвідомих рухів в процесі відтворення якої-небудь дії. До таких характеристик відносяться голос людини, особливості його підпису, динамічні параметри листа, особливості введення тексту з клавіатури і так далі.

2.8.2 Біометрична система робочих станцій підприємства

Біометрична система дозволяє розпізнавати деякий шаблон і встановлювати автентичність конкретних фізіологічних характеристик користувача. Біометричну систему (Рис.2.5) можна розділити на два модулі: реєстрації і ідентифікації. Модуль реєстрації відповідає за те, щоб система навчилася ідентифікувати конкретну людину. На етапі реєстрації біометричні датчики сканують його необхідні фізіологічні характеристики, створюючи їх цифрове зображення. Спеціальний модуль обробляє зображення для того, щоб виділити характерні особливості і згенерувати

компактніше і виразніше зображення, яке зветься шаблоном. Шаблон для кожного користувача зберігається в базі даних біометричної системи.

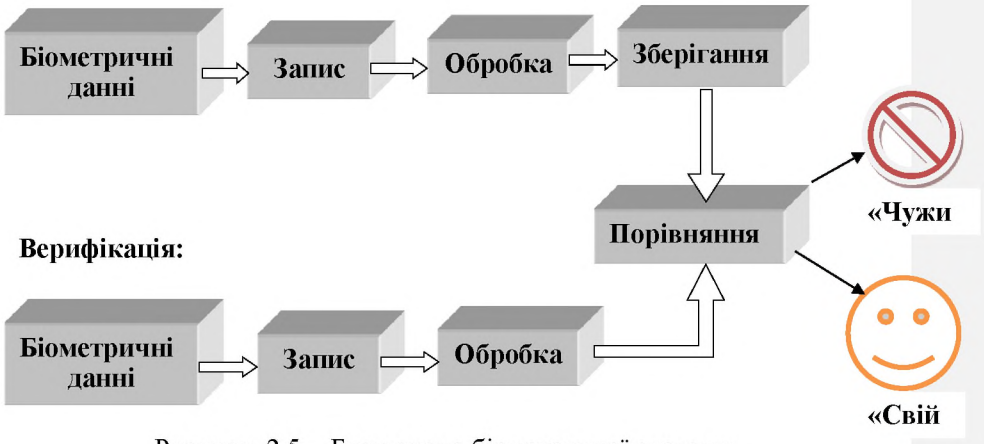

Рисунок. 2.5 - Блок-схема біометричної системи.

Модуль ідентифікації відповідає за розпізнавання людини. На етапі ідентифікації біометричний датчик реєструє відбитки людини, ідентифікація якої проводиться, і перетворить ці характеристики в той же цифровий формат, в якому зберігається шаблон. Отриманий шаблон порівнюється із тим, що зберігається, з тим щоб визначити, чи відповідають ці шаблони один одному. При використанні в процесі аутентифікації технології ідентифікації відбитків пальців ім'я користувача вводиться для реєстрації, а відбиток пальця замінює пароль. Ця технологія використовує ім'я користувача як покажчик для здобуття облікового запису користувача і перевірки відповідності "один до одного" між шаблоном скануємого при реєстрації відбитку і збереженим раніше шаблоном для даного імені користувача. У іншому випадку введений при реєстрації шаблон відбитку пальця зіставляється зі всім набором збережених шаблонів.

Вбудований біометричний сканер запам'ятовує до 20 еталонів відбитків пальців, що дозволяє зберігати паролі 20 користувачів в одній

комп'ютерній системі. Для ідентифікації користувачеві досить прикласти до пристрою палець, при цьому конструкція менеджера паролів забезпечує точне сканування відбитку. Завдяки технології AuthenTec TruePrint менеджер сканує відбитки пальців, аналізуючи їх дійсну біологічну структуру під поверхнею шкіри, незалежно від таких її типових дефектів, як сухість, потертість, мозоляста, забруднення і жирові плівки.

У основі цього методу лежить унікальність малюнка папілярних узорів на пальцях у кожної людини (мал. 6). Відбитки пальців - найбільш точна, сприятлива до користувача і економічна біометрична характеристика зі всіх, використовуваних в комп'ютерних системах ідентифікації. Усуваючи для користувачів потребу в паролях, технологія розпізнавання відбитків пальців скорочує число звертань до служби підтримки і знижує витрати на мережеве адміністрування.

Рисунок 2.6 - Папілярні узори унікальні.

Переваги доступу по відбитку пальця - простота використання, зручність і надійність. Існують два основоположні алгоритми розпізнавання відбитків пальців: по окремих деталях (характерним точкам) і по рельєфу всієї поверхні пальця. Відповідно в першому випадку пристрій реєструє лише деякі ділянки, унікальні для конкретного відбитку, і визначає їх взаємне розташування. У другому випадку обробляється зображення всього відбитку. У сучасних системах все частіше

використовується комбінація цих двох способів, що дозволяє уникнути недоліків обоє і підвищити достовірність ідентифікації.

Одноразова реєстрація відбитку пальця на оптичному сканері займає мало часу. ПЗС-камера вбудована в клавіатуру, робить знімок відбитку пальця. Потім за допомогою спеціальних алгоритмів отримане зображення перетвориться в унікальний "шаблон" - карту мікроточок цього відбитку, які визначаються наявними в нім розривами і пересіченнями ліній. Цей шаблон (а не сам відбиток) потім шифрується і записується в базу даних для аутентифікації мережевих користувачів. У одному шаблоні зберігаються від декількох десятків до сотень мікроточок.

Перевага ультразвукового сканування - в можливості визначити необхідні характеристики на брудних пальцях і навіть через тонкі гумові рукавички. Варто відзначити, що системи розпізнавання не можна обдурити навіть свіжовідрубаними пальцями (мікросхема вимірює фізичні параметри шкіри).

Вірогідність помилки при ідентифікації користувача набагато менша, ніж в інших біометричних методів. Якість розпізнавання відбитку і можливість його правильної обробки алгоритмом сильно залежать від стану поверхні пальця і його положення відносно скануючого елементу.

2.8.3 Захист на фізичному рівні чипами ASIC

Безпека WiMax-мережі забезпечується на фізичному рівні спеціально розробленими чипами ASIC, які вбудовані в пристрої безпровідного зв'язку і управляють процесом передачі даних по радіоканалу:

— Вони захищають від спроб порушення конфіденційності.

— Запобігають порушенню цілісності даних.

— Запобігають фальсифікації (порушення автентичності джерела – споживача).

— Виключають відмову в обслуговуванні.

При авторизації на базовій станції на неї відсилаються реквізити абонентського комплекту (сертифікат, цифрові підписи, запит на

авторизацію), після чого абонентський пристрій отримує свій конфігураційний файл і починає працювати відповідно до його. При цьому сертифікат унікальний для кожного абонента, підписаний hash- функцією SHA-1 і не може бути змінений, оскільки «зашитий» в само пристрій, що має унікальний номер і MAC-адрес. Термін дії цього сертифікату складає, згідно із стандартом 802.16 – 10 років.

Що стосується забезпечення інформаційної безпеки, то, на відміну від стандартів серії 802.16, які по суті справи не забезпечували захисту від несанкціонованого доступу, в стандарті 802.16 офіційно затверджені заходи для запобігання злому. Так в процесі передачі даних від базової станції до абонента і назад трафік шифрується. При цьому використовуються одночасно два ключі з тими, що перекриваються часом життя, і тому трафік ніколи не буває незашифрований. Одночасна робота двох ключів пояснюється необхідністю працювати в середовищі з можливою втратою пакетів. Відбувається також періодична реавторизація і періодична зміна ключів.

2.8.4 Захист на фізичному рівні Kensington lock

Кенсингтонський замок (англ. Kensington lock) — невеликий отвір в корпусі ноутбуків (Рисунок 2.7.), ЖК-мониторів і інших пристроїв, призначене для сполучення із спеціальним замком (на на зразок велосипедного замку) із сталевим тросом, що охоплює який-небудь нерухомий, великогабаритний або важкий предмет. Застосування такої конструкції дозволяє декілька знизити ризик крадіжки пристрою, що захищається.

