Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз алгоритмів захисту систем безпровідного зв’язку

Виконав: студент IV курсу, групи СНс-42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Спільник В.Р.
(підпис) (прізвище та ініціали)

Керівник _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Максимчук О.О.
(підпис) (прізвище та ініціали)

Тернопіль 2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«__» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Спільнику Василю Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз алгоритмів захисту систем безпровідного зв'язку

Керівник роботи Матійчук Любомир Павлович, к.е.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » березня 2022 року № _

2. Термін подання студентом завершеної роботи 24 червня 2022р.

3. Вихідні дані до роботи Літературні та Інтернет-джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Історія та різновиди бездротового зв'язку. 1.1. Огляд предметної області задачі проектування. 1.2. Початок розвитку безпровідної передачі даних. 1.3. Різновиди передачі інформації. 1.3.1. Інфрачервона безпровідна мережа. 1.3.2. Одночастотна передача даних. 1.3.3. Технологія SST для передачі даних. 1.4. Технології передачі інформації в діяльності людини. 1.5. Безпровідна локальна мережа. 1.6. Постановка завдань до кваліфікаційної роботи. 1.7. Висновок до першого розділу. Розділ 2. Функціонування мереж безпровідного зв'язку. 2.1. Алгоритм захисту даних та його складова. 2.2. Методи побудови алгоритмів захисту даних. 2.3. Вимоги для криптографічних систем захисту даних. 2.4. Передача даних в клієнт серверній технології. 2.5. Переваги та недоліки клієнт сервер. 2.6. Сучасна технологія передачі інформації. 2.7. Висновки до другого розділу. Розділ 3. Безпека життєдіяльності, основи охорони праці. 3.1. Доілкалська допомога при уражені електричним струмом. 3.2. Загальні вимоги безпеки до обладнання та процесів. 3.3. Висновки до третього розділу.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Слайд 1. Вступ. Слайд 2. Огляд та дослідження предметної області. Слайд 3. Безпровідні технології передачі. Слайд 4. Завдання до кваліфікаційної роботи. Слайд 5. Алгоритми захисту інформації. Слайд 6. Методи створенян алгоритмів безпеки даних. Слайд 7. Клієнт серверна технологія в мережі передачі інормації. Слайд 8. Сучасна технологія передачі даних. Слайд 9. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О. Я., доцент кафедри МТ		

7. Дата видачі завдання 24 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Провести огляд літературних джерел по темі випускної бакалаврської роботи	04.01.2022-30.01.2022	*Виконано*
3.	Провести порівняльну характеристику програмних продуктів	31.01.2022-06.02.2022	*Виконано*
4.	Розробити функціональну схему роботи об’єкта проектування	07.02.2022-13.02.2022	*Виконано*
	Розробка моделі бази даних		
5.	Практична реалізація об’єкта проектування	14.02.2022-06.03.2022	*Виконано*
6.	Описати та розробити організаційні заходи спрямовані на поліпшення стану охорони праці	07.03.2022-03.04.2022	*Виконано*
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	04.04.2022-17.04.2022	*Виконано*
8.	Виконання завдання до підрозділу «Основи хорони	18.04.2022-01.05.2022	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат	10.06.2022	*Виконано*
12.	Попередній захист кваліфікаційної роботи	07.06.2022	*Виконано*
13.	Захист кваліфікаційної роботи	24.06.2022	

Студент _____ Спільник В.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Матійчук Л.П.

АНОТАЦІЯ

Аналіз алгоритмів захисту систем безпровідного зв’язку // Кваліфікаційна робота освітнього рівня «Бакалавр» // Спільник Василь Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНс-41 // Тернопіль, 2022 // С. 51 , рис. – 16 , табл. – 0 , кресл. – 0 , додат. – 0, бібліогр. – 24 .

***Ключові слова**: алгоритми захисту, шифрування, Wi-Fi, ПК, БЗ, WAP, WiMAX, безпровідні локальні мережі, звіт, предметна область.*

В кваліфікаційній роботі розглянуто теоретико-методологічні аспекти безпровідної мережі передачі інформації. Робота складається із вступу, трьох розділів, висновків, списку посилань на використану літературу і додатків. У вступі обґрунтовується актуальність теми та формуються задачі подальшого дослідження.

В першому розділі було розглянуто різновиди передачі інформації . Класифікації технологій безпровідних мереж передачі інформації, оптимізацію та поєднання їх з сучасними технологіями. Визначено завдання, які були поставлені до кваліфікаційної роботи.

У другому розділі було розглянуто алгоритми захисту інформації в мережі Інтернет. Розглянуто методи побудови алгоритмів захисту інформації. Проаналізовано клієнт серверну технологію, методи, якої чітко та дуже тісно пов’язані з новітніми технологіями передачі даних. Аспекти алгоритмів захисту у поєднанні з безпровідними технологіями передачі даних.

У третьому розділі розглянуто долікарську допомогу при уражені струмом. А також вимоги безпеки до обладнання та технологічний процесів.

ANNOTATION

Protection algorithms analysis for wireless communication systems// qualification work of educational level "bachelor" // comrade vasyl romanovych // ternopil national technical university named after ivan pulyuy, faculty of computer information systems and software engineering, department of computer science, group sns-41 // ternopil, 2022 // p. 51, fig. – 16, table. – 0, chair. – 0, add. – 0, bibliogr. – 24.

Keywords: protection algorithms, encryption, wi-fi, pc, database, wap, wimax, wireless local area networks, report, subject area.

Theoretical and methodological aspects of wireless information transmission network are considered in the qualification work. The work consists of an introduction, three chapters, conclusions, a list of references and appendices. The introduction substantiates the relevance of the topic and forms the tasks of further research.

In the first section, the types of information transfer were considered. Classifications of technologies of wireless networks of information transmission, optimization and their combination with modern technologies. The tasks that were set for the qualification work are determined.

In the second section, algorithms for protecting information on the internet were considered. Methods of constructing information protection algorithms are considered. The client's server technology is analyzed, the methods of which are clearly and very closely related to the latest data transfer technologies. Aspects of security algorithms in combination with wireless data transmission technologies.the third section considers pre-medical care for electric shocks. As well as safety requirements for equipment and technological processes.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Bluetooth – це технологія бездротового зв'язку, створена у 1998 році групою компаній.

Campus Area Network – кампусна мережа – об'єднує локальні мережі близько розташованих будівель.

Enhanced Data Rates for GSM Evolution – найбільш швидкісна технологія передавання даних в мережах GSM.

General Packet Radio Service – загальний сервіс пакетного радіо передавання.

Globalstar (Глобалстар) – це система із групи супутників низької навколоземної орбіти, що призначена для супутникових телефонів і низько швидкісного передавання даних.

GSM – міжнародний стандарт для цифрового безпровідного зв’язку другого покоління.

Local Area Network – локальні мережі, що мають замкнуту інфраструктуру до виходу на постачальників послуг.

LTE – мобільний стандарт високошвидкісного передавання даних четвертого покоління, що базується на мережевих технологіях GSM/EDGE та UMTS/HSPA.

SST – технологія яка використовує розподіл сигналу за спектром частот. Це дає змогу значно підвищити перепускну здатність каналу завдяки більшій завадостійкості.

WAP – це протокол бездротового доступу до Інтернет сайтів безпосередньо з мобільних телефонів.

WiMAX – стандарт безпровідного зв’язку четвертого покоління, який забезпечує широкосмуговий зв’язок на значні відстані.

Комп’ютерна мережа – система зв'язку комп'ютерів та/або комп'ютерного обладнання (сервери, маршрутизатори та інше обладнання).

Комутатор – пристрій, який визначає, кому саме адресовано отримані дані, а тому надсилає їх не всім пристроям, а лише одержувачу.

Мережа – сукупність яких-небудь шляхів, ліній зв'язку, каналів і т. д., розташованих на певній території.

Роутер – сполучна ланкою між двома різними мережами, яка передає дані, ґрунтуючись на певному маршруті, зазначеному в його таблиці маршрутизації.

Сервер - це комп'ютер у локальній чи глобальній мережі, який надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів.

Супутниковий зв'язок – один з видів радіозв'язку, що базується на використанні штучних супутників Землі, на яких змонтовані ретранслятори.

ЗМІСТ

ВСТУП

В наш час пристрої набувають все більшої популярності, настає з кожним днем період комп’ютерного розвитку. Збільшується обсяг інформації, який створює інформаційний вибух в житті та усіх сферах діяльності людини. Ці всі пристрої уже є невід’ємною частиною життя і роблять нас залежними від них, адже в них знаходяться всі важливі документи і технології, які спрощують буденну роботу.

Актуальність дослідження. Безпровідні технології також відіграють важливу роль у передачі даних там, де неможливе або дороге прокладання кабельних ліній на значні відстані. При передачі даних слід враховувати, що обробка цієї інформації проходить декілька етапів роботи. При передачі даних, необхідно приділити увагу алгоритмам, які будуть використанні для шифрування повідомлень в мережі. Через збільшення безпровідних технологій, зросла необхідність у підвищенні захисту інформації при передачі та її отриманні. Методи та засоби, які необхідно визначити для забезпечення цілісності системи обміну даними призвело до дослідження алгоритмів захисту у безпровідних технологіях.

Допомагають виконувати будь-яку роботу за більш короткий термін, при цьому ефективність і зручність зростає. Завдяки безпровідним пристроям вільний доступ до пакетів даних, раніше вважався цінною системою передачі, а зараз в час новітніх технологій є звичним ділом.

У зв’язку зі збільшенням технологій сучасної передачі даних через бездротовий зв’язок, протягом останніх років статистика показує, що в результаті широко застосовуючи пристроїв та технологій, ціни на обладнання стає все доступнішим для всіх охочих. Час технологій щільно охоплює наше життя і складається враження, що бездротове з’єднання оточує нас скрізь: на ноутбуках, ПК, пристроях кишенькового застосування, мобільних телефонах і маршрутизаторах. Бездротовий зв'язок являє собою процес передачі інформації

електромагнітними хвилями на відстань через вільне повітряне середовище, а не за допомогою традиційних провідних або інших фізичних каналів. Значення надійного забезпечення мобільних обчислювальних і телекомунікаційних послуг стрімко росте. Отже, потрібно забезпечити кращий захист даних від несанкціонованого входу в мережу. Гарантувати надійність алгоритмів безпеки від небажаного втручання. Основні механізми безпеки конфіденційність, цілісність та доступність. У разі бездротового зв'язку (як і в багатьох інших мережах), основні механізми безпеки: аутентифікація, авторизація і також контроль доступу будуть досягнуті.

Мета та практичне значення роботи – аналіз підвищення захищеності та надійності мереж безпровідного доступу для захисту від будь-яких атак з використанням технічного підходу, який реалізує процес аутентифікації і шифрування.

В даній роботі розглянуто алгоритми та основні безпровідні мережі передачі інформації. Детальніше розглянуто методи захисту даних та роль безпровідних технологій, а також принципи їх роботи.

РОЗДІЛ 1. ІСТОРІЯ ТА РІЗНОВИДИ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

1.1. Огляд предметної області задачі проектування

У системах телекомунікації вирішити проблему захисту інформації є можливим при використанні алгоритмів та методів їх шифрування в мережі та при передачі даних. Базою для забезпечення даних є криптографічний захист. Алгоритми, які виконує криптографічний захист дозволяє забезпечити умови збереження цілісності та конфіденційності інформації. Покращити анонімність у відкритій мережі, сигнали чи повідомлення, які передаються безпровідним шляхом.

Насамперед, що являє собою криптографія. Криптографія – це поєднання методів та засобів, алгоритмів, які здійснюються для збереження та захисту даних, при передачі їх одержувачу в мережі. Криптографічні алгоритми, протоколи та засоби, які застосовуються при захисті даних називають криптографічною системою [6].

Повідомлення, яке відправник бажає надіслати одержувачу в криптографічній системі називають відкритим текстом. За для того щоб приховати інформацію, яку несе повідомлення через мережу використовують шифрування. Процес, який відбувається при перетворенні шифруванні повідомлень у вільний текс має назву розшифрування. Схема криптографічної системи зображено на рисунку 1.1.

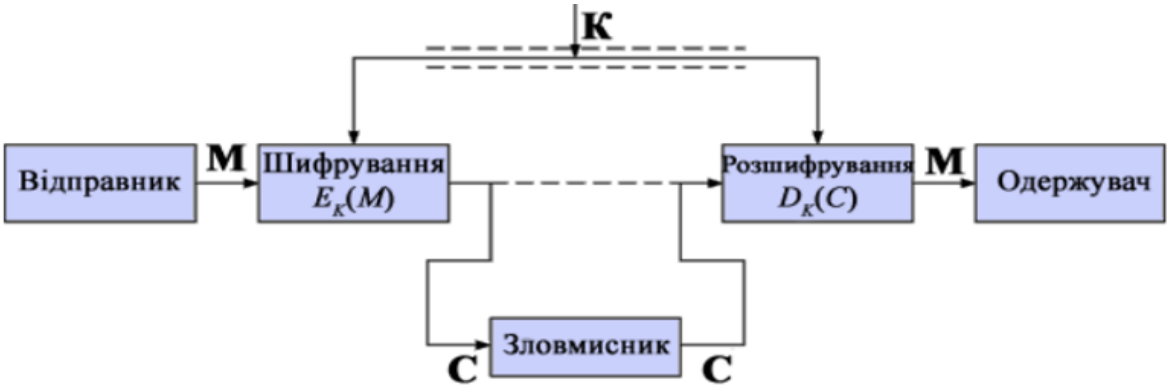

Рисунок 1.1 – Загальна схема криптографічної системи

У прикладній математиці є окремий розділ, під назвою криптоаналіз. Даний розділ вивчає методи, алгоритми, моделі, засоби для того, щоб відкритий текст можна було вільно передавати будь-яким користувачам мережі, при цьому не думаючи про захищеність та надійність передачі. Відкритий текст, який слугує повідомленням при шифруванні не стискає інформацію, що є важливим елементом в передачі даних.

