Київський національний торговельно-економічний університет
Кафедра інформаційних технологій

ВИПУСКНИЙ КВАЛІФІКАЦІЙНИЙ ПРОЕКТ
на тему:

« Проектування інформаційної мережі обміну даними КНТЕУ»

(за матеріалами Інформаційно-обчислювального центру Головного центру інформаційних технологій КНТЕУ, корпус А,Б)

Студента 2 курсу, 10м групи,
факультету обліку, аудиту та інформаційних систем,
денної форми навчання
спеціальності
122 «Комп'ютерні науки» _____ Решетніка Артема Володимировича

Науковий керівник
науковий ступінь
вчене звання _____ Нагірна А.М.
канд. фіз.-мат. наук, доцент

Гарант освітньої програми
науковий ступінь
вчене звання _____ Краскевич В. Є.
доктор технічних наук, професор

Київ 2018

ЗМІСТ

ВСТУП

Корпоративна інформаційна система - це система, що використовує сучасні інформаційні та комп'ютерні технології, безпосередньо здійснює організаційну, управлінську та виробничу діяльність підприємства або організації і не є допоміжною або сервісною.

Корпоративна мережа яка базується на технології Wi-Fi - це складна система, що включає тисячі найрізноманітніших компонентів: комп'ютери різних типів, починаючи з настільних і закінчуючи смартфонами та планшетами, системного та прикладного програмного забезпечення, мережевих адаптерів, концентраторів та роутерів. А оскільки життя не стоїть на місці, то і зміст корпоративної інформації, інтенсивність потоків та способи її обробки постійно змінюються так само як і небезпеки пов’язані з незаконним вторгненням в безпровідну мережу та зловмисним маніпулюванням інформації в ній.

Використання технологій Wi-Fi - недороге та доступне практично всім підприємствам (а через голобальну мережу Internet і одиночним користувачам) - істотно полегшило завдання побудови територіально розподіленої корпоративної мережі, одночасно висунувши на перший план завдання захисту корпоративних даних при передачі їх через загальнодоступну публічну мережу з багатомільйонним "населенням".

Актуальність роботи пов'язана з усе зростаючою роллю, яку відіграють бездротові корпоративні Wi-Fi мережі для забезпечення ефективності управління і успішного функціонування самих різних організацій. При цьому практично в кожній такій мережі спостерігається загальна тенденція збільшення числа користувачів, обсягів циркулюючої інформації, інтенсивності трафіку і пов'язаних з цими обставинами

погіршення якості мережевих послуг.

Мета роботи - дослідити особливості пов'язані з принципами побудови та функціонування мереж передачі даних в розподілених корпоративних системах на основі Wi-Fi та їх захист. Для досягнення поставленої мети необхідно вирішити ряд **завдань**:

- дати розширене визначення поняттю «розподіленій корпоративній мережі»;
- розглянути процес створення корпоративної мережі;
- розглянути структуру корпоративної мережі;
- дослідити роль Internet в корпоративній мережі;
- виявити особливості використання методів захисту інформації в бездротовій мережі Wi-Fi;
- охарактеризувати особливості атак на корпоративні мережі.

Об'єктом дослідження є розподілена корпоративна мережа.

Предметом дослідження є способи та методи захисту інформації в бездротовій корпоративній мережі на основі Wi-Fi.

Методи дослідження: аналіз, класифікація, систематизація узагальнення.

Теоретичне значення даної дипломної роботи визначається тим, що її основні положення можуть бути використані у дослідницьких роботах, присвячених подальшій розробці систем захисту інформації в бездротовій мережі.

Практичне значення роботи полягає в тому, що її матеріали і результати можуть бути використані при написанні курсових та дипломних робіт, наукових статей, у викладанні курсів теорії та практиці створення сучасних корпоративних систем та їх захисту.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та списку літератури. Зміст дослідження представлено у трьох

розділах. У першому розділі дипломної роботи були розглянуті особливості структури корпоративних мереж. Принципи, за якими будується така мережа, та безпека Wi-Fi мереж. В другому розділі обговорюються сценарій проектування та перші кроки впровадження технології Wi-Fi в корпоративних мережах підприємств. Третій розділ являє собою проект створення безпровідної локальної мережі на основі Wi-Fi та її захист.

РОЗДІЛ 1. КОРПОРАТИВНА МЕРЕЖА

Корпоративна мережа - це система, що забезпечує передачу інформації між різними додатками, використовуваними в системі корпорації. Корпоративна мережа являє собою мережу окремої організації.

Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP / IP і використовує комунікаційні стандарти Інтернету, а також сервісні додатки, що забезпечують доставку даних користувачам мережі [10]. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення і звукозапису), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. В цьому керівництві всі служби публікації називаються "службами Інтернету" незалежно від того, де вони використовуються (в Інтернеті або корпоративній мережі).

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одної. Принципи, за якими будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі слід вживати всіх

заходів для мінімізації обсягів передаваних даних. В іншому ж корпоративна мережа не повинна вносити обмежень на те, які саме додатки і яким чином обробляє передавану по ній інформацію [5].

Процес створення корпоративної інформаційної системи

Можна виділити основні етапи процесу створення корпоративної інформаційної системи:

• провести інформаційне обстеження організації, за результатами обстеження вибрати архітектуру системи та апаратно-програмні засоби її реалізації, вибрати та/або розробити ключові компоненти інформаційної системи:

• система управління корпоративною базою даних;

• система автоматизації ділових операцій та документообігу;

• система управління електронними документами;

• спеціальні програмні засоби;

• системи підтримки прийняття рішень [1].

Розглянемо послідовно кожен із перелічених етапів.

Інформаційне обстеження

Інформаційна система потрібна організації для того, щоб забезпечувати інформаційно-комунікаційну підтримку її основної та допоміжної діяльності. Тому перш, ніж вести мову про структуру та функціональне наповнення інформаційної системи, необхідно розібратися в цілях і завданнях самої організації, щоб зрозуміти, що ж потрібно автоматизувати.