Рисунок 2.7 – розташування кенсингтонського замку

Кенсингтонський замок легко долається зловмисником з відповідними інструментами, тому не запобігає спланованій крадіжці — до того ж багато моделей кенсингтонских замків легко зламуються. Зате він дуже ефективний проти крадіжок «на ривок», коли злодій хапає пристрій і біжить — в магазинах, готелях і так далі.

2.9 Реалізація захисту зв'язку

Абонентські станції розділяють один захищений зв'язок для авторизації. Захищений зв'язок для авторизації визначається:

— сертифікатом X.509, що ідентифікує абонентську станцію, а також сертифікатом X.509, що ідентифікує виробника абонентської станції.
— 160-бітовим ключем авторизації (authorization key, AK). Використовується для аутентифікації під час обміну ключами TEK (Traffic Encryption Key, ключ шифрування трафіку).
— 4-бітовим ідентифікатором ключа авторизації.

— Часом життя ключа авторизації. Може набувати значення від 1 дня до 70 днів. Значення за умовчанням 7 днів.
— 128-бітовим ключем шифрування ключа (Key encryption key, KEK). Використовується для шифрування і розподілу ключів TEK.
— Ключем HMAC для витікаючих повідомлень при обміні ключами TEK.
— Ключем HMAC для висхідних повідомлень при обміні ключами TEK.
— Списком data Security Association (SA), для яких дана абонентська станція авторизована.

KEK обчислюється таким чином:

1 Проводиться конкатенація шістнадцятиричного числа 0x53 із самим собою 64 рази. Виходять 512 біт.
2 Справа приписується ключ авторизації.
3 Обчислюється хэш-функция

Перші 128 біт беруться як KEK, останні відкидаються.

Ключі HMAC (hash message authentication code, хеш-кодування-код ідентифікації повідомлень) обчислюються таким чином:

Проводиться конкатенація шістнадцятиричного числа 0x3A (uplink) або 0x5C (downlink) з самим собою 64 рази. Справа приписується ключ авторизації.

Обчислюється хэш-функція SHA-1 від цього числа. Виходять 160 біт на виході. Це і є ключ HMAC.

2.9.1 Авторизація

Протокол авторизації і ключів шифрування (Privacy and Key Management Protocol (PKM Protocol)) — це протокол для здобуття авторизації і ключів шифрування трафіку TEK.

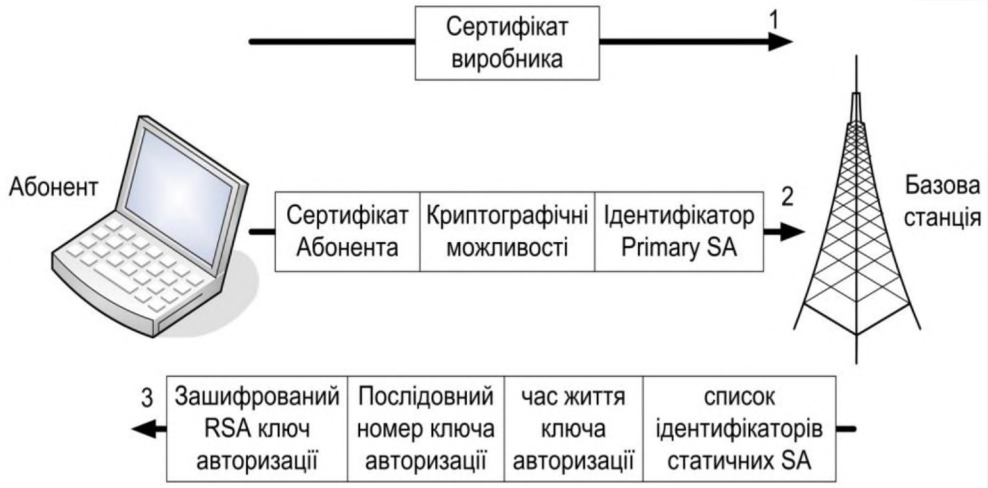

Рисунок. 2.8. - Схема авторизації

1 Абонентська станція починає обмін, посилаючи повідомлення, X.509, що містить, сертифікат виготівника абонентської станції. Цей сертифікат дозволить базовій станції авторизувати лише абонентські станції від виробників, що довіряють.

2 Відразу після першого повідомлення, абонентська станція відправляє повідомлення, X.509, що містить, сертифікат самої абонентської станції, її криптографічні можливості і ідентифікатор первинної SA (Primary SA).

3 Базова станція по сертифікату абонента визначає, чи авторизований він. Якщо він авторизований, вона посилає повідомлення, що містить зашифрований ключ авторизації, послідовний номер даного ключа авторизації, його час життя, а також список ідентифікаторів статичних SA, в яких абонент авторизований. Ключ авторизації шифрується алгоритмом RSA із з публічним ключем, що отримується із сертифікату абонентської станції.

Одного разу авторизувавшись, абонентська станція буде періодично авторизуватися знову.

Повторна авторизація:

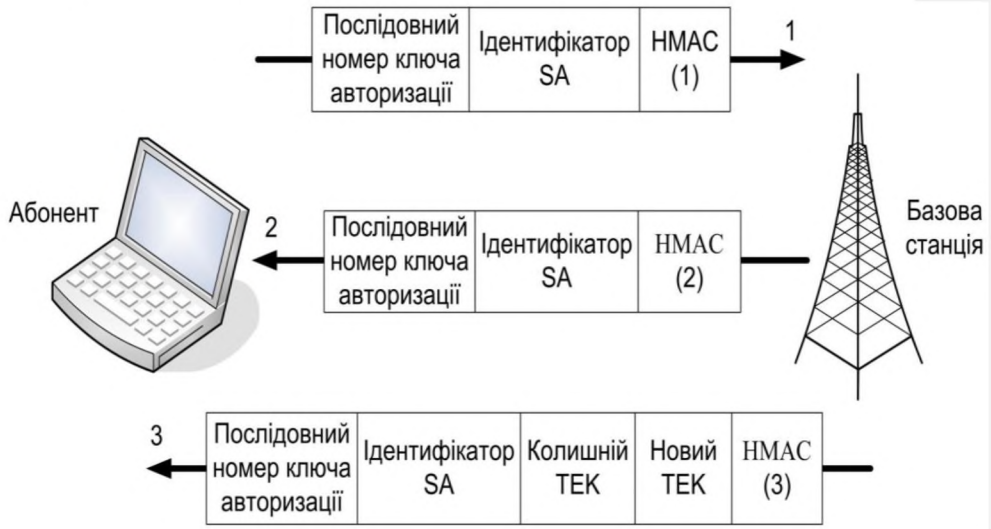

Рисунок 2.9 - Обмін ключами при повторній авторизації

1 Базова станція посилає повідомлення, що змушує абонентську станцію відновити ключ шифрування трафіку TEK. Повідомлення містить:

— послідовний номер ключа авторизації, який був використаний при генерації HMAC

— ідентифікатор того SA, TEK якого необхідно відновити

— HMAC для того, щоб абонентська станція могла перевірити достовірність цього повідомлення.

2 У відповідь на перше повідомлення (при успішній перевірці HMAC), або ж за власною ініціативою абонентська станція посилає запит на оновлення ключа TEK, що містить:

— послідовний номер ключа авторизації, який був використаний при генерації HMAC

— ідентифікатор того SA, TEK якого необхідно відновити (збігається з ідентифікатором з першого повідомлення, якщо воно було)

— HMAC для того, щоб базова станція могла перевірити достовірність цього повідомлення.

3 Якщо попереднє повідомлення пройде аутентифікацію HMAC, базова станція посилає повідомлення, що містить:

— послідовний номер ключа авторизації, який був використаний при генерації HMAC

— ідентифікатор SA, для якого проводиться оновлення ключа TEK

— колишній TEK, тобто поточний TEK того SA, для якого запитано оновлення

— новий TEK, тобто TEK, який використовуватиметься, коли закінчиться термін життя поточного TEK

— HMAC для перевірки достовірності даного повідомлення.

Обидва ключа TEK передаються в зашифрованому вигляді. У IEEE 802.16 для цього використовується потрійний AES в режимі електронної кодової книги з ключем KEK.