Криптографічний алгоритм, або шифр – це математична функція, яка застосовується для шифрування та розшифрування вільного тексту при передачі в мережі. Вузьке застосування має обмежений алгоритм, дані якого є в таємниці. Але в сучасному світі технологій, він не відповідає стандартам. Причиною є те, коли автор групи алгоритму залишає її, усі члени повинні надавати повторний запит до алгоритму, що займає певний час [22].

Для захищення даних, а також вирішення проблем обмежувальних алгоритмів застосовують ключі. Ключ – це певний стан параметрів алгоритму, при якому відбувається умова підбору однієї правильної відповіді в криптографічній системі з усіх наведених та можливих. Кількість можливих відповідей для певного алгоритму називають середовищем ключів. Бувають і винятки при яких, ключі шифрування та розшифрування відрізняються між собою. Якщо алгоритм при шифруванні залежить від ключа, використовують операції керування. Даний шифр буде керованим.

Криптографічні системи, поділяються в загальному на класи базою яких є незалежні характеристики:

– Вибір типу операції, у процесі перетворення повідомлення в шифрування;

– Кількість ключів, які застосовують;

– Методи для обробки повідомлень.

Система алгоритму може бути симетричною, в тому випадку, коли: відправник та одержувач застосовують для шифрування однакові ключі. І асиметричною, при відкритому та секретному ключах [23].

1.2. Початок розвитку безпровідної передачі даних

Бездротове передавання даних здійснюється завдяки електромагнітних сигналів між двома або більше точками, які не повинні бути з'єднанні електричним провідником. Одними із перших найбільш потребуючих безпровідних мереж зв'язку були радіохвилі. Одним із представників передачі даних за допомогою радіохвиль була технологія Bluetooth, відстань передачі була короткою водночас існувала ще одна мережа, яка передавала інформацію на мільйони кілометрів так звана: зв'язком космічних кораблів. Вперше концепцію застосування було досліджено в Массачусетському технологічному інституті Кевіном Ештоном (англ. Kevin Ashton) в 1999 році. У дослідженні йшлося про створення на запровадження методів, а також засобів радіочастотної ідентифікації допоможе покращити та змінити систему керування логістичними ланцюгами в корпорації і дасть змогу аналізувати кількість та відстежити продукти технологій без діяльності людини [2].

Поняття безпровідний був використаний два рази в історії під час спілкування, в дещо іншому контексті. Приблизно перший раз був використаний з 1890 р. Через велику кількість конкуренції, а також використання спільного середовища важливою умовою ефективності роботи бездротових мереж мають процеси, які виконуються на підрівні доступу до фізичного середовища. Через чималий недолік бездротових мереж є неможливість вузлом мережі «відчути» колізію при передачі кадру у ефірі, в основу методу розподіленого доступу до фізичного середовища було закладено метод запобігання колізії, який, в свою чергу, є модифікацією методу доступу до середовища з виявленням колізії, що раніше широко використовувався в провідних мережах.

Крім того, при черговому збільшенні швидкості передачі сигналів протокол управління доступом до середовища стає перешкодою усієї системи, забороняє отримати значний приріст пропускної здатності навіть при використанні найдієвіші технології фізичного рівня. Наприклад, при функціонуванні безпровідної мережі згідно специфікації стандарту 802.11n пропускна здатність підрівня MAC (Media Access Control) управління доступом до фізичного середовища може бути навіть в п’ять разів нижча, ніж швидкість передачі сигналів [3].

Розвиток можливостей технологій бездротової передачі сигналу в мережі є реалізацію та покращенням методу керування доступу до пакетів даних. У результаті з поєднанням недоліків використання методів з’єднання з базою даних через фізичний рівень виникає проблема у створенні та використанні бездротової мережі інноваційних можливостей, а також сучасних технологій [1].

Через високу популярність мобільних пристроїв та інших технологій люди частіше почали використовувати мобільні пристрої, як спосіб отримання нової інформації, відстеження своєї діяльності, виконання роботи, перегляд поширених ресурсів, наприклад Facebook чи You Tube і т. д. У зв’язку з цим, збільшується навантаження на сервери мережі мобільних операторів, супроводжуючи погіршенням ефективності на якість та надійність мережі та зв'язку. Під час моніторингу мобільної мережі Інтернет користувачі більшу частину трафіку використовували на перегляд онлайн-відео (Див. рисунок 1.2.)

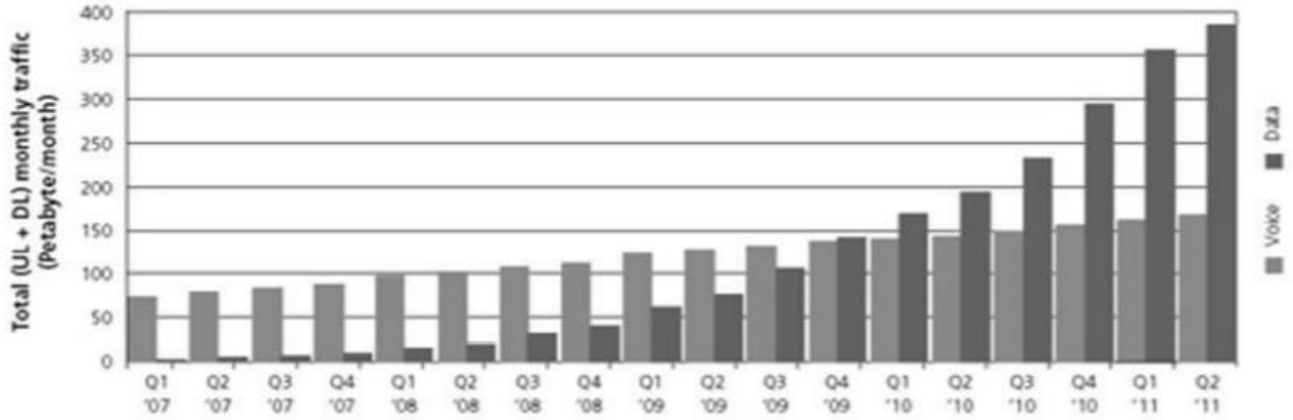

Рисунок 1.2 Аналіз дослідження онлайн-відео трафіку

В ході аналізу графіку спостерігається збільшення голосового трафіку ніж обмін пакетними даними. Ці чинники визначають більш стрімке зростання використання трафіку абонентами операторів мобільного зв'язку. Чимало методів видозміни технології доступу до простору віддана оптимізації стартової ідентифікації одного або більше вирішальних можливостей MAC-підрівня станції не беруть до уваги збільшення зміни навантаження системи, кількості станцій, різне співвідношення видів трафіку, рівень вимог в середовищі. Окрім цього, застосування більшої кількості алгоритмів потребує важливих змін існуючих методів доступу до середовища. Через це виникає проблема в сумісності з передачею даних вузлам мережі функції яких та ефективність роботи залежить від стандартних схем доступу [5].

1.3. Різновиди передачі інформації

З кожним роком розвиток комунікацій безпровідних мереж передачі даних зростає. На ринку комунікацій збільшується вибір приладів та обладнання бездротового з'єднання, зокрема технологій для створення мереж зв'язку. Загалом є декілька видів застосування мереж, серед яких: офіси компаній, концертні зали, з'єднання між собою локальних мереж на відстані, збільшення кількості територіальних розподілених мереж. Першими технологіями передачі інформації безпровідним шляхом були побудовані на основі інфрачервоних променів [1].

1.3.1. Інфрачервона безпровідна мережа

Суть інфрачервоної безпровідної мережі полягає у передачі даних з одної точки відправника в іншу точку отримувача через інфрачервоні промені. Щоб ефективно відбувалась передача даних важливим фактором є генерування

сильних сигналів тому, що інший вплив на мережу будуть здійснювати окремі джерела. Прикладом такого методу передавання даних є світло через вікно. Завдяки такому способу передача сигналів здійснюється швидко, оскільки інфрачервоні промені мають більший діапазон частот. Для повноцінної роботи інфрачервоної мережі необхідно виконувати передачу даних на швидкості 10 Мбіт/с. Лазерна технологія передачі даних в локальній мережі за допомогою інфрачервоних каналів зображено на рисунку 1.3.

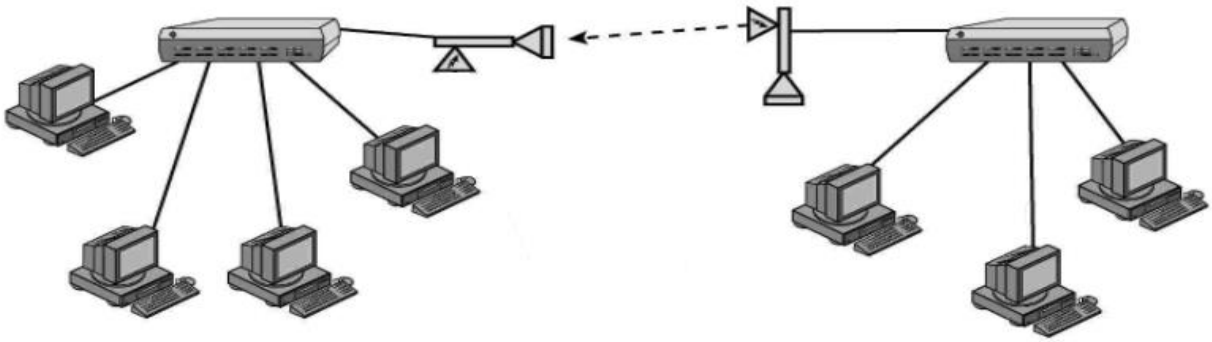

Рисунок 1.3 Локальна мережа з використанням інфрачервоних каналів

Технологія лазером подібна на інфрачервону тим, що вимагає прямої видимості між передавачем і приймачем. Якщо з якої-небудь причини промінь буде перерваний, то це зупинить і передачу. Буває чотири типи інфрачервоних мереж показано на рисунку 1.4 [7].

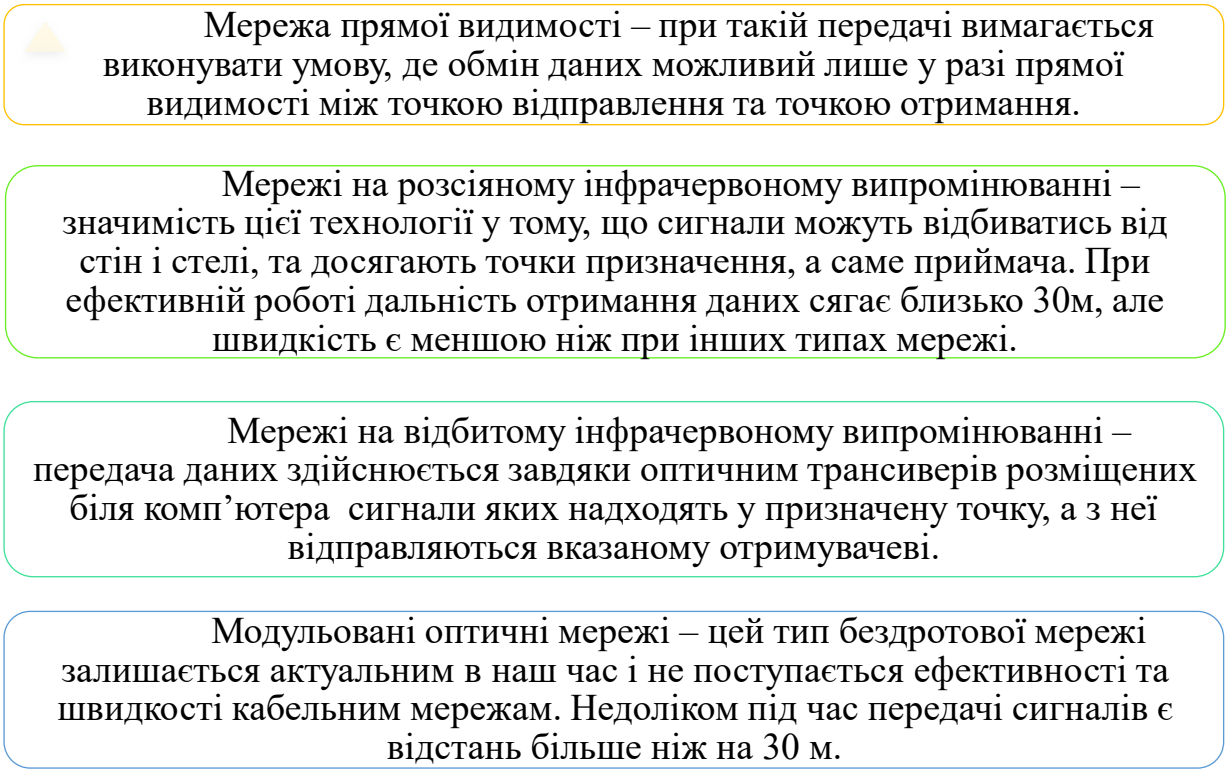

Рисунок 1.4 – Типи інфрачервоних мереж

1.3.2. Одночастотна передача даних

Радіоканал передачі даних – слугує каналом отримання та відправлення даних, але необхідним елементом цієї ланки є наявність антенної системи. Частиною даного середовища слугує поширення радіохвиль на спеціальні пристрої реагування для отримання сигналів їх ще називають так звані радіоприймальні пристрої. Технічна складова радіоканалів відрізняється своїми функціями і призначеннями. Поділяється на види сигналів передачі в залежності від зони обслуговування, частоти та потужності сигналів, пропускна здатність чи діапазон смуги передавання. Окремою ознакою радіопередачі даних є випромінювання сигналів вільним чином у середовище, що негативно впливає на передачу та їх отримання радіоприймачем. Оскільки, радари, станції зв'язку чи передавачі отримують пакети даних вільно, це погано впливає на сумісність з іншими пристроями радіохвиль. При передачі радіосигналів застосовується

діапазон частот і модуляція яких поєднається з сигналом частоти для отримання даних. Одним із важливих недоліків радіочастот та сигналів радіохвиль є низький рівень захисту від несанкціонованого доступу. У зв'язку, із цим прослуховуванням сигналів відбувається занадто часто, тому сигнали радіохвиль здійснюють передачу неконтрольовано [2].

