АНОТАЦІЯ

Дана магістерська робота присвячена вирішенню задачі захисту інформації в радіоканалах, шляхом застосування комплексних заходів для захисту від можливих атак спрямованих на перехоплення і підміну переданих даних.

Метою магістерської дисертації є проведення аналізу безпеки бездротових мереж, виділення методів їх захисту та створення моделі захисту бездротових мереж.

Для того, щоб досягнути поставленої мети, виконано наступний перелік завдань:

1. Проаналізовано існуючі рішення у галузі захисту інформації через радіомережі
2. Зроблено опис запропонованої розробленої моделі
3. Описано алгоритми, експерименти, досліди даної моделі

Метод дослідження – описовий, методи аналізу та синтезу, експериментальний метод, метод узагальнення.

Науковою новизною цієї розробки є те, що розроблено засіб захисту інформації через радіомережі, використання якого дозволило значно підвищити рівень інформаційної безпеки в радіоканалі.

Практичне значення цієї розробки полягає в тому, що отримані теоретичні та практичні результати рекомендуються для використання в організаціях, які використовують радіоканал для передачі конфіденційної інформації з високими вимогами до безпеки.

Ключові слова: БЕЗДРОТОВА МЕРЕЖА, ШИФРУВАННЯ, ПРОТОКЛОЛ, АУДИТ, АВТОРИЗАЦІЯ, АВТЕНТИФІКАЦІЯ, АЛГОРИТМ.

ABSTRACT

This master's thesis is devoted to solving the problem of information protection in radio channels, by applying comprehensive measures to protect against possible attacks aimed at intercepting and substituting transmitted data.

The purpose of the master's dissertation is to analyze the security of wireless networks, identify methods for their protection and create a model for the protection of wireless networks.

In order to achieve this goal, the following list of tasks:

1. Review the existing solutions in the field of information security through theradio network
2. Make a description of the proposed model
3. Describe algorithms, experiments, experiments of this model

Research method - descriptive, methods of analysis and synthesis, experimental method, method of generalization.

The scientific novelty of this development is that a means of protecting information through radio networks has been developed, the use of which has significantly increased the level of information security in the radio channel.

The practical significance of this development is that the obtained theoretical and practical results are recommended for use in organizations that use a radio channel to transmit confidential information with high security requirements.

Keywords: WIRELESS NETWORK, ENCRYPTION, PROTOCOL, AUDIT, AUTHORIZATION, AUTHENTICATION, ALGORITHM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AP (Access Point) – точка доступу в безпровідну мережу

SSID (Service Set Identifier) – ідентифікатор безпровідної мережі

SSL (Secure Socket Layers) – протокол передачі шифрованих даних

WEP (Wired Equivalent Privacy) – протокол захисту даних при передачі по радіоканалу

АІС – автоматизована ідентифікаційна система

КЗЗІ – комплекс засобів захисту інформації

МРК – мобільний робототехнічний комплекс

ОС – операційна система

СЗІ – система захисту інформації

НСД – несанкціонований доступ

ЕОМ – електронно-обчислювальна машина

IV (Initialization Vector) – вектор ініціалізації

ВСТУП

В даний час, триває активна робота зі створення мобільних робототехнічних систем (МРК). Сфера застосування таких комплексів широка, пріоритетним є завдання, під час якого мобільний робот працює в умовах, небезпечних для розташування людини. Застосування автоматизованих робототехнічних систем виявляє перспективу в умовах, коли життя оператора знаходиться під загрозою. Як частина команди пошуку, МРК можуть виконувати функції віддаленого розпізнавання, працюючи автономно і передаючи дані по бездротовому каналу.

Вчені створюють пристрої, призначені для виконання різноманітних завдань, у тому числі - для використання лише в екстремальних умовах. Як правило, комплекс включає мобільний робот зі спеціальним обладнанням на борту та систему управління, яка включає, серед іншого, віддалений комп'ютер, встановлений на станції управління станції оператора, а також бортовий комп'ютер, встановлений для потрапляння в мобільний робот. Зв'язок відбувається через бездротовий канал.

Одним із найважливіших завдань є забезпечення необхідної умови інформаційної безпеки. Дані, що передаються по радіо, є найбільш вразливими. Команди управління передаються від контрольної станції на бортовий комп’ютер, а з бортового комп’ютера на віддалений комп’ютер повертаються дані про стан мобільних систем та інформація від датчиків (відеокамери, радар, сканер поверхні тощо). Команди, передані по бездротовому каналу, можуть бути перехоплені та змінені. Дані, що надходять від мобільного робота на пункт пропуску, також можуть бути перехоплені та змінені.

Система аутентифікації в бездротовій мережі підлягає підвищеним вимогам безпеки. Необхідно використовувати криптографічно стабільні алгоритми, що дозволяють взаємну автентифікацію сторін.

Необхідно розробити технологію, яка дозволить ефективно шукати несанкціоновану станцію.

Дана магістерська робота присвячена вирішенню проблеми захисту інформації в радіоканалах мобільних робототехнічних систем шляхом використання комплексних заходів захисту від можливих атак, спрямованих на перехоплення та заміну переданих даних. Мета проаналізувати безпеку бездротових мереж, визначити методи їх захисту та створити модель захисту бездротових мереж.

Для досягнення цієї мети визначаються та вирішуються наступні завдання:

- аналізуються існуючі рішення в галузі інформаційної безпеки через радіомережі

- робиться опис запропонованої розробленої моделі

- описуються алгоритм, експерименти, дослід моделі

Метод дослідження – описовий, методи аналізу та синтезу, експериментальний метод, метод узагальнення.

Науковою новизною цієї розробки є те, що розроблено засіб захисту інформації через радіомережі, використання якого дозволило значно підвищити рівень інформаційної безпеки в радіоканалі.

Практичне значення цієї розробки полягає в тому, що отримані теоретичні та практичні результати рекомендуються для використання в організаціях, які використовують радіоканал для передачі конфіденційної інформації з високими вимогами до безпеки.

Схвалення. Про деякі результати дослідження було повідомлено під час 7-ї науково-технічної конференції “Інформаційні моделі, системи та технології” Національного технічного університету в Тернополі імені Івана Пулюя.

Пояснювальна записка обсягом 65 сторінки містить 5 таблиці, 5 рисунків, 7 формул. Список використаних джерел розміщується на 6 сторінках і містить 17 джерел.

РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ РАДІОТЕХНОЛОГІЄЮ

1.1. ПРОБЛЕМИ ЗАХИСТУ ІНОРМАЦІЇ

Загроза, як правило, визначається або характером (видом, методом) дестабілізуючого впливу на інформацію, або наслідками. Однак такі терміни можуть мати багато пояснень. Інший підхід до визначення загрози інформаційній безпеці базується на понятті "загроза".

Іншими словами, поняття загрози суворо пов'язане з правовою категорією "шкоди", яку Цивільний кодекс визначає як фактичні витрати, понесені суб'єктом господарювання внаслідок порушення його прав (наприклад, після здійснення операції або використання конфіденційної інформації), втрати або пошкодження майна та витрати, які він повинен буде здійснити, щоб відновити порушене право та вартість пошкодженого або втраченого майна.

Аналіз негативних наслідків реалізації загроз передбачає виявлення можливих джерел загроз, вразливостей, способів їх прояву та способів їх реалізації. І тоді ланцюжок переростає у схему, зображену на (рис. 1. 1).

Загрози класифікуються залежно від можливості заподіяння шкоди предмету відносин з порушенням цілей безпеки. Шкода може бути заподіяна будь-яким суб'єктом (злочином, виною чи необережністю), а також бути наслідком, який не залежить від предмета проявів. Загроз не так багато. Забезпечуючи конфіденційність інформації, це може бути викрадення (копіювання) інформації та засобів її обробки, а також її втрата (ненавмисна втрата, витік).

Окрім забезпечення цілісності інформації, перелік загроз включає наступне: зміна інформації; заперечення точності інформації; нав'язування неправдивої інформації. Окрім надання доступу до інформації, її можна заблокувати або видалити та засоби її обробки.

Рисунок 1.1. Модель реалізації загроз інформаційній безпеці

Вразливості також можна розділити на класи відповідно до джерела вразливості, а класи на підгрупи за проявами. Методи реалізації можна згрупувати за типом методу реалізації. Важливо мати на увазі, що термін "метод" може використовуватися лише для позначення реалізації антропогенних загроз.

1.2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

Розглядаючи існуючі рішення щодо захисту інформації при передачі даних за допомогою радіотехніки, відзначимо, що останнім часом у зв'язку з постійним зростанням кількості завдань, пов'язаних з взаємодією між віддаленими об'єктами і, відповідно, необхідністю передачі конфіденційної інформації, проблема забезпечення безпеки цієї інформації стає дуже важливою .

Наприкінці минулого століття був запропонований метод передачі цієї інформації в цифровій голосовій суміші для вирішення проблеми забезпечення безпеки інформації, що передається за каналами зв'язку, що забезпечує приховування переданих зашифрованих або незашифрованих каналів зв'язку від потенційних зловмисників. Розроблено та досліджено комп'ютерна модель, що реалізує запропонований спосіб передачі, яка продемонструвала досить високу надійність вилучення корисної інформація від їх суміші з цифровим шумом [12] на приймальному кінці каналу зв'язку. Кілька років тому вони були уточнені і сформульовані завдання [6] , які необхідно опрацювати для реалізації таких моделей в реальних системах, рекомендуються методи, що дозволяють знизити ймовірність вибору «зломщика» каналів зв'язку від його суміші з цифровим шумом до майже нуля. У ці завдання входить вирішення проблем початку і закінчення передачі та прийому корисної інформації.

Методи енергетичного маскування можна використовувати для маскування інформації, що передається по дротових лініях. Це можливо, оскільки водій має очевидні обмеження у просторі. Для захисту від безконтактного видалення пасивних методів використовується кабельний екран із заземленим екраном від активних лінійних шумів.

Бездротові технології зосереджені на питаннях безпеки, оскільки проблема надійного захисту інформації є однією з головних перешкод для розвитку бездротових мереж та систем на їх основі.

Радіомережі дозволяють обмін даними між локальними комп’ютерними мережами, коли використання традиційних дротових технологій є складним або недоцільним. Прикладом ефективного використання бездротової радіотехнології є забезпечення зв'язку між сегментами локальних мереж за відсутності коштів, відсутності дозволу на виконання кабельних робіт або відмови телефонної станції в оренді спеціального каналу. Внутрішня прокладка кабелю може бути неможливою, якщо установка заборонена.

В основі будь-якої бездротової мережі лежить її протокол. Протокол зазвичай регулює топологію мережі, маршрутизацію, адресацію, порядок доступу мережевих вузлів до каналу даних, формат переданих пакетів, набір команд для управління мережевими вузлами та системою. інформаційна безпека. Тому ця стаття зосереджена на короткому описі протоколів.

Опис протоколів. Повний спектр бездротових протоколів даних можна класифікувати по-різному, причому одним параметром, таким як топологія мережі, швидкість або алгоритми безпеки, є головний. Найпоширеніший метод класифікації в технічній літературі базується на максимальному радіусі дії бездротової мережі. Далі наводиться класифікація протоколів, що розглядаються у порядку зменшення радіуса.