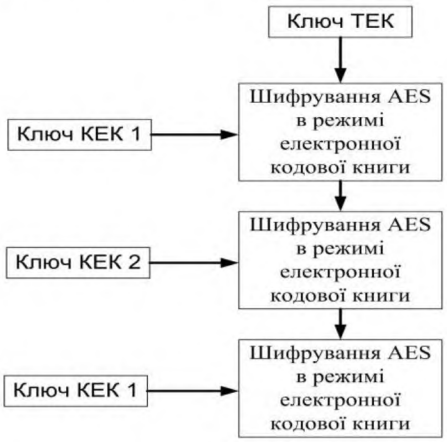

Рисунок 2.10 - шифрування ключа TEK

Де: KEK 1 — це перші 64 біт ключа KEK

KEK 2 — останні 64 біт ключа KEK

2.9.2 Шифрування

Стандарт IEEE 802.16 використовує алгоритм DES в режимі зчеплення блоку шифрів для шифрування даних. В даний час DES вважається ненадійним, тому в даній роботі вирішив використовувати новіший алгоритм AES, даний алгоритм був доданий в новий стандарт IEEE 802.16e.

Стандарт 802.16e визначає використання шифрування AES в чотирьох режимах:

— Cipher Block Chaining (CBC, режим зчеплення блоку шифрів)

— Counter Encryption (CTR, шифрування лічильника)

— Counter Encryption with Cipher Block Chaining message authentication code (CCM, лічильникове шифрування з message authentication code, отриманим зчепленням блоку шифрів). Додає можливість перевірки достовірності зашифрованого повідомлення до режиму CTR.

— Electronic Code Book (ECB, режим електронної кодової книги). Використовується для шифрування ключів TEK.

Структура пакету Nonce

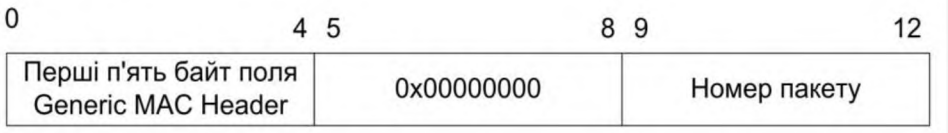

Рисунок. 2.11 - Структура пакету Nonce

У режимі CCM, для шифрування корисної інформації передавальна станція генерує на кожен пакет nonce — байтову послідовність, перші 5 байтом якої є початок Generic MAC Header. Далі йдуть 4 зарезервованих байта, таких, що мають нульові значення. Потім слідує 4-байтовий номер пакету Packet Number (PN) в даному data SA. Значення Packet Number ставиться в 1 при встановленні нового data SA або нового TEK.

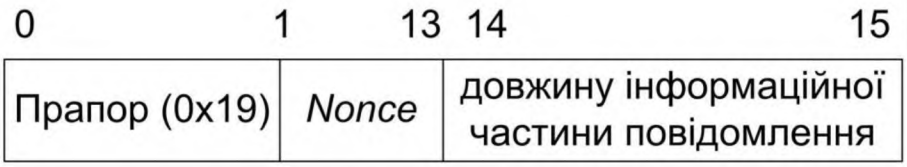

Рисунок. 2.12 - Структура блоку CBC

Блок CBC складається з однобайтового прапора, що має значення 00011001, послідовності nonce і поля, що містить довжину інформаційної частини повідомлення.

Рисунок. 2.13 - Структура блоку Counter

Блок Counter складається з однобайтового прапора, що має значення 00000001, послідовності nonce і поля, що містить номер «i» Counter-блока. Число «i» може змінюватися від нуля до n, де n — кількість Counter-блоков, необхідних для покриття всього повідомлення і коди message authentication code.

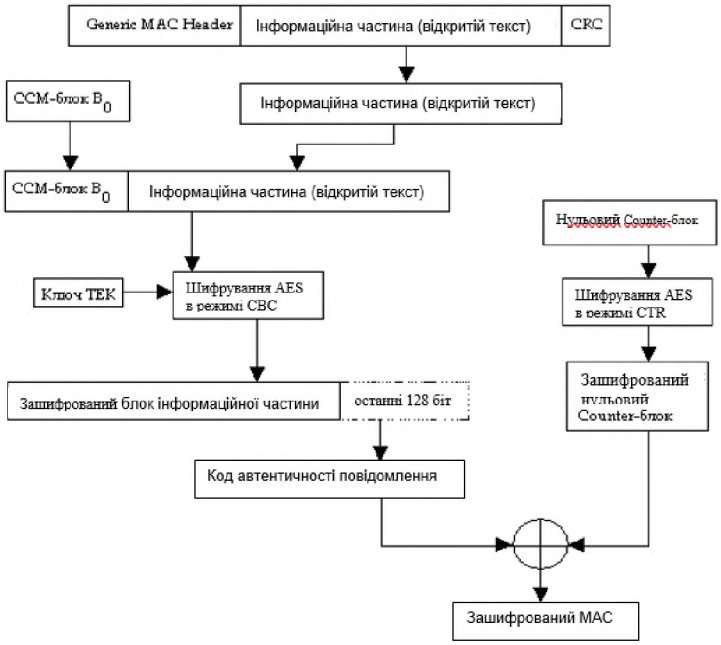

Рисунок 2.14 - Створення і шифрування коду автентичності повідомлення

При створенні message authentication code (код автентичності повідомлення) використовується модифікований режим CBC, в якому замість вектора, що ініціалізує IV, на початок інформаційної частини повідомлення приєднується початковий (нульовий) блок CBC. Далі ця пара зашифровується алгоритмом AES в режимі CBC з ключем TEK. Останні 128 біт зашифрованого тексту беруться як код автентичності повідомлення. Далі код автентичності повідомлення шифрується побітовим складанням по модулю два початкового коду автентичності і зашифрованого за допомогою алгоритму AES в режимі CTR початкового (нульового) Counter-блока.

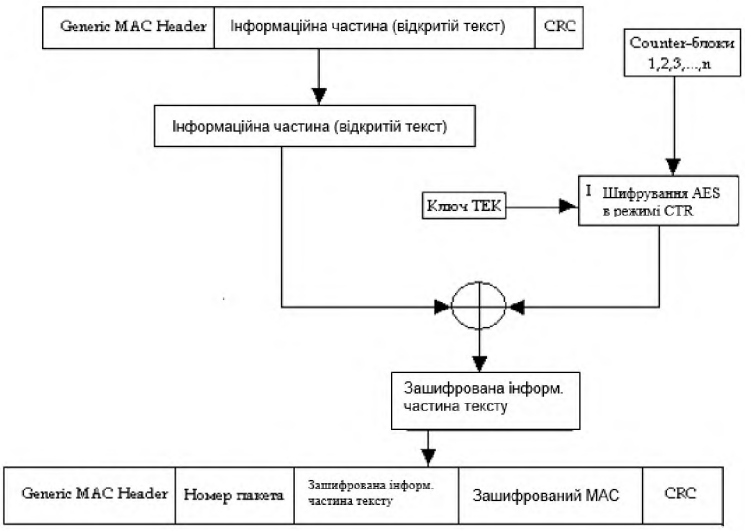

Рисунок. 2.15. - Схема шифрування інформаційної частини

Кожен з n Counter-блоков (нульовий вже був задіяний в шифруванні message authentication code), що залишилися, зашифровують методом AES в режимі CTR з ключем TEK. Потім результат складають побітовим складанням по модулю два з інформаційною частиною повідомлення. Отриманий зашифрований текст разом із зашифрованим кодом автентичності повідомлення, номером пакету даних, заголовком Generic MAC Header і CRC-кінцівкою вирушає на фізичний рівень. При цьому в заголовку GMH поле EC (Encryption Control) встановлюють в одиницю, оскільки дані були зашифровані, а в двобітовому полі EKS (Encryption Key Sequence) коштує індекс використаного при цьому ключа TEK (traffic encryption key).

2.9.3 Захист дисків за допомогою шифрування диска BitLocker

BitLocker виконує дві взаємодоповнюючі, та різні функції. По-перше, він забезпечує шифрування всього тому ОС Windows. По-друге, він

дозволяє перевірити цілісність завантажувальних компонентів до запуску Windows.