Відповіді на поставлені питання можна отримати тільки після детального інформаційного обстеження компанії, цілями якого є:

• формулювання і опис функцій кожного підрозділу компанії, а також розв'язувані ними задачі;

• опис технології роботи кожного з підрозділів компанії і розуміння, що необхідно автоматизувати і в якій послідовності;

• опис технології роботи кожного з підрозділів та пов'язаних з ними інформаційних потоків;

• відображення технології на структуру, визначення її функціонального складу і кількості робочих місць в кожному структурному підрозділі компанії, а також опис функцій, які виконуються (автоматизуються) на кожному робочому місці;

• опис основних шляхів і алгоритми проходження вхідних, внутрішніх та вихідних документів, а також технології їх обробки.

Результатом обстеження є моделі діяльності компанії, і її інформаційної інфраструктури, на базі яких розробляються проект корпоративної інформаційної системи, вимоги до програмно-апаратних засобів і специфікації на розробку прикладного програмного забезпечення, якщо в цьому є необхідність. При виборі описуваних засобів необхідно звернути увагу на те, щоб робота з ними була б доступна не тільки професійним працівникам, але й більш широкому класу [14, 8].

Архітектура

За результатами обстеження необхідно вибрати архітектуру системи. Для корпоративних систем рекомендується архітектура клієнт / сервер. Архітектура клієнт / сервер надає технологію доступу кінцевого користувача до інформації в масштабах підприємства. Таким чином, архітектура клієнт /сервер дозволяє створити єдиний інформаційний простір, в якому кінцевий користувач має своєчасний і безперешкодний (але санкціонований) доступ до корпоративної інформації. Інформаційне обстеження дозволяє вибрати апаратно-програмну реалізацію системи [16].

Вибір СУБД

Вибір системи управління для корпоративної бази даних - один з ключових моментів у розробці інформаційної системи. На Українському ринку присутні практично всі СУБД, що належать до елітного класу - Oracle, Informix, Sybase, Ingres. Питання, яку СУБД використовувати,

можна вирішити тільки за результатами попереднього обстеження та отримання інформаційних моделей діяльності.

Вибір системи автоматизації документообігу

Плутанина з документами (їх затримки, втрати, дублювання, довге переміщення від одного виконавця до іншого і т.д.) - болюча проблема для будь-якої компанії. Тому система автоматизації документообігу, яка дозволяє автоматизувати ручні, рутинні операції, автоматично передавати і відслідковувати переміщення документів усередині корпорації, контролювати виконання доручень, пов'язаних з документами і т.д. - одна з найважливіших складових інформаційної системи.

Вибір програмних засобів для управління документами

Поява на ринку систем управління електронними документами - EDMS (Electronic Document Management Systems) викликана прагненням скоротити потік паперових документів і хоча б частково зменшити труднощі, що виникають у зв'язку з їх зберіганням, пошуком і обробкою. На відміну від документів на паперових носіях електронні документи забезпечують переваги при створенні, сумісного використання, пошуку, поширенні та зберіганні інформації. Системи EDMS реалізують введення, зберігання і пошук всіх типів електронних документів, як текстових, так і графічних. За допомогою систем цього класу можна організувати зберігання в електронному вигляді адміністративних і фінансових документів, факсів, технічної бібліотеки, зображень, тобто всіх документів, що входять в організацію і циркулють в ній [18, 22].

Вибір спеціалізованих прикладних програмних засобів

При всій описаній спільності кожна компанія має свою специфіку, яка визначається родом її діяльності. Вибір спеціалізованих програмних засобів в значній мірі залежить від цієї специфіки.

Абсолютно для всіх компаній необхідно мати в складі інформаційної системи стандартний набір додатків, таких як текстові редактори,

електронні таблиці, комунікаційні програми і т.д. Одним із критеріїв вибору подібних систем повинна бути можливість їх нескладної інтеграції в корпоративну інформаційну систему.

Системи підтримки прийняття рішенью

Необхідно відзначити спеціальний клас додатків - систем підтримки прийняття рішень, що дозволяють моделювати правила і стратегії бізнесу і мати інтелектуальний доступ до неструктурованої інформації. Системи подібного класу засновані на технологіях штучного інтелекту.

Структура корпоративної мережі

Для підключення віддалених користувачів до корпоративної мережі самим простим і доступним варіантом є використання телефонного зв'язку. Там, де це можливо, можуть використовуватися мережі ISDN. Для об'єднання вузлів мережі в більшості випадків використовуються глобальні мережі передачі даних. Навіть там, де можлива прокладка виділених ліній (наприклад, в межах одного міста) використання технологій пакетної комутації дозволяє зменшити кількість необхідних каналів зв'язку і - що важливо - забезпечити сумісність системи з існуючими глобальними мережами [17].

Підключення корпоративної мережі до Internet виправдано, якщо потрібен доступ до відповідних послуг. Використовувати Internet як середовище передачі даних варто тільки тоді, коли інші способи недоступні і фінансові міркування переважують вимоги надійності та безпеки. Якщо використовувати Internet тільки як джерело інформації, краще користуватися технологією "з'єднання по запиту" (***dial-on-demand***), тобто таким способом підключення, коли з'єднання з вузлом Internet встановлюється тільки з вашої ініціативи і на потрібний вам час. Це різко знижує ризик несанкціонованого проникнення у вашу мережу ззовні.

Для передачі даних усередині корпоративної мережі також варто використовувати віртуальні канали мереж пакетної комутації. Основні

переваги такого підходу - універсальність, гнучкість, безпека.

Обладнання корпоративних мереж

Корпоративна мережа - це досить складна структура, що використовує різні типи зв'язку, комунікаційні протоколи і способи підключення ресурсів.