Існує інший спосіб передачі у вузькому діапазоні, завдяки передачі даних мовленням простої радіостанції. Суть якої, у передачі інформації на певну частоту який користувач сам вказує при налаштуванні приймача. Видимість сигналу є не обов'язкова, діапазон передачі даних розподіляється на середню відстань сигналів, яка становить 45 400 м². Сигнал зменшує свій радіус дії, якщо проходить через перешкоди, це може бути металеві чи залізобетонні об'єкти. Доступ до такого типу передачі інформації відбувається через людину, яка уповноважена і має права до отримання даних [2]. Найбільш поширеним методом моніторингу та автоматизованого керування передачі даних бездротової мережі є модуль аналізу показаного на рисунку 1.5.

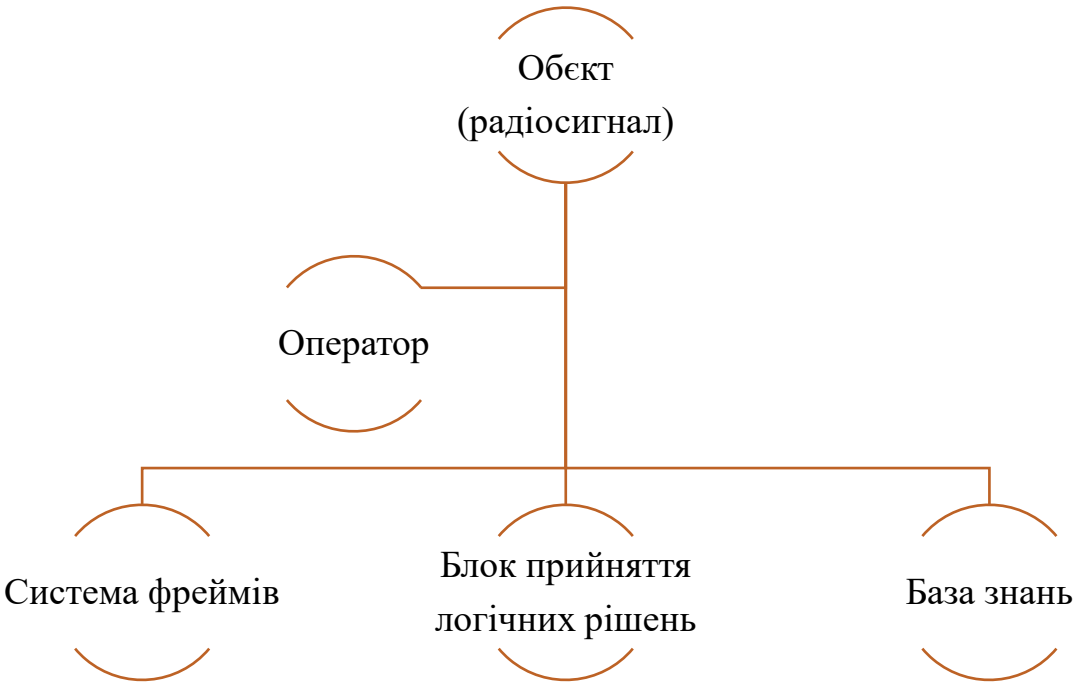

Рисунок 1.5 – Структура методу

Спостерігається також розсіяний спектр радіосигналів спосіб якого, отримання та передача відбувається на різні частоти. Цей спосіб дає одну важливу перевагу, що допомагає усунути вразливості, як при одно частотному спектрі. Частоти, які є вільними для використання поділені на канали. Звукознімач під час обробки даних у період отриманні і опрацювання налаштований на окремий канал, після виконаної операції переходить на інший. Перехід одного сигналу на інший у персональних комп'ютерах є автоматизований, усі дії відбуваються синхронно. Особливість даного способу є у індивідуальному захисті даних. Захистом є алгоритм, який здійснює перехід на інші канали, прослуховування не може бути виконаним, до поки не буде введений ключ доступу [8].

Для більш захищеного доступу до середовища використовують кодування, яке дає змогу уникнути несанкціонований вхід у систему. Цей спосіб є один із найповільніших, оскільки передача здійснюється на швидкості 240 Кбіт/с. Існують також мережі, швидкість яких значно збільшується у відкритій місцевості, та становить одну третю швидкості в приміщенні.

Для отримання приймачем даних і відправлення його іншому приймачу використовують діапазони частот ультразвукового та короткохвильового зв'язку. Кожен пристрій отримання даних має антену та передавач для н передавання сигналів у певну точку [3].

1.3.3. Технології SST для передачі даних

У технології SST (Spread Spectrum Technology) використано розподіл сигналу за спектром частот. Це дає змогу значно підвищити перепускну здатність каналу завдяки більшій завадостійкості. Технологію SST уже тривалий період застосовували для військових потреб. Є два різновиди мереж SST (Див. рисунок 1.6.)

Рисунок 1.6 – Різновиди мереж SST

Завдяки технології SST можна збільшити пропускну здатність, а також забезпечити більш захищений спосіб шифрування мережі від прослуховування. Зовнішній приймач який не має доступу до отримання даних такі сигнали бачить, як «білий шум». У поєднанні з технологією SST працює система VSAT. Принцип роботи є у розташуванні стаціонарних супутників геолокації, які розміщені на відстані близько 38 тис. км від екватору Землі. км. Особливістю даної технології каналу VSAT (Див. рисунок 1.7.).

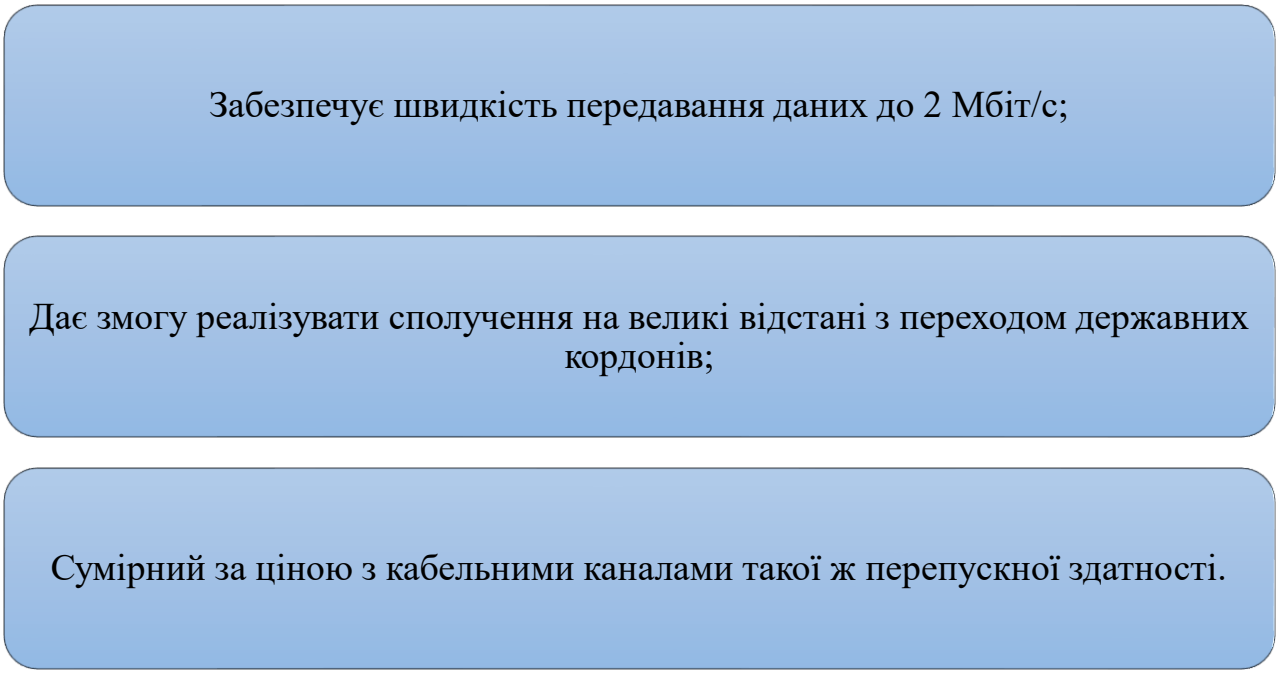

Рисунок 1.7 – Особливості технології VSAT

Попри його особливість, відмінність полягає цього каналу у затримці передачі даних, що зумовлює значно більший час виконання процесу чим технологія SST. Через цю досить значну причину при обробці даних, канал VSAT не можна застосовувати у системах реального часу [4].

Для покращення ефективності та функціонування бездротових технологій та приладів використовують сучасні методи, а також низько звукові обладнання. Передача сигналів виконується на радіочастотах, які сприймає приймач напрямлений у певну точку. Наявність засобів і високотехнологічних методів забезпечує шифрування каналів зв’язку на новому рівні, застосовуючи їх в цифрових мережах. Праця дослідників в галузі передачі пакетів даних дозволила покращити ефективність виконання отримання сигналів та їх безпосередньо відправлення в поставлену точку.

Результатом дослідження та методів їх реалізації розроблено обмежену кількість шаблонів аутентифікації для отримання як найкращих технологій при передачі інформації в сучасному просторі інформаційної мережі. Підходи їх виконання, а також втілення методів специфікації значно зросли під час

дослідження та аналізу безпровідного зв’язку передаванням даних моделлю мовного повідомлення. У зв’язку зі збільшеним напливом використання мереж та середових, а також пристроїв отримання сигналів зросла необхідність у реалізації методів зниження помилок в системі та атак включно з усуненням їх завчасно. Для отримання найбільш ефективного захисту системи важливим питання є функціональність передачі та оцінювання ризиків при застосуванні нових методів обробки інформації в телекомунікаційних системах мережі та зв’язку [22].

Для покращення та ефективного надання послуг враховуючи якість та безпеку при передачі інформації доцільно використовують актуальні цифрові системи обрахування даних з кодуванням сигналу від несанкціонованого доступу. Високий рівень пропускної здатності каналів забезпечує єдність та надійність передачі сигналу що в свою чергу зменшує варіанти втручання та атак на систему керування. Цілісність даних залежить від моделі захисту їх забезпечення з урахуванням безпеки на апаратному чи програмному рівні. З кожним роком підходи і засоби подачі інформації для нових слухачів та глядачів, які вирішили здобути нові знання у галузі комунікаційних технологій активно покращуються [4].

1.4. Технології передачі інформації в діяльності людини

З кожним роком розвиток технологій різко збільшується, передача даних переходить на новий рівень. Пакети даних та захист їх алгоритмів постійно вдосконалюється. Варто зазначити що, технології, які допомагають передавати дані широко застосовують в освітньому процесі. Велика кількість інформації проходить обробку в мережі. Захист даних повинен відповідати високому рівню шифрування інформації. Інформація, яка надходить одержувачу не завжди може використовуватись відкрито. Тому, варто акцентувати увагу на алгоритми їх захисту. Метою технологій передачі в діяльності людини є поєднати

саморозвиток та заохочення нових осіб в пізнання нової інформації та технологічного процесу. Серед критеріїв можна відокремити одні із головних, які є необхідними в процесі їх використання в системі та мережі зв'язку (Див. рисунок 1.8).

