КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.634
УДК 004.056.2

Жураковський Богдан Юрійович
Доктор технічних наук, професор
Київський політехнічний інститут ім. Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0003-3990-5205
zhurakovskiybyu@tk.kpi.ua

Недашківський Олексій Леонідович
Доктор технічних наук, професор
Київський політехнічний інститут ім. Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0002-1788-4434
al_1@ua.fm

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ В РАДІОКАНАЛІ

Анотація. Дана стаття присвячена вирішенню задачі захисту інформації в радіоканалах, шляхом застосування комплексних заходів для захисту від можливих атак спрямованих на перехоплення і підміну переданих даних. Метою роботи є проведення аналізу безпеки безпровідних мереж, виділення методів їх захисту та створення моделі захисту безпровідних мереж. Для того, щоб досягнути поставленої мети, виконано наступний перелік завдань: проаналізовано існуючі рішення у галузі захисту інформації через радіомережі; зроблено опис запропонованої розробленої моделі; описано алгоритми, експерименти, досліди даної моделі. Розроблено засіб захисту інформації через радіомережі, застосування якого має значне підвищення рівня безпеки інформації в радіоканалі. Практична цінність даної розробки в тому, що отримані теоретично і практично результати рекомендуються до впровадження в організаціях, що використовують радіоканал для передачі конфіденційної інформації з підвищеним вимогам до безпеки.

Ключові слова: авторизація, автентифікація, безпровідна мережа, Wi-Fi, модель, алгоритм шифрування, ключі, цифровий підпис, пароль, інформаційна безпека.

ВСТУП

У безпровідних мереж дуже багато спільного з провідними, але є і відмінності. Для того, щоб проникнути в поводову мережу, хакеру необхідно фізично до неї підключитися. У варіанті Wi-Fi йому досить встановити антену поблизу, в зоні дії мережі.

Хоч сьогодні в захисті Wi-Fi-мереж і застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних, контролю цілісності їх передачі, тим не менше, на початкових етапах поширення Wi-Fi нерідко з’являлися повідомлення про те, що навіть не використовуючи складного обладнання і спеціальних програм можна було підключитися до деяких корпоративних мереж просто проїжджаючи повз з ноутбуком.

Для того, щоб правильно спланувати безпеку безпровідної мережі потрібно враховувати вартість цінностей, що захищаються, вартість впровадження системи безпеки, а також здатності потенційних атакуючих. Іншими словами, перш ніж впроваджувати всі заходів захисту, відомі людству, розумніше впровадити заходи захисту від найбільш частих погроз.

Аналіз останніх досліджень і публікацій.

Останнім часом спостерігається тенденція інтегрування передавання різних видів інформації (мова, дані, зображення, інформація для телеуправління і контролю) та послуг у єдину мережу, яка оснащена різними видами апаратури. Управління такими

мережами можливе тільки із застосуванням нових способів та систем управління мережами. Використання системи управління операторами мобільного, фіксованого зв'язку забезпечує економічне і ефективне управління мережею, що є ключем до успішної роботи мережі - гарантуючи низькі витрати та високу надійність мережі. Це означає швидке виявлення, локалізацію та усунення несправностей, зі зниженням витрат на трудові ресурси, обладнання та навчання, в той же час гарантує забезпечення найкращої якості і безпеки.

До системи аутентифікації в безпровідній мережі пред'являються підвищені вимоги з безпеки. Необхідно використовувати криптографічно стійкі алгоритми, що дозволяють здійснити взаємну аутентифікацію сторін. Окремим важливим завданням є локалізація активної станції - порушника в межах захищеної безпровідної мережі. Необхідно розробити технологію, що дозволяє здійснювати ефективний пошук неавторизованої станції.

Цим питанням присвячені експериментальні дослідження вітчизняних та закордонних вчених: Конахович Г.Ф., Толюпа С.В., Бурячок В.Л., Семко А.А., Хорошко В.О., Гнатюк С.О., Samonas S., Jacques, R. J., Andress, J., Schlienger T., Гайдур Г.І., Сайко В.Г. та інші.

Мета статті.

Метою роботи є проведення аналізу безпеки безпровідних мереж, виділення методів їх захисту та створення моделі захисту безпровідних мереж.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Безпека безпровідних мереж.

Безпека безпровідних мереж залежить від використання ряду технологій: шифрування, цифрового підпису, паролів, зміни ключів та іншого. Те, як використовуються ці технології сильно впливає на рівень захищеності мережі. Іноді, методика використання деяких технологій така, що вони ніяк не впливають на рівень захищеності мережі.

Стандарт шифрування E0. У стандарті Bluetooth застосовується потоковий шифр E0, побудований на базі трьох лінійних генераторів зсуву. Ця схема застосовується в Bluetooth в режимах забезпечення безпеки 2 і 3. Дані режимні безпеки застосовуються в протоколі Bluetooth v4.2.

Основою процедури шифрування в протоколі *Bluetooth* служить алгоритм потокового шифрування E0. Ключ потоку підсумовується, але схемі XOR з бітами відкритого тексту і передається на пристрій. Ключ потоку генерується за допомогою криптографічного алгоритму на базі лінійного рекурентного регістра (ЛРР). Функція шифрування отримує такі вхідні дані: головний ідентифікатор (BDADDR). 128-бітне випадкове число (EN_RAND), номер слота і ключ шифрування, який також ініціалізує ЛРР, якщо шифрування включено. Номерслота, який використовується в потоковому шифрі, змінюється з кожним пакетом, змінюючи тим самим ініціалізацію ядра шифру, інші ж неременні при цьому не змінюються [1].

Ключ шифрування *КС* генерується з поточного сеансового ключа і може мати довжину від 8 до 128 біт. Встановлення розміру ключа відбувається в ході встановлення сеансу шифрування між пристроями. Початковий розмір ключа вноситься в пристрій виробником, і розмір його не завжди максимальним. Слід зазначити, що алгоритм E0 не сертифікований FIPS як національний стандарт. Є теоретична оцінка стійкості даного

ISSN 2663 - 4023

алгоритму. При атаці зі знанням відкритого тексту потрібно 238 переборів, в той час як при атаці грубої сили необхідно перебрати 2128 можливих ключів.

Шифр Діффі-Хеллмана на еліптичних кривих. У режимі безпеки протоколу Bluetooth v4.2 використовується пара ключів безпечного простого сполучення (*SecureSimplePairing* SSP). Ця пара ключів являє собою ключі алгоритму асиметричного шифрування Діффі Холмана на еліптичних кривих.

Даний алгоритм надійний: реалізованих на практиці ефективних атак на EAM алгоритм в даннвій момент не існує. Але є ймовірність того, що атака виявиться успішною при програмній і апаратній реалізації алгоритму.

Стандарт шифрування AES. Даний стандарт шифрування найбільш широко застосовується для захисту бездротових каналів передачі інформації. Він використовується в протоколах UWB, ZigBee, RuBee, WI-FI і WIMAX. У зв'язку з широким розповсюдженням даного алгоритму його опис в даній роботі нс наводиться. Якщо ключі генеруються на кожен сеанс надійною системою розподілу секрету, ефективних атак на даний алгоритм [2].

Шифр CMEA. Безпека зв'язку забезпечується також застосуванням процедур аутентифікації та шифрування повідомлень. У CDMA для генерації 128 біт ключа стільникового зв'язку використовується стандартний алгоритм аутентифікації і шифрування мови CAVE (Cellular Authentication Voice Encryption). Ключ називається SSD (Shared Secret Date «загальні секретні дані»). Ці дані генеруютьсяна основі *a*-ключа, який зберігається в мобільній станції, з отриманого від мережі псевдовипадкового числа. Загальні секретні дані (SSD) генерує алгоритм CAVE. Вони поділяються на дві частини: SSD-A (64 біта), призначену для вироблення цифрового підпису (authentication signature), і SSD-B (64 біта), призначену для генерації ключів, використовуваних для шифрування мови і передачі сигналу повідомлення. SSD може використовуватися постачальниками послуг для місцевої аутентифікації при роумінгу. Нові загальні секретні дані (SSD) можуть генеруватися при переміщенні мобільної станції до чужої мережі або з поверненні до домашньої мережі [2] .

Алгоритм Rolling code system. Цей шифр, названий також *KccLoq,* використовує лінійний рекуррентний регістр зсуву. Довжина основного регістру 32 біта, довжина додаткового регістра 5 біт. Шифрування проводиться побитним підсумовуванням *e* ключем. Для даного алгоритму існують ефективні атаки [3]. Наприклад, щоб отримати систему лінійних рівнянь, що дозволяє відновити початкове заповнення лінійного регістру, досить ноутом прослуховування ключової послідовності перехопити її 216 символів.

Алгоритм Crypto 1. Даний алгоритм використовує комбінацію лінійних і нелінійних рекурентних регістрів. Довжина ключа 48 біт.

Класифікація типів атак на радіоканал

До можливих ризиків при використанні мережевої інфраструктури стандарту 802.11 b відносяться атаки на конфіденційність інформації, цілісність і доступність мережевих ресурсів.

ISSN 2663 - 4023

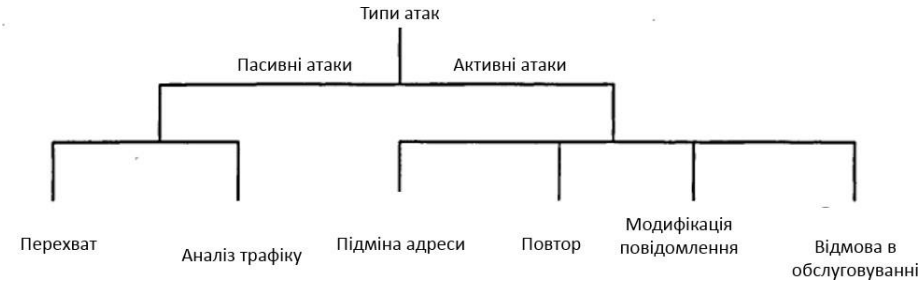

Рис. 1. Типи атак на безпровідну мережу стандарту 802.11

Як показано на Рис. 1, атаки, спрямовані на порушення безпеки безпровідної мережі діляться на активні і пасивні. Вони, в свою чергу, поділяються на кілька підкласів [4].

Пасивні атаки - до цього класу належать атаки, в ході яких неавторизована сторона просто отримує доступ до даних, не модифікуючи їх. Для системного адміністратора неможливо встановити факт пасивної атаки. Пасивними атаками вважається як перехоплення даних, так і застосування аналізатора трафіку.

Перехоплення - Атакуюча сторона переглядає зміст повідомлень, що передаються в мережі. Як приклад можна привести перехоплення повідомлень міждвома робочими станціями в мережі або між станцією і точкою доступу.

Аналіз трафіку - в даному випадку застосовується підхід з фільтрацією трафікуза певними критеріями. Проводиться накопичення статистики за повідомленнями, що містить заздалегідь відомі фрагменти.

Активні атаки - атаки, при яких неавторизована сторона виробляє модифікацію повідомлень. Можна виявити факт атаки даного класу, але не завжди можливо запобігти її. Активні атаки виіляються на чотири підкласу: підміна адреси, повтор,модифікація повідомлення і відмова в обслуговуванні.