Все обладнання мереж передачі даних можна умовно розділити на два великі класи - *периферійне*, яке використовується для підключення до мережі кінцевих вузлів, і *магістральне* або *опорне*, що реалізує основні функції мережі (комутацію каналів, маршрутизацію і т.д.). Чіткої межі між цими типами немає - одні й ті ж пристрої можуть використовуватися в різній якості або поєднувати ті й інші функції. Слід зазначити, що до магістрального обладнання зазвичай пред'являються підвищені вимоги в частині надійності, продуктивності, кількості портів і подальшої розширюваності. Периферійне обладнання є необхідним компонентом будь-якої корпоративної мережі. Функції ж магістральних вузлів може брати на себе глобальна мережа передачі даних, до якої підключаються ресурси. Як правило, магістральні вузли у складі корпоративної мережі з'являються тільки в тих випадках, коли використовуються орендовані канали зв'язку або створюються власні вузли доступу.

Периферійне устаткування корпоративних мереж з точки зору виконуваних функцій також можна розділити на два класи. По-перше, це маршрутизатори (routers), слугуючі для об'єднання однорідних LAN (як правило, IP або IPX) через глобальні мережі передачі даних. У мережах, що використовують IP або IPX в якості основного протоколу - зокрема, в тому же Internet - маршрутизатори використовуються і як магістральний устаткування, що забезпечують стиковку різних каналів і протоколів зв'язку. Маршрутизатори можуть бути виконані як у вигляді автономних пристроїв, так і програмними засобами на базі комп'ютерів і спеціальних комунікаційних адаптерів.

По-друге широко використовуваний тип периферійного обладнання - шлюзи (gateways), реалізовують взаємодію додатків, що працюють в різних типах мереж. У корпоративних мережах використовуються в основному шлюзи OSI, що забезпечують взаємодію локальних мереж з ресурсами X.25 і шлюзи SNA, що забезпечують підключення до мереж IBM. Повнофункціональний шлюз завжди являє собою програмно-апаратний комплекс, оскільки повинен забезпечувати необхідні для додатків програмні інтерфейси [19, 21].

Всі найбільші постачальники мережевого обладнання пропонують набори продуктів, що надають керівникам інформаційних служб широкі можливості для побудови корпоративних мереж. Вони включають різноманітні апаратні засоби (концентратори, маршрутизатори, комутатори), орієнтовані на створення систем на базі передових комунікаційних технологій, включаючи Fast Ethernet, режим асинхронної передачі (ATM) і віртуальні мережі. Інтеграція цих технологій в широкомасштабні інформаційні системи спрямована на підвищення пропускної спроможності [19].

Багатошарове представлення корпоративної мережі

Корпоративну мережу корисно розглядати як складну систему, що складається з декількох взаємодіючих шарів. В основі лежить шар комп'ютерів-центрів зберігання і обробки інформації, і транспортна підсистема, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами.

Над транспортною системою працює шар мережевих операційних систем, який організовує роботу додатків в комп'ютерах і надає через транспортну систему ресурси свого комп'ютера в загальне користування.

Над операційною системою працюють різні додатки, але через особливу роль систем управління базами даних, що зберігають у впорядкованому вигляді основну корпоративну інформацію і виконують

над нею базові операції пошуку, цей клас системних додатків звичайно виділяють в окремий шар корпоративної мережі.

На наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації серед мільйонів і мільярдів байт, збережених на дисках, надають кінцевим користувачам цю інформацію в зручній для прийняття рішення формі, а також виконують деякі загальні для підприємств усіх типів процедури обробки інформації. До цих сервісів відноситься служба World Wide Web, система електронної пошти, системи колективної роботи та багато інших.

І, нарешті, верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для даного підприємства або підприємств даного типу. Прикладами таких систем можуть служити системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проектування, управління технологічними процесами і т.п.

Кінцева мета корпоративної мережі втілена в прикладних програмах верхнього рівня, але для їх успішної роботи абсолютно необхідно, щоб підсистеми інших верств чітко виконували свої функції.

Стратегічні рішення, як правило, впливають на вигляд мережі в цілому, зачіпаючи кілька шарів, хоча спочатку стосуються тільки одного конкретного шару або навіть окремої підсистеми цього шару. Такий взаємний вплив продуктів і рішень потрібно обов'язково враховувати при плануванні технічної політики розвитку мережі, інакше можна зіткнутися з необхідністю термінової і непередбаченої заміни, наприклад, мережевої технології, через те, що нова прикладна програма відчуває гострий дефіцит пропускної здатності для свого трафіку [9, 15].

1.1 Безпека корпоративної мережі

Завдяки тому, що вся історія побудови безпечної інформаційної системи пов'язана або з зміцненням захисту по периметру, або з організаційними та фізичними заходами захисту, сьогодні рідко можна побачити корпоративну мережу, яка стійка до злому і атакам зсередини.

Сьогодні вже ніхто не може уявити як завгодно серйозну організацію без робочих місць, оснащених комп'ютерами, підключеними до загальної корпоративної мережі. Як правило, корпоративна мережа підключається до загальнодоступних мереж, зазвичай до Інтернету. Оскільки більша частина життєво важливої інформації компанії, включаючи і конфіденційну, знаходиться в корпоративній мережі, то виникає серйозне питання, хто може отримати доступ до цієї інформації [23].