WWAN (WirelessWideareanetwork) - це в основному стільникова мережа, їх радіус дії становить кілька десятків кілометрів. Ці мережі включають такі протоколи: GSM, CDMAone, iDEN, PDC, GPRS та UMTS.

WMAN (WirelessMetropolitanAreaNetworks) - це міська бездротова мережа на відстань у кілька кілометрів. Прикладом цього мережевого протоколу є WiMAX.

WLAN (WirelessLocalAreaNetwork; WLAN) - це бездротова локальна мережа. Дальність дії цього класу мереж становить кілька сотень метрів. Сюди входять такі протоколи: UWB, ZigBee, Wi-Fi.

WPAN використовуються для зв'язку різних пристроїв, включаючи комп'ютери, офісні пристрої та обладнання, засоби зв'язку тощо. Діапазон дії WPAN становить від декількох метрів до декількох десятків метрів. WPAN використовується як для підключення окремих пристроїв між собою, так і для підключення їх до мереж вищого рівня.

Ці протоколи були відібрані для аналізу через їх широке використання в сучасних бездротових мережах. Цей параметр дозволяє переглянути поточний стан інформаційної безпеки в бездротових мережах, незалежно від завдань, що виконуються бездротовими мережами.

АНТ. Протокол розроблений Dynastream Innovations.

Цей протокол призначений насамперед для компактних пристроїв з автономним джерелом живлення (трансивери, які використовують цей протокол, мають дуже низьке енергоспоживання) для передачі відносно коротких пакетів даних. Протокол передбачає організацію відкритих та приватних бездротових мереж, включаючи складні типи з динамічною конфігурацією. Він побудований на технології PAN (Personal Area Network) і підтримує рівні з 1 по 4 стека OSI (OpenSystemsInterconnectionnetworkmodel). Застосування протоколу - бездротові датчики.

Несуча частота за протоколом ANT становить 2,4 ГГц, кількість частотних каналів - 125 (крок від 1 МГц до 2400. в діапазоні 2524 МГц). Швидкість передачі даних на радіоканалі може досягати 1 Мбіт/с.

РУБІН. RuBee - це двосторонній протокол бездротової локальної мережі, який використовує пропускну здатність великого діапазону (LW) та пакети даних, що не перевищують 128 байт. Протокол RUBee подібний до протоколів серії IEEE 802, також відомих як Wi-Fi (IEEE 802.11.4), WPAN (IEEE 802.15.4) та Bluetooth (IEEE 802.15.1). RuBeenetworked, працює на основі та представляє розробку стандартів RFID. RuBee дозволяє працювати на низькочастотних носіях (131 кГц), дозволяючи використовувати вузькі мережеві вузли.

БЕЗДРОТОВИЙ. Wi-Fi був створений у 1991 році компанією NCR (пізніше Lucent Technologies та AgereSystems) у Нідерландах. Wireless Fidelity - це торгова марка Wi-Fi Alliance for Wireless Networks, заснована на стандарті IEEE 802

Як правило, мережа Wi-Fi містить принаймні одну точку доступу (так званий інфраструктурний режим) і принаймні одного клієнта. Ви також можете підключити двох клієнтів у режимі "точка-точка", коли точка доступу не використовується, а клієнти підключаються за допомогою мережевих адаптерів "безпосередньо". Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних пакетних сигналів зі швидкістю 0,1 Мбіт/с кожні 100 мс. Таким чином, 0,1 Мбіт/с - це найнижча швидкість передачі даних для Wi-Fi. Знаючи SSID мережі, клієнт може знати, чи можна підключитися до цієї точки доступу. Коли дві точки доступу з однаковим SSID потрапляють у діапазон, приймач може вибирати між ними на основі даних рівня сигналу.

Методи аналізу ризиків в інформаційних системах (ІС).

В даний час завдання створення моделі інформаційної загрози має особливе значення при побудові СЗІ [5]. Існує багато алгоритмів, що виконують аналіз ризику ІВ. Найвідомішими алгоритмами є CRAMM та RiskWatch. Ці алгоритми мають багато переваг і широко використовуються.

Метод CRAMM був розроблений Службою безпеки Великобританії за дорученням уряду Великобританії і застосовувався як національний стандарт урядами та бізнес-організаціями Великобританії з 1985 року.

CRAMM передбачає розподіл всього процесу на три послідовні фази. Завданням першого кроку є відповідь на запитання: "Чи достатньо захистити систему від основних інструментів, що реалізують традиційні функції безпеки, чи потрібно провести більш детальний аналіз?". На другому етапі визначають ризики та оцінюють їх величину. На третьому етапі вирішується питання про вибір відповідних контрзаходів.

Методологія CRAMM для кожної фази визначає набір вихідних даних, послідовність дій, анкети запитів, контрольні списки та набір документів звітності. Якщо результати першого етапу показують, що рівень критичності ресурсів дуже низький, а існуючі ризики навмисно не перевищують жодного базового рівня, система має мінімальний набір вимог безпеки. При цьому більшість заходів другого етапу не реалізуються, але здійснюється перехід на третій рівень, що створює стандартний перелік контрзаходів для забезпечення відповідності базовому набору вимог безпеки.

Другий етап аналізує загрозу безпеці та цілісності. Аудитор отримує відповідну інформацію для оцінки від уповноважених представників організації під час відповідних вимог.

Третій етап вирішує проблему управління ризиками, що включає вибір відповідних контрзаходів.

Керівництво організації вирішує, запроваджувати нові механізми безпеки або модифікувати існуючі. Робота аудитора полягає в обґрунтуванні рекомендованих контрзаходів для управління організацією.

Метод RiskWatch. Програмне забезпечення RiskWatch розроблено американською компанією RiskWatchInc. і є потужним інструментом для аналізу та управління ризиками. Сімейство RiskWatch включає програмні продукти для різних типів засобів контролю безпеки.

Метод RiskWatch використовує "річний прогноз збитків" (ALE) та "рентабельність інвестицій" (ROI) як критерії для оцінки та управління ризиками. Програмне забезпечення RiskWatch має багато переваг.

RiskWatch допомагає в аналізі ризиків та ретельному підборі заходів та інструментів. Техніка, що використовується в програмі, складається з 3 етапів.

Першим кроком є визначення предмета дослідження. На цьому етапі описуються параметри організації - тип організації, склад досліджуваної системи. Опис доповнено кількома абзацами. Далі кожен з обраних пунктів детально

описаний. Щоб полегшити використання аналізатора, шаблони перелічують категорії захищених ресурсів, втрати, загрози, вразливості та заходи безпеки. Серед них потрібно вибрати ті, які насправді присутні в організації.

Другим кроком є введення даних, що описують конкретні характеристики системи. Дані можна вводити вручну або імпортувати із звітів, створених засобами дослідження вразливості комп'ютерної мережі. На даний момент докладно описані ресурси, збитки та класи інцидентів. Класи інцидентів отримують шляхом порівняння категорії збитків та категорії ресурсів. Для виявлення можливих вразливих місць використовується опитувальник, що містить понад 600 запитань. Питання стосуються категорій ресурсів. Дозволяється вирішувати проблеми, виключати або додавати нові, визначати частоту кожної з виявлених загроз, ступінь вразливості та цінність ресурсів. Все це використовується згодом для розрахунку ефективності використання коштів.

Третє - це оцінка ризику. Вперше встановлено зв'язок між ресурсами, втратами, загрозами та вразливими місцями, виявленими на попередніх етапах. З точки зору ризику розраховуються математичні очікування збитків за рік:

$L = P * V$

L - сума втрати інформаційної загрози за рік;P - частота загроз протягом року;V - вартість ресурсу, що перебуває під загрозою.

Розглянуті методи дозволяють оцінити або переоцінити рівень поточного статусу інформаційної безпеки АС, розробити концепцію та політику безпеки АС та запропонувати плани захисту від виявлених загроз та вразливостей.

Недоліки аналізованих методів аналізу:

1. Обмежений обсяг. Метод аналізу інформаційного ризику CRAMM набагато краще підходить для аудиту існуючих операційних систем, ніж для інформаційних систем, що розробляються.

2. Нездатність інтегрувати підхід до аналізу ризиків. Метод RiskWatch проводить аналіз ризиків на рівні програмного та апаратного захисту без

урахування організаційних та адміністративних факторів. Метод не враховує комплексного підходу до інформаційної безпеки.

3. Неможливість розширити базу знань. Сучасні засоби аналізу інформаційного ризику (наприклад, CRAMM) не вимагають розширення бази знань. Відсутність такої можливості спричиняє значні труднощі в процедурі аналізу ризиків даної організації.

4. Висока вартість ліцензії. Існуючі засоби аналізу інформаційного ризику мають високу вартість ліцензії.

Безпека бездротової мережі слід за використанням багатьох технологій: реєстрація, цифровий підпис, паролі, зміни ключів тощо.

Спосіб використання цих технологій має значний вплив на безпеку мережі. У деяких випадках метод, що використовується для використання вищезазначеної технології, полягає в тому, що вона не впливає на рівень безпеки мережі. Ці питання детальніше обговорюються нижче.

Стандарт шифрування E0. Стандарт Bluetooth використовує потоковий код E0, який базується на трьох генераторах лінійного зсуву. Ця схема використовується в Bluetooth в режимах безпеки 2 і 3.

У Bluetooth v4. 2 (і попередні версії в режимах безпеки 2 та 3), два пристрої у вашому пристрої отримають один і той же ключ сеансу одночасно, якщо користувач встановив для них однаковий PIN-код. Слід зазначити, що якщо PIN-код менший за 16 байт, тоді BD ADDR використовується для генерації сеансового ключа на додаток до значення поточного PIN-коду. Перехват даних при шифруванні зображений на (рис. 1.2).

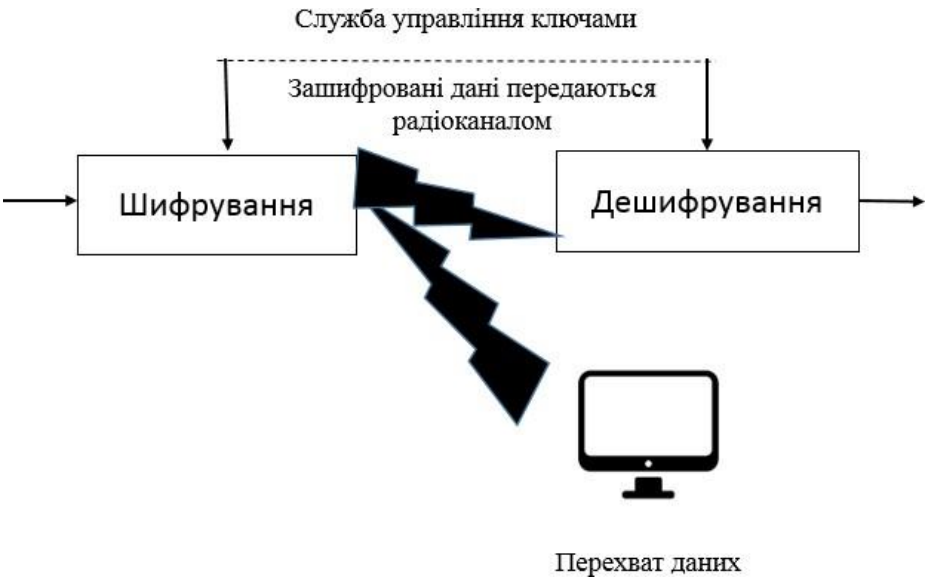

Рисунок 1.2. Перехват даних при шифруванні

Стандарт AES. Цей стандарт шифрування в основному використовується для захисту бездротових каналів зв'язку. Він використовується в протоколах UVB, RuBee, VI-FI та VIMAX.