Підміна адреси - шляхом підміни адреси атакуюча сторона може отримати всіабо частину привілеїв авторизованого користувача.

Повтор - атакуюча сторона перехоплює повідомлення і передає їх під виглядом авторизованого користувача

Модифікація повідомлення - проводиться модифікація повідомлення шляхом додавання, вилучення або модифікації даних.

Відмова в обслуговуванні - атакуюча сторона шляхом формування повідомлень певного виду унеможливлює нормальне використання або управління бездротовою мережею.

Аналіз стандартних засобів і методів захисту інформації в радіоканалі 802.11

Основою захисту даних, що передаються в безпровідних мережах, є протокол WEP. Як випливає з результатів досліджень протокол WEP не володіє достатньою стійкістю і має ряд структурних недоліків [5].

Одним з методів захисту інформації в мережі є приховування імені мережі або SSID. Однак, у багатьох рішеннях, запропонованих постачальниками безпровідного обладнання, зокрема в обладнанні фірми Lucent, присутній ряд уразливості всистемах, що забезпечують контроль доступу до мережі. Деякі керівні кадри містять ім'я мережі або SSID, причому ці повідомлення, що розсилаються якточками доступу, так і клієнтами, є широкомовними і не зашифровуються. Видкеруючого фрейму, що містить

ISSN 2663 - 4023

SSID, залежить від конкретного виробника. В результаті атакуюча сторона отримує інформацію про ім'я мережі, що в поєднанніз підібраним секретним ключем дає доступ до захищеної мережі. Цей недолік проявляється в не залежності від активації режиму шифрування з допомогоюпротоколу WEP, так як керуючі фрейми при цьому передаються відкритим текстом. Механізм захисту, заснований на застосуванні таблиці MAC-адрес для станцій, яким дозволений доступ, теоретично гарантує високу стійкість при використаннінадійної ідентифікації клієнта. Але на практиці так не відбувається, в результатітого, що MAC-адреса повинна передаватися у відкритому вигляді, навіть у разіактивації протоколу WEP. Всі сучасні мережеві карти стандарту 802.11 мають можливість програмної зміни MAC-адреси. Таким чином, при перехопленні адреси,якій дозволений доступ, можлива підміна значення MAC на станції атакуючої сторони і отримання доступу в захищену мережу.

Злом протоколу аутентифікації із загальним секретним ключем можна здійснити за допомогою пасивної атаки з перехопленням фреймів, що передаються в процесі взаємної аутентифікації [6]. Можливість атаки визначається недоліками, зазначеними в статичній структурі протоколу. Єдина відмінність між повідомленнями при аутентифікації полягає в вмісті перевірочного тексту.

Спочатку атакуюча сторона перехоплює другий і третій керуючий фрейм, що передаються в процесі аутентифікації. Другий фрейм містить перевірочний текст в незашифрованому вигляді, а третій той же текст, але вже зашифрований за допомогою загального секретного ключа. Таким чином, атакуючій стороні стає відомий незашифрований текст *P*, той же текст, але вже зашифрований З і значення IV, яке передається в незашифрованому вигляді. Далі можна обчислити псевдовипадкову послідовність WEPKIV, згенеровану із застосуванням секретного ключа *к* і значення вектора ініціалізації IV використовуючи формулу 1.

$$WEPKM=C®P \quad (1)$$

Розмір псевдовипадкової послідовності буде точно таким же, як і розмір кадру аутентифікації. При цьому всі елементи кадру заздалегідь відомі: номер алгоритму, номер послідовності, код стану, ідентифікатор елемента, довжина і контрольний текст.

Таким чином, атакуюча сторона має можливість успішноаутентифицироваться в захищеній мережі навіть при невідомому секретному ключі *К*. Атакуюча сторона надсилає запит до тієї точки доступу, до якої потрібно підключитися. Точка доступу відповідає керуючим фреймом, що містить перевірочний текст. Атакуюча сторона розраховує тіло фрейму аутентифікаціїшляхом обчислення *XOR* (виключає «або») від значень отриманого випадкового тексту *R* і послідовності WEP. Наступним кроком необхідно обчислити нове значення контролю цілісності (ICV). Для цього застосовується методика, докладноописана в розділі «Активна атака з метою підміни трафіку» [7]. Після цього станція стає авторизованою для захищеної мережі. Якщо в захищеній мережі застосовується протокол WEP, то атакуючій стороні не вдасться обмінюватися інформацією з іншими станціями без застосування спеціальних засобів.

Основні проблеми, пов'язані з безпекою безпровідних мереж стандарту 802.1 lb:

1. Засоби безпеки, вбудовані виробником обладнання, дуже часто не використовуються. Незважаючи на недоліки механізмів безпеки, реалізованих різними виробниками у своїх продуктах, їх використання знижує ймовірність виникнення проблем з безпекою даних [8].
2. Діапазон значень IV малий або використовується статичний IV. З огляду на те,

що IV - 24 бітне число, можлива атака, заснована на дешифрування повідомлень, зашифрованих за допомогою одних і тих же значень ключового потоку (*key stream*).

3. Довжина криптографічного ключа мала довжина ключа в 40 біт не адекватнадля захищених систем. В даний час рекомендована довжина не менше 80 біт. Велика довжина ключа ускладнює атаку методом перебору.

4. Використання загального криптографічного ключа використання загального ключа може призвести до проблем в області захисту інформації. Безпека мережі залежить від збереження секретного ключа, який має бути відомий кожній станції.

5. Криптографічний ключ не може бути змінений автоматично і з потрібною частотою Криптографічний ключ необхідно часто змінювати для попередження можливих атак методом перебору.

6. Слабкість алгоритму RC4 внаслідок особливостей його застосування в алгоритмі WEP Так як значення IV є частиною ключового потоку для алгоритму RC4 і передається у відкритому вигляді, може бути зроблена атака з метою отримання криптографічного ключа. Даний недолік алгоритму RC4 непроявляється у випадках, відмінних від WEP, так як не відкривається частина ключового потоку і не проводиться перезапуск алгоритму для кожного пакету даних.

7. Алгоритм захисту цілісності має недоліки. Алгоритми лінійної блочної структури, подібні CRC32 не можуть забезпечити надійний захист цілісності для застосування в криптографії. Можлива зміна вмісту пакета. Лінійні алгоритми схильні до атаки, спрямованої на підміну вмісту пакету. Використання в процесі підготовки пакету некриптографічних алгоритмів часто полегшує можливі атаки назашифровану інформацію.

8. Недоліки в системі аутентифікації на основі списку MAC адрес При використанні аутентифікації на основі списку MAC - адрес вкрадений пристрій може безперешкодно увійти в мережу, так як не здійснюється перевірка користувача.

9. Проблеми при використанні аутентифікації на основі ідентифікатора SSID при аутентифікації на основі ідентифікатора мережі можливе перехоплення пакетів з подальшим отриманням значення SSID.

10. Недоліки аутентифікації влаштування на основі загального криптографічного ключа Одностороння аутентифікація на основі запиту-відповіді із застосуванням загального криптографічного ключа вразлива до атаки, так як може бути здійснено перехоплення і аналіз переданих даних. Потрібна додаткова аутентифікація користувача для визначення його прав на доступ в мережу.

Дослідження методів захисту інформації протоколуWEP

В зв'язку з зростанням і розвитком індустрії безпровідного доступу постало питання про надійність передачі і ступеня захищеності радіомережі [9]. Припересиланні даних по радіохвилях вони можуть бути легко перехоплені і змінені. Таким чином, необхідний механізм безпеки для забезпечення захисту інформації врадіоканалах.

Зазвичай в мережах стандарту 802.11 відбувається взаємодія між клієнтською станцією і точкою доступу (AP - Access Point), використовуючи радіохвилі. Якщо перешкод (стін, штучні або природні перешкоди) між AP і клієнтської станцією не екранують радіосигнал, то пряма видимість не потрібна. Поряд зі специфікаціями з передачі даних стандарт визначає протокол WEP (*Wired Equivalent Privacy*), що слугує механізмом захисту даних при передачі по радіоканалу від перехоплення. Захист інформації здійснюється за допомогою зовнішнього сервісу управління ключами,

створеними для процесів шифрування і розшифровки повідомлень, що передаються по мережі. Основні властивості алгоритму WEP визначаються в [10].

Стандартна система аутентифікації має недоліки, основні з них наведені нижче:

1. Необхідність доставки загального секретного ключа WEP, неможливість частої зміни ключа;
2. Підміна MAC адреси;
3. Перехоплення пакетів з подальшим отриманням значення SSID;
4. Одностороння аутентифікація на основі запиту-відповіді із застосуванням загального криптографічного ключа.

Система аутентифікації радіоканалу стандарту 802.11 b побудована на основі стандарту IEEE 802.їх. 802.їх визначає, як використовувати розширений протокол аутентифікації (*Extensible Authentication Protocol - EAP*) [11].

Серед EAP методів розроблених спеціально для безпровідних мереж варто особливо виділити сімейство, засноване на стійких паролях.

Алгоритм SPEKE був розроблений з метою подолати проблеми, пов'язані з низьким ступенем безпеки і високою складністю в реалізації властиві методів аутентифікації, заснованим на сертифікатах. Дослідження призвели до розробки нового сімейства алгоритмів аутентифікації на основі паролів, причому були усунені недоліки, присутні в традиційних алгоритмах, що використовують паролі. Тоді ж був введений термін "стійкий пароль", що показує приналежність алгоритму до даного сімейства. Головна перевага алгоритмів на основі стійких паролів в тому, що обидві сторони можуть довести один одному, що вони знають секретний пароль, при цьому не викриваючи його при третьої сторони, яка може перехоплювати повідомлення. Алгоритми на основі стійких паролів дозволяють зробити захищену аутентифікацію із застосуванням коротких, легко запам'ятовуються паролів. Основою таких алгоритмів є метод обміну Діффі-Хелмана (Diffie-Hellman) [12]. Метод Діффі-Хелмана дозволяє двом сторонам створювати ключ шифрування, причому третя сторона, яка може мати можливість перехоплювати повідомлення, не зможе отримати цей ключ.

Безпека методів, застосованих у криптографічних алгоритмах системи аутентифікації, базується на припущенні, що зведення в ступінь є односторонньою функцією, основною небезпекою є можливість для атакуючої сторони обчислити дискретний логарифм від результату. Всі відомі методи обчислення дискретного логарифма вимагають великих обсягів передобчислень для кожного конкретного значення модуля.

Алгоритми SPEKE і DH-EKE володіють нижче перерахованими характеристиками:

1. Запобігають можливість відкладеної (*off-line*) атаки по словнику пароль
2. Протистоять атаці за словником в реальному часі
3. Забезпечують можливість взаємної аутентифікації
4. Мають вбудовану систему обміну ключів
5. Немає необхідності в довготривалих (*persistent recorded secret data*) секретних або специфічних (*sensitive host-specific data*) даних.