Посилення безпеки корпоративної мережі: зміна акцентів

Безпека сьогодні є «модним» словом. Якщо розглянути рішення проблеми захисту доступу до ресурсів корпоративної мережі в розвитку, то можна відзначити суттєві зміни за останнє десятиліття. В кінці 80-х найбільше турбували фізичні уразливості системи, загрози фізичного доступу сторонніх осіб до системи. Тому рішення в основному стосувалися організаційних заходів. До середині 90-х акценти змістилися, сильний вплив зробили підключення корпоративної мережі до Інтернету і побудова розподілених мереж - підключення до головної корпоративної мережі філій компанії, а також небезпека, пов'язана з комп'ютерними вірусами. Комп'ютерна безпека корпоративної мережі в цей період перестала визначатися тільки коректністю посадових інструкцій та «стійкістю дверей» в кімнаті з серверами і в основному перейшла у відання IT-персоналу компанії. Схема рішень даних завдань в більшості випадків полягала в пошуку і виявленні вразливостей системи, а потім в усуненні знайдених «дірок». Тому велике значення придбали різні мережеві сканери та сканери безпеки, системи аудиту подій і його подальшого аналізу. Компанії в максимальному ступені захищали периметр своєї мережі від

стороннього доступу випадкових осіб, реальних хакерів і комп'ютерних вірусів, які проникали в мережу разом з корпоративною поштою або з Інтернету. З кінця 90-х рішення в області інформаційної безпеки від пошуку та усунення "дірок" в системі безпеки переходять у сферу управління ризиками. Для кожної інформаційної системи виробляється аналіз вразливостей і ризиків, при цьому посилюється активний мережевий контроль і ведеться постійне розслідування різних інцидентів. Саме на таких підходах базуються сучасні системи мережевої безпеки [26].

Управління ризиками як фактор оцінки рішень

Вирішуючи проблему безпеки корпоративної мережі, фахівець, що відповідає за вибір того чи іншого рішення, як правило, повинен відшукати «золоту середину» як мінімум у трьох показниках інформаційної системи в цілому. Цими показниками, або характеристиками інформаційної системи є вартість володіння, продуктивність, безпека. Причому всі ці параметри взаємопов'язані. При підвищенні безпеки системи та зниження ризиків вартість системи в цілому зростає, а продуктивність, як правило, знижується. Іншими конфліктуючими параметрами інформаційної системи є відкритість і зручність, з одного боку, і захищеність і надійність - з іншого. Безумовно, задовольнити всі вимоги неможливо - при побудові або модернізації інформаційної системи важливо знайти прийнятний компроміс. Таким чином, побудова безпечної сучасної інформаційної системи - це управління виникаюче внаслідок певних компромісів ризиками.

Управління ризиками варто розглядати в контексті життєвого циклу корпоративної мережі або інформаційної системи в цілому. Саме такий підхід дасть можливість перейти від «латання дірок» і пошуку виходу з надзвичайних ситуацій до дієвого контролю і управлінню безпекою системи. При побудові системи варто задуматися над питаннями доступу до системи. Наскільки ті або інші бізнес-операції і дані критичні? Які

системи і користувачі повинні отримувати доступ до тих чи інших ресурсів компанії? Що є найбільш критичними об'єктами системи?

Ще на етапі планування системи стоїть розробити політики безпеки, визначити порядок робіт (які продукти, як, ким і в якому порядку будуть впроваджуватися), описати планований аналіз інцидентів. На етапі впровадження системи засобами управління і адміністрування вибудувати спланована систему політик безпеки, встановити доступні на поточний момент пакети оновлення і доповнення до всіх застосовуваним рішенням і продуктам в системі, налаштувати мережевий аудит. У ході експлуатації системи необхідний постійний моніторинг і розслідування інцидентів, аналіз зібраного аудиту. На основі цих даних можна буде коригувати політики безпеки, конфігурувати вже впроваджені і додавати нові мережеві рішення. На цьому кроці ми знову переходимо до етапу планування, але вже не системи в цілому, а її доробок і вдосконалення.

Побудова безпечної інформаційної системи на основі управління ризиками неможлива без вивчення досвіду і статистичних даних, отриманих при експлуатації вже існуючих інформаційних систем. Якщо розглянути розподіл втрат в корпоративній мережі за їхніми джерелами, то для сучасних систем буде характерно превалювання втрат, пов'язаних з внутрішніми джерелами і людським фактором. Так, за даними Computer Security Institute, реальні втрати через комп'ютерних вірусів становлять лише 4% від всіх понесених організаціями втрат внаслідок проблем з безпекою інформаційної системи. Через проблеми, пов'язані з фізичним захистом, включаючи електроживлення, втрачається 20%, а через зовнішні напади (у тому числі хакерських атак) - всього 2%. При цьому втрати внаслідок помилок персоналу - 55%, і втрати від зловмисних дій нечесних і скривджених співробітників - 19%. Аналізуючи цю статистику, можна говорити про те, що головна «діра» - беззахисність корпоративної мережі зсередини. Дійсно, завдяки тому, що вся історія побудови безпечної

інформаційної системи пов'язана або з зміцненням захисту по периметру, або з організаційними та фізичними заходами захисту, сьогодні рідко можна побачити корпоративну мережу, яка стійка до злому і атакам зсередини. Звичайно, не варто думати, що сьогодні не потрібна фізична охорона або захист по периметру, але ці заходи безсилі проти внутрішніх загроз і дій самих співробітників. Важливо відзначити, що під атаками і зломом системи зсередини розуміються не стільки дії зловмисників, які підключилися безпосередньо до корпоративної мережі і при цьому є професіоналами в комп'ютерних атаках. Швидше за все, їх якраз небагато. Набагато частіше зустрічаються випадки, коли звичайні співробітники компанії бажають отримати більший доступ до мережевих ресурсів, скористатися заблокованими або недозволеними програмами, або просто через незнання, або всупереч корпоративним інструкціям встановити додаткове програмне забезпечення, «попрацювати» з даними свого колеги. Така атака на корпоративну мережу виникає раптово, без видимих передумов і порівнянна лише з партизанською війною, де немає лінії фронту. Саме таких атак і боїться як вогню будь-який співробітник IT-безпеки. Причина криється в складності і багатофункціональності (одну і ту ж дію можна виконати різними способами) сучасних операційних систем, а також в труднощі надати тільки ті можливості користувачам, які їм дійсно потрібні [28].