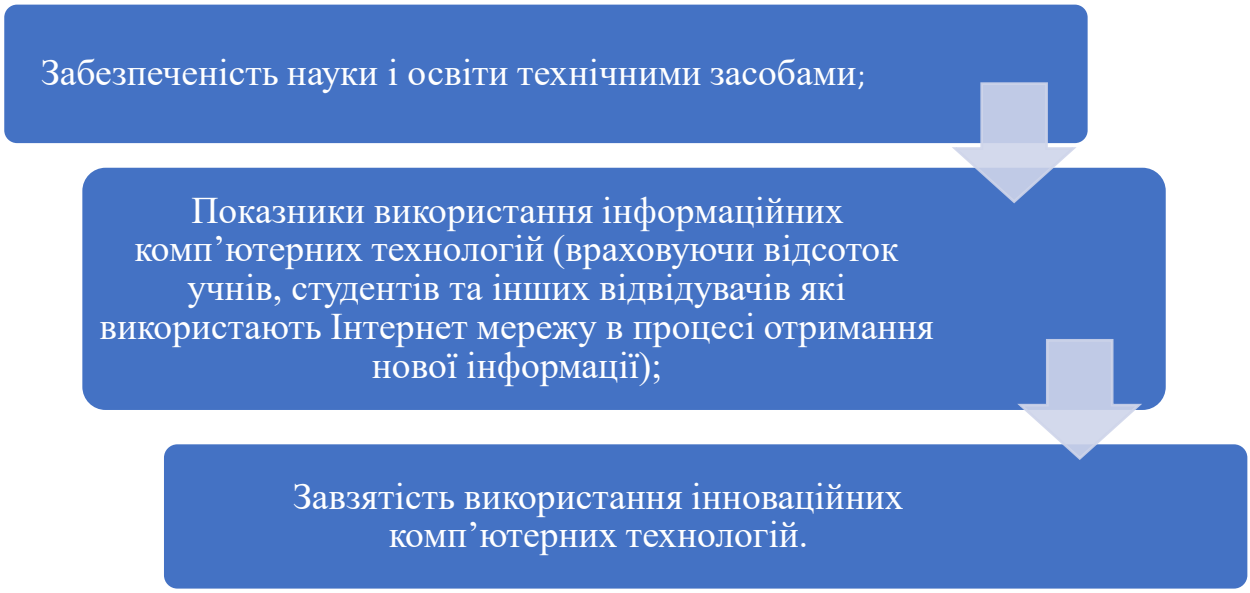

Рисунок 1.8 – Критерії для досягнення ефективності

Інноваційні технології передачі даних та їх використання в діяльності людини забезпечують швидкість та ефективність роботи. А також суттєво полегшують виконання поставленого завдання, при цьому час на їх реалізацію зменшується мінімум в два рази. Щоб процес був цілком успішний і не виникало проблем про роботі з технологіями отримання та передачі інформації необхідно запровадити перелік критеріїв для доцільного використання. Запровадження критеріїв значною мірою впливають на досягнення та залежать від певної галузі на процес та якість.

1.5. Безпровідна локальна мережа

Бездротова локальна мережа відома під назвою Wireless Fidelity, була розроблена на базі сімейства стандартів IEEE 802.11. Раніше поняття Wi-Fi застосовували лише для позначення пристроїв та обладнання, які передають дані в певних частотах. В наш час цей термін використовують безпосередньо для технологій комунікації безпровідного зв’язку та іншого обладнання у даній сфері. Для забезпечення зв’язку між двома локальними мережами використовують пристрій під назвою міст, принцип роботи полягає у передачі кадрів з однієї мережі до іншої. Відмінність повторювача від моста у неможливій підтримці побітового синхронізму в обох зв’язаних між собою мережах [9].

Завдяки тому, шо протоколи працюють на канальному рівні всі протоколи в мережі не відрізняються одним від іншого, перевагою цього слугує недоступна інформація для протоколів, які розміщені на високих рівнях даної моделі. Керування доступу до середовища прямолінійно залежить від мостів, які утворюються при їх зв’язку. Перевірка усього трафіку та підключених пристроїв до їх портів, а також сегментів є основною функцією виконання мостів. Передача пакетів даних, перевірка адрес одержувача та залежність усієї системи все це належить до прямих функцій моста, який має спільну мережу отримання інормації. Для кращого розуміння на рисунку 1.9. продемонстровано конфігурацію, яка належить до розряду однокомірної безпровідної локальної мережі [15].

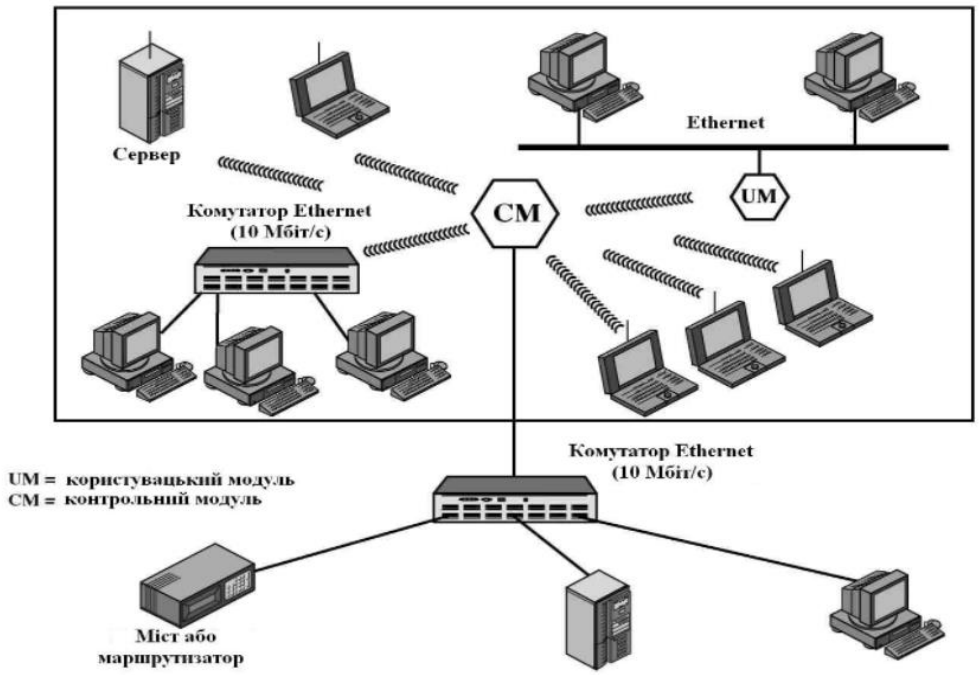

Рисунок 1.9 – Приклад однокоміркової конфігурації безпровідної локальної мережі

Даний приклад представлений для більшості середовищ, які застосовують конфігурацію локальної мережі. Існує різновид локальної мережі на основі Ethernet, забезпечує підтримку серверів, станцій робочого середовища, в залежності від застосування одного чи більше мостів, і приладів для покращення зв'язку з іншими мережами [9].

Одним із елементів управління є модуль, який в свою чергу працює, як пристрій з'єднання однієї безпровідної мережі та іншої. Модуль управління має схожі за функціоналом можливості маршрутизатора, тобто пристрою який роздає сигнал, а також функції, які напряму відносяться до моста. З'єднює між собою декілька мереж, безпровідним чином. Відповідає за регулювання доступу до сховища, схема передачі даних, зв'язана між іншими мережами та механізмом виконання операції.

При збільшенні потреб передачі та навантаження системи доцільно використовують багатокоміркову локальну безпровідну мережу проілюстровано на рисунку 1.10.

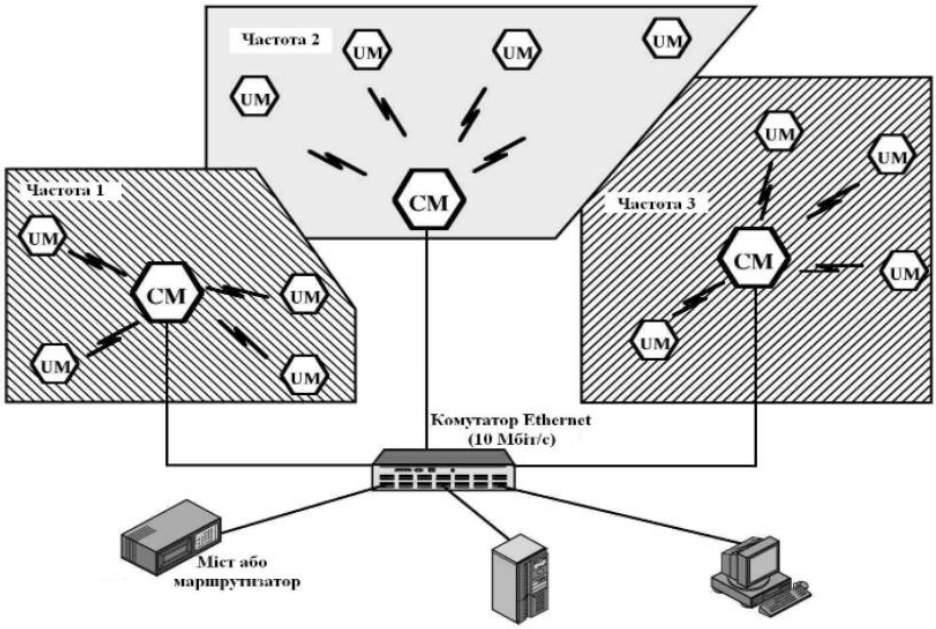

Рисунок 1.10. – Приклад багатокоміркової конфігурації мережі

Деякі кінцеві системи є самостійними і не залежать від механізму передачі, до них можна віднести робоча станція чи сервер виконання дій. Наприклад, технологія передачі зв’язку буде інфрачервоний сигнал, радіус дії передачі зменшується до меж одного приміщення [22].

1.6. Постановка завдань до кваліфікаційну роботу

В час, де технології передачі інформації відіграють одну із важливих ролей, а також займають не останнє місце в діяльності людини. Розвиток пристроїв та обладнання покращується, захист даних має відповідати сучасним технологіям. Методи та засоби для реалізації захисту алгоритмів та пристроїв підключення їх в мережу, а також передавання даних з одного приймача в інший є в пріоритеті. В час сучасних технологій допомагають налагодити, покращити, збільшити ефективність навчання освіти нових осіб, які бажають отримати нові знання. Варто акцентувати увагу саме на алгоритмі захисту даних. Саме ці аспекти захисту передачі даних завдяки безпровідним технологіям варто

детальніше вивчити та проаналізувати. Досягнення саме цієї мети й буде завданням до кваліфікаційної роботи.

1.7. Висновок до першого розділу

В першому розділі було розглянуто різновиди передачі інформації. Історію виникнення пристроїв та обладнання для отримання пакетів даних на відстані безпровідним шляхом. Проаналізовано працю вчених в даній галузі дослідження, аспекти використання технологій у різних галузях людської діяльності. Класифікації технологій безпровідних мереж передачі інформації, оптимізацію та поєднання їх з сучасними технологіями. Визначено та досліджено завдання, які були поставлені до кваліфікаційної роботи, що в свою чергу привело до висновку.

РОЗДІЛ 2. ФУНКЦІЮВАННЯ МЕРЕЖ БЕЗПРОІДНОГО ЗВ'ЯЗКУ

2.1. Алгоритм захисту даних та його складова

Перед тим, як говорити про методи захисту алгоритмів варто ознайомитись, що таке криптографічна стійкість шифрів. Криптографічна стійкість – здатність алгоритму протидіяти атакам, які можуть бути при передачі даних в мережі. Алгоритм буде стійким, за умови якщо час на зламування ключа до шифру буде більший від часу передачі інформації відправника до одержувача. Для визначення стійкості алгоритму використовують оцінку атаки на криптосистему та її заподіяну шкоду. Давніше криптографія належала до розрядку військових технологій, але зі збільшенням безпровідних технологій в сучасному світі спричинило потребу алгоритмів захисту даних.

З появою систем, які мають відкритий ключ захист інформації в криптосистемах збільшився. Раніше основним завдання криптографічного захисту було шифрування даних. То в наш час, область криптографії збільшилась до меж ліцензування, електронного підпису, електронні гроші, онлайн конференції та схеми обміну голосів. Ключі, які надходять у систему перевіряються одержувачем чи адміністратором, який відповідає за надання доступу до криптосистеми через ключ. Якщо ключ є вільним, він з легкістю може бути опублікований в мережі з відкритим доступом.

Тому, значна кількість алгоритмів криптосистеми має свої особливості, різниця полягає від найпримітивніших характеристик системи до принципів їх захисту. Через це, половина з них є оформлена, як стандарти і не несе жодної користі для захисту даних. Створення методів надійного криптографічного алгоритму є дуже важлива задача [22].

2.2. Методи побудови алгоритмів захисту даних

Найбільш поширенішим видом атаки на шифр є метод перебору всього шифрування. Метод перебору – базове вирішення проблем захисту шляхом перебору усіх можливих варіантів атак на криптосистему. Шифр можна вважати стійким, якщо метод перебору відповідає захисту усіх можливих варіантів підбору ключів. Атаки, які були здійснені на методі перебору є найбільш поширеними та були довготривалими.

Керування доступом – метод захисту даних завдяки налагодженій роботі усіх ресурсів системи. Метод керування доступом має ряд функцій представлені на рисунку 2.1.

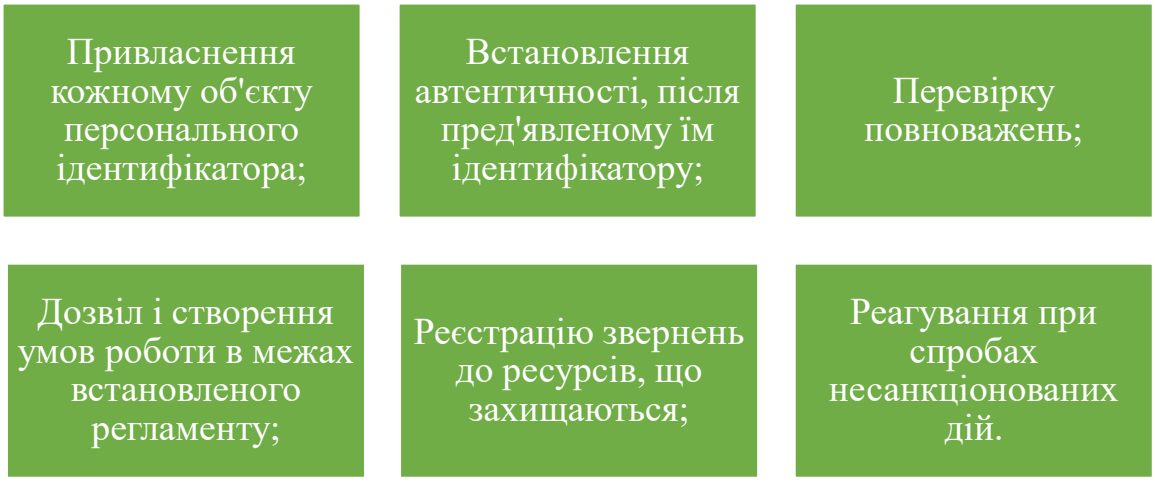

Рисунок 2.1 – Функції методу керування доступом

Традиційний метод захисту побудований на базі секретного ключа, який відправник ділиться з отримувачем повідомлення. При такому методі, шанс на несанкціонований доступ до мережі є значно менший, але має свої недоліки. Передача секретного ключа здійснюється через шлях, який є менш зашифрований. Спираючись на те, що ключ містить низьку оцінку даних і шанс

що, на нього звернуть увагу є дуже низьким. Також важливим питанням є узгодження обох сторін, як буде відбуватись передача секретного ключа [23].