Код CMEA. Безпека зв'язку забезпечується також використанням процедур автентифікації та шифрування повідомлень. CDMA використовує стандартний алгоритм автентифікації та шифрування стільникової голосової аутентифікації (CAVE) для генерації 128-бітового ключа в стільниковому зв'язку. Ключ називається SSD (Shared Secret Date). Ці дані генеруються на основі ключа, який зберігається в мобільній станції з псевдовипадкового числа, отриманого від мережі. Спільна секретна інформація (SSD) генерується за допомогою алгоритму CAVE. Вони розділені на дві частини: SSD-A (64-розрядна), призначена для генерації цифрового підпису (підпис для автентифікації) та SSD-B (64-розрядна), призначена для генерації ключів для шифрування мови та передачі сигналу. SSD-накопичувачі можуть використовуватися постачальниками послуг для місцевої автентифікації в роумінгу. Нова спільна секретна інформація (SSD) може бути

створена при переміщенні мобільної станції в іншу мережу або назад до домашньої мережі.

Дійсний алгоритм кодової системи. Цей код, який також називається KccLok, використовує лінійний рекурсивний регістр зсуву. Довжина основного регістру - 32 біти, довжина додаткового регістру - 5 бітів. Шифрування здійснюється побітовим додаванням ключів. Для цього алгоритму існують ефективні атаки. Наприклад, для того, щоб отримати систему лінійних рівнянь, яка дозволяє повернути початкове заповнення лінійного реєстру, досить прослухати послідовність ключів, щоб перехопити його 216 символів.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. Проаналізовано питання інформаційної безпеки та розглянута модель реалізації загроз інформаційній безпеці. Були розглянуті існуючі рішення щодо захисту інформації при передачі даних по радіо.
2. Метод перетворення звукового сигналу, такий як інтегровані мозаїчні перетворення.
3. Також описана класифікація протоколів WWAN, WMAN, WLAN, WPAN.
4. Проаналізовано протоколи Bluetoooth, ANT, RuBEE.
5. Обговорюються методи аналізу ризиків інформаційних систем CRAMM та Risk Watch.
6. Наведені E0, CMEA, система кодування.

РОЗДІЛ 2. АНАЛІЗ МОДЕЛІ

2.1 БЕЗДРОТОВІ МЕРЕЖІ СТАНДАРТУ 802.11

Протокол 802. 11 містить ряд вразливостей при розробці механізму захисту інформації. Одним з таких недоліків є протокол WEP, який дозволяє шифрувати інформацію за допомогою секретного ключа [17]. Стандарт 802. 11 не вирішує таких важливих питань, як розподіл секретних ключів між станціями мережі і механізм аутентифікації.

Найпоширеніша версія стандарту IEEE 802. 11 - 802. 1lb, що забезпечує швидкість передачі даних до 11 Мбіт/с. Пристрої, що працюють за цим стандартом, використовують кілька каналів в діапазоні частот від 2400 до 2483,5 МГц. Максимальна дальність стабільного зв'язку може досягати 300 м в поле зору, але зі збільшенням відстані це може значно знизити швидкість передачі даних.

Стандарт IEEE 802. 11 розроблений для створення захищеної мережевий архітектури для зв'язку між мережевими пристроями з використанням радіоканалу. Однак з точки зору критеріїв безпеки існують серйозні ігноровані прогалини, які можуть привести як до можливий витік інформації, так і до загального відмови.

У порівнянні зі звичайною провідний мережею, доступ до якої може бути обмежений фізичними методами, використання радіоканалів не може гарантувати відсутність перехоплення і модифікації переданих даних.

Серед стандартних засобів захисту, які забезпечуються стандартом 802. 11, слід особливо виділити протокол WEP.

Основні характеристики WiFi мережі 802. 11 перераховані в таблиці (2.1).

Характеристика	Опис
Фізичний рівень	Метод прямої послідовності (Direct Sequence Spread Spectrum), метод частотних стрибків (Frequency Hopping Spread Spectrum), передача в інфрачервоному спектрі (IR)
Частотний діапазон	2,4 ГГц і 5ГГц
Швидкість передачі даних	1 Мбіт/с, 2 Мбіт/с, 5.5 Мбіт/с, 11 Мбіт/с (lib), 54 Мбіт/с (Па), 54 Мбіт/с (11 g)
Безпека мережі та даних	Потоковий алгоритм шифрування на основі на RC4 для захисту даних, перевірки на цілісність і аутентифікації.
Дальність дії	Від 50 до 500 метрів в залежності від умов
Гідність	Бездротова передача даних зі швидкістю кабельних аналогів, багато розробки програмного забезпечення, низька вартість адаптерів та точок доступу.
Недостатки	Недостатня безпека при використанні стандартних інструментів, зменшення швидкості залежно від відстані та навантаження мережі

Таблиця 2.1 Основні характеристики мереж стандарту 802.11

Робота над стандартом 802. 11, що стосується технологій бездротової передачі даних, організована за принципом Ethernet, проводиться з 1997 року в Інституті IEEE. Зараз найпопулярнішим стандартом є 802. 11 b, який входить до сімейства 802. 11. Перевагою є використання смуги частот 2,4 - 2,5 ГГц для роботи в більшості країн, не вимагає ліцензування. У режимі ad-hoc кожен клієнт мережі безпосередньо спілкується з іншим клієнтом (Рис. 2.1).

У цьому режимі всі клієнти повинні бути на відстані, щоб передавати інформацію. Якщо клієнт хоче спілкуватися з клієнтом у неспеціалізованій мережі, один із членів мережі повинен виконувати функції шлюзу та маршруту.

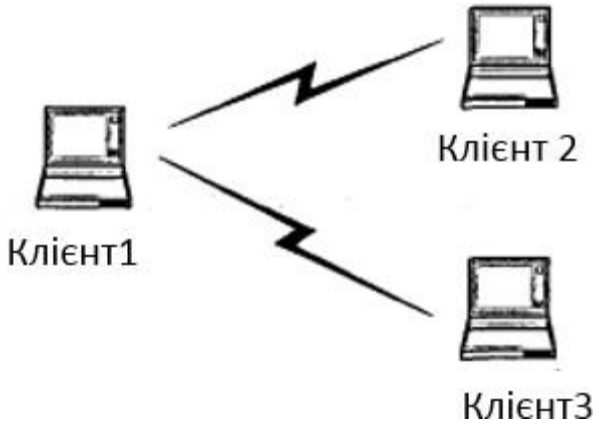

Рисунок. 2.1 Режим без використання центральної станції

При використанні центральної станції в режимі весь потік інформації проходить через точку доступу (AP). Точка доступу виконує роль мосту Ethernet, який забезпечує шлях до іншої дротової або бездротової мережі (див. Рис. 2.2).

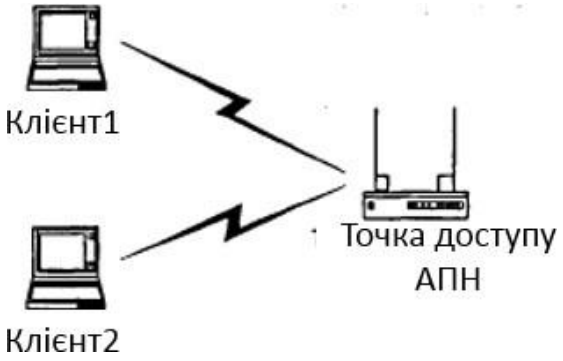

Рисунок. 2.2 Метод, що використовує центральну станцію

Перш ніж ви зможете спілкуватися, бездротова станція та точка доступу повинні встановити з'єднання. Лише після встановлення зв’язку дві бездротові станції можуть обмінюватися даними. Процес встановлення зв’язку проходить у дві фази і включає три стани, в яких клітина може перебувати:

1. Нерозпізнана і не пов’язана;
2. Визнаний і пов’язаний;
3. Визнаний і пов’язаний.

Для переходу з одного стану в інший обмінюються повідомленнями, які називаються кадрами управління. Точка доступу надсилає спеціальний кадр управління маяком. З боку клієнта такі кадри збираються з точок доступу, розташованих у зоні зв'язку. Клієнт також може надіслати кадр контролю запиту зонду, щоб знайти точку доступу з певним SSID. Після визначення точки доступу партії розпочати процедуру взаємної автентифікації з обміну управлінського персоналу. Після успішної автентифікації клієнт переходить до наступного етапу - автентифікації та відсутності з'єднання. Щоб увійти до третього стану, клієнт повинен надіслати кадр запиту на підключення (кадр запиту асоціації), куди точка доступу повинна, в свою чергу, надіслати підтвердження (кадр відповіді асоціації). Потім клієнтська станція стає повноправним членом бездротової мережі і може обмінюватися даними з іншими мережевими станціями.

2.2. КЛАСИФІКАЦІЯ АТАК НА РАДІОКАНАЛ

Потенційні ризики при використанні стандарту 802.11 b включає атаки шифрування, конфіденційність та доступ до мережевих ресурсів.

Як показано (рис. 2. 3), атаки, що порушують безпеку WiFi, поділяються на пасивні та активні. Вони, в свою чергу, поділяються на кілька підкласів.

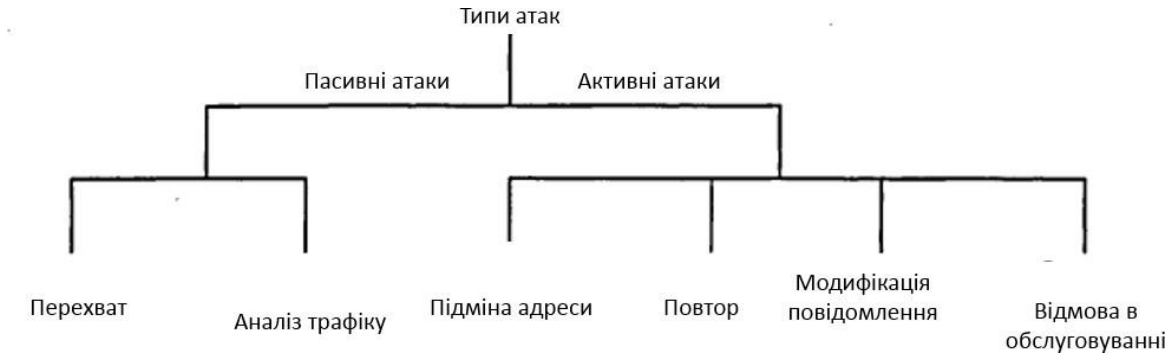

Рисунок. 2.3 Типи атак на WiFi стандарту 802.11

Пасивні атаки - це атаки в цьому класі, в яких сторонні особи просто отримують доступ до даних, не змінюючи їх. Системному адміністратору неможливо довести факт пасивної атаки. Збір даних та використання аналізатора трафіку вважаються пасивними атаками.