Можливість здійснення атаки по словнику в реальному часі (*On-line dictionary attacks*) може бути легко виявлено і попереджено, наприклад простим підрахунком кількості невдалих входів в систему. Але проблема відкладеної атаки за словникомна пароль становить велику небезпеку. Атакуюча сторона може маскуватися під другого учасника аутентифікації, або перехоплювати повідомлення, якими обидві сторони обмінюються при взаємної аутентифікації. Витік будь-якої, навіть незначної частини інформації при обміні може призвести до успішної атаки. Алгоритм повинен бути

ISSN 2663 - 4023

стійкий до атак такого типу, навіть при застосуванніпаролів невеликої довжини.

Взаємна аутентифікація бажана для того, щоб кожна з двох сторін була впевнена, що інша знає пароль.

У той же час, використовуючи пароль генерується ключ сесії для забезпечення безпеки обміну даними між двома сторонами. Необхідність у вбудованій системі обміну ключів при аутентифікації детально обговорюється в [13]. Основна ідея полягає в тому, що, розділяючи кроки аутентифікації і обміну ключами, створює можливість третій стороні здійснити атаку, перехоплюючи повідомлення. Захищений обмін ключами вимагає спільної участі обох сторін, і повинен бути невід'ємною частиною процесу.

Відсутність потреби у зберіганні довготривалих секретних даних означає, що користувачеві не потрібні додаткові симетричні, відкриті або приватні ключі. Існуєбезліч способів для створення захищеного каналу, через який може бути переданийу відкритому або хешированном вигляді пароль. Методи, засновані на паролі (*password-only method*) дозволяють використовувати пароль як незалежний фактор і спростити налаштовувану частина системи. З одного боку довготривалі дані необхідно згенерувати, поширити і захистити при зберіганні, що створює додатковіпроблеми. З іншого боку секретні дані не повинні бути розкриті, зашифровані дані треба оберігати від несанкціонованого втручання. Отже, потрібне застосування спеціальних захищених областей пам'яті, що погіршує систему безпеки і створює додаткові можливості для порушення захисту. Системи, в яких безпека пароля залежить від збереженого ключа набагато простіше при розробці, але вони лише переміщують основу безпеки з пароля на ключ. Якщо ключ викрадений, пароль може бути скомпрометований. Відмова від власних ключів позбавляє від цієї проблеми, також зникає необхідність використовувати захищене сховище.

Алгоритми SPEKE і DH-EKE володіють всіма вищепереліченими перевагами і мають інші бажані характеристики, які будуть розглянуті нижче.

Розробка моделі

Поряд з багатьма перевагами в алгоритмі WEP є недоліки в області безпеки [4, 5, 14]. У WEP використовується поширений симетричний алгоритм генерації псевдовипадкових чисел RC4 PRNG (*Ron's Code 4 Pseudo Random Number Generator*) [15]. Однак реалізація містить ряд недоробок в області безпеки. Дані недоліки дозволяють здійснювати ряд як активних, так і пасивних атак по перехопленню і підміні повідомлень, що передаються по бездротових мережах [16].

У протоколі реалізований класичний 40 бітний ключ і 24 бітний IV, проте конкретними виробниками зазвичай розробляються розширені версії, що підтримують велику довжину ключа. Чим коротше довжина ключа, тим більше вінє схильним атаці шляхом перебору комбінацій (*brute-force attack*), що цілком під силу більшості сучасних комп'ютерів. При збільшенні розрядності секретного ключа, приміром, до 128 біт, перебір стає неможливим навіть для спеціальних обчислювальних систем. Однак залишаються можливості для атак, що невикористовують метод перебору і зводять нанівець всі переваги довгого ключа [17].

В результаті за відносно невеликий проміжок часу можливе перехоплення двох пакетів даних, які зашифровані однією і тією ж ключовою послідовністю. Далі можливий статистичний аналіз для відновлення вихідного незашифрованого тесту,що міститься в одному повідомленні. У випадку вдалого підбору, провівши операцію «*виключне АБО*» (XOR) над зашифрованим повідомленням і розпізнанимтекстом зловмисник відновлює

ISSN 2663 - 4023

відповідну ключову послідовність, що дозволяє йому переглядати всі інші зашифровані повідомлення, зашифровані з допомогою даного IV:

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

Навіть якщо не вдасться розпізнати звістку контекст повідомлення, про нього можна здогадатися, використовуючи передбачувану структуру і надмірність IP трафіку.

Іншими словами застосування операції XOR над двома такимизашифрованими повідомленнями дозволяє виключити вплив ключової полідовності і аналізувати різницю незашифрованих даних, що даєнабагато більше шансів у розкритті вмісту пакетів методом статистичного аналізу. Якщо зловмисник зміг зіставити вихідний і зашифрований текст, то він, очевидно, зможе згенерувати ключову послідовність. Володіючи цими відомостямине складно організувати передачу зашифрованого трафіку на станцію жертви, причому приймач повідомлень пізнає приходять пакети як коректні.

Дана атака може проводитися і іншим способом. Навіть якщо зловмисник недосяг повної розшифровки вмісту пакета, він може довільно змінювати значення бітів у повідомленні, потім додавати обчислене значення контролю цілісності ICV для отримання коректної версії модифікованого пакета. Операція XOR має властивість дистрибутивності: $c(x \oplus y) = C(x) \oplus c(y)$ для будь-яких x і y. Розглянемоситуацію, в якій проведено перехоплення пакету з даними, де зашифровані дані.

При цьому можливе створення такого зашифрованого повідомлення яке відповідає p. Далі з'являється можливість підміни пакету з даними:

$$(A)\text{->}B: (IV \parallel C)$$

Рис. 2. Схема аутентифікації стандарту

ISSN 2663 - 4023

В цьому випадку станція в отримає змінений пакет даних p' з коректним значенням контролю цілісності.

Можлива ситуація, в якій зловмисник, перехоплюючи трафік в мережі, має уявлення тільки про заголовку кадру, а не про вміст повідомлення. Наприклад, або заздалегідь відомий або обчислений IP адреса жертви. Маючи цю інформацію, зловмисник може замінити відповідні біти пакету' для підміни IP адреси на адресу станції знаходиться під його контролем, за умови, що мережа, на яку ведеться атака,підключена до мережі Інтернет. Далі пакет потрапляє на точку доступу, що з'єднує бездротову мережу з Інтернет, розшифровується, і у відкритому вигляді пересилається на комп'ютер зломщика [17]. При цьому модифікований пакет переміщається з бездротової мережі в Інтернет, отже, він не буде затриманий більшістю стандартних мережевих екранів.

Для здійснення даної атаки недостатньо просто замінити IP адресу одержувача пакету, необхідно щоб контрольна сума зміненого пакету була коректною. Припустимо, що *DL* і *DH* - це дві 16-бітні частини вихідного IP адреси одержувача, їх необхідно замінити на '*L* і *D H*. Позначимо значення старої контрольної суми як *S*, причому її значення не обов'язково може бути відомо. Тоді нове значення обчислюється за формулою:

$$S' = S + DL + DH\text{-}D\ L\text{-}D\ H$$

Якщо значення *S* заздалегідь відомо, то нескладно обчислити значення *S'* і модифікувати пакет операцією XOR зі значенням $S \oplus S'$. Якщо S заздалегідь не відомо, то завдання набагато складніше. Відомо значення $E = S'\text{-}S$, необхіднообчислити $\Delta = S \oplus S'$. При використанні методів статистичний аналіз і володіючи певною структурою повідомлення, велика ймовірність підбору потрібного значення.

Відносно мала кількість можливих значень IV дозволяють атакуючій стороні побудувати таблицю розшифровки. При вдалій спробі розшифровки вмісту будь- якого пакету даних стає можливим відновити-ключову послідовність, - згенеровану при поточному IV. Ця ключова послідовність потім може бути використана для розшифровки всіх інших пакетів, які використовують те ж саме значення IV. При досить добре відпрацьованої технології статистичного аналізу зловмисник може побудувати таблицю відповідності IV векторів і відповідних їм ключових послідовність. Така таблиця буде містити близько 2 (більше 16 мільйонів) записів, що складе обсяг близько 24 Гб. Користуючись цією таблицею, зловмисник зможе розшифрувати будь-який пакет без зусиль, досить з'ясувати тільки значення ключової послідовності по його IV.

За повідомленнями аналітиків на сьогоднішній день лише в 40% безпровідних мереж стандарту 802.11 активований протокол WEP [18, 19, 20]. Це призводить до втрати конфіденційності переданої інформації і робить можливим здійснення атак на мережеву інфраструктуру. Для протидії необхідно використання протоколу WEPі якомога частіше міняти секретний ключ. При конфігуруванні необхідновстановлювати довгі, - стійкі до підбору ідентифікатори SSID.

Застосування фільтрації MAC адрес або використання WLAN дозволить заборонити доступ неавторизованим бездротових карт. Необхідно обов'язково закрити доступ до інтерфейсу конфігурування точок доступу в бездротовій мережі.Використання програми антивіруса і мережевого екрану усуне можливість появи на клієнтських машинах сторонніх програм-шпигунів і перехоплювачів.

ISSN 2663 - 4023

Об'єднуючи захист за допомогою брандмауера і технології IPsec, SSH або SSL можливо з високою часткою ймовірності виключити можливість перехоплення інформації і запобігти доступ для невпізнаних клієнтів [17].

Основні зусилля додаються в області розмежування функцій шифрування і аутентифікації для того, щоб не було необхідності у спільному використанні секретного ключа на всіх станціях бездротової мережі. Був прийнятий чорновий варіант стандарту попередньо названий *Enhanced Security Network (ESN)*, в якій передбачений посилений варіант захищеної аутентифікації і система управління 128-бітними ключами. У системі шифрування ESN буде замінено алгоритм генерації псевдовипадкових чисел RC4 PRNG на сучасний стандарт *AdvancedEncryption Standard* (AES). З прийняттям нової версії WEP2 рівень безпеки безпровідних мереж може досягти рівня безпеки їх проводових аналогів.

Розробка засобів захисту від атак на системуаутентифікації, заснованої на алгоритмі SPEKE

В роботі обговорюються проблеми обчислення дискретного логарифма, і обговорюється вибір параметрів для основної DH аутентифікації, особливо із застосуванням коротких значень експоненти. Таблиця 1 - скорочена зведенатаблиця, присвячена методам захисту для обох алгоритмів.

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

- Обчислення дискретного логарифма
- Витік інформації
- Обмеження по невеликих підгрупах

В атаці "обчислення дискретного логарифма" проводиться зворотне перетворення від зведення в ступінь по модулю *m*, з метою відновити показник ступеня, і, в кінцевому рахунку, пароль *S*. Труднощі цих обчислень залежать від розміру і властивостей числа *m*. Стійкість алгоритму до даної атаки грунтується на практичній неможливості подібного обчислення [21].

Необхідно відзначити, що перехоплення значень експоненти, можливо зашифрованої, не призводить до витоку інформації про пароль *S*. Витік навіть одного біта інформації про пароль може бути критичнм, у разі якщо застосовується атака з підбором по словнику, дозволяє розділити можливі паролі на дві групи: відповідні і свідомо неправильні [22]. Такий тип атак - «розподілена атака» (*partition attack*) може зменшити словник великого розміру до кількох значень за відносно малу кількість проходів.