BitLocker шифрує весь том ОС Windows зі всіма даними. Це ключовий аспект в захисті конфіденційної інформації, що міститься на комп'ютерах підприємства, особливо переносних. Переносні комп'ютери крадуть і втрачають щодня. Завдяки збільшеним можливостям переносних пристроїв, а також все більшої долі мобільності в роботі один співробітник може мати при собі сотні гігабайт промислових секретів підприємства, секретних документів або відомостей, що забезпечить документам збереження.

Головна відмінність BitLocker в тому, що він працює автоматично, прозоро і поширюється на весь том. Наприклад, в EFS потрібно явно вказувати, які файли і папки шифрувати. А BitLocker шифрує все, що записується на захищений ним том, включаючи файли операційної системи, реєстр, файли сплячого режиму і підкачки, застосування і їх дані.

Не шифруються три елементи: завантажувальний сектор, пошкоджені сектори, вже відмічені як нечитані, і метаданні томи. Останні складаються з трьох надлишкових копій даних, використовуваних BitLocker, включаючи статистичну інформацію про том і захищені копії деяких ключів розшифровки. Ці елементи не вимагають шифрування, оскільки не є унікальними, цінними або дозволяючими визначити особу.

Шифрування всього тому захищає від атак з виключенням (offline attack), які мають на увазі обхід операційної системи. Типовий приклад — крадіжка офісного комп'ютера, витягання жорсткого диска і установка його як другий диск іншого комп'ютера (під управлінням іншої копії Windows або взагалі іншою ОС), що дозволяє обійти дозволи NTFS і введення пароля. Прочитати таким чином диск, захищений BitLocker, неможливо.

BitLocker використовує алгоритм AES з ключем 128 біт. Для більшої надійності довжину ключа можна збільшити до 256 біт за допомогою

групових політик або через постачальник інструментарію управління Windows (WMI) для BitLocker.

Кожен сектор тому шифрується окремо, при цьому частина ключа шифрування визначається номером цього сектора. В результаті два сектори, що містять однакові незашифровані дані, в зашифрованому вигляді виглядатимуть по-різному, що сильно затрудняє визначення ключів шифрування шляхом запису і шифровки наперед відомих даних.

Перед застосуванням шифрування BitLocker використовує алгоритм, званий дифузором (diffuser). В результаті його застосування навіть найдрібніша зміна початкового тексту приводить до абсолютної зміни всього сектора зашифрованих даних. Це також серйозно затрудняє визначення ключів або дешифровку.

2.9.4 Ключі BitLocker

Самі сектори шифруються ключем шифрування всього тому (full-volume encryption key, FVEK). Користувачі, проте, з цим ключем не працюють і доступу до нього не мають. Сам ключ FVEK шифрується основним ключем тому (volume master key, VMK). Такий рівень абстракції дає унікальні переваги, але робить весь процес важчим для розуміння. Ключ FVEK зберігається в суворій секретності, тому що при його розголошуванні було б потрібно перешифровати всі сектори. Оскільки перешифрования займе значний час, варто не допускати розголошування ключа. Тому система працює з ключем VMK.

Ключ FVEK (зашифрований ключем VMK) зберігається на диску серед метаданих тому. При цьому він ніколи не потрапляє на диск в розшифрованому вигляді.

Ключ VMK також шифрується, і охороняється, одним або декількома запобіжниками ключів. Для додаткової захищеності об'єднаємо пароль з частковим ключем, що зберігається на USB- накопичувачі. І те, і інше — зразок двохфакторної перевірки достовірності.

При запуску система шукає відповідний запобіжник ключа, опитуючи TPM (довірений платформений модуль), перевіряючи порти USB або, якщо необхідно, запрошуючи користувача. Виявлення запобіжника ключа дозволяє Windows розшифрувати ключ VMK, яким розшифровується ключ FVEK, яким розшифровуються дані на диску.

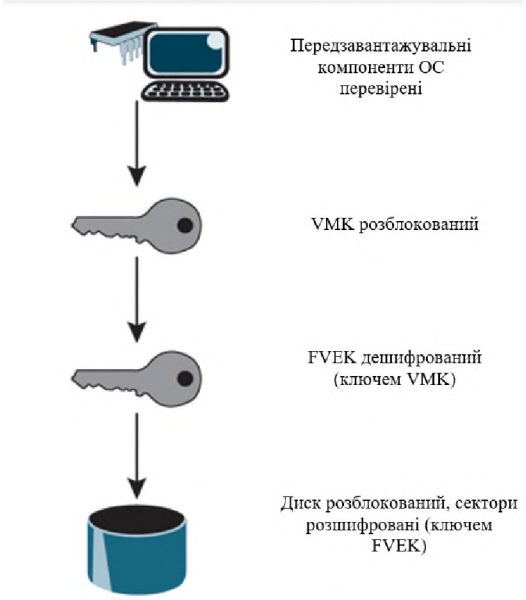

Рисунок. 2.16 - Запуск системи

2.10 Організаційні заходи

Організаційні заходи являються одною з найважливіших вимог аби зменшити кількість помилок обумовлених дією працівників на підприємстві.

Для цього розробляються спеціальні інструкції для персоналу підприємства, які представлені в таблиці 2.5

Таблиця 2.5 - розроблені інструкції користувача

Суб'єкт	Інструкція	Опис

Користувач	По роботі з віддаленим підключенням до мережі.	Ця інструкція розроблена з метою підвищення працездатності персоналу, а також забезпечити спостережливість інформації.
	По та авторизації в мережі.	Ця інструкція розроблена з метою покращити конфіденційність інформації та знизити кількість помилок при авторизації в мережі.
	По роботі з системою антивірусного захисту.	Ця інструкція розроблена з метою знизити ризик зараження клієнтського обладнання вірусами чи шкідливими програмами які можуть задати шкоду цілісності інформації.
	По роботі з між мережевим екраном.	Ця інструкція розроблена з метою підвищення кваліфікаційного рівня який дозволить покращити конфіденційність та доступність інформації.
	По роботі з системою шифрування BitLocker.	Ця інструкція розроблена з метою покращити конфіденційність інформації при втраті або крадіжці клієнтського обладнання.

2.11 Профіль захищеності підприємства ТОВ «Рубін

Профіль захищеності підприємства ТОВ «Рубін» представлений в таблиці 2.6

Таблиця 2.6 - профіль захищеності підприємства ТОВ «Рубін»

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)

	Адміністративна конфіденційність	КА-2 (Базова адміністративна конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-2 (базова конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Адміністративна цілісність	ЦА-2 (базова адміністративна цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-2 (базова цілісність при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Достовірний канал	НК-1 (однонаправлений достовірний канал)
	Розподіл обов'язків	НО-2 (розподіл обов'язків адміністраторів)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1 (автентифікація вузла)

Профіль захищеності:
3.КЦД.2={ КД-2,КА-2,КО-1,КВ-2,ЦД-1, ЦА-2, ЦО-1, ЦВ-2,ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2 Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується на підприємстві ТОВ «Рубін» здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта .
Запити на зміну прав доступу до об'єкта оброблятися на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.
Система аудентіфікації надає користувачу можливість для захищеного об'єкта, що належить його домену, визначити конкретних користувачів і групи користувачів, які мають право одержувати інформацію від об'єкта .

КА-2 Базова адміністративна конфіденційність
Політика адміністративної конфіденційності, що реалізується на підприємстві ТОВ «Рубін» здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта .
Запити на зміну прав доступу оброблятися тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.
Система розмежування доступу надає можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і групи користувачів, які мають право одержувати інформацію від об'єкта.
Система розмежування доступу надає можливість адміністратору повноваження, визначити конкретних користувачів або групи користувачів, які мають право ініціювати процес.
КО-1 Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується на підприємстві ТОВ «Рубін» відноситься до всіх об'єктів комп'ютерної системи.
Перш ніж користувач або процес одержить в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта

будуть скасовані.
Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КВ-2 Базова конфіденційність при обміні
Політика конфіденційності при обміні, реалізується шифруванням методом AES, він визначає множину об'єктів і інтерфейсних процесів, до яких він відноситься.
Політика конфіденційності при обміні, що реалізується методом шифруванням AES, забезпечує високий рівень захищеності, який забезпечується механізмами AES, що використовуються.
Шифрування AES забезпечує захист від безпосереднього ознайомлення з інформацією яка передається.
Запити на призначення або зміну рівня захищеності обробляються тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

ЦД-1 Мінімальна довірча цілісність
Політика довірчої цілісності, що реалізується на підприємстві ТОВ «Рубін» здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.
Запити на зміну прав доступу до об'єкта обробляються на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.
Система аутентифікації надає користувачу можливість для захищеного об'єкта, що належить його домену, визначити конкретних користувачів або групи користувачів, які мають право модифікувати об'єкт.