«Слабка ланка»: доступ користувача до інформаційної системи за паролем

Надійність інформаційної системи в цілому не може бути вище надійності найслабшої ланки. Саме ця слабка ланка може звести нанівець всі зусилля по зміцненню безпеки всієї системи. Якщо розглядати зміни в способах захисту корпоративної мережі за останні 10 років, то можна з упевненістю сказати, що змінилося практично все, крім одного, - для доступу до мережі користувач повинен набрати на клавіатурі «щось»,

після чого він отримає доступ до всієї своєї інформації. Пароль та ім'я користувача, як правило, є цим «щось», а в деяких компаніях до цих пір можна зустріти порожній пароль навіть для користувачів-адміністраторів та менеджерів вищої ланки. Сьогодні в більшості середніх і великих компаній від простого секретаря до члена ради директорів для входу в мережу всі набирають ім'я і пароль, хоча при цьому володіють відмінним один від одного рівнем повноважень і влади.

На сьогоднішній день однофакторна аутентифікація, заснована на простому паролі, є основною вразливістю багатьох корпоративних мереж і додатків, і інформаційної системи в цілому. Коротко перерахуємо основні причини, за якими пароль в сучасній корпоративній системі неприйнятний для хоч скільки-небудь серйозного рівня захисту.

Зниження впливу людського чинника при аутентифікації

Всі зазначені проблеми аутентифікації користувача за паролем базуються на так званому людському факторі. Для того щоб уникнути описаних вище проблем, необхідно використовувати багатофакторну аутентифікацію, яка базується не тільки на тому, що користувач знає - паролі, але і на тому, що він має - смарт-карта або токен, або на те, чим він володіє - від відбитка пальця і тембру голосу до структури ДНК. Таким чином, найбільш просто значно підвищити стійкість системи аутентифікації користувача - перейти від однофакторної аутентифікації до двухфакторної, наприклад, на основі смарт-карти і PIN-коду (по суті пароля для смарт-карти).

Спеціаліст з проектування інформаційної системи безпеки компанії сьогодні стоїть перед вибором, що використовувати в якості другого чинника - смарт-карти, електронні ключі, токени або біометрію. Сьогодні більшість систем підтримує або біометрію, або смарт-карти і токени. Принципова різниця пристроїв біометрії від смарт-карт і токенів полягає в тому, що біометрія лише із заданою вірогідністю, завжди відмінної від

100%, визначає користувача, що передбачає як помилкові спрацьовування на «чужака», так і можливість відмови у доступі реальному власнику. Більшість сучасних систем побудовано на архітектурі відкритих ключів (PKI) і припускає наявність у користувача захищеного сховища для особистих ключів - смарт-карти або токену, а універсальних систем, що працюють і з тим і з іншим, лічені одиниці.

Крім того, варто врахувати, що закупівельна вартість серйозного рішення на основі біометрії в рази перевищує рішення на смарт-картах або токенах, зіставні по стійкості до злому. Так, наприклад, вартість тільки апаратної частини в розрахунку на одне робоче місце для читання відбитків пальців становить близько 100-140 доларів США, комплект з смарт-карти і зчитувача до неї - 50-70 доларів, а для USB-токена - 40-50 доларів. Виходячи з цих цін стає зрозуміло, що, посилювати безпеку корпоративної мережі, навряд чи варто починати з впровадження біометрії. Можливо, в майбутньому біометрія забере більше місце в рішеннях систем безпеки і без її вживання не буде обходитися жодна система. Проте сьогодні її застосування - скоріше доповнення до чогось, ніж окрема або головна роль.

Всі рішення для управління аутентифікацією користувачів можна розділити на три групи:

- системи управління паролями (password management product, PMP);
- рішення, що реалізують єдиний доступ (single sign-on, SSO);
- інфраструктура управління аутентифікацією (authentication management infrastructure, AMI) [12].

Системи управління паролями

Системи управління паролями (PMP) зберігають пароль у захищеному сховищі, наприклад, смарт-карті або токені. Для передачі такого пароля системі користувач повинен підключити захищене сховище до комп'ютера і ввести PIN-код, який дозволяє взаємодіяти системі зі

сховищем. Рішення з управління паролями, як правило, реалізує наступний набір функцій:

• автоматична синхронізація пароля (якщо пароль змінюється в одній з систем, то він синхронізується з іншими системами);

• сервіс скидання пароля (дозволяє користувачеві скинути і автоматично призначити нові паролі для всіх систем);

• сервіс адміністративного скидання пароля (дозволяє адміністратору системи або офіцеру безпеки скинути і автоматично призначити нові паролі для всіх систем).

Рішення з управління паролями допомагають користувачеві при зміні і призначенні нових паролів, а також істотно спрощують систему синхронізації пароля. Користувач такої системи повинен знати лише PIN-код - пароль для доступу до свого захищеного сховища, і мати саме сховище. Реальні паролі, що знаходяться в самому сховищі і використовувані в процедурах мережевої аутентифікації, користувач не знає. Реальний пароль або паролі можуть генеруватися випадковим чином і бути досить великої довжини - користувачеві їх пам'ятати все одно не доведеться, а зловмиснику безглуздо використовувати атаку за словником. Підвищення зручності у роботі користувача в наявності - немає необхідності пам'ятати безліч паролів та імен входу, необхідно мати ключ або смарт-карту і пам'ятати PIN-код. При такому рішенні користувач вже не може сказати свій пароль колезі, а на ключ як матеріальний об'єкт простіше накласти організаційні заходи, наприклад, отримувати і здавати під розпис. У такий ключ або смарт-карту може бути вбудований і проксіміті-чіп (безконтактна смарт-картка) і на його основі побудований доступ в саме приміщення.