Нарешті, атакуюча сторона, яка знає структуру *Zm*, може бути здатна обмежити область можливих значень *K* до розміру невеликий підгрупи, яка дозволяє здогадатися про значення або застосувати атаки перебором. При аналізахбезпеки алгоритму *Діффі-Хелмана (Diffie-Hellman)* передбачається, що K завжди розташоване з рівномірною ймовірністю в *Zm*. Це припущення є невірним, так як, починаючи з першого зведення *g* в ступінь, що є випадковим числом, відбувається потрапляння результатів в меншу підгрупу, принаймні, в половині випадків. На цій закономірності грунтується атака "обмеження по невеликих підгрупах".

Таблиця 1

Методи захисту для обох алгоритмів

Метод захисту	Відвернена атака	SPEKE	DH-KE
Модуль *m* повинен бути великим числом	Обчислення дискретного логарифма	+	+
Перевірка на Q_x ! = 0, у разі не зашифрованих значень	Форсування значення *K* = 0	+	+
Значення *m* -1 повинно мативеликий просто множник *q*.	Обчислення логарифма за методом Полінгу-Хелмана	+	+
Шифрування Q_x, розбитого начастини і зібраного у випадковому порядку	Витік інформації ззначення $E_s(Q_x)$		+
База *g* повинна бути першоподібним коренем від *m*.	Розподілена атака на Es(Q_x)		+
База повинна бути генератором для *q*	Розподілена атака Q_x	+	
База у вигляді S_x *mod p*	Атака типу «пароль векспоненті»		
Необхідно шифрувати *Qx* приперевірці *K*	Підбір пароля використовуючи Q_x, R_xсловник паролей		+
Використання одностороннього хешуваннязначення *K*	Атака на обмеженнязначень	+	+
Перший біт *m* повинендорівнювати 1	Розподілена атака на$E_к(Q_x)$		+
Шифрування значень Q_a,Q_b	Обмеження по підгрупамдля *K*		+
Переривання роботи, якщо *K*малого порядку	Обмеження по підгрупамдля *K*	+	

Атака через обчислення дискретного логарифма

Безпека методів, застосованих в алгоритмах, базується на припущенні, що зведення в ступінь є односторонньою функцією, основною небезпекою є можливість атакуючої сторони обчислити дискретний логарифм від результату. Всівідомі методи обчислення дискретного логарифма вимагають великих обсягів передобчислень для кожного конкретного значення модуля [23].

Розмірність модуля - основа захисту. На сьогоднішній день не відомі методи обчислення дискретного логарифма розмірністю більшої близько сотні біт, проте цілком ймовірно, що в недалекому майбутньому можливі успішні атаки на модулі розміром в 512 біт. Десь у діапазоні від 512 до 1024 біт знаходиться ідеальний розмір модуля, збалансований за вимогами безпеки і швидкості обчислень, для конкретних додатків.

Більше того, потрібно правильно підібрати модуль *m* з метою запобігти можливість швидкого обчислення дискретного логарифма. Якщо *m*-1 має великий простий множник *q*, то він може протистояти атаці на обчислення дискретного логарифма Поліга-Хелмана

ISSN 2663 - 4023

(Pohlig-Hellman). Використання безпечних простихчисел у вигляді $m = 2q+1$, є одним із способів подолати цю вразливість.

Передбачається, що необхідні передобчислення дискретного логарифма виконані для певного модуля, в атаці на основі' підбору пароля необхідно розрахувати конкретний логарифм для кожного запису в словнику паролів, поки небуде знайдено правильне значення. Будь-яка сесія, що використовує модулі євразливою для атаки з логарифмування. Таким чином, необхідно дотримуватися ситуацію робить проблему обчислення дискретного логарифмування як можна більш важкою [24]. В цьому разі здійсненність преобчислювань є першорядною проблемою.

Розподілена атака

У методі Діффі-Хелмана використовується група Z_m, де m - велике ціле число, причому m-1 має великий простий множник q. При цьому g є первісним коренем від m. На практиці g має бути простим для того, щоб запобігти атаці. Третя сторона може здійснити пробне дешифрування $E_s(gRx \bmod m)$ використовуючи словник паролів S_i. E_s - симетрична функція шифрування, що використовує ключ Si. Якщо gне просте число, не вірне Si підтвердитися простим результатом. В загальному випадку для запобігання атаки на *DH-EKE* зашифроване значення Qx не повинно містити передбачуваної структури. Умова, що g є простим числом, дозволяє домогтися рівномірного розподілу значень всередині Z_m.

Також необхідно звернути увагу на можливі недоліки методу шифрування як такого, зокрема необхідно заповнювати порожні повідомлення випадковим текстом, що відноситься до обмежень, що накладається на функцію E_s. З урахуванням всього цього інші рекомендовані обмеження для *DH-EKE*:

- m повинна бути виду m -1
- розбиття на блоки при шифруванні Es у випадковому порядку

Для алгоритму SPEKE не потрібно цих обмежень, так як в ньому не використовується симетричне шифрування.

У алгоритмі SPEKE не потрібне використання простої основи. Якщо основа $f(S)$ - випадковий член групи Z_m, сторона, що перехоплює значення може їх перевірити на належність до малих підгрупах. Якщо результат є першоподібним коренем від т, значить база так само просте число. Для безпечних цілих m це означаєрозкриття 1 біта інформації про пароль S. Якщо значення m буде змінюватися, як рекомендовано для підвищення безпеки, атакуюча сторона може отримати нову інформацію, що дозволить зменшити розмір словника для пошуку S_j [25].

У разі якщо для будь-якого значення S, підстава $f(S)$ є генератором великої підгрупи, то для атакуючої сторони неможливо отримати потрібну інформацію з результату. У подальших міркуваннях ми будемо припускати використання в якості базису великого простого числа [26].

Так як в алгоритмі SPEKE не шифруються значення Qx, формальний аналіз набагато спрощується в порівнянні з *DH-EKE*.

Атака з відомим ключем сесії

У роботі розглянута атака, при якій викрадений ключ сесії K використовується для проведення атаки на пароль за словником. Стійкість до цієї атаки близько пов'язана з поняттям повної прямої безпеки, завдяки якій відбувається ізоляція одного типу

ISSN 2663 - 4023

секретних даних від атак на інші [27].

В алгоритмі DH-EKE, відоме значення R_a в доповненні до відомого K дозволяє здійснити атаку по словнику з метою відкрити пароль S. Для кожного пробного пароля S_i, атакуюча сторона обчислює:

$$K' = (Esi^{-1}(Es(g^R b)))^R a$$

При цьому якщо $K' = K$, то відповідно S_i дорівнює S. Алгоритм SPEKE так само схильний цій атаці, при якій за допомогою R_a обчислюється S. У зв'язку з цимнеобхідно негайно знищувати тимчасові змінні шифрування, такі як R_a і R_b.

Атака на стадії перевірки

На стадії перевірки в протоколах DH-EKE і SPEKE обидві сторони доводять один одному, що їм відомо значення загального ключа K. Через те, що K є великим криптографічним числом, друга стадія вважається захищеною до атаки методом перебору (*brute-force attack*), таким чином, перевірка значення K може бути виконана традиційними метод.

Виявлення атак в реальному масштабі часу

Небезпека повторюваних в реальному масштабі часу спроб підібрати пароль може бути зменшена за умови ведення історії та підрахунку невдалих спроб підключення. Необхідно обмежити кількість невірних спроб доступу до облікових записів, вимагаючи зміни пароля, при досягненні певного порогу. Поріг повинен бути заснований виходячи з довжини пароля. Так само необхідно зберігати кількість невдалих спроб підібрати пароль як при атаці на окремий обліковий запис,так і при спробі масової атаки, при якій не досягається порогу для будь-кого з користувачів.

Часто виникає бажання пробувати відокремлювати випадкові помилки від спроб проникнення, припускаючи, що більшість помилок супроводжуються успішним входом [28]. Проте атакуюча сторона може передбачити або спробуватизатримати легітимний доступ і зробити кілька пробних спроб на цей обліковий запис до успішного входу в систему користувача. Таким чином, навіть здаються очевидними помилки повинні бути ретельно досліджені обома сторонами.

Необхідно зберігати записи невдалих спроб з'єднання, як на хост-системі, такі на користувача системи. Настроювана система повинна зберігати як мінімум список останніх невдалих спроб і передавати цю інформацію по захищеному каналуна хост-систему кожний раз, коли здійснюється успішний вхід. Хост-система так само може повідомляти користувача про кількість невдалих спроб доступу з його боку. Цей метод серйозно знижує ймовірність атаки спрямованої на підбір пароля по відношенню до обох сторін.

Методи збільшення швидкодії алгоритмів

Використання короткого модуля

Для збільшення швидкості операції зведення в ступінь, розмірність модуля може бути зменшена. Але так як великий розмір модуля є умовою безпеки алгоритму Діффі-Хелмана, необхідно проявити обережність при виборі оптимальної розмірності. При зменшенні розмірності модуля, наприклад до 600 біт, можливість дискретного логарифмічного перетворення зростає багаторазово [29].

ISSN 2663 - 4023

Для синхронізації розмірності модуля для обох сторін, передбачається, що одна зі сторін вибирає цей параметр для іншої. Таким чином, постає питання в безпеці даного підходу. Третя сторона зможе, варіюючи даний параметр отримати додаткову інформацію про паролі.

Використання несертифікованих змінюваних параметрів

Наступне питання, що стосується безпеки пов'язане з необхідністю використання змінюваних параметрів. Припустимо, що одна зі сторін вибирає m і g з заздалегідь сформованого списку і пересилає їх іншій стороні перед операцією обміну. Так як в даному алгоритмі не використовується відкритий ключ, дані параметри є сертифікованими.

Найбільш простим рішенням даної проблеми є вбудовування фіксованих безпечних параметрів в систему, де модуль є досить великим, щоб запобігти атаці, пов'язану з обчисленням дискретного алгоритму. На даний момент довжини в 1000 або 2000 біт достатньо для забезпечення довгострокового захисту [30]. У поєднанні з використанням короткого значення в експоненті робить рішення відповідним для більшості ситуацій.

У роботі [31] особливо звертається увага на наступні обмеження:

– модуль m повинен бути великим простим числом, інакше можливеприскорене обчислення дискретного логарифма;

– q має бути простим числом, так як при безпечному значенні m можливо прискорене обчислення дискретного логарифма.

Використання короткого значення в експоненті

Менш радикальним підходом до проблеми збільшення швидкодії полягає в зменшенні значення експоненти до достатнього для забезпечення прийнятного рівня безпеки розміру. Кількість біт в експоненті (Q_a, Q_b) має бути, як мінімум вдвічі більше ніж кількість біт (t), необхідного для K, зазвичай це менше, ніж кількість біт в m.

Можна використовувати два безпечних підходи, коли експонента може бути зменшена до розміру в $2t$ біт:

1. Використовуючи велике безпечне значення модуля m з вихідним базисом 2.
2. Використовуючи великий простий модуль m з великим простим базисом порядку q, де q має розмірність як мінімум в $2t$ біт.