ЦА-2 Базова адміністративна цілісність

Політика адміністративної цілісності, що реалізується на підприємстві ТОВ «Рубін» здійснює розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Запити на зміну прав доступу обробляються тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Система аутентифікації надає можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси або групи процесів, які мають право модифікувати об'єкт.

Система аудентіфікації надає можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів або групи користувачів, які мають право ініціювати процес.

ЦО-1 Обмежений відкат

Політика відкату, що реалізується на підприємстві ТОВ «Рубін» здійснюють автоматизовані засоби, які дозволяють авторизованому користувачу відкотити або відмінити певний набір операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2 Базова цілісність при обміні

Політика цілісності при обміні, що реалізується на підприємстві ТОВ «Рубін» визначає множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів керувати рівнем захищеності.

Код автентичності повідомлення (message authentication code, MAC) забезпечує можливість виявлення порушення цілісності інформації, яка передається, а також фактів його видалення або дублювання.

Запити на присвоєння або зміну рівня захищеності обробляться КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

ДР-1 Квоти

Політика використання ресурсів, що реалізується на підприємстві ТОВ «Рубін» визначає обмеження, які накладаються, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень оброблятися тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1 Ручне відновлення

Політика відновлення, що реалізується на підприємстві ТОВ «Рубін» визначає множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Прописані чітко рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування абонент повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

НР-2 Захищений журнал

Політика реєстрації, що реалізується на підприємстві ТОВ «Рубін» визначає перелік подій, що реєструються захищеним журналом, здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації містить інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації містить інформацію, достатню для встановлення користувача, процесу або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратори і користувачі, яким надані відповідні повноваження, мають в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2 Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується на підприємстві ТОВ «Рубін» визначає атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися в мережі.

НК-1 Однонаправлений достовірний **канал**

Політика достовірного каналу, що реалізується на підприємстві ТОВ «Рубін» визначає механізми встановлення достовірного зв'язку між користувачем і базовою станцією.

Достовірний канал використовується для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу ініціюється виключно користувачем.

НО-2 Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується на підприємстві ТОВ «Рубін» визначає ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків визначає дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

НЦ-2 КЗЗ з гарантованою цілісністю

Політика цілісності на підприємстві ТОВ «Рубін» визначає домен, а також механізми захисту, що використовуються для реалізації розподілення доменів.

Адміністратор підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації або втрати керування.

Також описані обмеження, дотримання яких дозволяє гарантувати, що

послуги безпеки доступні тільки через інтерфейс адміністратора і всі запити на доступ до захищених об'єктів контролюються адміністратором.

НТ-2 Самотестування при старті

Політика самотестування, що реалізується на підприємстві ТОВ «Рубін» визначає властивості КС і реалізовані процедури, які будуть використані для оцінки правильності функціонування комплексу засобів захисту . Самотестування здатне виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при і автентифікації.

НВ-1 Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується на підприємстві ТОВ «Рубін» визначає множину атрибутів і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим абонентами.

2.12 Політика резервного копіювання

При резервному копіюванні рекомендується використовувати декілька резервних копій (2 і більше), що будуть зберігатися на різних знімних носіях. При додаванні резервної копії на знімний носій, вона заноситься до теки, ім’я якої повинно містити порядковий номер резервної копій та дату резервного копіювання.

Технологічна інформація, конфігурації ПЗ і т.д. необхідно копіювати на окремі знімні носії, які має право використовувати лише системний адміністратор. Резервне копіювання цих даних має проводитися як мінімум раз на місяць.

Рекомендується для резервного копіювання та відновлення системи використовувати ПЗ «Veeam Backup & Replication», яке сумісне з засобами Active Directory. Засобами ПЗ «Veeam Backup & Replication» системний адміністратор повинен створити архів, що містить необхідну технологічну інформацію.

До технологічної інформації, що підлягає резервному копіюванню належить:

- групові політики;
- атрибути розмежування доступу;
- конфігурації ПЗ;
- дані про облікові записи.

Рекомендується проводити періодичний аналіз стану серверу: використовувати ПЗ «Viktoria» для перевірки стану жорстких дисків.

2.13 Політика вибору та зміни паролів

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ електронних документів.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики паролів користувачами системи є системний адміністратор.

Політика безпеки:

– паролі видаються системним адміністратором особисто, відповідальність за видачу паролів згідно приведеним нижче критеріям несе системний адміністратор.

- паролі користувачів мають бути унікальними і не повинні повторюватись;
- паролі мають бути довжиною не менше ніж 8 символів (але не більше 16 символів) і повинні включати у себе:
  - латинські заголовні букви (A-Z);
  - латинські прописні букви (a-z);
  - цифри (0-9);
  - символи, відмінні від букв чи цифр (наприклад: !,$,%,#);
- пароль не має містити ім'я облікового запису;
- паролі заборонено передавати третім особам;
- паролі не можна вставляти до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді;

– паролі мають змінюватися кожні 3 місяці (чи раніше при виникненні загрози розголошення пароля чи його втрати).

При створенні паролю рекомендується використовувати метод «півслова». У такому випадку, частина паролю, що генерується системним адміністратором має бути не коротшою ніж 8 символів, а частина, що генерується системою не має містити повторюваних символів.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює системний адміністратор підприємства за допомогою вбудованих засобів аутентифікації в ОС. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики. Після ознайомлення з даною політикою користувач має підписатися у спеціальному журналі з техніки безпеки.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів. До співробітників, що порушили дану політику безпеки, будуть прийняті дисциплінарні міри.

2.14 Політика оновлення програмного забезпечення

Відповідальною особою за виконання політики є системний адміністратор.

Політика безпеки:

Рекомендується створити регламент планової перевірки актуальності версії. Строки перевірки мають перепадати на 1-5 число кожного нового календарного місяця. Оновлення ПЗ має проводити тільки системний адміністратор.

Системний адміністратор повинен перевіряти кожну нову версію програмного забезпечення у захищеному середовищі, наприклад – на віртуальній машині. Після тестування нової версії, системний адміністратор повинен відправити директору запит із проханням дозволу проведення технічних робіт з оновлення ПЗ. За 3 дні до схваленого оновлення, системний адміністратор повинен сповістити усіх працівників письмово та в електронному вигляді про планове оновлення ПЗ.

Після проведення оновлення ПЗ, системний адміністратор повинен надати директору звіт про проведення технічних робіт з оновлення та налагодження програмного забезпечення, що повинен містити:

- назву ПЗ;
- дату оновлення;
- номер старої версії;
- номер нової версії.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює директор підприємства, контролюючи звітність системного адміністратора про оновлення ПЗ. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.15 Політика захисту бездротової мережі

Область дії політики захисту мережі розповсюджується на мережеве покриття Wi-MAX.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики є системний адміністратор.Усі дії, пов'язані з забезпеченням безпеки мережі повинні виконуватися системним адміністратором.

Для забезпечення надійного захисту рекомендується змінювати пароль для роутерів кожні 2 місяці. Пароль генерує системний адміністратор використовуючи правила створення паролів, описані в політиці вибору та зміни паролів.

Рекомендується змінювати пароль для Wi-MAX мережі кожен місяць (наприклад 1 числа кожного місяця). Пароль генерує системний адміністратор використовуючи правила створення паролів, описані в політиці вибору та зміни паролів. Для кожної окремої робочої станції пароль вводиться окремо системним адміністратором, що дозволяє мінімізувати кількість осіб, що знають пароль.

Рекомендується вимкнути видимість точки доступу, задля унеможливлення виявлення її без спеціалізованого обладнання.

Режим WPS повинен бути вимкненим у налаштуваннях роутерів, оскільки він вважається нестійким до зламу.

Рекомендується вимкнути протокол DHCP та використовувати список довірених MAC-адрес, задля унеможливлення виділення IP-адреси при спробі несанкціонованого підключення.