Підслуховування - Сторона, яка атакує, відстежує вміст повідомлень, що передаються по мережі. Прикладом є прослуховування між двома робочими станціями в мережі або між станцією та точкою доступу.

Аналіз трафіку - у цьому випадку буде використаний підхід до фільтрації трафіку на основі певних критеріїв. Збирається статистика звітів, що містять відомі раніше фрагменти.

Активні атаки - це атаки, при яких несанкціонована сторона модифікує повідомлення. Можна виявити факт нападу цього класу, але не завжди вдається запобігти цьому. Активні атаки поділяються на чотири підкласи: заміна адреси, повторна спроба, модифікація повідомлення та відмова в обслуговуванні [9].

Заміна адреси - замінивши адресу, зловмисник може отримати всі або частку привілеїв уповноваженого користувача.

Повторити спробу - сторона, що атакує, перехоплює повідомлення та передає його під приводом уповноваженого користувача. Редагування повідомлення - повідомлення модифікується шляхом додавання, видалення або редагування даних.

Відмова в обслуговуванні - Нападаючи на певні типи повідомлень, сторона, що напала, перешкоджатиме нормальному використанню або керуванню бездротовою мережею.

2.3. АНАЛІЗ ЗАСОБІВ І МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ WIFI

Основою захисту даних, що передаються через бездротові мережі, є протокол WEP.

Згідно з дослідженнями, WEP не має достатньої стабільності та має кілька структурних обмежень.

Здатність атакувати визначається спостережуваними прогалинами та статичною структурою протоколу. Єдина різниця між повідомленнями про автентифікацію - це вміст тексту перевірки.

По-перше, сторона, що атакує, перехоплює другий і третій кадри управління, які передаються в процесі аутентифікації. Друге поле містить текст перевірки в незашифрованому вигляді, а третє - той самий текст, але вже зашифрований спільним секретним ключем. Таким чином, зловмисникові стає відомо про незашифрований текст P, той самий текст, але вже зашифрований C, та значення IV, яке подається в не зашифрованому вигляді. Потім можна обчислити згенерований псевдовипадковий масив WEPKIV, використовуючи секретний ключ k і значення вектора ініціалізації IV за допомогою формули 2.1.

$$WEPKM=C®P \quad (2.1)$$

Розмір псевдовипадкової послідовності буде точно таким же, як розмір кадру аутентифікації. У цьому випадку всі елементи кадру відомі заздалегідь: номер алгоритму, порядковий номер, код стану, ідентифікатор елемента, довжина та текст управління.

Таким чином, сторона, що атакує, може успішно пройти автентифікацію в захищеній мережі, навіть маючи невідомий секрет K. Сторона, що атакує, надсилає запит точці доступу, до якої ви хочете підключитися. Точка доступу - це кадр управління, що містить текст управління. Зловмисник обчислює тіло кадру автентифікації, обчислюючи XOR (виключаючи "або") із випадкових текстових значень, отриманих за допомогою R та послідовності WEP. Наступним кроком є обчислення нового значення перевірки цілісності (ICV). Для цього скористайтеся технікою, описаною в розділі «Активна альтернативна передача трафіку».

Потім станція отримує авторизацію в захищеній мережі. Якщо захищена мережа використовує WEP, зловмисник не зможе обмінюватися інформацією з іншими станціями без використання спеціальних інструментів.

Основні проблеми із захистом бездротових мереж 802. 1lb:

1. Довжина криптографічного ключа має невелику довжину ключа 40 біт, що не підходить для захищених систем. В даний час рекомендується щонайменше 80 біт. Довга довжина ключа ускладнює пошукову атаку.

2. Слабкість алгоритму RC4 внаслідок особливостей його використання в алгоритмі WEP. Оскільки значення IV є частиною потоку ключів алгоритму RC4 і передається відкритим. Ця помилка в алгоритмі RC4 не виникає в інших випадках, крім WEP, оскільки вона не відкриває частину потоку ключів і не перезапускає алгоритм для кожного пакету даних.

3. Алгоритми захисту цілісності мають свої недоліки. Алгоритми з лінійною структурою блоків, такі як CRC32, не можуть забезпечити надійний захист цілісності для використання в криптографії. Можна змінити вміст упаковки. Лінійні алгоритми вразливі до атак заміни пакетного вмісту. Використання некриптографічних алгоритмів при підготовці пакетів часто полегшує можливі атаки на зашифровану інформацію.

4. Недоліки системи аутентифікації списку MAC-адрес. Якщо ви використовуєте автентифікацію за MAC-адресою, викрадений пристрій може легко підключитися до мережі, оскільки немає автентифікації користувача.

2.4. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРОТОКОЛУ WEP

З ростом та розвитком індустрії бездротового зв'язку підвищується надійність та безпека радіопередачі. При передачі даних на радіохвилях [17] їх можна легко захопити та змінити.

Тому радіоканалам потрібен механізм безпеки для забезпечення захисту даних.

Як правило, мережа 802. 11 - це радіозв'язок між клієнтською станцією та точкою доступу (AP). Якщо перешкоди між AP та клієнтською станцією (настінні, штучні або природні перешкоди) не захищають радіосигнал, прямий видимість не потрібна. На додаток до технічних специфікацій передачі даних, стандарт визначає протокол Wired Equival Privacy (WEP), який служить механізмом захисту даних від перешкод під час радіопередачі. Інформація захищена зовнішньою службою управління ключами, призначеною для шифрування та шифрування повідомлень, переданих через мережу.

Основні особливості алгоритму WEP включають:

• Опір вибору ключів. Інформаційна безпека забезпечується алгоритмом, заснованим на складності пошуку секретного ключа при атаці шляхом пошуку можливих комбінацій (жорстокі атаки). Стабільність залежить від довжини секретного ключа та частоти змін ключів.

• Синхронізуйте себе. Алгоритм WEP дозволяє синхронізувати кожне повідомлення. Ця функція особливо корисна для алгоритмів шифрування, заснованих на каналах, де надійність передачі підвищується, і пакет даних швидше втрачається.

• Ефективне впровадження. Алгоритм WEP може бути реалізований на апаратному та програмному рівні.

Стандартна система автентифікації має недоліки, основними з яких є:

1. Необхідність надання секретного ключа WEP, ключ не можна часто міняти;

2. Змінити MAC-адресу;

3. Переривати пакети, отримуючи наступне значення SSID;

4. Одностороння автентифікація на основі відповіді на запит із використанням загального криптографічного ключа.

802.11b базується на стандарті IEEE 802. 802. Визначає, як використовується розширений протокол автентифікації (EAP).

Серед методів EAR, спеціально розроблених для бездротових мереж, слід виділити сильну сім'ю, засновану на паролях.

Алгоритм SPEKE призначений для подолання проблем безпеки та високої складності при впровадженні унікальних методів перевірки на основі сертифікації.

Це дослідження призвело до розробки нового сімейного алгоритму ідентифікації на основі паролів, який подолав недоліки традиційних алгоритмів використання паролів.

Наприклад, підрахунок кількості невдалих записів може легко виявити та запобігти атакам на словник у режимі реального часу. Однак тривалі атаки на словники паролів можуть бути дуже небезпечними. Сторона, що атакує, може замаскуватися під іншу сторону автентифікації або перервати перевірені повідомлення один одного. Втрата будь-якої, навіть незначної інформації під час обміну може призвести до успішної атаки. Навіть якщо використовується короткий пароль, алгоритм повинен бути спроможним протистояти такому типу атак.

Одночасно ключ сеансу створюється за допомогою пароля безпеки для обміну інформацією між двома сторонами. Потреби вбудованої системи обміну ключами детально обговорюються для перевірки. Ідея полягає в тому, щоб дозволити третій стороні атакувати, перериваючи повідомлення, обмінюючись аутентифікацією та діями обміну ключами. Забезпечення безпечного обміну ключами вимагає взаємної участі обох сторін і повинно бути невід’ємною частиною цього процесу.

Існує багато способів створити захищений канал, який дозволяє передавати ваш пароль у відкритому або змішаному форматі. Алгоритми SPEKE та DH-EKE мають усі перераховані вище переваги та інші бажані функції, про які буде сказано нижче.

2.5 ОПИС АЛГОРИТМІВ SPEKE І DH-EKE

Алгоритми SPEKE та DH-EKE засновані на методі обміну ключами Діффі Хеллмана. Класичний обмін DH дозволяє двом сторонам створити спільний секретний ключ сеансу без попередньої згоди.

Сама DH не забезпечує автентифікацію і піддається атакам "людина посередині".

Алгоритми SPEKE та DH-EKE є частиною одного з типів автентифікованих протоколів обміну ключами. Використання DH захищає пароль від затримки словникової атаки, тоді як механізм використання пароля в цих алгоритмах запобігає можливості атаки "людина посередині". Дві сторони, що діляться коротким паролем (S), можуть пройти автентифікацію через незахищений канал, довести знання одне одного про S та сформувати новий великий сеансовий ключ (K).

Ці алгоритми використовують арифметику у великій кінцевій групі. Кілька типів таких груп можна використовувати в DH, але ми обмежимось Zm, де t - велике просте число.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Розроблені методи вдосконалення системи безпеки на основі алгоритму WEP;

2. Складено класифікацію типів атак, наведено методи вирішення проблем безпеки даних для кожного з типів атак;

3 Розроблені методи запобігання та зменшення ймовірності успішних атак на стандартну систему безпеки;

4. Розроблені методи захисту від атак на системи автентифікації на основі алгоритмів SPEKE та DH-EKE;

5. Розроблена класифікація типів атак на систему автентифікації та розроблені методи захисту.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ

3.1 АРХІТЕКТУРА ЗАБЕЗПЕЧЕННЯ

Протокол WEP реалізує класичний 40-розрядний ключ і 24-розрядний IV, але конкретні виробники зазвичай створюють вдосконалені версії, які підтримують великі довжини ключів. Чим менша довжина ключа, тим більш сприйнятливий він до атаки шляхом пошуку комбінацій (атака грубої сили), що цілком можливо для більшості сучасних комп'ютерів. Коли швидкість передачі даних секретного ключа збільшується, наприклад, до 128 біт, пошук стає неможливим навіть для спеціальних комп'ютерних систем. Однак все ще існують можливості для атак, які не використовують метод пошуку і знищують усі переваги ключа long.

Як результат, можна відносно короткий час перехопити два пакети даних, зашифровані в одній і тій же послідовності ключів. Потім статистичним аналізом можна відновити оригінальний зашифрований тест, що містить одне повідомлення. Після успішного вибору зашифрованого повідомлення та виконання "ексклюзивної або" (XOR) операції з розпізнаним текстом, зловмисник скидає відповідну послідовність ключів, дозволяючи йому переглядати всі інші зашифровані повідомлення за допомогою цього зашифрованого IV:

$$M \oplus C = M \oplus (M \oplus RC4\,(IV, K)) = RC4QV, K)$$

Навіть якщо значення повідомлення неможливо визначити, повідомлення можна оцінити за допомогою формату передбачення та зменшення IP-трафіку. Постійне знання структури змісту тексту дозволяє зменшити вивчення можливого значення.