Перший підхід застосуємо як до DH-EKE, так і до SPEKE, однак DH-EKE потребує додаткового захисту від атаки пов'язаної з обмеженням значень у невеликих підгрупах. Використання базису $g = 2$ дозволяє значно збільшити швидкість роботи алгоритму. Застосовуючи $g = 2$ необхідно відзначити, що. для цихпротоколів використовуються різні безпечні прості числа. Безпечне просте число p в алгоритмі DH-EKE повинно мати первісний корінь 2, тоді як безпечне просте, підходяще для SPEKE має в ідеалі дорівнювати 2 в ступені q. Використання великих простих підгруп, де $q << m$ дозволяє прискорити розрахунок DH параметрів. Це застосовується для SPEKE, але не може бути використано в DH-EKE, так як для цього алгоритму потрібна проста база.

Розробка вдосконаленої системи безпеки, для радіоканалу стандарту 802.11

Розглянемо механізм роботи системи безпеки. У структурі мережевої моделі OSI

протокол 802.11b займає найнижчий (фізичний) рівень та частина вищерозміщеного канального рівня - підрівень управління доступом до середовища (MAC). У додатку стандарт визначає використання протоколу 802.2 для управління логічним каналом (LLC).

Слабкі сторони системи безпеки протоколу 802.11b викликані як чисто фізичними факторами, так і особливостями реалізації. Основними недоліками є [32]:

- Можливість перехоплення пакета з інформацією;
- Недостатньо надійна система аутентифікації;
- Недоліки, пов'язані з шифруванням.

Можливість перехоплення пакета з інформацією.

Проблема проявляється у зв'язку з тим, що дані передаються по радіоканалу. Будь-яка станція, що знаходиться в зоні прийому сигналу, може здійснити збір інформаційних пакетів. Якщо при цьому не використовувалося шифрування, то дані можна досить тривіально витягти з окремих пакетів і - використовувати, залежно від подальших намірів перехоплює сторони не вдаючись до застосування спеціальних засобів. Для такого роду завдань досить встановити простий мережевий монітор, який дозволяє переглядати вміст пакетів і виробляє їх фільтрацію за певними ознаками, наприклад IP адресою. Ситуація ще більше погіршується тим, що не представляється можливим встановити, прослуховується в даний момент радіоканал чи ні. Таким чином, перехоплення може відбуватися абсолютно непомітно для системних адміністраторів мережі.

Недостатньо надійна система аутентифікації.

Протокол WEP визначає використання секретного ключа, який повинен бути заздалегідь відомий всім станціям мережі, інакше кажучи, наявність ключа біля станції означає, що вона пройшла процес аутентифікації. Проте, сам протокол WEP не регламентує як спосіб передачі секретний ключа, так і з якою частотою даний ключ необхідно міняти. Це призвело до того, що багато виробників обладнання не реалізують механізми по доставці ключа, змушуючи тим самим користувачів самостійно конфігурувати пристрої і вручну переносити значення ключа на всі стації мережі. Це призводить до того, що секретний ключ змінюється рідко або можливо взагалі не змінюється досить тривалий час.

Ідентифікатор *SSID (Service Set Identifier)* дозволяє ділити безпровідну мережу класу *Basic Service Set (BSS)* на логічні сегменти, будучи свого роду ідентифікатором підмережі [33]. З допомогою SSID відбувається обмеження доступу для будь-якого клієнтського пристрою, який не володіє необхідним SSID. Однак найчастіше AP (точка доступу) виробляє широкомовну розсилку ідентифікатора SSID своєї підмережі. Навіть у разі відключення функції розсилки SSID, зловмисник може отримати значення SSID, аналізуючи трафік між станціямимережі.

Крім того, можна заборонити доступ на основі фільтрації MAC-адрес. Але не дивлячись на те, що всі стандартні мережні карти повинні мати унікальний MAC адресу існує програмне забезпечення або часто є апаратна можливість по заміні MAC адреси в мережевому інтерфейсі.

Недоліки, пов'язані з шифруванням.

WEP є протоколом шифрування інформації, його специфікації описані в стандарті IEEE 802.11. Цей стандарт і протокол WEP розташовані на нижчих рівнях (фізичному і канальному) моделі OSI [34], це означає, що вони незалежні і прозорі для протоколів високого рівня, таких як TCP/IP.

У реалізації тієї, яка передбачена стандартом 802.11, протокол WEP має кілька слабких місць в архітектурі, які дозволяють розшифрувати дані зловмиснику [3]. У WEP використовується алгоритм шифрування RC4 в поєднанні з 64 або 128 бітнимключем, що складається з секретного ключа і значення вектора ініціалізації IV. Причина, по якій можливий злом WEP в загальному випадку не в недоліках RC4 яктакого і навіть не в довжині ключа, а скоріше в невдалій реалізації самого алгоритму.Система безпеки стандарту IEEE 802.11 потребує серйозного поліпшення. Для цього необхідно застосувати комплексний підхід до даної проблеми.

У найпростіших випадках достатньо застосування NAT маршрутизатора для з'єднань з публічними мережами, але для побудови дійсно захищеної мережі цього недостатньо. В даному списку наведені основні сфери є основою стратегії безпеки безпровідних мереж [35]:

- фільтрація вхідного і вихідного трафіку за допомогою міжмережевого екрану;
- шифрування з'єднань для віддаленого доступу;
- подвійна аутентифікація для віддаленого доступу;
- багаторівневі зони безпеки для публічно доступних ресурсів;
- засоби виявлення спроб несанкціонованого доступу.

Розглянемо систему безпеки протоколу 802.11 з точки зору даної стратегії. Важливим фактором є те, що всі поліпшення, внесені в систему безпеки, не порушують внутрішню структуру, описану в стандарті, вони лише доповнюють і покращують її. Це дозволяє добитися повної сумісності з існуючими на ринку компонентами і технологіями від різних виробників. Модульний підхід заснованийна застосуванні стандартних, добре зарекомендували себе алгоритмах і залишають можливість використовувати нові технології без необхідності зміни існуючої структури. Дана система безпеки безпровідної мережі дуже добре вписується в рамки вже існуючої політики безпеки мережі.

Тепер більшість даних, що містяться в пакеті WEP, є вже зашифрованими з допомогою IPSec, що не дозволяє використовувати атаку, засновану на зіставленні заздалегідь відомого повідомлення його зашифрованому аналогу. Слід, однак, звернути увагу, що при даному підході заголовок LLC і заголовок IPSec зашифровані тільки засобами WAP, що може трохи знизити криптографічну стійкість моделі безпеки.

У зв'язку з тим, що основні дані захищені за допомогою алгоритмів IPSec (DEC3) і WEP (RC4), інформація, яку можна отримати, використовуючи відкриті значення SSID, IV and Key ID не принесе відчутної користі стороні здійснює перехоплення. Значенням FCS є контрольне значення CRC від MAC пакета, що використовується для контролю цілісності даних, після того як вони були передані. Найбільшу небезпеку з точки зору безпеки являє незашифрована передача значення MAC адреси джерела, який може бути підмінений атакуючою стороною.

Тому аутентифікацію по MAC адресу слід сприймати лише як додатковий спосіб захисту від вторгнення [36].

У запропонованій моделі безпеки аутентифікації піддаються як користувач, так і сам пристрій. Пристрій автентифікується за допомогою значення ключа WEP.При цьому

ключ повинен змінюватися досить часто і поширюватися через захищений канал. Перед тим, як пристрою будуть видані права на обмін даними через міжмережевий екран, користувач повинен пройти процедуру реєстрації в центральній базі даних управління користувачами мережі, в якій зберігаютьсяоблікові записи та політики безпеки.

Міжмережевий екран не тільки запобігає несанкціонований доступ в мережу, але і блокує широкомовні розсилки, які можуть містити дані про внутрішню структуру мережі. Зашифрований пакет IPSec в тунельному режимі не містить додаткової інформації про структуру, доступною зовнішнього перехоплення, так яквона шифрує, а потім замінює заголовок IP пакету, який містить IP адреса пункту призначення, на власний заголовок в якому вказаний IP адреса кінцевої точки - міжмережевого екрану.

В першу чергу для успішного застосування розробленої системи, при необхідності в посиленні безпеки вже наявної безпровідної мережі стандарту 802.11b або планується розгортання нової мережі, необхідно впевнитись, що протокол WEP налаштований належним чином і функціонує. Довжину ключа рекомендується встановити в 104 біт.

Наступним кроком необхідно вибрати спосіб розподілу секретного ключа. Одним з можливих рішень є застосування захищених за допомогою SSL каналів зазаздалегідь заданим розкладом. У разі непридатності даного підходу в кожному конкретному випадку може бути обраний альтернативний підхід. Найкращий метод з точки зору безпеки - призначити системного адміністратора, відповідального за зміну секретних ключів на всіх пристроях, але це може призвести до того, що ключібудуть змінюватися недостатньо часто. Деякі виробники включають власні методирозподілу ключа в свою продукцію, але так як стандарт IEEE 802.11 не визначає, як саме це повинно бути зроблено, всі подібні рішення є не стандартизованими.

Далі необхідно вирішити, який міжмережевий екран найкращим чином підходить для вирішення завдань щодо забезпечення безпеки мережі.

Екран є критичним компонентом, розміщуваним між безпровідною підмережеюі внутрішньою мережею. При виборі слід звернути увагу на основні фактори:

- Міжмережевий екран повинен забезпечувати тунельний режим роботи з зашифрованим трафіком для всіх типів безпровідних пристроїв, які будуть використовуватися;
- Метод аутентифікації повинен бути сумісний з центральною базою управління користувачами;
- Підтримка аутентифікації віддалених користувачів заснована на політиках безпеки, що зберігаються в базі управління користувачами.

Наступним кроком необхідно визначити чи є застосовною технологія IPSec для наявної інфраструктури. В якості альтернативи може бути застосована технологія SSL. Але в даному підході є недоліки. Так неможлива робота в тунельному режимі між-міжмережевим екраном і віддаленим користувачем, це означає, що можливе перехоплення реальних IP адрес. Протокол SSL займає більш високий рівень в стеку TCP/IP, ніж IPSec, відповідно більша кількість незашифроване інформації може бути отримано при перехопленні і аналізі пакетів. Технологія SSL первинно була розроблена як протокол для роботи в Інтернет, таким чином, деякі з додатків можуть виявитися непрацездатними в бездротової мережі.

Проведене дослідження радіоканалу стандарту IEEE 802.11 b показало, що, незважаючи на недоліки в області захисту даних, використання стандартних методів сильно знижує можливість атаки на безпровідну мережу.

ISSN 2663 - 4023

ПРАКТИЧНЕ ЗАСТОСУВАННЯ СИСТЕМИ

При практичних вимірах був застосований підхід, що об'єднує експериментальні дані і теорію поширення радіосигналу в приміщенні.