Додатковим плюсом таких рішень є відносна простота їх впровадження. Як правило, всі рішення базуються на клієнті та станції адміністратора і практично не зачіпають сервер - не вимагають постійно

запущених на сервері модулів. У більшості випадків дані рішення не вимагають впровадження інфраструктури відкритих ключів (PKI), що, з одного боку, скорочує час і знижує вартість впровадження, але з іншого - не веде до значного посилення безпеки, оскільки не змінює докорінно процедури аутентифікації, базуючись на вже прийнятих процедурах і стандартах, розширюючи і доповнюючи їх.

Сьогодні існує велика кількість рішень, побудованих на принципах, описаних вище. Більшість таких рішень вбудовується в існуючі процедури аутентифікації або базується на можливостях розширення цих процедур.

При виборі системи управління паролями варто звернути увагу, чи не дасть вбудована система додаткових вразливостей в існуючий захист. Вбудована система не повинна змінювати щось у ядрі операційної системи - хоча деякі системи і міняють Microsoft GINA і деякі системні бібліотеки DLL; строго кажучи, таке вбудовування не можна назвати надійним. Оскільки Microsoft перешкоджає подібного підходу, при установці оновлень до операційної системи і пакетів оновлень можуть виникати серйозні проблеми. Варто звернути увагу на використовувані модулів для шифрування хеш-функцій. Встановлювана система повинна використовувати вбудовані рішення криптосервіспровайдерів (CSP) або додавати свої. Важливо також відзначити, що вбудовується система повинна бути перевірена на відсутність конфліктів і стійку працездатність з поточними механізмами захисту, наприклад, міжмережевим екранами [14, 13].

Інфраструктура управління аутентифікацією

Описані вище рішення так чи інакше пов'язані з паролем. Ці системи замінюють пароль, записують в захищене сховище, накладають політики, синхронізують і скидають. Проте всі вони так чи інакше прив'язані до одного і того ж фактору - паролю. Тому хоча користувач буде мати двухфакторну аутентифікацію і реальний пароль буде збережений у

надійному сховищі, все ж частина вразливостей системи і атак, наприклад, побудованих на ловлі пароля по мережі, потенційно залишається, і зловмисники можуть скористатися такими лазівками. Ні для кого не секрет, що вже зараз існує клас систем, що реалізують аутентифікацію користувача за допомогою цифрового сертифіката та особистого ключа, що базуються на технології PKI. Такі системи реалізують новий підхід до побудови аутентифікації в цілому і роблять принципово недоступними старі технології атаки на систему. Одними з важливих елементів технології PKI є центр сертифікації (ЦС), який реалізує виписку і відгук сертифікатів, і сховище сертифікатів, вирішальна доступність відкритого ключа та списку відкликаних сертифікатів. При цьому передбачається, що користувач зберігає свій особистий ключ у захищеному сховищі - смарт-карті або електронному ключі, доступ до якого неможливий без знання PIN-коду. Більшість таких систем пропонує власну реалізацію всіх компонентів системи, за винятком захищеного сховища. Безумовно, це може бути зручно, якщо ви користуєтеся тільки однією такою системою [7].

Хорошим прикладом, що ілюструє переваги та недоліки такого підходу, може бути система аутентифікації по смарт-карті в мережі Microsoft Windows 2000. Дана технологія має назву SmartCard-Logon. Для реалізації рішення необхідно встановити і налаштувати сервер сертифікатів - він здійснюватиме виписку і відгук сертифікатів. При цьому відкриті частини всіх виписаних сертифікатів будуть публікуватися в службі каталогу - Active Directory, а особисті ключі - в смарт-картах. На перший погляд рішення просто і відносно легко для впровадження в корпоративній мережі. Але це рішення застосовано, якщо вся мережа побудована на серверах Windows 2000 і в якості робочих місць використовуються станції тільки Windows 2000 або Windows XP. Однак у більшості корпоративних інформаційних систем це не так - мережі

гетерогенні, що не дозволяє реалізувати дане рішення. Інша важлива проблема для реалізації подібного рішення - відсутність доцільності мати на всіх робочих місцях операційні системи Windows 2000 або XP і захищений вхід по смарт-карті, так як не всі користувачі працюють з критично важливими даними. Також дане рішення не дозволить пройти аутентифікацію користувачеві, чиє робоче місце не підключено до мережі. Це створює неможливість застосування даного рішення для співробітників компанії, що працюють поза офісом.

При необхідності додати в таку систему аутентифікацію на основі біометрії, одноразових паролів або будь-якого іншого пристрою, відмінного від підтриманого стандартно Microsoft, фахівець з безпеки зіткнеться з проблемами сумісності стандартного клієнта Microsoft з рішеннями третіх виробників. Як правило, розширення подібного клієнта будується на недокументованій можливості та швидше завдає шкоди безпеці. Ще однією серйозною проблемою, буде відсутність єдиної точки адміністрування. Частина користувачів, що використовують паролі і смарт-карти для входу в мережу, доведеться адмініструвати за допомогою стандартних утиліт Microsoft, а інша частина користувачів буде недоступна для адміністрування за допомогою цих утиліт. Відсутність єдиної точки адміністрування користувачів сильно ускладнить адміністрування системи і може призвести до серйозних помилок. Тому при виборі системи вкрай важливо мати єдину точку адміністрування, особливо систем з великою кількістю користувачів. Враховуючи проблеми, описані вище, дане рішення, що базується на стандартних можливостях Windows 2000 і умовно-безкоштовне для власників цих систем, не набуло широкого поширення.

Виходячи з описаного вище прикладу, можна уявити, яким вимогам повинна відповідати система, що надає інфраструктуру управління аутентифікацією (AMI), для задоволення більшості сучасних потреб

середнього та великого підприємства. Дана система безумовно повинна базуватися на технології PKI, при цьому вкрай бажано, щоб така система могла не тільки мати свій центр сертифікатів, а й інтегруватися з зовнішнім центром сертифікатів. У першому випадку це важливо, якщо в корпоративній мережі в поточний момент відсутній центр сертифікатів або компанія не передбачає задіяти зовнішні центри сертифікатів, наприклад, з причини їх дорожнечі. У другому випадку, якщо вже в організації існують які-небудь рішення на PKI-технології, то впроваджувана система не повинна ламати усталені рішення. Впроваджувана система інфраструктури управління аутентифікацією повинна щільно інтегруватися з будь службою каталогу, де і будуть розміщуватися публічні частини системи. Враховуючи, що більшість корпоративних систем гетерогенна, такий каталог не повинен бути прив'язаний до однієї з платформ, а представляти кроссплатформне рішення.