Оскільки зловмисник має два або більше прихованих пакетів з однаковим IV, він може застосувати XOR до вмісту та побачити відмінності та подібності у структурі (див. рис. 3.1):

Рисунок 3.1. Схема аутентифікації стандарту

Іншими словами, застосування операції XOR до двох таких зашифрованих повідомлень усуває ефект послідовності ключів та аналізує різницю в незашифрованих даних (M / F M2), надаючи набагато більше шансів виявити вміст пакетів шляхом статистичного аналізу. Якби зловмисник міг збігатися з джерелом та зашифрованим текстом, він, очевидно, зміг би створити послідовність ключів. З цією інформацією неважко організувати передачу зашифрованої передачі на станцію жертви, і одержувач повідомлень розпізнає вхідні пакети як правильні.

Про цю атаку можна повідомити іншим способом. Навіть якщо зловмисник не розшифрував повністю вміст пакету, він може довільно змінити значення бітів повідомлення, а потім додати розраховане значення перевірки цілісності ICV, щоб отримати правильну версію модифікованого пакета. Операція XOR має властивість розподілу: $(x \oplus y) = C(x) \oplus c(y)$ для всіх x та y.

Розглянемо ситуацію, коли пакет даних перехоплюється під час шифрування даних: ви можете створити таке зашифроване повідомлення, яке відповідає p. Де, і можна вибрати зловмисника. Потім ви можете замінити пакет даних: (A) -> B: (IV || C), у цьому випадку станція отримає модифікований пакет даних з правильним значенням перевірки цілісності.

Для здійснення цієї атаки недостатньо просто змінити IP-адресу одержувача пакету, необхідно, щоб контрольна сума зміненого пакета була правильною. Наприклад, DL і DH - це дві 16-бітові частини вихідної IP-адреси одержувача, їх слід замінити на L та D H. Позначте старе значення контрольної суми як S, і його значення n 'n' не обов'язково відомо. Тоді нове значення обчислюється за формулою: S' = S + DL + DH-D L-D H

Якщо значення S відомо заздалегідь, легко розрахувати значення S 'і змінити пакет за допомогою операції XOR зі значенням S $\oplus$ S'. Якщо S невідомий заздалегідь, завдання набагато складніше. Значення E = S'-S, відоме, необхідно обчислити Δ = S $\oplus$ S'. Якщо ви використовуєте методи статистичного аналізу і маєте певну структуру повідомлень, існує велика ймовірність обрати бажане значення.

3.2. МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМ З БЕЗПЕКОЮ

За даними аналітиків, сьогодні лише 40% бездротових мереж 802. 11 мають ввімкнену WEP . Це призводить до втрати конфіденційності переданої інформації і дає можливість здійснювати атаки на мережеву інфраструктуру. Проти цього необхідно використовувати протокол WEP і змінювати секретний ключ якомога частіше. Під час конфігурації потрібно вказати довгий та еластичний SSID.

Використання фільтрації MAC-адрес або використання WLAN запобігає несанкціонованому доступу до бездротових карток. Не забудьте закрити інтерфейс конфігурації бездротової точки доступу. Використання антивірусного

програмного забезпечення та брандмауера запобігає появі сторонніх програм-шпигунів та інтерпретаторів на клієнтських комп'ютерах.

Захист брандмауера в поєднанні з технологією IPsec, SSH або SSL може усунути можливість розпізнавання інформації та запобігти доступу невпізнаних клієнтів до неї.

Основні зусилля докладаються до того, щоб розділити функції шифрування та автентифікації, щоб не було необхідності ділитися секретними ключами всіх станцій у бездротовій мережі. Стандартна версія стандарту, яка раніше називалася Мережею посиленої безпеки (ESN), була прийнята для забезпечення вдосконаленої версії захищеної автентифікації та 128-бітової системи управління. Система шифрування ESN замінить алгоритм генерації псевдовипадкових чисел RC4 PRNG на сучасний стандарт шифрування (AES). З введенням нової версії WEP2 рівень безпеки бездротових мереж може досягти рівня безпеки їх дротових комп'ютерів.

3.3. РОЗРОБКА ЗАСОБІВ ЗАХИСТУ ПРОТИ СИСТЕМИ АТАКИ В АЛГОРИТМІ SPEKE

У статті розглядаються проблеми обчислення дискретного логарифму та вибір параметрів для базової аутентифікації DH, зокрема за допомогою коротких показників експоненти. Таблиця 3. 1 - це скорочена зведена таблиця методів безпеки двох алгоритмів.

Можливі атаки на процес обміну DH можна розділити на наступні класи:

- Дискретний розрахунок логарифму
- Витік інформації
- Обмеження по невеликих підгрупах

При атаці, "дискретний розрахунок логарифму" протилежний - перехід від зменшення до потужності за модулем m для скидання показника ступеня i, нарешті, пароля S.

Складність цих обчислень залежить від величини та властивостей числа m. стабільність алгоритму проти цієї атаки базується на практичній неможливості такого розрахунку.

Метод захисту	Відвернена атака	SPEKE	DH-EKE
Модуль m повинен бути великим числом	Обчислення дискретного логарифма	V	V
Перевірка на Qx ! = 0, у разі не зашифрованих значень	Форсування значення K = 0	V	V
Значення m -1 повинно мати великий просто множник q.	Обчислення логарифма за методом Полінгу-Хелмана	V	V
Шифрування Qx, розбитого на частини і зібраного у випадковому порядку	Витік інформації з значення Es(Qx)		V
База g повинна бути першоподібним коренем від т.	Розподілена атака на Es (Qx)		V
База повинна бути генератором для q	Розподілена атака Qx	V	
База у вигляді Sx mod p	Атака типу «пароль в експоненті»		
Шифрування значень Qa,Qb	Обмеження по підгрупам для K		V

Таблиця 3.1 Методи захисту алгоритмів

Атака шляхом обчислення дискретного логарифму

Безпека методів, що використовуються в алгоритмах, базується на припущенні, що скорочення є односторонньою функцією, основною загрозою є здатність сторони, що атакує, обчислити дискретний логарифм результату. Усі відомі методи дискретного логарифму вимагають великої кількості початкових обчислень кожного конкретного значення модуля.

Розмір модуля є основою захисту. В даний час не існує методів обчислення дискретних логарифмів, які перевищують сто біт, але цілком ймовірно, що найближчим часом можуть відбутися успішні атаки на 512-бітові модулі. Десь у діапазоні від 512 до 1024 біт є ідеальний розмір модуля, зі збалансованою безпекою та швидкістю обчислень, для конкретних програм.

Припускаючи, що необхідному дискретному логарифму передує конкретний модуль, певний логарифм повинен бути обчислений для кожного запису в словнику паролів під час атаки на основі "вибору пароля", поки не буде знайдено правильне значення.

Будь-який сеанс, який використовує модулі, схильний до логарифмічної атаки. Таким чином, необхідність спостерігати за ситуацією максимально ускладнює проблему обчислення дискретних логарифмів. У цьому випадку пріоритетом є можливість перерахунку.

Атака за допомогою відомого ключа сеансу

У статті йдеться про атаку, при якій викрадений ключ сеансу k використовується для атаки пароля за допомогою словника. Опір цій атаці тісно пов'язаний з концепцією повної прямої безпеки, яка ізолює один тип конфіденційної інформації від нападів на інших.

В алгоритмі DH-EKE певне значення Ra, крім відомого K, дозволяє словнику відкрити пароль для атаки. Для кожного тестового пароля зловмисник розраховує: $K' = (Esi^{-1}(Es(g^R b)))^R a$

У цьому випадку, якщо K '= K, тоді Si =S. Алгоритм SPEKE однаково чутливий до цієї атаки, в якій S. обчислюється за допомогою Ra. Тому тимчасові змінні шифрування, такі як Ra та Rb, слід негайно знищити..

Атака на стадії перевірки

У разі дослідження протоколів DH-EKE та SPEKE обидві сторони доводять, що вони знають ключове значення, спільне одне для одного через високе значення K-криптографічного числа, вважається захищеним від атаки другим кроком пошуку.

Виявляйте атаки в режимі реального часу

Ви можете зменшити ризик повторного повторного введення пароля в режимі реального часу, створивши резервну копію історії та підрахувавши невдалі входи. Ви повинні обмежити кількість неправильних спроб отримати доступ до своїх облікових записів, вимагаючи зміни пароля при досягненні певного ліміту. Порогове значення повинно базуватися на довжині пароля. Також необхідно поважати кількість невдалих спроб знайти пароль як при атаці на автономний обліковий запис, так і при спробі масової атаки, яка не досягає порогу для жодного з користувачів.

Ви повинні вести облік невдалих спроб входу в систему хосту та користувача. Налаштована система повинна підтримувати щонайменше список останніх невдалих спроб і передавати цю інформацію через захищений канал до домашньої системи кожного разу, коли встановлюється успішне з'єднання. Хост-система також може повідомляти користувача про кількість невдалих спроб доступу. Цей метод значно зменшує ймовірність атак паролем з обох сторін.

3.4. РОЗРОБКА БЕЗПЕКИ ДЛЯ РАДІОКАНАЛУ 802.11

Можливість перехоплення інформаційного пакета.

Проблема в тому, що дані передаються по радіо. Кожна станція, розташована в зоні прийому сигналу, може збирати інформаційні пакети. Якщо шифрування не було використано, дані можна досить тривіально витягти з окремих пакетів і використовувати залежно від подальших намірів сторони, яка їх перехоплює, не вдаючись до використання спеціальних інструментів. Для цього типу завдань досить встановити простий мережевий монітор, який дозволяє переглядати вміст пакету та фільтрувати за певними функціями, наприклад, за IP-адресою. Ситуація ще більше погіршується тим, що неможливо визначити, слухається радіо в даний час чи ні. Таким чином, перехоплення може відбутися абсолютно непоміченим адміністратором мережі.

Недоліки, пов'язані з шифруванням.

WEP - це протокол шифрування інформації, технічні характеристики якого описані в IEEE 802. 11.

При реалізації того, що передбачено, протокол WEP має кілька недоліків в архітектурі, що дозволяють шифрувати інформацію зловмиснику [3]. WEP використовує алгоритм шифрування RC4 у поєднанні з ключем на 64 або 128 сторінок, що складається із прихованого ключа та значення вектора ініціалізації. Злом WEP не є загальними недоліками RC4, навіть не в довжині ключа, а скоріше у відмові алгоритму.

IEEE 802. 11 систем безпеки потребують серйозних удосконалень. Це вимагає комплексного підходу до проблеми.

У найпростішому випадку для підключення до загальнодоступних мереж досить використовувати маршрутизатор NAT, але недостатньо для побудови справді захищеної мережі.