Умови тестування

Тестування проводилося в офісному приміщенні, розмірами приблизно 30 на 20 м. Структура міжкімнатних перегородок - бетон з включенням металевих конструкцій. Для чистоти експерименту були використані три окремі точки доступу, розставлені у випадкових місцях. Перші дві - Cisco AP350s. На першій було встановлено дві антени, друга не містила антени. Третя модель Orinoco AP-1000 з антеною Lucent.

Збір даних

Рис. 3. Схема системи при тестуванні

Першим завданням був збір значень залежності сили сигналу від дистанції, базуючись на даних, представлених драйвером безпровідної карти. Для збору даних використовувалася програма *iwspy*, налаштована на певну MAC адресу:

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

Послідовний виклик "*iwspy eth0*" буде повертати значення рівня сигналу пакетів, отриманих від даного передавача.

Тестуюча станція переміщається по території, вимірюючи потужність сигналуу випадкових точках. Для обробки представляється файл, що складається з двох колонок, в першій відстань від передавача, в другій рівень сигналу. Графічно значення показані на Рис. 4 - Рис. 6

ISSN 2663 - 4023

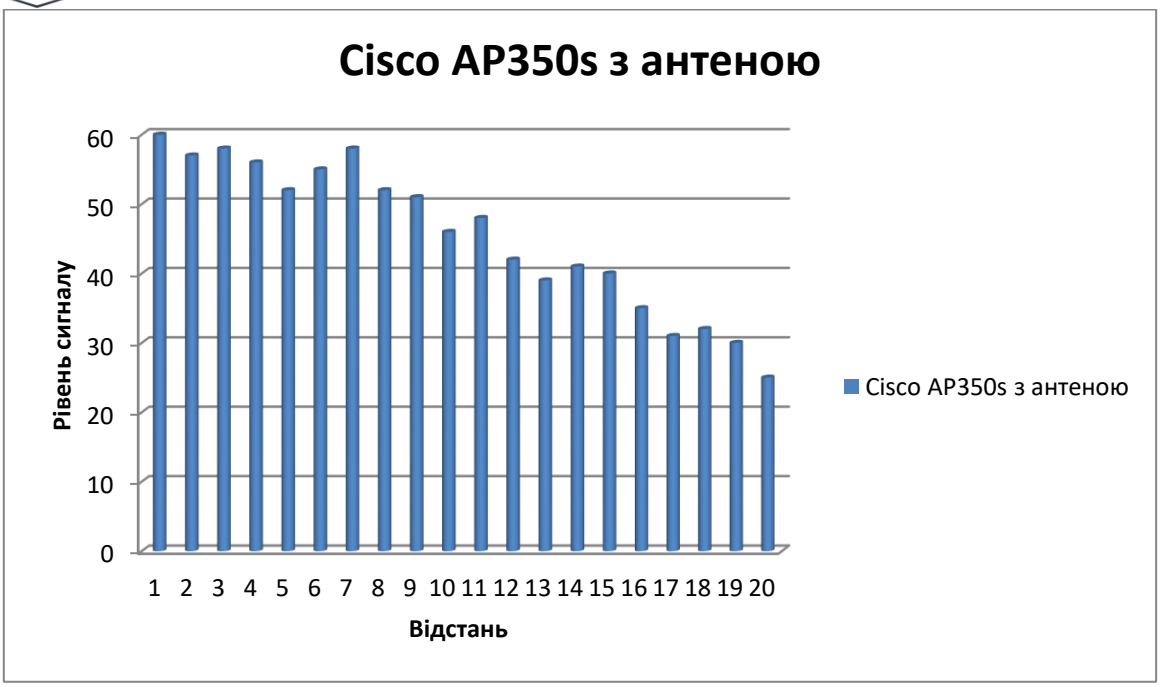

Рис. 4. Cisco AP350s з антеною

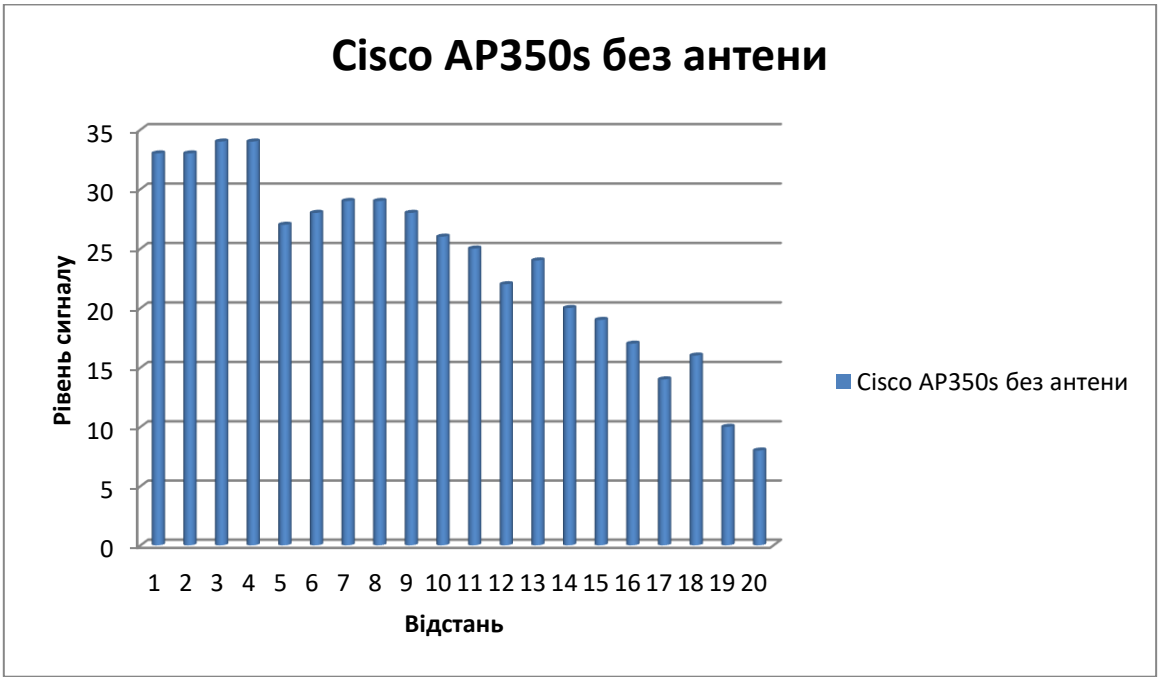

Рис. 5. Cisco AP350s без антени

ISSN 2663 - 4023

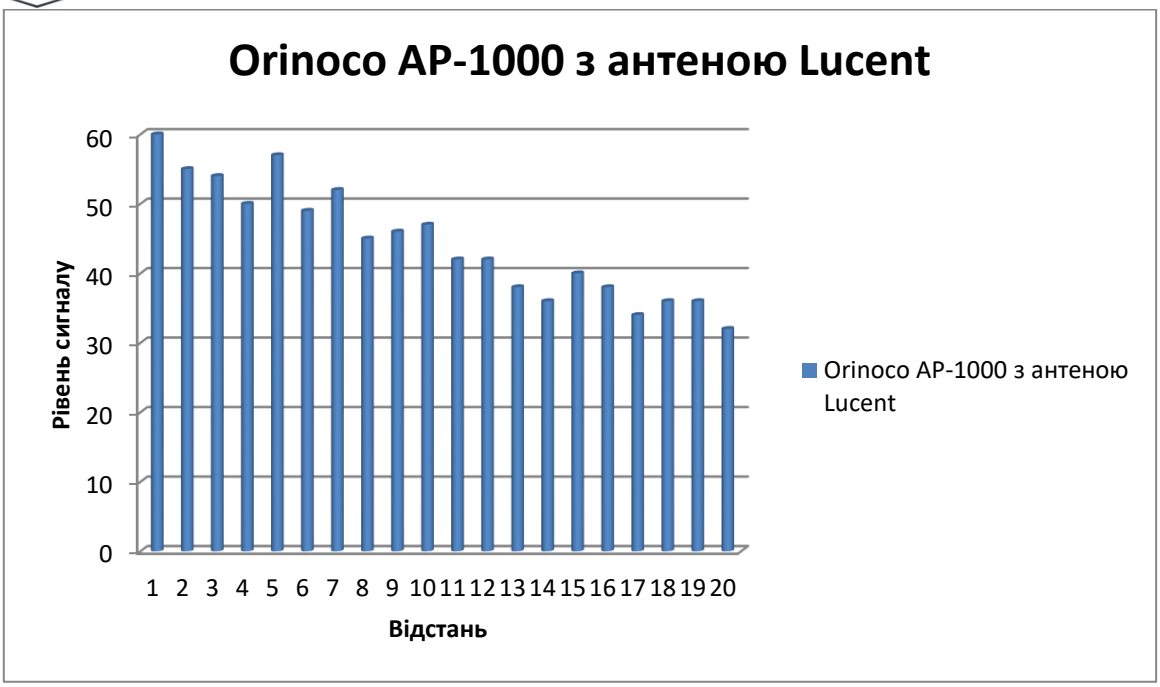

Рис. 6. Orinoco AP-1000 з антеною Lucent

Знаходження залежності сили сигналу від дистанції

Наступним кроком необхідно визначити, чи можуть дані, отримані в ході попереднього експерименту, задовольняти співвідношенню, наведеним на початку.

Для цього необхідно спочатку перевести значення (RSSI - значення рівня прийнятого сигналу), отримані за допомогою утиліти *iwspy*, в Дб. Експерементально отримані наступні залежності:

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

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

Де: P_{dBm} - значення рівня сигналу в ДБ, P_{RSSI} - значення, отримане за допомогою утиліти *iwspy*.

Якщо значення видаються в нормалізованому вигляді (дана опція встановлюється в драйвері безпровідної карти), рівняння набувають вигляду:

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

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

В даний час *iwspy ioctl* для *Linux* повертає не нормалізовані значення (проте, клієнт *Cisco* для *OC Windows* повертає нормалізовані значення).

Наступним етапом є побудова функції апроксимації кривих, в яку включені наведені вище залежності. В якості базису використовується рівняння, що враховуєяк загасання при поширенні радіохвиль в приміщенні, так і відображення, рефракцію і

ISSN 2663 - 4023

інтерференцію.

В результаті експериментів і досліджень було отримано наступнеспіввідношення для поширення радіосигналу в будівлі на частоті 2,4 ГГц.

Таким чином, на 10 метрів втрати складуть приблизно 75 Дб на 100 метрів 110Дб. Очікувана похибка перебувати в діапазоні 13 Дб.