Метод захисту з ключем алгоритм якого поділяють на дві основні групи асиметричного та симетричного шифрування. Симетричне шифрування – алгоритми у яких, для захисту інформації застосовується один ключ розшифрування або шифрування, що легко обчислюється навпаки. Саме симетричне шифрування теж розділене на блоковий та потоковий вид. Блоковий алгоритм поділений на блоки, зазначеної довжини. Згодом ці блоки потрібно по черзі шифрувати. Потокове шифрування відбувається перш за все, коли дані, які необхідно захистити неможливо розбити на блоки. Це стосується символів, які не можуть бути розділені між собою. Через це, цей вид шифрування полягає у захисті даних по символьно [22].

Асиметричне шифрування – використовують два види ключів. Першим менш важливим ключем є відкритий шифр даних використовують його як, зашифровування інформації. І секретний ключ, від якого все залежить, для розшифрування. Цінність цього методу – будь-яка інформація, набір даних, символи, які захищені відкритим шифром можуть бути розшифровані лише одним секретним ключем.

Алгоритми аутентифікації – є високо захищеними, оскільки дозволяють перевірити чи клієнт, який надсилає запит на отримання даних є особою, яка є власником цієї інформації. Простий спосіб аутентифікації – пароль з певною кількістю символів чи букв. Більш складним способом можна вважати перевірку відпечатку відбитка пальця чи сітківки ока.

Алгоритми електронного підпису – метод забезпечення цілісності даних у підписі користувача, перевірка якого має ряд нюансів. Наприклад, вхід в систему при введені паролю та аутентифікації, особливість кожної людини у її написанні букв, які є у підписі, нахилу їх та інше.

Генератори випадкових чисел – метод, захисту даних якого є випадкові числа, використовується він у поєднанні з іншими методами. Найбільш поширенішими методами з генератором чисел є аутентифікації та цифрового підпису.

Існують методи, які використовують лише один та два ключі алгоритмів. Одно ключовий алгоритм є вільний шифр, захист його є мінімальний. Двох ключовий алгоритм є секретний та вільний шифр, безпека цього захисту є значно більшою [23].

2.3. Вимоги для криптографічних систем захисту даних

В результаті створених та перевірених методів захисту інформації було поставлено ряд вимог, які варто дотримуватись при захисті інформації в криптосистемах. Криптографічна система – поєднює перетворення шифру та ключів. Опис та залежність шифру від ключа не є криптосистемою, а методи їх поєднання та особливості використання. Незалежно від того, як буде реалізовано криптосистему алгоритму є сформовані певні вимоги:

– Алгоритм шифрування не має бути нищим за рівень стійкості криптосистеми.

– Повідомлення, тобто шифр може бути прочитаним лише в тому випадку, коли буде підібрано правильний ключ.

– Повідомлення, яке є зашифрованим повинно бути стійким до атак, навіть в тому варіанті, коли відомо більшу кількість даних про методи захисту даних.

– Кількість операцій, які потрібні для розшифрування повідомлень мають бути добре захищеними від усіх атак, які може здійснити сучасний комп’ютер.

– Якщо змінити хоча б один елемент ключа алгоритму, це має призвести до проблеми та збільшенні часу входу в систему.

– Елементи структури алгоритму обов’язково мають бути незмінними від будь-яких несанкціонованих втручань.

– Залежність між ключами та будь яким методом криптосистеми не повинен відповідати усім можливим варіантам входу.

При дотриманні вимог для криптографічних систем зростає цілісність та захищеність доступу до інформації через безпровідну мережу. Поєднання методів алгоритмів збільшують безпеку даних. Передача інформації є стійкою до зловмисників, які хочуть отримати доступ до системи управління [22].

2.4. Передача даних в клієнт серверній технології

Технології розвиваються надзвичайно швидко обчислювальні системи в світі є дуже затребуваними. Серед цих систем самою популярною є клієнт-сервер. Вона займає особливе місце в сучасному світі, її використання широко застосовується практично кожен день у різних програмах та додатках. Клієнт-сервер використовує деякі стандартизовані протоколи, які взаємодіють між собою та займаюсь окреме місце в діяльності людини [12].

Поняття клієнт-сервер можна охарактеризувати, як програмну архітектуру взаємодії клієнта та сервера. Принцип роботи полягає у надсиланні запитів від клієнта, в свою чергу сервер реагує і виконує перелік дій при отриманні запитів. Забезпечення міжпроцесового зв’язку на пряму залежить від клієнт-сервер. Оскільки, при обміні даними кожен з компонентів системи виконує свої функції. Поділ процесу на обов’язки відбувається між персональним комп’ютером та сервером отримання пакетів обробки даних, або робочою станцією вищого класу виконання дій. При цьому необхідним критерієм для обробки даних повинно слугувати збільшена потужність комп’ютера, що отримує дані. Завданням, яке виконує ПК залежить від обробки даних, які повертає сервер і формує результати для їх виведення з системи. Процесори запитів, що відбуваються в час виконання процесу можна зберігати на персональний комп’ютер та виконувати дії над ними.

Трафік мережі, який безупинно рухається реалізує та здійснює декілька маніпуляцій з запитами, після чого вони відправляються на сервер бази даних розміщеного в середовищі. Після виконання маніпуляції над запитами результатом є зменшений трафік мережі і збільшена продуктивність виконання процесу. Архітектура клієнт-сервер здійснює обмін пакетами даних за допомогою обміну повідомлень через локальну мережу. Базою стандартів локальної мережі є Ethernet (Див. рисунок 2.2.), але використання старих локальних мереж все ще здійснюється, таких як, Token Ring [11].

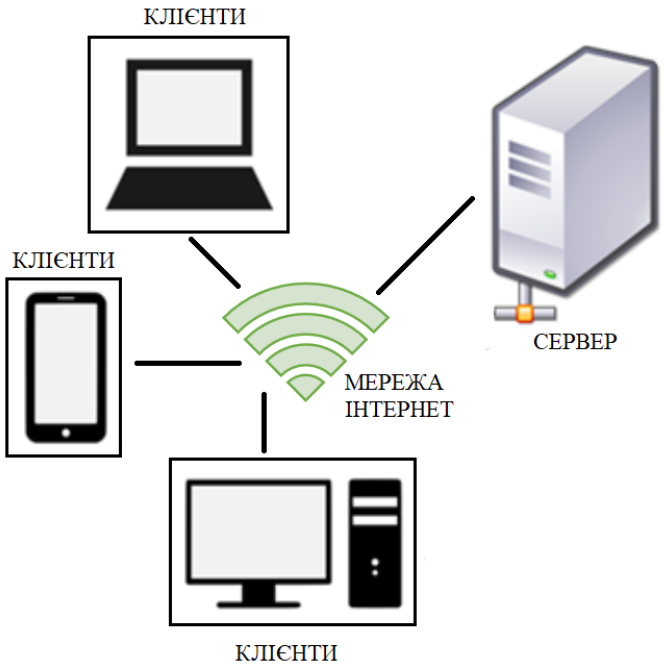

Рисунок 2.2. – Архітекура клієнт-сервер

Архітектура клієнт-сервер має подібні властивості, як стандартна централізована система, база даних пакетів даних розміщена на одному з персональних комп'ютерів. Сучасні високопродуктивні комп'ютери все ще працюють, як швидкісні сервери. У зв'язку з потребою великої кількості обробки даних, відмінність полягає у зміненні їх збереження для обробки інформації [13].

Популярність архітектури значною мірою в мережі Інтернет, виникла завдяки розвитку сучасних методів обробки та збереження в базах даних, а також

серверах масової реалізації процесу. Іншими словами архітектуру передачі даних можна охарактеризувати, як концепція інноваційної мережі, частина інформації збережена на серверах та очікує обрахування. Різні типи компонентів надають характеристику наборів даних на сервер, використовуючи мережу взаємодії сервера, який обробляє дані та клієнта, який надсилає запити у відповідь [12].

Протокол обміну складова якого, взаємозв’язок сервера даних і клієнта. В результаті спільної роботи утворює міцний зв'язок під назвою – відносини протоколу. Розділити операції виконання процесу можна на три рівні (Див. рисунок 2.3.).

Рисунок 2.3. – Розподіл процесу на три рівні

Особливістю клієнт-серверної двох подільної архітектури є зв'язок клієнтського та серверного модулів, взаємозв’язок залежить між ними від ряд критеріїв та функцій. Частиною складу цих модулів є модель товстого та тонкого клієнта. Принцип роботи залежить від механізму керування даними, які знаходяться на сервері обробки. Клієнтський модуль відповідає за рівень

представлення функцій в середовищі. Прилади та обладнання з обмеженою потужністю можна віднести до розряду кишенькових, їх ще називають товстими клієнтами. Клієнт-серверна модель поділена технологією, в якій представлено поділ елементів одного процесора між іншими. [11].

Є безліч веб-сайтів, які містять величезну кількість нової інформації. Простий варіант цих веб сторінок є набір даних, що зберігаються на окремому сервері під виглядом файлів. Складніший варіант, коли більша частина ресурсів знаходиться в активному стані користування, їх створення виникає під час обробки нових даних чи пакетів нової інформації.

Підґрунтя заснування ідеї клієнт-сервер виникла завдяки розподілу архітектури на частини чи компоненти мережі, передача даних, здійснювалась провідним шляхом. Це стало, однією з переломних моментів застосування технології бездротового зв'язку. В свою чергу це дозволило збільшити швидкість передачі даних, пришвидшити продуктивність мережі загалом. Для виконання операцій над пакетами даних було розроблено ролі [12].

Роль – функція сервера, яку налаштовано користувачем, для виконання поставленої задачі. Враховуючи ефективність, функціональність, якість виконання в конкретно зазначений термін. Сервер має можливості застосовувати при роботі одну або більше ролей. В залежності від ролі. Також, багато впливає роль на сервера і взаємозв'язок інших компонентів в рамках одного процесу конкретної задачі [13].

2.5. Переваги та недоліки клієнт-сервер архітектури передачі даних

Серед усіх переваг, які містить архітектура передачі даних клієнт-сервер можна назвати декілька головних із них: Оптимізований обмін даними. Дані зберігаються завдяки пакетів даних – процесів і зміни, які відбуваються на сервері стають доступні для користувача. В цьому допомагає автоматизований вхід даних, заощаджує час та спрощує доступ до ресурсів від клієнта до серверів.

Наступним елементом який потрібно врахувати, коли клієнт отримує доступ до інформації, завдяки інтерфейсу робочого місця, за допомогою встановлення контролю даних нехтуючи необхідність введення даних через термінальний режим чи процесор [12].

Ресурси при передачі даних суттєво зменшуються, що дозволяє системі швидше обробляти дані і надавати кращий та ефективніший вхід в систему користувачу. Додаток, який працює в поєднанні з моделлю клієнт-сервер виникає через апаратну платформу, або в іншому випадку завдяки технічному досвіду відповідного програмного забезпечення, супроводжує відкрите обчислення інформації даних пакетів у середовищі, заставляючи користувача отримувати послуги та реалізувати їх на сервері.

Збільшення умов для аналізу даних не дивлячись на місцерозташування гарантує користувачу вхід в систему незалежно від його перебування. При передачі даних весь процес відбувається на сервері, що дає змогу зменшити простоту обслуговування системи. Клієнт-сервер – це розподілена модель, яка в свою чергу являє собою поділені на обов’язки між комп’ютерами, які не залежать між собою підключичними в мережу. Це дає змогу легко та зручно в будь який момент часу вести зміни, замінити чи оновити сервер. Цей процес, який не контролюється називається інкапсуляція [13].

І найбільш важливим елементом будь якої системи передачі даних є безпека. Сервери забезпечують найефективніший контроль ресурсів та доступ, щоб забезпечити, вхід в мережу автоматизованим клієнтам до даних та змінювати і корегувати функціонал системи передачі. При цьому оновлення серверів чітко та надійно документуються адміністратором.

Як і всіх технологіях існують свої нюанси та недоліки. Це стосується і клієнт-сервер. Через те, що сервер отримує велику кількість даних навантаження на сервер відбувається значно більше, це спричиняє загрузку трафіку.

У разі критичного збою сервера клієнтські запити не виконуватимуться. Тому архітектура клієнт-сервер втрачає надійність мережі. Враховуючи всі

вищенаведені факти, можна сказати, що плюси переважають мінуси, але це показує, наскільки важливою і необхідною є технологія клієнт-сервер.