Наступними ключовими областями є стратегії бездротової безпеки:

• фільтрація вхідного та вихідного трафіку за допомогою брандмауера;

• шифрування з'єднань для віддаленого доступу;

• подвійна автентифікація для віддаленого доступу;

• багаторівневі зони безпеки для загальнодоступних ресурсів;

• засоби виявлення спроб несанкціонованого доступу.

Розглянемо безпеку протоколу 802. 11 у контексті цієї стратегії. Важливо те, що будь-які вдосконалення системи безпеки не порушують внутрішню структуру, описану в стандарті, а лише доповнюють та вдосконалюють її. Це забезпечує повну сумісність із компонентами та технологіями різних виробників, що існують на ринку. Модульний підхід заснований на використанні стандартних, усталених алгоритмів і залишає можливість використання нових технологій без необхідності змінювати існуючу структуру. Ця бездротова система безпеки дуже добре підходить до існуючої політики безпеки мережі.

Більшість даних, що містяться в пакеті WEP, уже зашифровані IPSec, що запобігає атаці зіставлення раніше відомого повідомлення із зашифрованим аналогом. Однак слід зазначити, що в цьому підході заголовок LLC та заголовок IPSec шифруються лише WAP, що може дещо знизити криптографічну стабільність моделі захисту.

MAC-адреса, SSID, IV, ідентифікатор ключа та FCS також залишаються доступними для можливого перехоплення. Ця інформація не може бути зашифрована, оскільки вона використовується на фізичному рівні та на рівні каналу (підрівню MAC).

Оскільки основні дані захищені алгоритмами IPSec (DEC3) та WEP (RC4), інформація, яку можна отримати за допомогою відкритих значень SSID, IV та Key ID, не матиме значної вигоди для сторони, яка перехоплює. Значення FCS - це контрольне значення CRC із пакета MAC, що використовується для перевірки цілісності даних після їх передачі. Найбільшою загрозою для безпеки є

незашифрована передача вихідного значення MAC, яке зловмисник може замінити.

Тому автентифікація MAC-адреси повинна розглядатися лише як додатковий засіб захисту від вторгнення.

Запропонована модель безпеки перевіряє справжність як користувача, так і пристрою. Пристрій аутентифікується за допомогою ключа WEP. Часто міняйте ключ і поширюйте його по захищеному каналу. Перш ніж пристрій зможе спілкуватися через брандмауер, користувач повинен завершити процес реєстрації в центральній базі даних управління користувачами мережі, яка зберігає рахунки-фактури та політики безпеки. Брандмауер не тільки запобігає несанкціонованому доступу до мережі, але і блокує трансляції, які можуть містити інформацію про внутрішню структуру мережі. Зашифрований пакет IPSec у тунельному режимі не містить додаткової інформації про структуру, доступну для зовнішнього захоплення, оскільки він шифрує, а потім замінює заголовок пакета IP, що містить цільову IP-адресу, на власний заголовок, що вказує цільову IP-адресу брандмауера.

Наступним кроком є вибір способу розподілу секретного ключа. Одне з можливих рішень - використання захищених каналів SSL. Найкращим методом безпеки є призначення системного адміністратора, який відповідає за зміну секретних ключів на всіх пристроях, але це може призвести до рідкісних змін ключів. Деякі виробники включають у свої продукти власні методи призначення ключів, але оскільки IEEE 802. 11 не вказує, як це зробити, не всі з цих рішень стандартизовані.

Далі вам потрібно вирішити, який брандмауер найкраще підходить для мережевої безпеки.

Дисплей є важливим компонентом, який знаходиться між бездротовою підмережею та внутрішньою мережею.

При виборі зверніть увагу на основні фактори:

• Брандмауер повинен відповідати тунельному режиму із зашифрованим трафіком усіх типів бездротових пристроїв;

• Метод перевірки повинен узгоджуватися з інтегрованою базою даних про клієнтів;

• Підтримка віддаленої ідентифікації користувачів базується на політиці безпеки, що зберігається в базі даних управління користувачами.

Наступним кроком є визначення того, чи відповідає технологія IPSec існуючій інфраструктурі. Або ви можете використовувати технологію SSL. Але у цього підходу є і недоліки. Тому неможливо працювати в тунельному режимі між брандмауером та віддаленим користувачем, а це означає, що можливо перехоплювати реальні IP-адреси. SSL займає вищий рівень у стеці TCP / IP, ніж відповідний IPSec, більше незашифрованої інформації можна отримати шляхом перехоплення та аналізу пакетів. Спочатку технологія SSL була розроблена як протокол для роботи в Інтернеті, тому деякі програми можуть не працювати в бездротовій мережі.

3.5 ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ

Практичні вимірювання використовують підхід, який поєднує експериментальні дані з теорією поширення радіосигналу в просторі.

Умови тестування

Тест проводився в офісному приміщенні розміром приблизно 30 м на 20 м. Конструкція внутрішніх перегородок виконана з бетону, включаючи металеві конструкції. Для експерименту були використані три окремі точки доступу, розташовані в випадкових місцях. Перші два - це Cisco AP350. Перша мала дві антени, друга не мала антен. Третя модель Orinoco AP-1000 з антеною Lucent.

Збір даних

Першим завданням було зібрати значення залежності потужності сигналу від відстані на основі даних, наданих драйвером бездротової карти. Для збору даних ми використовували програму iwspy, налаштовану на певну MAC-адресу:

iwspy eth0 0b:0b:0b:0b:0b:0b

Послідовний виклик "iwspy eth0" поверне рівень сигналу пакетів, отриманих від цього передавача.

Випробувальна станція рухається по території, вимірюючи силу сигналу у випадкових точках. Для обробки використовується файл, що складається з двох стовпців, на першій відстані від передавача, на другому рівні сигналу. Графічно значення показані на (рис. 3. 3 - рис. 3. 5).