Всі невідомі константи, в тому числі значення «40», яке отримано в результаті експериментів, буде об'єднано в одну константу C, де C - невідома константа, що визначає вихідну потужність з урахуванням впливу загасань, конфігурації антени та інших факторів.

$$R_d = C - 35log_{10}D$$

За допомогою співвідношення, наведеного нижче, проведемо перетворення значення в не нормоване (для відповідності значень вихідним даними утиліти *iwspy* під *Linux*):

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

Створимо програму, для побудови апроксимаційної функції в середовищі *Gnuplot*:

```
set view ,,.5
sstodbm(ss) = ss * 1.205 - 101.07 dbmtoss(dbm) = dbm * .83-+ 83.891
f(x) = dbmtoss { a - 35 * (log(x)/log(10)) )
fit f(x) "ld-distance-data/cisco-chan6-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/cisco-chan6-antenna.txt", f(x)pause -1 "Hit
return to continue"
fit f(x) "ld-distance-data/cisco-chan6-no-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/cisco-chan6-no-antenna.txt",  f(x)pause -1
"Hit return to continue"
fit f(x) "ld-distance-data/orinoco-chan3-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/orinoco-chan3-antenna.txt",  f(x)pause -1
"Hit return to continue"
```

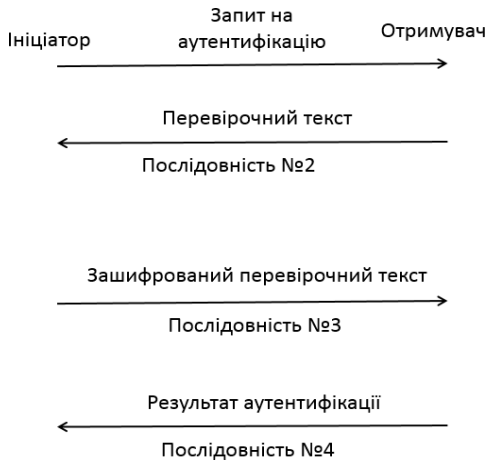

Рис. 7. Схема роботи системи

ISSN 2663 - 4023

Шляхи підвищення ефективності пошуку:

1. Підвищення достовірності результатів, незалежність від числа каналів. В ідеалі, пошукова станція повинна сканувати всі частоти по всьому спектру одночасно;
2. Отримане співвідношення між значеннями рівня сигналу в Дб і значенням, обчисленим драйвером карти *Cisco*, не завжди точно, і, в деяких ситуаціях, може бути не лінійно;
3. Включення до складу комплексу *GPS* навігації може значно поліпшити результати і спростити збір даних;
4. Залучення як мінімум 3-х пошукових станцій значно поліпшить результати;
5. Застосування спеціального аналізатора пакетів, спеціально розрахованого на роботу з безпровідною мережею;
6. Розробка протоколу, що дозволяє пошуковим станціям обмінюватися даними і здійснювати спільний моніторинг;
7. Розробка вдосконаленого алгоритму, що дозволяє зменшити вплив похибок при вимірюванні відстані;
8. Створення математичної моделі ландшафту з урахуванням можливостейзагасання сигналу;
9. Збір бази даних, що описує очікувану потужність передавачів різних виробників, в тому числі із застосуванням антени, так і без, що дозволить більш точно локалізувати джерело сигналу;
10. Комбінувати даний підхід з методами, в яких використовуються спрямовані антени.

Аналіз результатів показав високу ефективність застосування даного комплексу заходів для запобігання можливості атаки на безпровідну мережу. Виявлені найбільш ймовірні причини виникнення помилок при обчисленнікоординат: загасання сигналу від антени передавача було велике. На шляху сигналу розташовувалися перешкоди; передавач розташовувався в середині приміщення, отже не вдалося зібрати достовірну інформацію про загасання сигналу на граничних відстанях; передавач розташовувався в приміщенні з великою кількістю металевихпредметів, що додатково послаблювало і екранувало сигнал в певних напрямках. До основних обмежень запропонованого методу відносяться: при використанні даної технології неможливо визначити місце розташування неактивної станції; драйвер і мережева карта Cisco обмежені в можливості сканування довільного трафіку, таким чином деяка кількість корисних даних могла бути загублена в ході експерименту. Карта Cisco не може сканувати кілька каналів одночасно. При виникненні сигналу: від неавторизованої станції, всі карти, задіяні для захисту мережі повиннніпреизупинити сканування і переключитися на цей канал, з метою найбільш повного збору інформації. Показано застосування вдосконаленої системи безпеки на практиці. Якщо застосовується більш ніж одна станція, всі вони повинні володіти ідентичними версіями мережевих карт (в тому числі антен) і драйверів. Збільшення кількості станцій, що беруть участь в пошуку збільшує шанс на вдале позиціонування. Пошукові станції, у разі, якщо вони розташовані стаціонарно, повинні бутирозташовані найбільш оптимально: на максимально можливій відстані один від одного, на відкритому просторі, максимально, виключаючи можливі ослаблення сигналу від перешкод або перешкод, але в той же час, щоб вони могли приймати сигнал з будь-якого місця охоронюваної зони. Слід встановити активно скануючу мережу станцію, яка в разі появи неавторизованого передавача буде посилати запити, що вимагають відповідей, за якими буде можливо визначити потужність сигналу. Для пошукових станцій необхідні

високочутливі антени. У разі мобільного неавторизованого пристрою дана технологія не зможе принести належних результатів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведено дослідження особливостей роботи стандартного протоколу потокового шифрування WEP. Для кожного з видів атак розроблено методи протидії, що дозволяють підвищити ступінь захисту даних в радіоканалі. Розроблено система аутентифікації, заснована на алгоритмі SPEKE. Проведено дослідження з точки зору захисту інформації, проаналізовано механізми виникнення атак, створено методи протидії. Розроблено систему яка є заміною стандартним засобам аутентифікації протоколу 802.11, що не володіють достатнім рівнем безпеки. На основі алгоритму SPEKE створено механізм захищеного обміну ключами сесії, відсутній у стандартній системі безпеки. Можливість зміни ключа сесії дозволить знизити ймовірність успішних атак на інформацію, зашифровану за допомогою алгоритму потокового шифрування WEP.

Створено вдосконалену систему захисту інформації, яка передається в радіоканалі 802.11, що дозволяє значно підвищити рівень захисту інформації, у порівнянні зі стандартною системою, за рахунок застосування комплексу криптографічно стійких засобів і методів шифрування, аутентифікації і обміну ключами. Розроблено технологію, що дозволяє використовувати особливості протоколу 802.11 для локалізації станції-порушника, розміщеної у зоні роботи безпровідної мережі. Створено методи підвищення ефективності роботи системи пошуку активних станцій-порушників. Це дозволить значно знизитиймовірність атак на інформацію в радіоканалах. Наведено методи збільшення швидкодії алгоритмів, засоби підвищення криптографічної стійкості системи захищеної аутентифікації. На основі розроблених методів і засобів побудовано удосконалену систему безпекидля радіоканалу стандарту 802.11. Показано застосування вдосконаленої системи безпеки на практиці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Вильям, С. (2001). *Криптография и защита сетей: принципы и практика* (2-ге вид.). Вильямс.
2 Партыка, Т., Попов, И. (2002). *Информационная безопасность*. Форум - Инфра.
3 Успенский, А. Ю., Иванов, И. П. (2002). Анализ проблем защиты информации в радиоканалах стандарта IEEE 802.11. *Вестник МГТУ. Сер. Машиностроение*, (4), 102–108.
4 Nedashkivskiy, O., Havrylko, Y., Zhurakovskyi, B. Boiko, J. (2020). Mathematical Support for Automated Design Systems for Passive Optical Networks Based on the β-parametric Approximation Formula. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 8207–8212. https://doi.org/10.30534/ijatcse/2020/186952020
5 Zetter, K. (2014). *How thieves can hack and disable your home alarm system*. Wired Magazine. https://www.wired.com
6 Успенский, А. Ю. (2002). Исследование возможности и методы противодействия перехвату защищенной при помощи протокола WEP информации в радиоканале стандарта IEEE 802.11. У *Студенческая научная весна* (с. 89–91).
7 Жураковський, Б.Ю, Варфоломеєва, О.Г., Гладких, О.В., Хахлюк, О.А. (2013). Об'єктно-орієнтована технологія проектування систем управління. *Вісник Державного університету інформаційно-комунікаційних технологій*, (1), 49-53.
8 Жураковський, Б.Ю. (2012). Об'єктно-орієнтована модель системи управління мережею NGN. *Вісник Державного університету інформаційно-комунікаційних технологій*, (2), 81-84.
9 Druzhynin, V., Toliupa, S., Pliushch, O., Stepanov, M., Zhurakovskyi, B. (2020). Features of processing signals from stationary radiation sources in multi-position radio monitoring systems. У *Cybersecurity*

Providing in Information and Telecommunication Systems 2020 (с. 46–65). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2746/

10 Jesse, R. (2000). Unsafe at any key size; An analysis of the WEP encapsulation.

11 Жураковський, Б. Ю. (2012). Дослідження використання нових завадостійких кодів для каналів зі стиранням. *Вісник Державного університету інформаційно-комунікаційних технологій*, (2), 93-96.

12 Nedashkivskyy, O.L., Zinenco, Yu.M., Tkachenko O.M. and Korshun, N.V. (2017) Methods of creating passive optical networks with the "distributing bus" topology, Control, Navigation and Communication Systems. *Academic Journal*, *2*(42), 206-217. http://journals.nupp.edu.ua/sunz/article/view/1175

13 Жураковський, Б. Ю. (2021). *Технології інтернету речей* (Б. Ю. Жураковський І. О. Зенів, Ред.). КПІ ім. Ігоря Сікорського. https://ela.kpi.ua/handle/123456789/42078

14 Жураковський, Б.Ю. Мошенченко, М.С. (2020). Стандарти Smart City. *Актуальные научные исследования в современном мире*, (2), 41–44.

15 Zhurakovskyi, B., Toliupa, S., Otrokh, S., Dudarieva, H., Zhurakovskyi, V. (2021). Coding for Information Systems Security and Viability. У Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" 2020 (с. 71–84). CEUR Workshop Proceedings.

16 Жураковський, Б.Ю. (2021). Модель безпровідної мережі інтерактивної інфраструктури SmartCity. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", *1*(13), 63-80. https://doi.org/10.28925/2663-4023.2021.13.6380

17 Nedashkivskiy, O. (2017). Precise method of balancing passive optical networks with irregular splitter with two or more outputs. У *2nd International Conference on Advanced Information and Communication Technologies (AICT)* (с. 228–231). https://doi.org/10.1109/AIACT.2017.8020107

18 Moshenchenko, M., & Zhurakovskyi, B. (2021). Information protection in “smart city” technologies. *Cybersecurity: Education, Science, Technique*, *3*(11), 100–109. https://doi.org/10.28925/2663-4023.2021.11.100109.

19 Barker, E. B., & Kelsey, J. M. (2007). *Recommendation for random number generation using deterministic random bit generators (revised)*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-90.

20 Жураковський, Б.Ю. (2007). Імітаційна модель каналу управління і математичні методи завадостійкого кодування. *Вісник Державного університету інформаційно-комунікаційних технологій*, Спецвипуск, 114 – 119.

21 Полторак, В. П., Жураковский, Ю. П., Жураковский Б. Ю. (1998). Полиномиальное кодирование информации в системах управления. У 5-а Українська конференція з автоматичного управління "Автоматика-98" (с. 270–271).

22 Zhurakovskiy, B., & Tsopa, N. (2019). Assessment technique and selection of interconnecting line of information networks. У *2019 3rd international conference on advanced information and communications technologies (AICT)*. IEEE. https://doi.org/10.1109/aiact.2019.8847726.