В Україні сьогодні в освіті використовується вітчизняна розробка навчально-змістовних модулів, що відповідають сучасним вимогам. Вони мають більше можливостей для відображення навчальної інформації, ніж використання традиційних друкованих матеріалів. Навчально-семантичні модулі – це не статичні тексти, які послідовно розміщені, а структуровані тексти з організацією ефективних переходів від однієї частини інформації до будь-якої іншої [11].

2.6. Сучасна технологія передачі інформації

Інтернет – глобальна мережа, всесвітня павутина нових знань, розваг, ресурс для здобуття навичок, перегляд чи прослуховування веб сторінок, медіа файлів, джерело безупинного напливу інформації. Але в такої глобальної мережі серед багатьох плюсів є й мінуси такі, як використання можливостей не за призначенням чи незаконних діях. Що може спричинити шкоду навколишнім особам, суспільству та інше. Визначити і зрозуміти стандарти є досить важким заняттям для людини. Тому варто почати з того, що являє собою твердження стандарт, які його особливості та застосування. Доєднатись до мережі в наш час не є чимось складним, для цього потрібно виконати ряд маніпуляцій, щоб бути в мережі Інтернет. Як показує статистика проведена з 2003 по 2020 роки, можна стверджувати що кількість користувачів, які почали використовувати мобільні оператори мережі (Див. рисунок 2.4.) різко зростає [8].

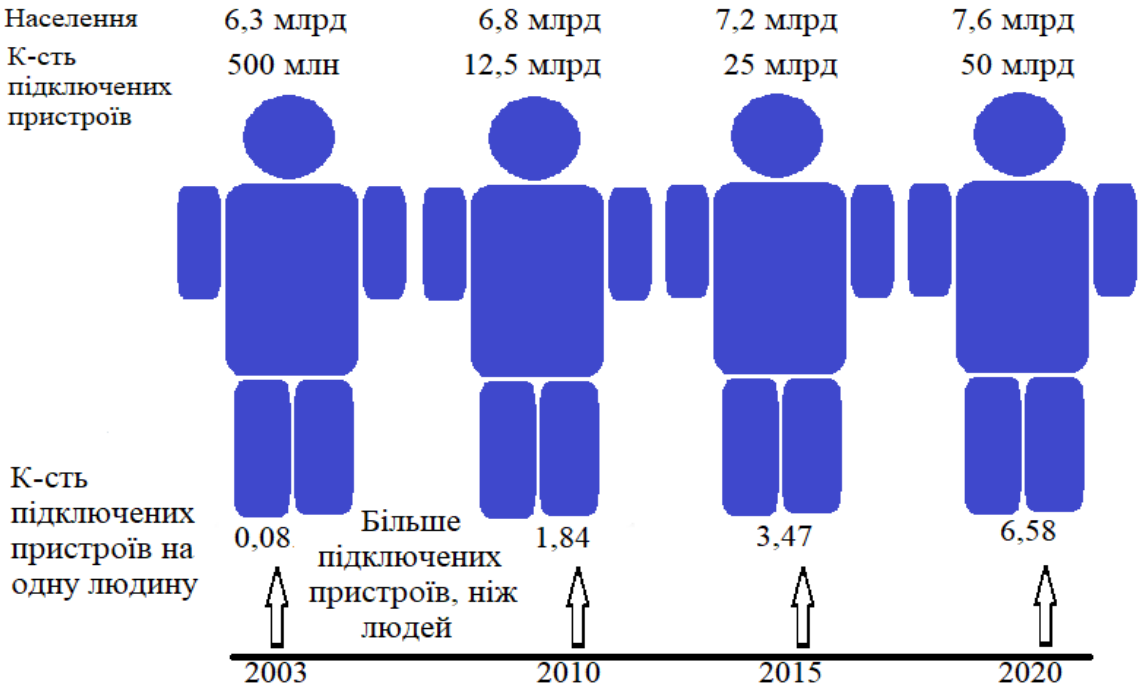

Рисунок 2.4. Кількість підключених пристроїв до мережі

З’єднання і комунікація перейшли на новий рівень і здійснюється безпровідним шляхом. Одною із головних проблем виникла небезпека перехоплення сигналів та отримання доступу до інформації несанкціонованим чином. Зламати бездротову мережу простіше чим дротову. Не треба з’єднуватись з проводами, потрібно тільки бути в межах радіусу дії передачі сигналу [5].

Новий стандарт безпровідного зв’язку розробила міжнародна компанія «Альянс зв’язку» під назвою: Wi-Fi 802.11ah. Частота цього стандарту близько 880 МГц, саме ця частота є найбільш популярною при під’єднанні на далеку відстань. Відстань, яку покриває діапазон частоти передачі сигналу значно більший за стандарти зв’язку з попередніми роками. Відмінність від стандартів, які використовуються зараз стандарт міжнародної компанії Альянс збільшує радіус дії практично в два рази. Що дозволяє, передавати сигнал через стіни, чи інші перешкоди (Див. рисунок 2.5). Крім цього, новому стандарту не заважає сигнали та імпульси від мікрохвильових приладів.

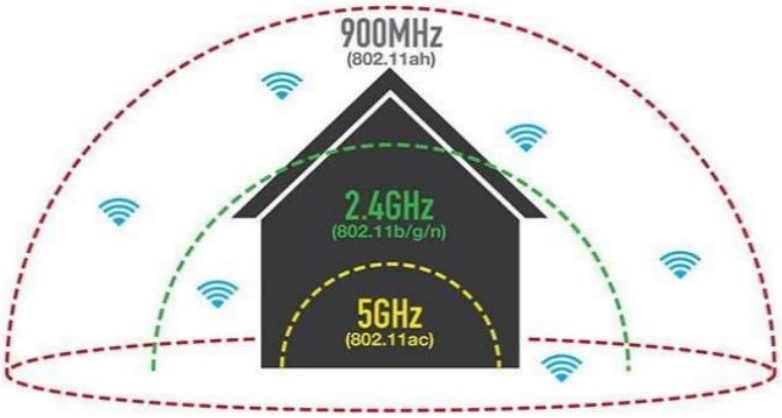

Рисунок 2.5. – Діапазон дії нового стандарту бездротового зв'язку Wi-Fi

Розробники стверджують, новий стандарт 802.11ah буде кращим ніж інші. Перевагами можна вважати простоту встановлення, сумісність з іншими видами обладнання чи приладів, покращений та більш захищений захист даних [3].

Якщо, не надати увагу налаштуванню та захисту мережі зловмисники можуть скористатись рядом дій, які використають в своїх потребах, для отримання прибутку (Див. рисунок 2.6.).

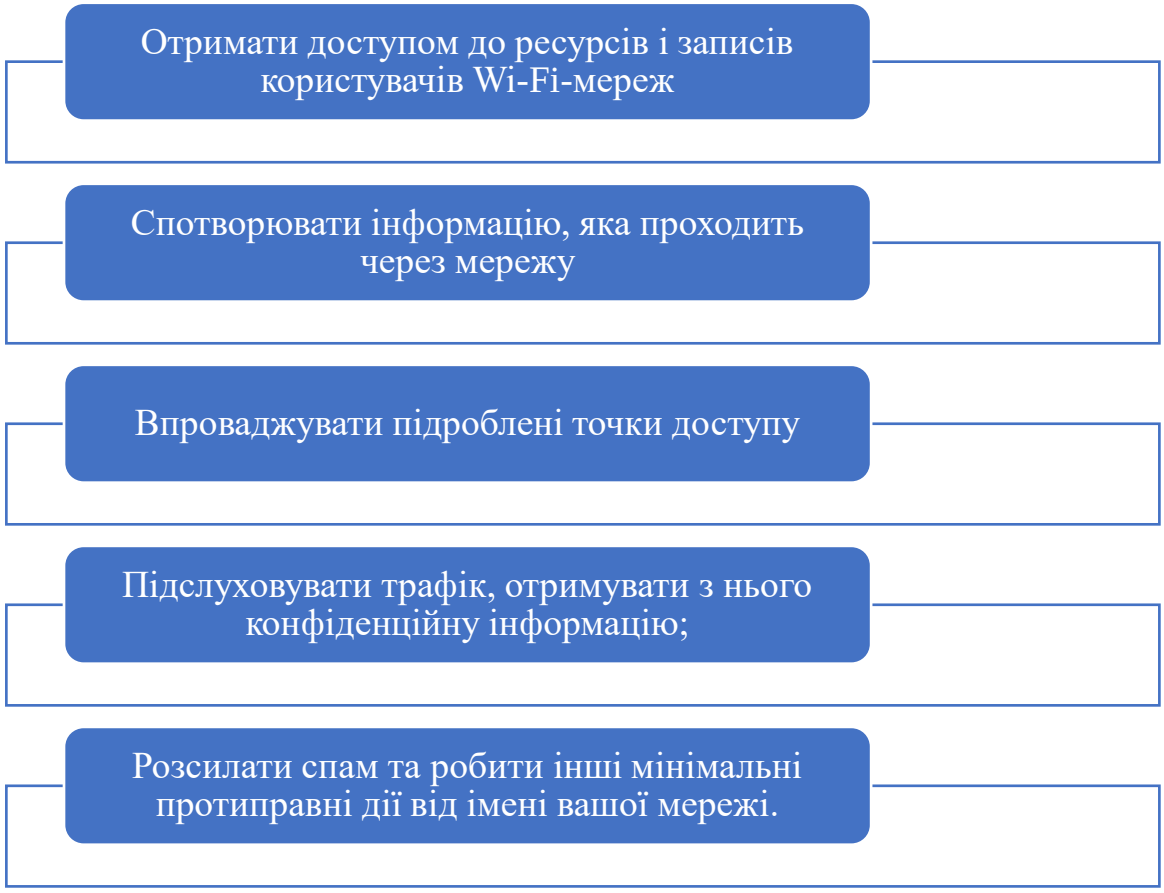

Рисунок 2.6 – Перелік небезпечних дій, які можуть здійснити зловмисники при не захисті мережі

По при те що в наш час широко застосовують захищені алгоритми, різні методи шифрування для захисту зв’язку, збільшену безпеку аутентифікації, все це є не точним захистом від несанкціонованого доступу чи втручання в мережу Wi-Fi. Тому необхідно приділити більше уваги при налаштуванні та захисті мережі для забезпечення цілісності усього зв’язку передачі даних.

З виникненням нових технологій, які мають за мету збільшити ефективність та продуктивність людини, зросла кількість й користувачів, які шукають вигоду та використати її не за призначенням. Крім використання технологій не за призначенням, є і ті хто шукає вигоду для отримання прибутку, чи наражають інших, коли оприлюднюють інформацію інших в мережі. В мережі є різні категорії людей, прості користувачі, які шукають нову інформацію, збагачують свої знання. І зловмисники, які отримують вигоду з використаних

даних чи перехопленого сигналу. Є ряд методів, які використовують для захисту інформації, в залежності від рівня небезпеки їх поділяють на класи представлені на рисунку 2.7.

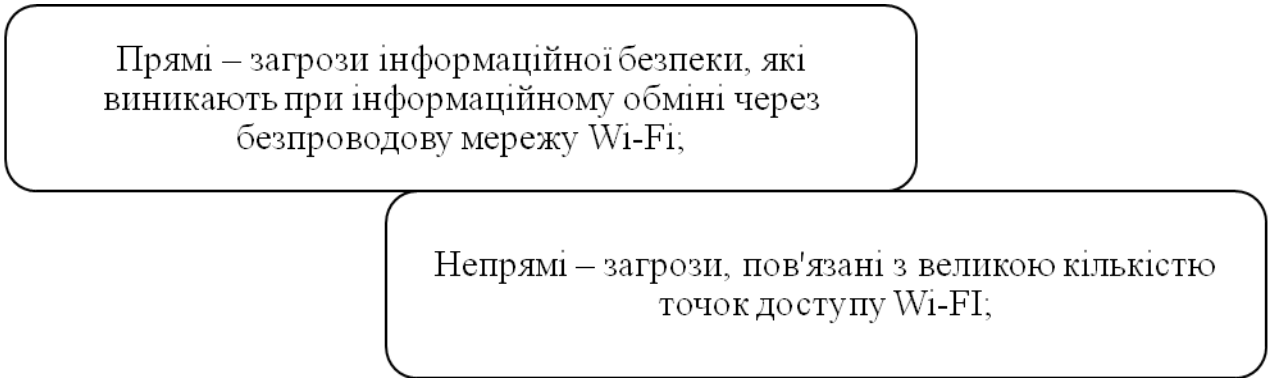

Рисунок 2.7 – Класи загроз

Канали радіопередачі роутера часто схильні до втручання сторонніх осіб. У стандартах IEEE 802.11, дотримання правил роботи визначає половину успіху, необхідність аунтифікації та шифрування є обов’язковим чинником для захисту даних від несанкціонованого доступу. Одною з поширених є так звана атака під назвою – чужинець.

Чужинець – периферійні обладнання та інші прилади, які допомагають обійти захист алгоритмів та отримання даних шляхом несанкціонованого доступу, без механізму втручання інших осіб. Роль чужинця може бути будь-що, що має безпровідний чи провідний інтерфейс. Серед них можуть бути: роутери, сканери чи проектори. Структура зв’язку може змінюватись, це означає, що бездротові технології, як Wi-Fi можуть з легкість підєднюватись з однієї точки дії до іншою. В залежності від межі покриття з’єднання, діапазон та частота залежить від сили передачі сигналу. Під час зміни точки сигналу користувач не помічає коли відбувається переключання з однієї точки сигналу на іншу [18].