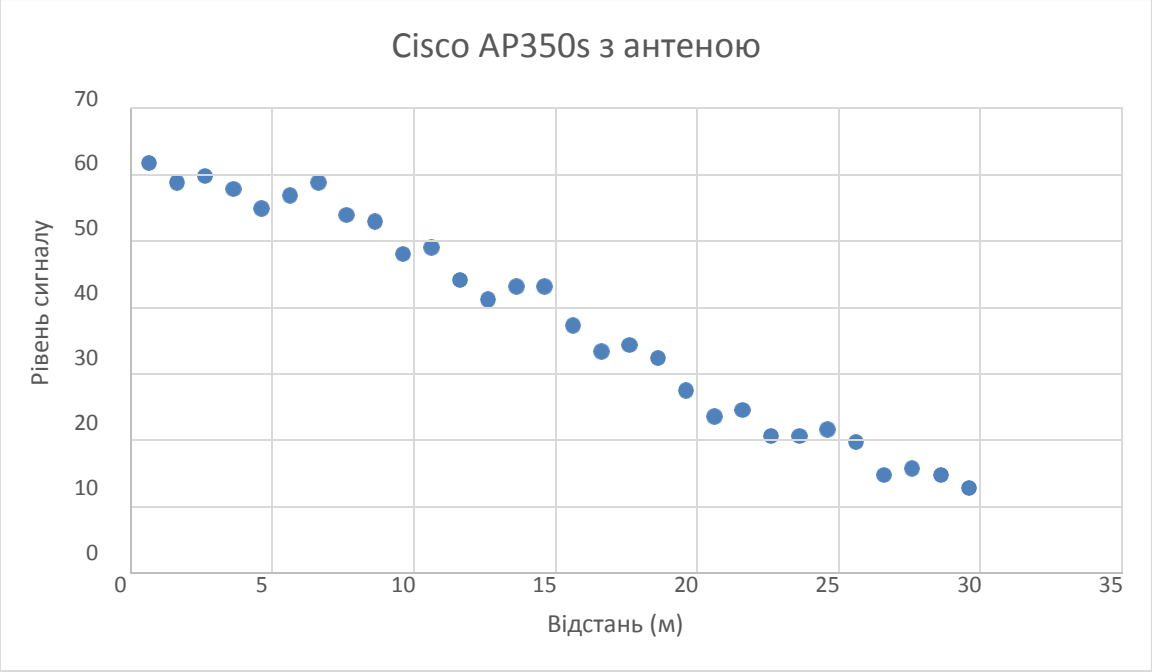

Рисунок 3.3 Cisco AP350s з антеною

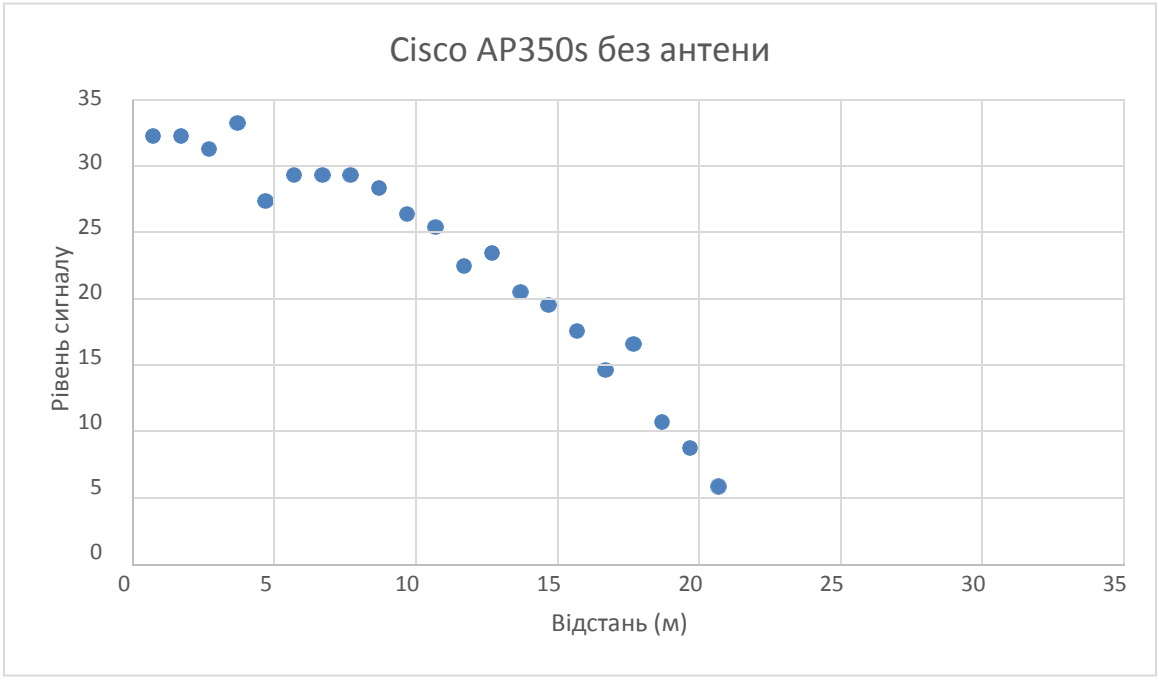

Рисунок 3.4 Cisco AP350s без антени

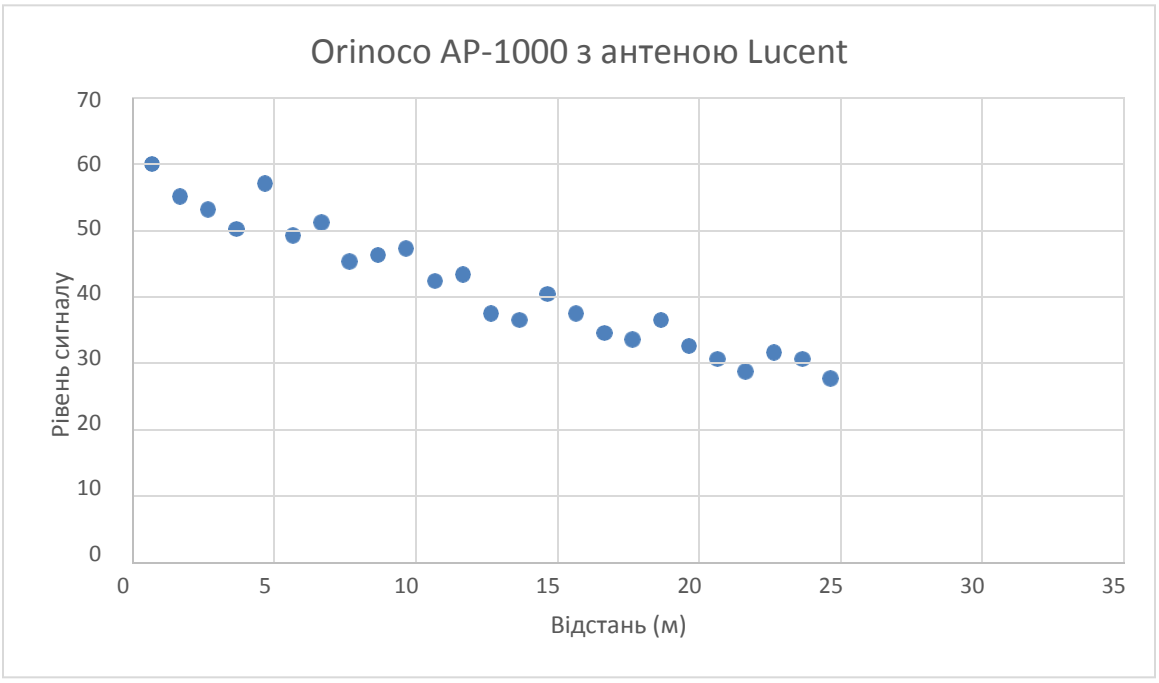

Рисунок 3.5 Orinoco AP-1000 з антеною Lucent

Визначення залежності сили сигналу на наступному кроці полягає в тому, щоб перевірити, чи можуть дані, отримані в попередньому тесті, задовольнити співвідношення, подане на початку глави.

Для цього потрібно спочатку перетворити значення (RSSI - значення стану прийнятого сигналу), отримане за допомогою iwspy, у дБ. Наступні обіцянки були отримані в результаті експериментів:

$$P_{dBm} = 1{,}205P_{RSSI} - 101{,}07$$

$$P_{RSSI} = 0{,}83P_{dBm} + 83{,}891$$

Де: PdBm - рівенб сигналу в ДБ, PRSSI - значення, яке отримали за допомогою iwspy.

Якщо значення виводяться у нормалізованому вигляді (цей параметр вказаний у драйвері бездротової карти), рівняння мають такий вигляд:

$$P_{dBm} = 0{,}62N_{RSSI} - 101{,}07$$

$$N_{RSSI} = 1{,}66P_{dBm} + 167{,}782$$

В даний час iwspy ioctl для Linux повертає ненормовані значення (однак, клієнт Cisco для Windows повертає нормалізовані значення).

Наступним кроком є створення функції наближення кривої, яка включає вищезазначені залежності. Він заснований на рівнянні, яке враховує як ослаблення радіохвиль у просторі, так і відбиття, заломлення та перешкоди.

В результаті експериментів та досліджень було отримано наступний звіт про поширення радіосигналу в будівлі з частотою 2,4 ГГц.

Таким чином, втрати на 10 метрів становитимуть приблизно 75 дБ на 100 метрів при 110 дБ. Очікувана помилка становить близько 13 дБ.

Всі невідомі константи, включаючи експериментально отримане значення "40", будуть об'єднані константою C, де C - невідома константа, що визначає вихідну потужність, враховуючи ефекти загасання, конфігурацію антени та інші фактори. $R_d = C - 35log_{10}D$

За допомогою посилання нижче ми перетворимо значення на значення за замовчуванням (порівнюючи значення даних за замовчуванням використання iwspy до Linux):

$$P_{RSSI} = 0{,}83(C - 35log_{10}D) + 83{,}891$$

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Аналіз результатів показав, що цей ряд заходів щодо запобігання атакам на бездротову мережу є високоефективними;

2. Виявлено можливі причини помилок при обчисленні координат:

2. 1. Затухання сигналу від антени передавача було великим. Перешкоди розташовані на сигнальному шляху;

2. 2. Передавач знаходився посередині кімнати, тому не було можливості зібрати достовірну інформацію про загасання сигналу на екстремальних відстанях;

2.3. Передавач розташований у приміщенні з великою кількістю металевих предметів, які послаблюють і захищають сигнал у певних напрямках.

3. Основними обмеженнями запропонованого методу є:

3. 1 Драйвер Cisco та мережева карта мають обмежені можливості. довільне сканування трафіку, тому деякі корисні дані можуть бути втрачені під час експерименту;

4. Картка Cisco не може сканувати кілька каналів одночасно. Коли спрацьовує сигнал тривоги: з несанкціонованої станції всі карти, що використовуються для захисту мережі, повинні припинити сканування та перейти на цей канал для збору повних даних. На практиці було продемонстровано застосування вдосконаленої системи безпеки.

5. Якщо використовується більше однієї станції, всі вони повинні мати однакові версії мережевих карт (включаючи антени) та драйвери;

6. Збільшення кількості станцій, які беруть участь у пошуку, збільшує шанси на успішне розміщення;

7. Пошукові станції, якщо вони нерухомі, повинні розташовуватися якомога оптимальніше: на відкритому просторі, на максимально можливій відстані одна від одної, виключаючи можливе послаблення сигналу від шуму або перешкод. одночасно з отриманням сигналу з будь-якої точки заповідної зони;

8. Необхідно створити активну мережеву станцію сканування, яка буде надсилати запити, що вимагають відповідей, які можуть виявити несанкціонований сигнал передавача;

9. Пошукові станції потребують високочутливих антен;

10. Якщо мобільний пристрій не має дозволу, ця технологія може не дати належних результатів;

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

4.1 Охорона праці

Метою магістерської роботи є реалізація ряду заходів щодо забезпечення надійного механізму захисту даних від NSD у бездротових мережах Wi-Fi (на основі раніше вивчених технологій та методів захисту). Оскільки розробка та використання системи передбачає використання комп'ютерного обладнання, включаючи комп'ютери та периферії, вимоги захисту та захисту дисертації повинні бути виконані.

Потрібно організувати середовище безпеки для ефективної та безпечної роботи команди розробників IT-програм, включаючи групу експертів для оцінки зрілості програми. При цьому керівник організації несе безпосередню відповідальність за будь-яке порушення правил безпеки.

Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин». Згідно Правил приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-13- 98), з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 № 151 зареєстрованих у Міністерстві юстиції України 29.04.2004 за № 554/9153 (НАПБ Б.03.001-2004), і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2004.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-13-98, НАПБ А.01.001-2004 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електроживлення комп’ютера та периферійних пристроїв повинна бути виконана як трипровідна мережа окремої групи шляхом розташування фазних проводів, обробки нульового дроту та захисту нульового дроту. Нульовий захисний провідник використовується для заземлення (нейтралізації) електричних навантажень. Заборонено використовувати нейтральний робочий провідник як нейтральний захисний провідник. Нейтральний захисний провід прокладається від групової шафи розподільних пристроїв, від точки розподілу до розеток. Неприпустимо підключати на платі до нульової робочої контактної клеми і нульового захисного провідника.

Перетин нейтрального робочого та захисного нульового провідника в груповій трипровідній мережі не повинен бути меншим за переріз фазного провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

- У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.
- У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним.

Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі.

Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При експлуатації програмної системи підтримки процесу розробки вимог, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-1.28-10.

Організація робочого місця фахівця із запровадження або оцінювання рівня зрілості вимог програмного забезпечення повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ГОСТ 12.2.032-78 "ССБТ. Робоче місце при виконанні роботи сидячи.

Загальні ергономічні вимоги ".

Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з побудови та оцінювання моделей і рівнів зрілості вимог програмного забезпечення при проектуванні комп’ютерних систем.

4.2 Вплив радіації на працездатність населення

Вплив радіації на організм людини називають опроміненням. Під час цього процесу енергія радіації передається клітинам, руйнуючи їх. Опромінення може викликати всілякі захворювання: інфекційні ускладнення, порушення обміну речовин, злоякісні пухлини і лейко, безпліддя і багато іншого. Коли радіоактивне випромінювання проходить через тіло людини або ж коли в організм потрапляють заражені речовини, то енергія хвиль і частинок передається нашим тканинам, а від них клітинам. Радіонукліди накопичуються в організмі поступово.

Як відомо, вплив радіації на організм людини або тварини може бути двох видів: зсередини або зовні. Здоров'я не додає ні один з них. Крім того, науці відомо, що внутрішній вплив радіаційних речовин небезпечніше зовнішнього. Найчастіше радіаційні речовини потрапляють в наш організм разом із зараженою водою і їжею. Вплив радіації на організм майже завжди негативний. Хоча доведено, що ультрафіолетова радіація підвищує

працездатність організму, оскільки такі промені не тільки мають терапевтичне значення, але при відсутності природного сонця, особливо восени та взимку, є незамінним профілактичним засобом відносно різних інфекцій. Багато районів з підвищеним радіаційним фоном є визнаними курортами (наприклад, Кавказькі Мінеральні Води, Карлові Вари і т.п.) В Україні в лікувальних закладах достатньо широко використовується корисне опромінення альфа-частинками в радонових ваннах як лікування.

Проте, в основному, радіація за своєю природою шкідлива для життя людини. Спочатку людина втрачає фізичну працездатність, а потім – розумову. Малі дози опромінення можуть призвести до тимчасової втрати працездатності, середні та великі – до онкологічних захворювань і, як наслідок, смерті. Науковий комітет по дії атомної радіації при ООН спробував висловити генетичні наслідки опромінення через такі параметри, як скорочення тривалості життя і періоду працездатності. Ці параметри, звичайно, не можуть дати адекватного уявлення про страждання жертв спадкових недуг або таких речах, як відчай батьків хворої дитини, але до них і неможливо підходити з кількісними мірками. Цілком віддаючи собі звіт в тому, що ці оцінки не більш ніж перша груба прикидка, ООН приводить в своїй доповіді наступні цифри: хронічне опромінення населення з потужністю дози 1 Гр на покоління скорочує період працездатності на 50 000 років, а тривалість життя – також на 50 000 років на кожен мільйон живих немовлят серед дітей першого опроміненого покоління; ті ж параметри при постійному опроміненні багатьох поколінь виходять на стаціонарний рівень корочення періоду працездатності складе 340 000 років, а скорочення тривалості життя – 286 000 років на кожен мільйон живих немовлят.