Рекомендується вимкнути функцію віддаленого доступу у налаштуваннях роутерів, задля унеможливлення отримання доступу до них через мережу Інтернет.

Рекомендується знизити рівень сигналу до такого рівня, щоб сигнал можна буде виявити лише на території підприємства.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює директор підприємства, контролюючи звітність системного адміністратора про стан мережі. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути

сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.16 Політика використання зовнішніх інтерфейсів робочих станцій

Область дії політики безпеки використання зовнішніх інтерфейсів робочих станцій розповсюджується на всіх користувачів, що мають доступ електронних документів та не мають права на використання зовнішніх інтерфейсів робочих станцій відповідно до своїх посадових обов'язків (оператори контактного центру).

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики паролів користувачами системи є системний адміністратор.

Політика безпеки:

До зовнішніх інтерфейсів робочих станцій слід віднести CD/DVD-дисководи та USB-порти.

CD/DVD-дисководи мають бути вимкнені на апаратному рівні системним адміністратором на усіх робочих станція користувачів, відносно яких діє ця політика.

CD/DVD-дисководи можуть бути використані лише системним адміністратором у разі виникнення потреби у встановленні і/або налагоджуванні системи. У такому разі, системний адміністратор має сповістити відповідного співробітника та директора у письмовій формі про проведення технічних робіт, не пізніше ніж за 2 дні. Після проведення робіт, системний адміністратор має подати директору звіт про проведення

технічних робіт з зазначенням причин та інвентарного номера робочої станції, на якій проводились роботи.

USB-порти мають бути опечатані системним адміністратором на усіх робочих станція користувачів, відносно яких діє ця політика. Пломба має містити підпис системного адміністратора. При опечатуванні системний адміністратор повинен робити запис у журналі використання зовнішніх інтерфейсів із вказанням номеру запису, дати опечатування та інвентарного номеру робочої станції. За наявності 2 і більше USB-портів, опечатування кожного порту відзначається окремим записом.

USB-порти можуть бути використані лише системним адміністратором у разі виникнення потреби у встановленні і/або налагоджуванні системи. У такому разі, системний адміністратор має сповістити відповідного співробітника та директора у письмовій формі про проведення технічних робіт, не пізніше ніж за 2 дні. У день проведення технічних робіт з USB-порта знімається опечатування. При знатті опечатування робиться відповідний запис у журналі використання зовнішніх інтерфейсів із вказанням номеру запису, дати опечатування та інвентарного номеру робочої станції. Після проведення робіт, системний адміністратор має знову опечатати USB-порт за вказаною вище процедурою та подати директору звіт про проведення технічних робіт з зазначенням причин та інвентарного номера робочої станції, на якій проводились роботи.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює системний адміністратор, раз на тиждень перевіряючи цілісність печаті та її істинність. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів. До співробітників, що порушили дану політику безпеки, будуть прийняті дисциплінарні міри.

2.16 Організаційні заходи щодо забезпечення реалізації політики безпеки

На організаційному рівні повинні бути проведені наступні заходи:

- розробка та впровадження посадових інструкцій користувачів та персоналу ІТС, а також інструкцій, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;
- обмеження доступ в приміщення, в яких відбувається обробка та зберігання інформації з обмеженим доступом;
- розробка та впровадження розпорядчих документів щодо використання робочих станцій користувачами із зазначенням у них, що користувач несе матеріальну відповідальність за цілісність робочої станції;
- розмежування прав користувачів ІТС із розділенням на групи користувачів, згідно з матрицею доступу, програмними методами ОС
- встановлення максимальної кількості спроб для входу у систему, після якої обліковай запис буде заблокований;
- впровадження механізмів контролю використання CD і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB-портів впровадження механізмів резервного копіювання з метою захисту локальних розділів диску від випадкового або навмисного форматування впровадження регламенту оновлення програмного забезпечення впровадження регламенту створення та зміни паролів (заборона користувачам завантаження, встановлення або оновлення будь-яких програм без відома системного адміністратора;

- проведення навчально-кваліфікаційних заходів, перевірки та закріплення навичок персоналу стосовно роботи з обчислювальною технікою, з метою запобігання помилок персоналу, що можуть зашкодити підприємству у той чи інший спосіб

2.17 Висновок спеціального розділу

В спеціальній частині було проаналізовано існуючий функціональний профіль захищеності, обрано новий профіль, що відповідає вимогам, необхідним для підвищення стану захищеності. Було розроблено перелік організаційних заходів, метою яких є підведення стану захищеності АС до необхідного рівня.

Окремою увагою відзначено вирішення актуальних для даного підприємства проблем інформаційної безпеки, описаних у першому розділі в моделі загроз.

Таким чином, були розроблені рекомендації, щодо доповнення та оновлення існуючої на підприємстві політики інформаційної безпеки стосовно наступних аспектів:

- розмежування доступу до інформаційних ресурсів АС;
- перепустковий режим підприємства;
- резервне копіювання;
- створення та зміна паролів;
- оновлення ПЗ;
- захист мережі.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є визначення економічної доцільності використання запропонованих засобів та заходів інформаційної безпеки на ТОВ «Рубін».

Для визначення цього необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити обсяги відвернених втрат, та, на основі цього, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі розрахованих показників можна буде визначити, наскільки прибутковим або збитковим є запропонований проект.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.[6]

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

- вартість розробки проекту інформаційної;
- витрати на залучення зовнішніх консультантів;
- вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);
- вартість створення основного й додаткового програмного забезпечення (ПЗ);
- витрати на первісні закупівлі апаратного забезпечення;
- витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання,

програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

У таблиці 3.1 наведено вартість обладнання та первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ)

Таблиця 3.1 - Вартість апаратного та програмного забезпечення

Найменування	Вартість за одиницю, грн.	Кількість, шт.	Загальна сума, грн.
Kensington Lock Kensington ComboSaver 64050	290	20	5 800
Абонентський термінал ProST 5.4-5.7GHz TDD - 17dBi Vert (excluding SDA)	3330	2	6660
Адаптер SDA-1-2-EU SDA-1 Type II - EU (for ProST)	185	2	370
USB modem WiMAX Modem Samsung SWC-U 200	395	20	7900
Мережевий коммутатор [DLink] 16port 10/100Base-TX	381	2	762
ДБЖ Mustek PowerMust 400 USB	405	2	810
Шлюз Voip D-Link DVG-5008S	2460	2	4920
Skypemate USB-P1K	150	20	3000
Всього			30222

Відповідно до специфіки розробленої ПБ та конкретних рішень, обраних у цій політиці, актуальними капітальними витратами можна вважати наступні:

– вартість розробки проекту інформаційної безпеки;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Трудомісткість у даному випадку буде розраховуватися за формулою 3.1:

$$t = t_{об} + t_{а} + t_{вз} + t_{озб} + t_{д}\ год, \qquad (3.1)$$

де $t_{об}$ – тривалість проведення обстеження АС підприємства; $t_{а}$ – тривалість процесу аналізу ризиків; $t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту; $t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації; $t_{д}$ – тривалість документального оформлення політики безпеки.

Показники часу, витраченого на розробку політики інформаційної безпеки наведені у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	Значення, год
$t_{об}$	65
$t_{а}$	16
$t_{вз}$	10
$t_{озб}$	16
$t_{д}$	16

Згідно з формулою 3.1 трудомісткість розробки ПБ становить:

$$t = 65\ год + 16\ год + 10\ год + 16\ год + 16\ год,$$

і, таким чином,

$$t = 123\ год.$$

Надалі потрібно розрахувати витрати на створення ПБ ($К_{рп}$), використовуючи наступні показники – витрати на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) та вартість витрат машинного часу ($З_{мч}$). Розрахунок проводиться за формулою 3.2:

$$К_{рп} = З_{зп}\ грн. \quad (3.2)$$

У свою чергу, витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб},\ грн, \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин; $З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, в загальному випадку, становить – 72 грн/год.

Згідно з формулою 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 123\ год \cdot 72\ грн/год,$$

і, таким чином,

$$З_{зп} = 8856\ грн.$$

Тож, витрати на створення ПБ за формулою 3.2 становлять:

$$К_{рп} = 8856\ грн.$$

У результаті розрахунків, маємо вартість розробки ПБ – 8856 гривень.