Зловмисники, які використовують пристрої несанкціонованого доступу можуть підключатись в будь-який момент часу, змінивши точку відправлення сигналу на свою, в подальшому використавши її. Існує варіант при якому

пристрій користувача підключений до локальної мережі, завдяки підключені шнурів з входом інтерфейсу стає чужаком. З розвитком мережі безпровідного зв'язку та поширенням її, зростає необхідність у використанні приладів та обладнання комунікації. Що пропорційно залежить від користувачів та поширення механізму відправлення даних до приймача і отримання пакетів даних для обробки. Це дозволяє швидкість передачі пакетів даних визначати у кількості мегабайтів чи гігабайтів за одну секунду. Технології, які використовувались раніше, залишають нас, і входять в історію розвитку. Займають особливе місце в початку їх виникнення, стають базою відштовхування від створення до майбутнього процесу, який проходять і з кожним роком все більше модернізуються. Сервіси радіо та телемовлення стають звичною справою [17].

Розробка технології обміну даними безпровідним шляхом мереж 3G є була широко застосовувалась декілька років тому. Але в час коли розвиток інноваційних технологій не стоїть на місці, недоліком таким, як затримка передачі хоча б в одну секунду стає значною проблемою для бізнес-аплікацій. Ця затримка може бути недоліком ціною в тисячу чи мільйон доларів. Отож, в таких випадках технологія UMTS є не достатньо хорошим варіантом для цих потреб. Для запровадження нових технологій та методів, які повинні були вирішити ряд проблем на шляху 4G досліджено ряд способів та методик усунення цих проблем, при цьому захист даних та їх якість передачі не мала знизитись. Початком стільникових мереж було лише простий спосіб передачі голосу, тому використання для чогось більшого було просто неможливим реалізувати [21].

Головним конкурентом 3G та 4G є створений стандарт бездротового передавання даних WiMAX. Межа, яку може покривати одна станція даної технології може сягати близько 5 км. Якщо, припустити, що в цьому радіусі проживає 200 – 250 тис. осіб. Можна стверджувати, що отримання даних для кожного із користувачів буде здійснюватися з швидкістю 1 Мбіт в секунду, а

максимальне число осіб, яке може обслуговуватись одночасно буде сягати близько 2 тис. До появи технології WiMAX були мережі, які через недостатньо широке розповсюдження обладнання були просто забутими.

Після реалізації мережі 4G, або так названої мережі четвертого покоління передача даних стала більш спрощеною та значно продуктивнішою, обробка даних відбувалась швидше, ніж це було раніше. Швидкість передачі даних в четвертому поколінні на пряму залежить від пакетної передачі даних, поєднаного з голосовим трафіком. Що у свою чергу дало можливість нехтувати технологіями, які гальмували весь процес обробки даних. А технології, які прийшли на зміну стали продуктивніші та ефективніші при роботі. Функціонал та використання їх не потребувало втручання користувачів [8].

Головна особливість четвертого покоління є швидкість передачі, значно менша затримка обробки даних, передача пакетів даних, які займали гігабайти пам’яті, стали звичним ділом. Технологія не зупиняється на досягнутому, наступне п’яте покоління стане не просто швидким зв’язком передачі, а миттєвим відправлення та отриманням даних взаємозв’язаних приладів та сигналів між ними. Зазвичай швидкість передачі даних, яка обробляє домашня мережа сягає від 20 до 90 Мбіт в секунду, а інші тарифи пропонують 1-2 Гб/с за більшу плату. Це достатньо висока швидкість, яка доступна не для всіх користувачів. П’яте покоління стандартів мережі буде лише початком такої швидкості.

Скоріш за все, в майбутньому буде значно краще придбати маршрутизатор технології 5G з сім-картою та роздавати дані мережі на всі домашні пристрої, ніж за допомогою кабелю Ethernet. Це буде лише початком покоління, що змінить історію технології безпровідного зв’язку. Переваги, які буде мати п’яте покоління є багато, серед основних:

– Кількість пристроїв, які будуть підключатись одночасно зростатиме, близько мільйона на один квадратний кілометр. Прилади, обладнання та інше стануть краще працювати, завдяки більшому радіусі дії. Безпілотні авто, які

працюють на базі електричних механізмів, і в поєднанні навігації GPS, стануть ефективніше виконувати свої дії, а причини помилок при їх роботі суттєво зменшиться, сигнал буде поширюватись в десятки разів швидше.

– Оптимізація сигналу, підсилення зв’язку збільшиться завдяки новим стандартам та протоколам вищого рівня. Випромінювачі, які використовує п’яте покоління є точно направлені, це дозволить зменшити втрати у оптимізації процесу передачі.

– Енергоефективність стає в три рази меншою, ніж у технології четвертого покоління. Енергія при отриманні та відправленні даних буде менше використовуватись.

Застосування технологій п’ятого покоління є надзвичайно широким, перелічити усі застосування та можливості технології майже неможливо.

Станом на початок 2020 до складу об'єднання 6G/NET-2030 входять кілька дослідницьких груп, чиї зусилля спрямовані на розробку тих технології, які не можна було реалізувати в рамках впровадження мереж 5G/IMT-2020 [21].

2.7. Висновки до другого розділу

У даному розділі було розглянуто алгоритми захисту інформації, проаналізовано методи їх захисту. Досліджено вимоги, які варто дотримуватись при захисті даних, а також більш сучасні технології передачі, які замінили їх прототипи. Проаналізовано клієнт серверну технологію, як систему передачі інформації. Методи якої чітко та дуже тісно пов’язані з новітніми технологіями обміну даними. Досліджено переваги та недоліки даної технології в сучасному світі технологій. Аспекти у поєднані з засобами захисту інформації від несанкціонованого доступу. Передачу інформації та пакет даних за допомогою мережі Wi-Fi. Основні вразливості мереж безпровідного доступу. Також розглянуто основні протоколи захисту мереж безпровідного доступу, що забезпечують цілісність інформації.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1. Долікарська допомога при ураженні електричним струмом

При ураженні електричним струмом необхідно якомога швидше звільнити потерпілого від струмопровідних частин обладнання.

Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом м'язів, тобто людина самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання, до якої доторкається людина.

Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев'яним сухим топорищем. Потерпілого можна також відтягнути від струмопровідних частин за одяг, уникаючи дотику до навколишніх металевих предметів та до відкритих частин тіла потерпілого. Відтягуючи потерпілого за ноги, не можна торкатися його взуття, оскільки воно може бути сирим і стає провідником електричного струму. Той, хто надає допомогу, повинен одягнути діелектричні рукавиці або обмотати їх шарфом, натягнути на них рукав піджака або пальта. Можна також ізолювати себе, ставши на гумовий килимок, суху дошку.

При звільненні потерпілих в електроустановках з напругою понад 1000В слід користуватися діелектричними рукавицями і взути діелектричні боти; діяти ізолюючою штангою або ізолюючими кліщами (рис 3.1) [8].

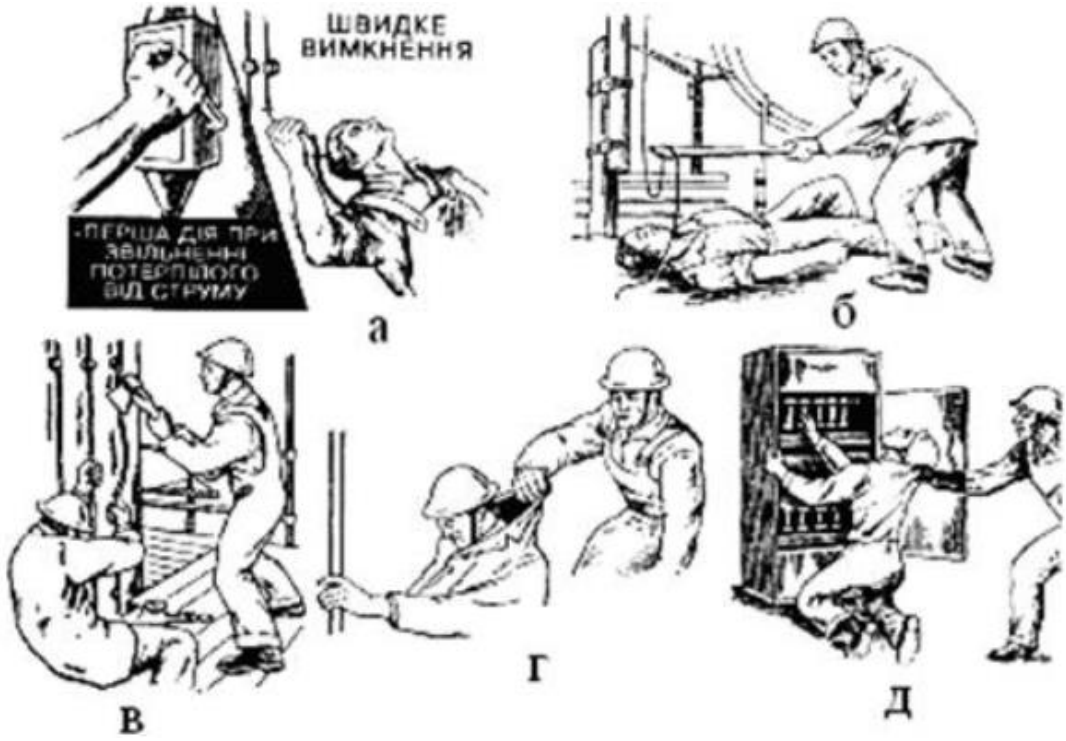

Рисунок 3.1. – Звільнення потерплого від дії струму

Якщо провід торкається землі, то необхідно пам’ятати про небезпеку крокової напруги. Тому після звільнення потерпілого від струмопровідних частин слід винести його з небезпечної зони. Без засобів захисту пересуватися в зоні розтікання струму по землі слід не відриваючи ноги одна від одної.

Якщо провід торкається землі, то необхідно пам’ятати про небезпеку крокової напруги. Тому після звільнення потерпілого від струмопровідних частин слід винести його з небезпечної зони. Без засобів захисту пересуватися в зоні розтікання струму по землі слід не відриваючи ноги одна від одної

Наслідки своєчасної і правильно наданої допомоги на місці події можуть бути зведені нанівець, якщо при підготовці до транспортування і доставці потерпілого до медичної установи не будуть дотримані відповідні правила. Головне не тільки в тому, як доставити потерпілого і яким видом транспорту, а наскільки швидко були вжиті заходи, які забезпечили максимальний спокій і зручне положення потерпілого.

Найкраще транспортувати потерпілого ношами. При цьому можна використовувати підручні засоби: дошки, одяг. Можна переносити потерпілого на руках. Передусім потерпілого слід покласти на ноші, які застеляють ковдрою, одягом, ставлять ноші з того боку потерпілого, де є ушкодження. Якщо тих, хто надає допомогу, двоє, вони повинні стати з двох боків нош. Один підкладає руки під голову і груднину, другий – під крижі і коліна потерпілого. Одночасно без поштовхів його обережно піднімають, підтримуючи ушкоджену частину тіла, і опускають на ноші. Слід накрити потерпілого тим, що є під руками, – одягом, ковдрою. Якщо є підозра на перелом хребта, потерпілого кладуть обличчям догори на тверді ноші (щит, двері). За відсутністю такого можна використати ковдру, пальто. В такому випадку потерпілого кладуть на живіт [9].

Якщо є підозра на перелом кісток тазу, потерпілого кладуть на спину із зігнутими ногами у колінах і у тазостегнових суглобах для того, щоб його стегна були розведені, під коліна обов’язково треба підкласти валик із вати, рушника, сорочки.

По рівній поверхні потерпілого несуть ногами вперед, при підйомі на гору або на сходах – головою вперед. Ноші весь час повинні бути у горизонтальному положенні. Щоб ноші не розгойдувались, необхідно йти не в ногу, злегка зігнувши коліна.

При перевезенні потерпілого слід покласти його до машини на тих самих ношах, підстеливши під них що-небудь м’яке (ковдру, солому) [8].

3.2. Загальні вимоги безпеки до обладнання та технологічних процесів

Безпека праці на виробництві охоплює такі три складники:

– безпеку виробничого обладнання;
– безпеку технологічних процесів;
– безпеку виконання робіт.

Безпека виробничого обладнання (за винятком обладнання, що є джерелом іонізуючих випромінювань) регламентується ДСТУ ГОСТ 12.2.003–91. ССБТ. Безпеку виробничого обладнання забезпечують такими методами:

– добором принципів дії, джерел енергії та параметрів робочих процесів;

– мінімізацією кількості енергії, що споживається чи накопичується;

– застосуванням вмонтованих у конструкцію засобів захисту та інформації про можливі небезпечні ситуації;

– застосуванням засобів автоматизації, дистанційного керування та контролю;

– дотриманням ергономічних вимог, обмеженням фізичних і нервово-психологічних навантажень на працівників [6].

Виробниче обладнання під час роботи, самостійно чи у складі технологічних комплексів повинно відповідати вимогам безпеки впродовж усього періоду експлуатації. Матеріали конструкції виробничого обладнання не повинні зумовлювати утворення небезпечних чи шкідливих факторів щодо дії на організм працівників, а навантаження, що виникають під час роботи в окремих елементах обладнання, не повинні сягати небезпечних величин. У разі неможливості реалізації останньої вимоги у конструкції обладнання необхідно передбачити спеціальні засоби захисту (огородження, блокування та ін.). Небезпечні зони виробничого обладнання (рухомі вузли, елементи з високою температурою), як потенційні джерела травмонебезпеки, повинні бути огороджені (відповідно ДСТУ ГОСТ 12.2.062–81), теплоізольовані або розміщені у недосяжних місцях. Допоміжні пристрої (затискачі, вантажозахоплювальні та вантажопідіймальні пристрої) повинні унеможливити виникнення небезпеки під час раптового вимкнення енергії, а також самовільну зміну стану цих пристроїв після відновлення енергоживлення.