Проникаюча радіація, поширюючись у середовищі, іонізує його, а при проходженні через живу тканину іонізує атоми і молекули, що входять до складу клітин. Це призводить до порушення нормального обміну речовин, зміни характеру життєдіяльності клітин, окремих органів і систем організму, як наслідок - виникає променева хвороба. Аналіз і узагальнення основних

результатів наукових досліджень показали, що медичні наслідки Чорнобильської аварії суттєво відрізнялися від прогнозованих ефектів, зокрема значно знижувалася працездатність населення аж до отримання інвалідності та настання смертельних випадків. Всі особи, що зазнали загального хронічного опромінювання в діапазоні потужності поглинених доз 10-4 — 5 * 10-4 Гр/добу (0,01—0,05 рад/добу) чи еквівалентних доз 0,05 — 0,15 Зв/рік (5 — 15 бер/рік), залишаються здоровими і працездатними.

Відомо, що ступінь променевих (радіаційних) уражень залежить від отриманої дози випромінювання та часу, впродовж якого людина підпадає під його дію. Якщо доза не перевищує 50Р, то виключена навіть втрата працездатності, не кажучи вже про променеву хворобу. Доза в 200-300Р, отримана за короткий час, може викликати тяжкі радіаційні ураження. Здоровий організм людини здатний за цей час виробляти нові клітин на заміну загиблих. Навіть найменші дози викликають необоротні генетичні зміни, які передаються з покоління в покоління, призводять до розвитку синдрому Дауна, епілепсії, появі інших дефектів розумового і фізичного розвитку. Особливо страшно те, що радіаційному зараженню піддаються і продукти харчування, і предмети побуту. Останнім часом почастішали випадки вилучення контрафактної та низькоякісної продукції, що є потужним джерелом іонізуючого випромінювання.

Найпростіший і ефективний спосіб захистити себе від негативного впливу смертоносних променів - триматися подалі від їхнього джерела. Якщо знати все про радіацію і вміти правильно користуватися приладами для її вимірювання, то можна практично повністю уникнути її негативного впливу. Незважаючи на високу небезпеку, яку несе в собі практично будь-яке джерело радіації, методи захисту від опромінення все ж існують.

Всі способи захисту від радіаційного впливу можна розділити на три види: час, відстань і спеціальні екрани. Хоча необхідно знати, що на сьогодні ідеального засобу захисту від радіації не існує. Найкращий спосіб захисту від радіації - взагалі не мати контакту з зараженими предметами і не перебувати в

місцях з підвищеним радіаційним фоном.

4.3 Планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації

Найбільш повне та організоване виконання заходів цивільного захисту (ЦЗ) на об’єкті досягається завчасною розробкою плану заходів, які необхідно проводити при загрозі або виникненні надзвичайної ситуації (НС).

План дій органів управління і сил ЦЗ (міністерств, відомств, областей, районів, міст, підприємств, установ і організацій) із запобігання і ліквідації НС розробляється на підставі законодавчих, директивних і нормативних документів і призначений для координації і діяльності центральних і місцевих органів виконавчої влади, керівництва, а також оперативності їх реагування на загрозу і виникнення НС, відвернення або зниження можливої загибелі людей, мінімізація матеріальних збитків і втрат та організацію задоволення першочергових потреб населення, яке постраждало [17]. План визначає порядок дій і відповідальність керівництва відповідних органів управління підприємств, установ і організацій, а також основні заходи щодо організації і проведення робіт із запобігання і ліквідації НС техногенного і природного характеру, узгодження термінів їх виконання, фінансові, матеріальні та інші ресурси, які необхідні для цих заходів і робіт. У план дій включаються заходи щодо захисту робітників і службовців, підтримування виробничої діяльності та інші з урахуванням обстановки після виникнення НС, передбачаються необхідна кількість сил і засобів для ліквідації наслідків НС. Основними вихідними даними при розробці плану дій на об’єкті є рішення та вказівки вищого штабу ЦЗ, розпоряджень начальника ЦЗ об’єкта, документів, що характеризують об’єкт (комунально-енергетичні мережі, стан будівель і споруд, вододжерела та ін.). План дій розробляється на підставі наказу начальника ЦЗ об’єкта. До розробки документів плану залучається керівний склад і спеціалісти об’єкта. Начальник штабу ЦЗ складає графік розробки окремих документів (розділів) і

контролює його виконання.

План дій розробляється у двох (при необхідності і більше) примірниках. Підписується план дій начальником штабу ЦЗ об’єкта, погоджується з територіальними управліннями (відділами) з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи і затверджується начальником ЦЗ об’єкта. Після затвердження зміст плану дій доводиться до виконавців. План дій органів управління і сил ЦЗ із запобігання та ліквідації НС – це програма здійснення запобіжних та захисних заходів. Він дозволяє цілеспрямовано та організовано вирішувати завдання ЦЗ в умовах НС мирного та воєнного часу. При визначенні цих заходів враховується важливість та особливості виробничої діяльності об’єкта, основні завдання органів управління та сил ЦЗ щодо запобігання і ліквідації НС.

План дій органів управління та сил ЦЗ на мирний час складається із п’яти розділів текстової частини і додатків до них. Текстова частина плану включає такі розділи: 1. Висновки із оцінки обстановки на території об’єкта.
2. Приведення в готовність та організація роботи органів управління в НС. 3. Сили ЦО об’єкта, що залучаються до виконання аварійно-рятувальних, пошукових та відновлювальних робіт. 4. Організація забезпечення заходів та дій ЦЗ. 5. Організація управління, оповіщення і зв’язку.

Окремо розробляється “План дій органів управління та сил ЦЗ об’єкта при переведенні з мирного на воєнний стан” за ступенями готовності воєнного часу та раптовому нападі супротивника. Крім цього, на об’єкті господарської діяльності розробляються плани служб ЦЗ, щодо забезпечення заходів і дій органів управління і сил ЦЗ при загрозі і виникненні НС та при переведенні органів управління і сил з мирного на воєнний стан.

Висновки до розділу 4

В цьому розділі описані важливі питання охорони праці, вплив радіації на працездатність населення та планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації.

ВИСНОВКИ

Досягнуто ступеня магістра з аналізу безпеки бездротової мережі, вибору методів їх захисту та розробки моделі захисту бездротової мережі.

1. Вивчення особливостей стандартного протоколу для шифрування потоку WEP. Для кожного виду атаки були розроблені контрзаходи для підвищення рівня захисту даних на радіоканалі.

2. Розроблена система автентифікації на основі алгоритму SPEKE. З метою захисту інформації було проведено дослідження, проаналізовано механізми нападу та розроблено метод реагування. Стандарт 802. 11 Розроблена система заміни засобів сертифікації, яка не забезпечує належного рівня безпеки.

3. На основі алгоритму SPEKE розроблено захищений механізм обміну ключами сеансу, який не доступний у стандартній системі безпеки. Можливість зміни ключа сеансу зменшує ймовірність успішної атаки на зашифровану інформацію за допомогою алгоритму шифрування потоку WEP.

4. Розроблено вдосконалену систему захисту інформації для 802.11 радіоканалів, що дозволило значно підвищити рівень захисту даних у порівнянні зі стандартними системами із застосуванням стабільного набору засобів шифрування та методів шифрування, сертифікація та обмін ключами.

5. Розроблена технологія, яка дозволяє вторгнення станції зловмисника, розташованої в частині бездротової мережі, використовуючи функції протоколу 802.11. Були розроблені методи підвищення ефективності роботи пошукових систем для активних порушувальних станцій. Це значно зменшить ймовірність компрометування інформації радіоканалу. Надійність наукових положень дисертації підтверджується наступним: експериментальні дослідження, результати фактичного впровадження та впровадження систем захисту даних у

радіоканалах.

Надано методи підвищення швидкості роботи алгоритму та інструменти для підвищення криптографічної стабільності надійної системи автентифікації.

На основі розроблених методів та засобів було створено вдосконалену систему безпеки WiFi.

ПЕРЕЛІК ПОСИЛАНЬ

1. Анохин В.Л., Батанов А.Ф., Гамазов Н.И. Принципы автоматизации работ, выполняемых в экстремальных условиях робототехническими комплексами // Вестник МГТУ. Сер. Приборостроение. -1997. - №.2. - С. 75-81.

2. Вильям С. Криптография и защита сетей: принципы и практика, 2-е изд.- М.: Вильяме, 2001. - С. 672.

3. Воротников С. А., Михайлов Б. Б., Ющенко А.С. Адаптивная робототехническая система с интеллектуальной сенсорикой // Вестник МГТУ. Сер. Машиностроение. - 1995. - №.3. - С. 55 -58.

4. Джерело: Вихорев С., Кобцев Р. Як визначити джерела загроз. //Відкрита система. – 2002. - №07-08.С. 43.

5. Дружинин В.В., Конторов Д.С, Конторов М.Д. Введение в теориюконфликта. - М.: Радио и связь, 1989. - 288 с.

6. Королев В.И. Морозова Е.В. Методы оценки качества защиты информации при ее автоматизированной обработке // Безопасность информационных технологий. - 1995. - № 2. - 215 с.

7. Партыка Т. Л. ,Попов И. И. Информационная безопасность. - М: Форум - Инфра, 2002. - С. 368.

8. Поспелов Д.А. Неметкие множества в моделях управления и искусственногоинтеллекта. - М.: Наука, 1986. - 312 с.

9. Ротштсйн А.П. Интеллектуальные технологии идентификации. - Винница: «Универсум-Винница», 1999. - 320 с.

10. Успенский А. Ю. Операционные системы реального времени // Компью-Лог. - 2001. - №3. - С. 11 -17. - Успенский А. Ю. Применение интерфейса Photon в~системе управления робототехническим комплексом // Компью-Лог. - 2001.-№5.-С. 13-20.

11. Успенский А.Ю. Исследование возможности и методы противодействия перехвату защищенной при помощи протокола WEP информации в радиоканале стандарта IEEE 802.11

// Студенческая научная весна - 2002. Сборник докладов студенческой научной конференции. - М.: 2002. - С. 89-91.

12. Успенский А.Ю., Иванов И.П. Анализ проблем защиты информации в радиоканалах стандарта IEEE 802.11 // Вестник МГТУ. Сер. Машиностроение. - 2002. - №. 4 - С. 102-108.

13. Ющенко А.С. Принципы інтерактивного управления роботами // Робототехника: новый этап развития. - М.: Наука, 1993. - С. 129-139.

14. International Conference on Mobile Computing and Networking - ScarfoneKaren, PadgetteJohn GuidetoBluetoothsecurity // NIST specialpublicationsep 2008.

15. Shim, Richard. How to Fill Wi-Fi's Security Holes, -Washington: ZDNet.-2001.-P.

16. Steiner M., Tsudik G., Waidner M.. Refinement and Extension of Encrypted Key Exchange II Operating Systems Review.-1995 - 29, Iss. 3.-1995-22-30 p. WEP Algorithm. II http://www.isaac.cs.berkeley.edu/isaac/wep