Одним з обов'язкових вимог до каталогу, на якому базуватиметься AMI, повинна бути можливість роботи з LDAP, протоколом, по суті стати стандартом для взаємодії багатьох додатків зі службою каталогу. Бажана повна підтримка специфікації LDAP v3, що зробить можливим SASL (Simple Authentication and Security Layer) аутентифікацію в службі каталогу.

Ще одним з бажаних вимог також є підтримка градуйованої (ступінчастої) аутентифікації на рівні служби каталогу. Зазначеним вище вимогам повністю відповідають такі каталоги, як Sun ONE і eDirec-tory, - ці каталоги повністю підтримують специфікацію LDAP v3 і градульовану (ступеневу) аутентифікацію. Однак eDirectory має переваги в силу своєї багатоплатформеності і низької вартості [3].

Система інфраструктури управління аутентифікацією повинна сама бути кросплатформним продуктом, що дозволить легко впроваджувати таку систему в гетерогенній інформаційній системі підприємства. Оскільки

дана система являє «ворота аутентифікації», то вона повинна підтримувати багатофакторну аутентифікацію, побудовану на різних методах - від простого пароля до смарт-карт і біометрії. Безумовно, в такій системі важливу роль відіграватиме підтримка різних вендорів виробників устаткування і рішень для аутентифікації. Така підтримка повинна бути побудована на принципах модульності і відкритих інтерфейсів взаємодії між системою і апаратними рішеннями. Наприклад, взаємодія з широким класом смарт-карт і електронних ключів може бути побудовано на основі стандарту PKCS # 11. Такий підхід дозволить з легкістю переходити на сучасні пристрої і при цьому не потребуючи перепрошивання програмних модулів.

1.2 Атаки на мережу Wi-Fi

Популярність бездротових технологій і розширення мобільного робочого простору сприяють становленню нового типу рівня доступу. "Корпорація, яка скрізь зі мною". - Все частіше так називають архітектуру, яка безпечно і надійно надає користувачеві корпоративну інфраструктуру скрізь - в офісі компанії, на віддалених сайтах, вдома, в будь-якому місці, де є доступ до інтернету. Однак мобільність, включаючи бездротові технології, має потенціал створювати умови, за яких можливий несанкціонований доступ в мережу, можливі втрати закритої інформації, а також можливі умови для проникнення в мережу вірусів і черв'яків. Якісне та повноцінне планування дозволяє уникати ці проблеми без надмірних капітальних і операційних витрат.

Якщо бездротова мережа доступу розгорнута, вона повинна моніторитись і захищатися проти хакерських атак. Діапазон їх варіюється від генерації простого широкосмугового шуму за допомогою радіоджаммерів до витончених атак типу «людина в промежку» (man in the middle / MITM), де атакуючий створює ситуацію, входячи в

комунікаційний шлях і отримуючи можливість додавати, видаляти або модифікувати дані.

Використання шифрування трафіку і аутентифікації усуває багато проблем, але важливо не забувати про більш просунуті технології нашого часу. Це, наприклад, системи запобігання вторгнень (IPS / Intrusion Prevention System), необхідні для виявлення і запобігання атак. Системи IPS давно існують і чудово себе показали не тільки в дротовому, але і в бездротовому світі. IPS дозволяє не витрачати значуще час на спроби вирішення проблем із з'єднанням у WLAN, в той час як фактична проблема, наприклад, у вже розпочатій атаці.

Побудова ефективної системи безпеки - це не просто покупка якоїсь системи, наприклад, IPS. Це комплексний проект, що включає в себе вирішення великої кількості завдань - від вдумливого проектування прав доступу і списків доступних ресурсів для кожного користувача до введення практики постійного відстеження рівня безпеки власної інфраструктури для виявлення слабких місць і розробки плану реакції на атаки і порушення безпеки. [23]

Деякі загальні спостереження:

1. Беручи до уваги загальні мережні рівні дротової і бездротової мережі, більшість атак, застосовуваних до провідної мережі, будуть працювати і проти бездротових клієнтів.

2. Через природу Радіо виявлення зловмисника, ворожої точки доступу або інфікованого комп'ютера й запобігання спроб доступу або атак може бути складним.

3. Керовані Точки Доступу і централізована архітектура є критичними факторами забезпечення безпеки.

Як вже було відмічено раніше, більшість відомих атак застосовується як в провідний, так і в бездротової мережі, тому проведемо комплексний аналіз аспектів мережевої Безпеки з урахуванням особливостей

бездротової мережі Wi-Fi. Розглянемо докладніше основні аспекти Мережевих Атак

Загальна класифікація мережевих атак

Одне з визначень мережевої атаки - мережева атака може бути визначена як будь-який метод, процес або засіб, що використовується для виконання зловмисної спроби порушення мережевої безпеки.

Існує багато причин, по яких люди хочуть атакувати корпоративні мережі. Людей, які проводять мережеві атаки часто називають хакерами або кракерами.

У цілому Мережеві атаки можна класифікувати чотирма типами:

1. Внутрішні небезпеки.
2. Зовнішні небезпеки.
3. Структуровані небезпеки.
4. Неструктуровані небезпеки.