Виробниче обладнання повинно бути пожежовибухобезпечним у передбачених умовах експлуатації та не накопичувати зарядів статичної

електрики у небезпечних для працівників кількостях. Виробниче обладнання, робота якого супроводжується виділенням шкідливих речовин чи організмів або пожежо- та вибухонебезпечних речовин, повинно включати вмонтовані пристрої для локалізації цих виділень. За відсутності таких пристроїв у конструкції обладнання мають бути передбачені місця для підключення автономних пристроїв локалізації виділень [6].

Якщо виробниче обладнання є джерелом шуму, ультра- та інфразвуку, вібрації, виробничих випромінювань (електромагнітних, лазерних), то його треба виконувати таким чином, щоб параметри перелічених шкідливих виробничих факторів не перевищували меж, встановлених відповідними чинними нормативами. Виробниче обладнання повинно бути забезпечене місцевим освітленням, виконаним відповідно до вимог чинних нормативів, якщо його відсутність може спричинювати перевантаження органів зору або інші небезпеки, пов’язані з експлуатацією цього обладнання.

Одна із складників безпеки виробничого обладнання – конструкція робочого місця, його розміри, взаємне розміщення органів управління, засобів відображення інформації, допоміжного обладнання. Розробляючи конструкції робочого місця потрібно дотримуватися вимог чинних нормативів. Розміри робочого місця і його елементів мають забезпечувати виконання операцій у зручних робочих позах і не ускладнювати рухи працівників.

Перевагу варто віддавати виконанню робочих операцій у сидячому положенні або почерговій зміні положень сидячи і стоячи, якщо виконання робіт не потребує постійного переміщення працівника. Конструкція крісла і підставки для ніг повинна відповідати ергономічним вимогам. Система управління виробничим обладнанням має забезпечувати надійне і безпечне його функціонування на всіх режимах роботи, а також у разі зовнішніх впливів. На робочих місцях повинні бути написи, схеми та інші засоби інформації щодо послідовності керуючих дій. Конструкція і розміщення засобів попередження

про небезпечні ситуації повинні забезпечувати безпомилкове, достовірне і швидке сприйняття цієї інформації.

Центральний пульт управління технологічним комплексом обладнується сигналізацією, мнемосхемою або іншими засобами відображення інформації про порушення нормального режиму функціонування кожної одиниці виробничого обладнання, засобами аварійної зупинки всього комплексу або окремих його одиниць, якщо це не призведе до подальшого розвитку аварійної ситуації.

Пуск виробничого обладнання в роботу, а також повторний пуск після його зупинки, незалежно від причини, має бути можливим тільки через маніпулювання органами управління пуском. Органи аварійної зупинки після спрацювання повинні залишатися у положенні зупинки до їх повернення у вихідне положення обслуговуючими працівниками. Повернення органів аварійної зупинки у вихідне положення не повинно призводити до пуску обладнання. Засоби захисту, що входять у конструкцію виробничого обладнання, повинні:

– забезпечувати можливість контролю їх функціонування; виконувати своє призначення безперервно у процесі роботи обладнання;

– діяти до повної нормалізації відповідного небезпечного чи шкідливого фактора, що спричинив спрацювання захисту;

– зберігати функціонування у випадку виходу з ладу інших засобів захисту.

За необхідності включення засобів захисту до початку роботи виробничого обладнання схемою управління повинні передбачатися відповідні блокування. Виробниче обладнання, під час монтажу, ремонту, транспортування та зберігання якого застосовуються вантажопідіймальні засоби, повинно мати відповідні конструктивні елементи або позначені місця для приєднання вантажозахоплювальних пристроїв із зазначенням маси обладнання.

Обладнання, переміщення якого передбачено вручну, повинно мати відповідні елементи або форму для захоплення рукою. Безпека виробничих

процесів регламентується ДСТУ ГОСТ 12.3.002–75 ССБТ. Безпека виробничого процесу визначається передусім урахуванням вимог безпеки до конкретного обладнання на етапі розробки проекту, випуску та випробуваннях випробного зразка та передачі його у серійне виробництво. Основні вимоги безпеки до технологічних процесів: - усунення безпосереднього контакту працівників з вихідними матеріалами, заготовками, напівфабрикатами, готовою продукцією та відходами виробництва, що можуть бути вірогідними чинниками небезпек;

– заміна технологічних процесів та операцій, пов’язаних з виникненням небезпечних і шкідливих виробничих факторів, процесами і операціями, за яких ці фактори відсутні або характеризуються меншою інтенсивністю;

– комплексна механізація та автоматизація виробництва, застосування дистанційного керування технологічними процесами та операціями за наявності небезпечних та шкідливих виробничих факторів;

– герметизація обладнання;

– застосування засобів колективного захисту працівників;

– раціональна організація праці та відпочинку задля профілактики монотонності праці, гіподинамії, а також обмеження важкості праці;

– своєчасне отримання інформації про виникнення небезпечних і шкідливих виробничих факторів на окремих технологічних операціях (системи отримання цієї інформації потрібно виконувати за принципом пристроїв автоматичної дії з виведенням на системи попереджувальної сигналізації);

– своєчасне видалення і знешкодження відходів виробництва, що є джерелами небезпечних і шкідливих виробничих факторів;

– забезпечення пожежної і вибухової безпеки [6].

3.3. Висновок до третього розділу

В третьому розділі кваліфікаційної роботи описано долікарську допомогу при ураженні електричним струмом, перелічено правила поведінки, а також надання першої допомоги. Проаналізовано загальні вимоги до обладнання під час технологічних процесів, визначено усі аспекти, які потрібно враховувати при роботі з обладнанням. Описано матеріал надання першої медичної допомоги працівникам при електричному струмі.

ВИСНОВКИ

На сьогоднішній момент бездротові мережі набули широкого поширення, що призводить до необхідності розробки технології захисту інформації бездротових мереж. Варто сказати що з появою однієї технології виникає питання у захисті її від не цільового використання.

У інноваційних системах позбутись проблеми захисту даних є можливим при створені алгоритмів та запровадженні методів їх шифрування в мережі та при передачі інформації. Криптографічний захист відповідає за алгоритми, які забезпечують умови збереження цілісності та конфіденційності інформації. Покращити анонімність у відкритій мережі, сигнали чи повідомлення, які передаються безпровідним шляхом.

Галузь, криптографія, яка відведена на захист інформації в мережі, займає особливе місце в сучасних технологіях. Криптографія – це сукупність методів та засобів, які запроваджені для підвищення та надійності даних, при передачі їх в мережі. Криптографічні алгоритми, протоколи та засоби, які застосовуються при захисті даних називають криптографічною системою.

Методи захисту алгоритмів є величезна кількість. Кожен з методів має свої особливості, інколи варто поднювати їх для кращої ефективності. Методи, які використовують для захисту даних залежать від криптографічної стійкості шифрів. Криптографічна стійкість – можливість алгоритму суперечити атакам, які можуть загрожувати при обміні даними в глобальній мережі. Алгоритм буде стійким, якщо буде виконуватись твердження при якому, час на зламування ключа до шифру буде більший від часу передачі інформації відправника до одержувача. Для визначення стійкості алгоритму використовують оцінку атаки на криптосистему та її заподіяну шкоду. Давніше криптографія належала до розрядку військових технологій, але зі збільшенням безпровідних технологій в сучасному світі спричинило потребу алгоритмів захисту даних.

Раніше базою завдання криптографічного захисту було шифрування даних. Але зараз область криптографії збільшилась до меж ліцензування, електронного підпису, електронних грошей, онлайн конференції. Ключі, які надходять у систему перевіряються одержувачем чи адміністратором, який відповідає за надання доступу до криптосистеми через ключ. Якщо ключ є вільним, він з легкістю може бути опублікований в мережі з відкритим доступом.

Безпровідні технології відіграють важливу роль у передачі даних там, де неможливе або дороге прокладання кабельних ліній на значні відстані. При передачі даних слід враховувати, що обробка цієї інформації проходить декілька етапів роботи. При передачі даних, необхідно приділити увагу алгоритмам, які будуть використанні для шифрування повідомлень в мережі. Через те, що безпровідні технології поширюються швидко, зросла потреба у підвищенні захисту даних при передачі та її отриманні. Методи та засоби, які варто визначити для забезпечення цілісності системи обміну даними призвело до дослідження алгоритмів захисту у безпровідних технологіях. Також досліджено, які ще існують технології передачі даних. Як розпочався розвиток передачі інформації, які технології прийшли на зміну старим та шо залишилось до сьогодення.

У результаті проведеного дослідження в даному дипломному проекті можна зробити наступні висновки: алгоритми захисту є важливим компонентом при захисті бездротової передачі даних. Обмін інформації містить в собі можливість несанкціонованого підключення до точок доступу, нефіксований зв'язок, підслуховування, для цього необхідно передбачити якісні засоби захисту, так як підключитися до мережі можна з автомобіля, який знаходиться в радіусі дії сигналів. Дослідження усіх аспектів алгоритму та передачі даних, вдосконалення методів та засобів, а також розвиток їх в сучасному світі призвело до висновку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бездротова передача даних: типи, технологія та пристрої. [Електронний ресурс] – Режим доступу: https://presa.com.ua/navchannia/bezdrotova-peredacha-danikh-tipi-tekhnologiya-ta-pristroji.html (14.04.2022);

2. Бездротові мережі передачі даних. [Електронний ресурс] – Режим доступу: https://androidas.ru/wireless-data-networks/ (20.03.2022);

3. Бездротові мережі. [Електронний ресурс] – Режим доступу: http://dolgomudova-anakonda.blogspot.com/2012/05/87.html (10.02.2022);

4. Бездротові технології [Електронний ресурс] – Режим доступу: https://www.wiki.uk-ua.nina.az/Бездротові_технології.html (29.12.2021);

5. Безпровідні WiFi мережі. [Електронний ресурс] – Режим доступу: https://infotel.ua/ua/bezprovidni-wifi-merezhi (06.03.2022);

6. Новітні криптографічні методи захисту даних. [Електронний ресурс] – Режим доступу: http://eprints.zu.edu.ua/13902/1/Mingaleva3.pdf (12.01.2022);

7. Безпровідні технології нашого часу. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/5006609/page:3/ (16.02.2022);

8. Визначення безпровідна локальна мережа. [Електронний ресурс] – Режим доступу: https://uk.theastrologypage.com/wireless-local-area-network (16.01.2022);

9. Інтернет загрози. [Електронний ресурс] – Режим доступу: https://www.wishkola.org.ua/typy-zahroz-v-interneti (13.02.2022);

10. Клієнт серверна архітектура та ролі серверів. [Електронний ресурс] – Режим доступу: https://medium.com/@IvanZmerzlyi/клієнт-серверна-архітектура-та-ролі-серверів-9893d8048229

11. Клієнт серверні технології. [Електронний ресурс] – Режим доступу: https://crashbox.ru/solving-problems/klient-servernye-tehnologii-ispolzovanie-tehnologii-klient-server-v-tehnologii-klient-server-klie/ (08.03.2022);

12. Концепція клієнта серверної технології. [Електронний ресурс] – Режим доступу: https://passportbdd.ru/uk/browsing-the-internet/ponyatie-klient-servernoi-tehnologii-chto-takoe-tehnologiya-klient-server/ (13.02.2022);

13. Криптографічний захист інформації. [Електронний ресурс] – Режим доступу: https://www.znanius.com/3851.html (13.04.2022);

14. Маршутизатори. Методи маршутизації. [Електронний ресурс] – Режим доступу: https://studopedia.com.ua/1_13250_marshrutizatori.html (14.04.2022);

15. Мережі передачі даних. [Електронний ресурс] – Режим доступу: https://rci-c.com/technology/merezhi/ (20.03.2022);

16. Міночкін А.І., Романюк В.А. Перспективи побудови тактичних систем зв'язку // III Науково-технічна конференція ВІТІ. – К.: ВІТІ НТУУ ―КПІ‖. – 2006. – С. 5–15.

17. Основи технології клієнт сервер. [Електронний ресурс] – Режим доступу: https://buklib.net/books/24515/ (11.01.2022);

18. Основні інтернет загрози. [Електронний ресурс] – Режим доступу: http://safe-city.com.ua/osnovni-internet-zagrozy/ (14.01.2022);

19. Радіоканал передачі даних. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Радіоканал_(канал_передачі_даних)(12.01.2022);

20. Романюк В.А., Жук О.В., Сова О.Я. Аналіз протоколів маршрутизації в бездротових сенсорних мережах // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2008. – №1. – С. 73 – 85.

21. Стандарти мобільного зв’язку. [Електронний ресурс] – Режим доступу: https://www.itbox.ua/ua/blog/Standarti-mobilnogo-zvyazku-4G5G6G--podibnist-vidminnosti-perspektivi/ (17.03.2022);

22. Технології захисту інформації. [Електронний ресурс] – Режим доступу:https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf (05.03.2022);

23. Технології захисту інформації. [Електронний ресурс] – Режим доступу: http://kist.ntu.edu.ua/textPhD/tzi.pdf (20.04.2022);

24. Шахнович В.В., Сучасні технології бездротового зв'язку. – М.: Техносфера, 2006. – С. 215–288.

ДОДАТКИ