У даному конкретному випадку повна вартість капітальних витрат розраховується за формулою 3.4:

$$К = Кз + К_{рп} + К_{навч}\ грн. \quad (3.4)$$

Під $К_з$ мається на увазі вартість закупівель обкладення та програмного забезпечення, під $К_{навч}$, мається на увазі одноразовий кваліфікаційний захід для співробітників, з питань ознайомлення з новою редакцією політики безпеки. Даний захід проводиться спеціалістом ІБ, тому додатково йому

виплачується сума у розмірі 500 грн, окрім виплати за розробку нової редакції ПБ.

Тож, згідно до формули 3.4, повна вартість капітальних витрат становить:

$$K = 30222\ грн + 8856\ грн + 500\ грн,$$

і, таким чином,

$$K = 39578\ грн.$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.[6]

Для даного підприємства актуальними будуть наступні витрати:

- заробітна плата обслуговуючого персоналу;
- кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки;
- технічне й організаційне адміністрування й сервіс.

Оскільки методи захисту, передбачені політикою безпеки, мають більш організаційний характер, поточними витратами можна вважати заробітну платню системного адміністратора, витрати на опечатування зовнішніх інтерфейсів робочих станцій та витрати пов'язані з діяльністю користувачів, тож поточні витрати розраховуються за формулою 3.5:

$$C = C_{за} + C_{оп} + C_{дк}\ грн, \qquad (3.5)$$

де $C_{за}$ – витрати на заробітну плату системного адміністратора; $C_{оп}$ – витрати на опечатування зовнішніх інтерфейсів робочих станцій; $C_{дк}$ – витрати, пов'язані з діяльністю користувачів.

У свою чергу, витрати на заробітну плату системного адміністратора розраховуються за формулою 3.6:

$$C_{зпад} = З_{дод1} + З_{дод2}\ грн, \qquad (3.6)$$

Де $З_{дод1}$ – додаткова заробітна плата системного адміністратора за проведення кваліфікаційних заходів та перевірку знать та навичок персоналу стосовно правил, регламентованих політикою безпеки; $З_{дод1}$ – додаткова заробітна плата системного адміністратора за додаткові обов'язки – відповідальність за виконання деяких розділів політики безпеки інформації.

Додаткова заробітна платня №1 складає 500 грн за проведення одного кваліфікаційного заходу. Такі заходи планується проводити раз на 2 місяці, тож фактично за місяць системний адміністратор отримуватиме 250 грн додаткової заробітної платні №1 на місяць. Додаткова платня №2 враховуватиме обсяг відповідальності, що покладатиметься на системного адміністратора політикою безпеки. Таким чином, розмір додаткової заробітної платні №2 становитиме – 1000 грн/місяць.

За формулою 3.6, можна розрахувати:

$$С_{зпад} = (250\ грн\ +\ 1000\ грн) \cdot 12\ місяців,$$

і, таким чином,

$$С_{зпад} = 15000\ грн.$$

Поточні витрати за опечатування зовнішніх інтерфейсів на рік включатимуть у себе вартість 2 журналів (200 грн) опечатування та 150 пломб-наліпок (450 грн). Тож:

$$С_{оп} = 200\ грн + 450\ грн,$$

і, таким чином,

$$С_{оп} = 650\ грн.$$

Витрати, пов'язані з діяльністю користувачів мають під собою на увазі витрати, що спричинені професійною діяльністю. Такою діяльністю вважається перенавантаження серверу і частий перезапис інформації на жорстких дисках серверу у процесі роботи, що приведе сервер у неробочий стан. Такі витрати включають у себе вартість полагодження серверу,

профілактична заміна компонентів. За рік, вартість таких витрат сягатиме 1500 грн. Тож:

$$C_{дк} = 1500\ грн.$$

Розрахунок повної вартості експлуатаційних витрат за формулою 3.5:

$$C = 15000\ грн + 650\ грн + 1500\ грн,$$

і, таким чином,

$$C = 17150\ грн.$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Далі буде вказано загрози з можливим економічним впливом на підприємство:

1 злам мережі, порушення нормального функціонування системи призводить до простою на підприємстві;

2 несанкціоноване ознайомлення з інформацією (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

3 несанкціонована модифікація/видалення інформації (співробітниками) призведе до порушення робочого процесу, що у свою чергу призведе до втрати частини запланованого заробітку;

4 несанкціоноване копіювання інформації на знімні носії (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу

може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

5 помилки персоналу, що дозволяють зловмисникам отримати доступ до системи мають схожий ефект зі зламом мережі;

6 несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками має схожий ефект з несанкціонованим ознайомленням з інформацією працівниками;

7 несанкціонована модифікація/видалення інформації конкурентами та зловмисниками має схожий ефект з несанкціонованою модифікацією/видаленням інформації співробітниками;

8 крадіжка/псування матеріальних цінностей (об'єктів ІТС) конкурентами та зловмисниками призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

9 використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами має схожий ефект зі зламом мережі;

10 злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди має схожий ефект зі зламом мережі;

11 збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює, у свою чергу це призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

12 відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи, що в свою чергу призведе до втрати частини запланованого заробітку.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V\,грн, \qquad (3.7)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн; $П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн; V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ і V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс}{F} \cdot t_п \ грн, \tag{3.8}$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_в = П_{ви} + П_{пв} + П_{зч} \ грн, \tag{3.9}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн; $П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн; $П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{О}{F} \cdot (t_п + t_в + t_{ви}) \ грн, \tag{3.10}$$

де F – місячний фонд робочого часу; $О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \ грн, \qquad 3.11$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в} \ грн, \qquad 3.12$$

де F – місячний фонд робочого часу; $З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

Відповідно до пронумерованого вище списку загроз, можна розрахувати ймовірні збитки. Враховуючи той факт, що деякі загрози мають схожі наслідки, розрахунки будуть проводитись для одного випадку з групи подібних, але надалі буде враховуватись кількість можливих подій на рік та ймовірність їх виникнення.

Відповідно до переліку загроз, вказаного вище, для загроз №1, №5, №9, №10 збитки від реалізації однієї з цих загроз розраховуються за формулами 3.7–3.11:

$$П_п = 13000 \ грн \cdot 14 \ чол/212 \ год \cdot 3 \ год,$$

$$П_п = 2575,47 \ грн.$$

$$П_{ви} = 0 \ грн.$$

$$П_{зч} = 0 \ грн.$$

$$П_{пв} = 14000 \ грн/212 \ год \cdot 1 \ год,$$

$$П_в = 66,03 \ грн.$$

$$П_в = 0 \ грн + 66,03 \ грн + 0 \ грн,$$

$$П_в = 66,03 \text{ грн.}$$

$$V = 3001065 \text{ грн}/212 \text{ год} \cdot (3 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 56623,86 \text{ грн.}$$

І таким чином,

$$U = 2575,47 \text{ грн} + 66,03 \text{ грн} + 56623,86 \text{ грн},$$

$$U = 59264,5 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз №1, №5, №9 або №10 становитиме – 59264 грн 50 копійок.

Для загроз №2, №4, №6 потрібно враховувати не збитки, а розмір не одержаної вигоди від реалізації однієї з цих загроз. Експертним висновком розмір неодержаної вигоди визначені у розмірі – 90031,95 грн/місяць (3% від планового місячного прибутку підприємство не буде отримувати).

Оскільки загрози №8 та №12 мають схожі наслідки, розмір збитку від реалізації однієї з загроз буде таким самим і для іншої і буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн}/212 \text{ год} \cdot 24 \text{ год},$$

$$П_п = 1471,70 \text{ грн.}$$

$$П_{ви} = 0 \text{ грн.}$$

Враховуючи специфіку роботи підприємства, одним з найцінніших ресурсів компанії є робочі станції (ноутбуки), тому в якості показника $П_{зч}$ враховується вартість заміни ноутбука.

$$П_{зч} = 8000 \text{ грн.}$$

$$П_{пв} = 14000 \text{ грн}/212 \text{ год} \cdot 120 \text{ год},$$

$$П_в = 7924,52 \text{ грн.}$$

$$П_в = 0 \text{ грн} + 7924,52 \text{ грн} + 8000 \text{ грн},$$

$$П_в = 15924,52 \text{ грн.}$$

$$V = 1478 \text{ грн}/212 \text{ год} \cdot (120 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 823{,}58 \text{ грн}.$$

І таким чином,

$$U = 1471{,}70 \text{ грн} + 15924{,}52 \text{ грн} + 823{,}58 \text{ грн},$$

$$U = 18219{,}8 \text{ грн}.$$

Тобто, збиток від одноразової реалізації загрози №8 становитиме – 18219 грн 80 копійок.