23 Nedashkivskyy, O.L. (2017). Methods of creating passive optical networks with the «bus» topology. *Scientific Proceeding of the State University of Telecommunications*, *3*(47), 42–49. http://journals.dut.edu.ua/index.php/sciencenotes/article/view/1648/1574.

24 Sandberg, J. (2001). *Hackers poised to land at wireless AirPort*. ZDNet.

25 Чмора, А. (2002). *Современная прикладная криптография*. Гелиос.

26 Zhurakovskyi, B., Toliupa, S., & Druzhynin, V. (2022). Calculation of Quality Indicators of the Future Multiservice Network. *Future Intent-Based Networking*, (831), 197–209. https://doi.org/10.1007/978-3-030-92435-5_11

27 Klove, T. (2007). *Codes for Error Detecting. Ch. 2.* World Scientific Publishing Company.

28 *WiFi Security: WEP, WPA, WPA2 And Their Differences*. NetSpot. https://www.netspotapp.com/wifi-encryption-and-security.html

29 Шнайер, Б. (2002). *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ*. Триумф.

30 Shevchenko, O., Bondarchuk, A., Polonevych, O., Zhurakovskyi, B., Korshun, N. (2021). Methods of the objects identification and recognition research in the networks with the IoT concept support. У *Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (с.* 277–282). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2923/

31 Encryption Algorithm II http://www.ncat.edu/~grogans/main.htm

32 Lima, L., Vilela, J. P., Barros, J., Medard, M. (2008). An information-theoretic cryptanalysis of network coding - is protecting the code enough? У *2008 International Symposium on Information Theory and Its Applications (ISITA)*. IEEE. https://doi.org/10.1109/isita.2008.4895420.

33 Novotny, M., Kasper, T. (2009). Cryptanalys is of kee Loqwith COPOCOBANA. У *SHARCS 2009 Conferece.*

34 Жураковський, Б. Ю. (2020). Комп'ютерні мережі. Частина 2 Навчальний посібник (Б. Ю. Жураковський І. О. Зенів, Ред.). КПІ ім. Ігоря Сікорського. https://ela.kpi.ua/handle/123456789/36641

35 Contributors to Wikimedia projects. (2007, 24 вересня). *IEEE 802.11a-1999 - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/IEEE_802.11a-1999

36 Shim, R. (2001). *How to Fill Wi-Fi's Security Holes*. ZDNet.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Bohdan Zhurakovskyi
Doctor of Technical Sciences, Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0003-3990-5205
zhurakovskiybyu@tk.kpi.ua

Oleksiy Nedashkivskiy
Doctor of Technical Sciences, Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-1788-4434
al_1@ua.fm

SYSTEM TO COLLECT INFORMATION WHEN TRANSFERRING DATA TO RADIO CHANNELS

Abstract. This article 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 aim of the work is to analyze the security of wireless networks, identify methods for their protection and create a model for protecting wireless networks. In order to achieve this goal, the following list of tasks was performed: the existing solutions in the field of information protection through radio networks were analyzed; the description of the offered developed model is made; algorithms, experiments, experiments of this model are described. A means of protecting information through radio networks has been developed, the application of which has a significant increase in the level of information security in the radio channel. The practical value of this development is that the theoretical and practical results are recommended for implementation in organizations that use the radio channel to transmit confidential information with high security requirements.

Keywords: authorization, authentication, wireless network, Wi-Fi, model, encryption algorithm, keys, digital signature, password, information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Vyliam, S. (2001). Kryptohrafyia y zashchyta setei: pryntsypy y praktyka (2-he vyd.). Vyliams.
2 Partyka, T., Popov, Y. (2002). Informatsyonnaia bezopasnost. Forum - Infra.
3 Uspenskyi, A. Yu., Yvanov, Y. P. (2002). Analyz problem zashchyty ynformatsyy v radyokanalakh standarta IEEE 802.11. Vestnyk MHTU. Ser. Mashynostroenye, (4), 102–108.
4 Nedashkivskiy, O., Havrylko, Y., Zhurakovskyi, B. Boiko, J. (2020). Mathematical Support for Automated Design Systems for Passive Optical Networks Based on the β-parametric Approximation Formula. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 8207–8212. https://doi.org/10.30534/ijatcse/2020/186952020
5 Zetter, K. (2014). *How thieves can hack and disable your home alarm system*. Wired Magazine. https://www.wired.com
6 Uspenskyi, A. Yu. (2002). Yssledovanye vozmozhnosty y metody protyvodeistvyia perekhvatu zashchyshchennoi pry pomoshchy protokola WEP ynformatsyy v radyokanale standarta IEEE 802.11. U Studencheskaia nauchnaia vesna (p. 89–91).
7 Zhurakovskyi, B.Iu, Varfolomeieva, O.H., Hladkykh, O.V., Khakhliuk, O.A. (2013). Obiektno-oriientovana tekhnolohiia proektuvannia system upravlinnia. Visnyk Derzhavnoho universytetu informatsiino-komunikatsiinykh tekhnolohii, (1), 49-53.
8 Zhurakovskyi, B.Iu. (2012). Obiektno-oriientovana model systemy upravlinnia merezheiu NGN. Visnyk Derzhavnoho universytetu informatsiino-komunikatsiinykh tekhnolohii, (2), 81-84.
9 Druzhynin, V., Toliupa, S., Pliushch, O., Stepanov, M., Zhurakovskyi, B. (2020). Features of processing signals from stationary radiation sources in multi-position radio monitoring systems. In *Cybersecurity Providing in Information and Telecommunication Systems 2020* (p. 46–65). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2746/
10 Jesse, R. (2000). Unsafe at any key size; An analysis of the WEP encapsulation.

11 Zhurakovskyi, B. Yu. (2012). Doslidzhennia vykorystannia novykh zavadostiikykh kodiv dlia kanaliv zi styranniam. Visnyk Derzhavnoho universytetu informatsiino-komunikatsiinykh tekhnolohii, (2), 93-96.
12 Nedashkivskyy, O.L., Zinenco, Yu.M., Tkachenko O.M. and Korshun, N.V. (2017) Methods of creating passive optical networks with the "distributing bus" topology, Control, Navigation and Communication Systems. *Academic Journal*, *2*(42), 206-217. http://journals.nupp.edu.ua/sunz/article/view/1175
13 Zhurakovskyi, B. Yu. (2021). Tekhnolohii internetu rechei (B. Yu. Zhurakovskyi I. O. Zeniv, Red.). KPI im. Ihoria Sikorskoho. https://ela.kpi.ua/handle/123456789/42078
14 Zhurakovskyi, B.Iu. Moshenchenko, M.S. (2020). Standarty Smart City. Aktualnye nauchnye yssledovanyia v sovremennom myre, (2), 41–44.
15 Zhurakovskyi, B., Toliupa, S., Otrokh, S., Dudarieva, H., Zhurakovskyi, V. (2021). Coding for Information Systems Security and Viability. In Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" 2020 (p. 71–84). CEUR Workshop Proceedings.
16 Zhurakovskyi, B.Iu. (2021). Model bezprovidnoi merezhi interaktyvnoi infrastruktury SmartCity. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", 1(13), 63-80. https://doi.org/10.28925/2663-4023.2021.13.6380
17 Nedashkivskiy, O. (2017). Precise method of balancing passive optical networks with irregular splitter with two or more outputs. In *2nd International Conference on Advanced Information and Communication Technologies (AICT)* (p. 228–231). https://doi.org/10.1109/AIACT.2017.8020107
18 Moshenchenko, M., Zhurakovskyi, B. (2021). Information protection in “smart city” technologies. *Cybersecurity: Education, Science, Technique*, *3*(11), 100–109. https://doi.org/10.28925/2663-4023.2021.11.100109.
19 Barker, E. B., & Kelsey, J. M. (2007). *Recommendation for random number generation using deterministic random bit generators (revised)*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-90.
20 Zhurakovskyi, B.Iu. (2007). Imitatsiina model kanalu upravlinnia i matematychni metody zavadostiikoho koduvannia. Visnyk Derzhavnoho universytetu informatsiino-komunikatsiinykh tekhnolohii, Spetsvypusk, 114 – 119.
21 Poltorak, V. P., Zhurakovskyi, Yu. P., Zhurakovskyi B. Yu. (1998). Polynomyalnoe kodyrovanye ynformatsyy v systemakh upravlenyia. In 5-a Ukrainska konferentsiia z avtomatychnoho upravlinnia "Avtomatyka-98" (p. 270–271).
22 Zhurakovskiy, B., & Tsopa, N. (2019). Assessment technique and selection of interconnecting line of information networks. In *2019 3rd international conference on advanced information and communications technologies (AICT)*. IEEE. https://doi.org/10.1109/aiact.2019.8847726.
23 Nedashkivskyy, O.L. (2017). Methods of creating passive optical networks with the «bus» topology. *Scientific Proceeding of the State University of Telecommunications*, *3*(47), 42–49. http://journals.dut.edu.ua/index.php/sciencenotes/article/view/1648/1574.
24 Sandberg, J. (2001). *Hackers poised to land at wireless AirPort*. ZDNet.
25 Chmora, A. (2002). Sovremennaia prykladnaia kryptohrafyia. Helyos.
26 Zhurakovskyi, B., Toliupa, S., Druzhynin, V. (2022). Calculation of Quality Indicators of the Future Multiservice Network. *Future Intent-Based Networking*, (831), 197–209. https://doi.org/10.1007/978-3-030-92435-5_11
27 Klove, T. (2007). *Codes for Error Detecting. Ch. 2*. World Scientific Publishing Company.
28 *WiFi Security: WEP, WPA, WPA2 And Their Differences*. NetSpot. https://www.netspotapp.com/wifi-encryption-and-security.html
29 Shnaier, B. (2002). Prykladnaia kryptohrafyia. Protokoly, alhorytmy, yskhodnye teksty na yazyke SY. Tryumf.
30 Shevchenko, O., Bondarchuk, A., Polonevych, O., Zhurakovskyi, B., Korshun, N. (2021). Methods of the objects identification and recognition research in the networks with the IoT concept support. In *Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (p.* 277–282). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2923/
31 Encryption Algorithm II http://www.ncat.edu/~grogans/main.htm
32 Lima, L., Vilela, J. P., Barros, J., Medard, M. (2008). An information-theoretic cryptanalysis of network coding - is protecting the code enough? У *2008 International Symposium on Information Theory and Its Applications (ISITA)*. IEEE. https://doi.org/10.1109/isita.2008.4895420.
33 Novotny, M., Kasper, T. (2009). Cryptanalys is of kee Loqwith COPOCOBANA. In *SHARCS 2009 Conferece.*
34 Zhurakovskyi, B. Yu. (2020). Kompiuterni merezhi. Chastyna 2 Navchalnyi posibnyk (B. Yu. Zhurakovskyi I. O. Zeniv, Red.). KPI im. Ihoria Sikorskoho. https://ela.kpi.ua/handle/123456789/36641

35 Contributors to Wikimedia projects. (2007). *IEEE 802.11a-1999 - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/IEEE_802.11a-1999

36 Shim, R. (2001). *How to Fill Wi-Fi's Security Holes*. ZDNet.