Оскільки загроз № 3, № 7 та №11 мають подібні наслідки, збиток від їх реалізації буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн} \cdot 14 \text{ чол}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_п = 2575{,}47 \text{ грн}.$$

$$П_{ви} = 14000 \text{ грн}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_{ви} = 198{,}11 \text{ грн}.$$

$$П_{зч} = 0 \text{ грн}.$$

$$П_{пв} = 0 \text{ грн}.$$

$$П_в = 198{,}11 \text{ грн} + 0 \text{ грн} + 0 \text{ грн},$$

$$П_в = 198{,}11 \text{ грн}.$$

$$V = 3001065 \text{ грн}/212 \text{ год} \cdot (3 \text{ год} + 3 \text{ год} + 0 \text{ год}),$$

$$V = 84935{,}80 \text{ грн}.$$

І таким чином,

$$U = 2575{,}47 \text{ грн} + 198{,}11 \text{ грн} + 84935{,}80 \text{ грн},$$

$$U = 87709{,}30 \text{ грн}.$$

Тобто, збиток від одноразової реалізації загроз № 3, № 7 або №11 становитиме – 87709 грн 30 копійок.

Таким чином, маючи дані про можливі збитки від реалізації загроз можна провести розрахунок збитків на рік від реалізації даних загроз. Зводні дані та кінцева величина збитку зазначені у таблиці 3.2:

Таблиця 3.2 – Розрахунок річних обсягів збитків від реалізації загроз

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Злам мережі, порушення нормального функціонування системи	59264,5	1	0,54	32002,83
Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Несанкціоноване ознайомлення з інформацією (співробітниками)	90031,95	1	0,3	27009,59
Несанкціонована модифікація/видалення інформації (співробітниками)	87709,30	2	0,3	52625,58
Несанкціоноване копіювання інформації на знімні носії (співробітниками)	90031,95	1	0,32	28810,22
Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи	59264,5	1	0,70	41485,15
Несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками	90031,95	1	0,5	45015,98

Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди	59264,5	1	0,72	42670,44
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює	87709,30	1	0,36	31575,35
Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи	18219,8	1	0,36	6559,13
ЗАГАЛОМ				372581.72

Для розрахунку коефіцієнтів вірогідності були використані дані з таблиць 1.8 і 1.9, а саме – коефіцієнти К2, що відповідають за мотивацію джерела загрози і зручність використання вразливості відповідно. Рівні коефіцієнта К2 були відповідно змінені на часткову шкалу (1 – 0,2; 2 – 0,4; 3 – 0,6; 4 – 0,8; 5 – 1). На підставі коефіцієнтів К2 джерела і коефіцієнтів К2 вразливості експертним шляхом були визначені коефіцієнти вірогідності реалізації зазначених вище загроз.

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою :

$$E = B \cdot R - C \text{ грн}, \tag{3.13}$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн; R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці; C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Тож, економічний ефект становить:

$$E = 372581{,}72 \text{ грн} - 17150 \text{ грн},$$

$$E = 355431{,}72 \text{ грн}.$$

В загальному вигляді, оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (TCO);
- коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій $T_{\text{О}}$.

У даному випадку TCO не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.14:

$$ROSI = E / K, \tag{3.14}$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн; K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Тож,

$$ROSI = 372581{,}72 \text{ грн} / 39578 \text{ грн},$$

$$ROSI = 9{,}4.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $E_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.15:

$$ROSI > (N_{деп} - N_{інф}) / 100 \qquad (3.15)$$

де $N_{деп} = 19$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %; $N_{інф} = 8$ – річний рівень інфляції, %.

9,4 > 0,11, отже проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.16:

$$T_o = E / K = 1 / ROSI = 0,11 \text{ року.} \qquad (3.16)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки капітальних та поточних витрат на введення та експлуатацію засобів захисту, що рекомендовані політикою безпеки.

В ході розрахунків було з'ясовано що введення в експлуатацію засобів та заходів захисту є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (0,025 року), а коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного

варіанта (9,4 > 0,11). Тож, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВОК

Під час виконання кваліфікаційної роботи було виконано обстеження об'єкта інформаційної діяльності відповідно до порядку обстеження, описаному в НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Окрім цього було проведена класифікація інформації що циркулює в ІТС ТОВ «Рубін» та яка підлягає захисту. Класифікація проводилась відповідно до положень ЗУ «Про інформацію», якими регламентується перелік інформації що може, або не може бути інформацією з обмеженим доступом.

При розробці дипломного проекту було створено комплекс методів та заходів для підвищення інформаційної безпеки ресурсів, що передаються клієнтським обладнанням WiMAX товариства з обмеженою відповідальністю «Рубін». Для поставленої мети були вирішені наступні завдання:

- проаналізовані сучасні тенденції розвитку безпровідних мереж;
- виділені основні проблеми безпеки і найбільш поширені види атак;
- проаналізовано систему авторизації та аутентифікації користувача;
- застосовані програмні та апаратні методи шифрування каналу ;
- розроблені заходи захисту клієнтського обладнання;
- розроблено профіль захищеності для даної мережі та його реалізацію щодо клієнтського обладнання;
- розроблено політики безпеки

У економічному розділі був проведений аналіз економічної ефективності впровадження методів та заходів по захисту інформаційних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1 Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: закон України редакції від 19.04.2014 № 1170-VII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр

2 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]: НД ТЗІ 3.7-003-05 від "8" листопада 2005 №125. – Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

3 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-004-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/

4 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-005-99 від 07.01.1999. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/

5 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 1.1-002-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/

6 Експлуатацію систем інформаційної безпеки [Електронний ресурс] – Режим доступу: https://lektsii.org/15-1904.html

7 Портал современных технологиях мобильной и беспроводной связи [Електронний ресурс]Режим доступу: http://1234g.ru/wimax/struktura-seti-wimax

8 Тестирование WiMAX - описание стандарта, приборы. [Електронний ресурс] Режим доступу: https://www.tehencom.com/Technologies/WiMAX/WiMAX.htm

9 Широкополосный беспроводной доступ по технологии WiMAX. [Електронний ресурс] Режим доступу: https://cyberleninka.ru/article/n/sovremennye-tehnologii-besprovodnogo-shirokopolosnogo-dostupa-802-16e

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	36	
6	А4	Розділ 2. Спеціальна частина	54	
7	А4	Розділ 3. Економічна частина	16	
8	А4	Висновок	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	

ДОДАТОК Б. Перелік документів на оптичному носії

- Давідян Д.А. 125-17-1.docx
- Давідян Д.А. 125-17-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника дипломної роботи

«Захист інформаційних ресурсів у бездротової мережі товариства з обмеженою відповідальністю «Рубін» студента групи 125-17-1 Давідяна Давида Армаісовича

Дипломний проект за спеціальністю 125 «Кібербезпека» Давідян Д.А представлена пояснювальною запискою на 125 стор., містить 28 рис., 13 табл., 4 додатка, 9 джерела.

Мета дипломної роботи – підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє корпоративну інформацію в бездротової мережі WiMAX. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання дипломного проекту були вирішені наступні питання: проаналізовані сучасні тенденції розвитку безпровідних мереж, виділені основні проблеми безпеки і найбільш поширені види атак, аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для ОІД ТОВ "Рубін", приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

До недоліків проекту слід віднести окремі невідповідності вимогам оформленні та не чітко розкрито аналіз ризиків.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до дипломного проекту спеціаліста і заслуговує оцінки "добре", а Давідяну Давиду Армаісовичу присвоєння йому кваліфікації "професіонал з управління інформаційною безпекою" освітньо-кваліфікаційного рівня "спеціаліст".

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.