> **Зовнішні небезпеки (і зовнішні атаки):** коли зовнішні атаки виконуються без участі внутрішніх співробітників. Такі атаки організовуються і виконуються досвідченими индивидуалами або їх групами, організаціями хакерів, а іноді і не досвідченими «новачками». Атакуючі зазвичай мають план і відповідний інструментарій, володіють відповідними стратегіями для виконання атаки. До основних характеристик зовнішніх атак можна віднести використання сканування системи та збір інформації. Таким чином можна визначати зовнішні атаки шляхом ретельного аналізу логів міжмережевих екранів. Для швидкої і зручної ідентифікації зовнішніх атак хороший підхід полягає в розгортанні системи запобігання вторгнень IPS. Для мереж Wi-Fi виробники рішень корпоративного класу запропоновують якісні і просунуті системи IPS, здатні не тільки пасивно моніторити інфраструктуру і ефір і виявляти атаки по шаблонах, а й активно протидіяти їм (приклади: трасування портів на комутаторах, до яких приєднані чужі пристрої, і блокування

даних портів; посилка фреймів деаутентіфікації від імені ворожого пристрою, який виконує атаку типу MITM і до якого приєдналися легітимні клієнти мережі тощо).

Зовнішні атаки можна розділити на структуровані атаки і неструктуровані атаки:

>> Зовнішні структуровані атаки: Цей тип атак ініціюється зловмисними индивидуалами або організаціями. Структуровані атаки зазвичай ініціюються з якоїсь мережі і мають продумані заздалегідь цілі, на які планується впливати для руйнування, пошкодження і т.п. Можливі мотиви:

- Бажання наживи;
- Політичні мотиви;
- Ідеологічні мотиви (тероризм, расизм);
- Мотиви помсти («розборки»).

Атакуючі в даному випадку звичайно мають великі знання в дизайні мереж, обході систем безпеки, включаючи обхід IDS (Intrusion Detection Systems), і мають просунутий інструментарій для злому. У їх арсеналі необхідні знання для розробки нових стратегій мережевих атак і можливість модифікації існуючого хакерського інструментарію під свої завдання. У деяких випадках внутрішній персонал компанії з правами доступу може допомагати атакуючим.

>> Зовнішні неструктуровані атаки: Такі атаки ініціюються зазвичай недосвідченими хакерами, аматорами. При такому підході атакуючий використовує простий інструментарій хакерського злому або скрипти, доступні в Інтернеті, для виконання мережевої атаки. Рівень знань атакуючого зазвичай низький для створення серйозної небезпеки. Нерідко це просто нудьгуючі молоді люди, які шукають слави шляхом злому корпоративного веб-сайту або іншої відомої мети в Інтернеті.

Зовнішні атаки можуть здійснюватися віддалено або локально

(часто зсередини мережі):

>> **Зовнішні віддалені атаки**: Такі атаки зазвичай націлені на послуги, які організація пропонує відкрито і публічно. Існують різні форми таких атак:

– Дистанційні атаки, націлені на сервіси, доступні для внутрішніх користувачів. Такі атаки зазвичай трапляються, коли відсутні міжмережеві екрани для захисту таких внутрішніх сервісів.

– Дистанційні атаки націлені на розташування точок входу в корпоративну мережу (бездротові мережі доступу, порти, модемні пули).

– Атаки типу відмова в обслуговуванні (DoS) для створення перевантаження процесорів на серверах тощо з метою формування ситуації, коли авторизовані користувачі не можуть користуватися послугами.

– Дзвінки на корпоративну телефонну станцію, (PBX).

– Спроби злому паролів систем аутентифікації.

>> Зовнішні локальні атаки (атаки зсередини): такі атаки зазвичай починаються, коли відкритий доступ в комп'ютерні приміщення, та можна отримати доступ до будь-якої системі.

> Внутрішні атаки: часто ініціюються незадоволеними або скривдженими на компанію колишніми або діючими співробітниками чи позаштатним персоналом. Внутрішні атакуючі мають ту чи іншу форму доступу до системи і зазвичай намагаються приховати атаку і видати її за звичайний робочий процес. Наприклад, нелояльний співробітник має доступ до будь-яких ресурсів внутрішньої мережі. Він може мати навіть деякі адміністративні права в мережі. Тут один з кращих підходів полягає в розгортанні системи виявлення вторгнень IDS (або IPS) і конфігуруванні її для сканування системи на предмет як зовнішніх, так і внутрішніх атак. Всі форми атак повинні бути занесені в журнал, ці логи необхідно перевіряти, розбиратися і вживати заходів щодо захисту від подібного надалі.

Важливо чітко розуміти, що мережеві атаки - це серйозна небезпека. Наступні основні компоненти повинні бути включені в дизайн мережі для побудови системи мережевої Безпеки:

- Запобігання мережевих атак,
- Визначення мережевих атак,
- Ізоляція мережевих атак,
- Відновлення від наслідків мережевих атак.

Крім описаних вище небезпек, велике поширення має створення широкосмугових перешкод за допомогою радіо-джаммерів. Це еквівалент DoS-атаки, але тільки на фізичному рівні радіосередовища. Протистояти подібного роду атаці засобами інфраструктури Wi-Fi практично неможливо, якщо потужність випромінювання висока, але можна використовувати спеціальні технології для ідентифікації типу пристрою, що створює перешкоди та визначення його фізичного місця розташування в зоні покриття. Наприклад, це може бути виконано з великою ефективністю у разі, якщо мережа побудована на обладнанні Cisco Systems і Точки Доступу підтримують технологію CleanAir (модельні ряди 3500, 3600, 1550). Після виявлення місця розташування випромінювача, в дану точку можуть бути направлені співробітники служби безпеки для фізичного усунення проблеми. Природно, подібні дії повинні бути сплановані та погоджені заздалегідь.

Існують програмні інструменти, доступні в Інтернеті, які можуть ініціювати DoS-атаки:

- Bonk
- LAND
- Smurf
- Teardrop
- WinNuke

Атакуючий може посилити потужність атаки DoS, використовуючи

безліч комп'ютерів проти однієї мережі. Цей тип атаки відомий як Розподілена відмова в обслуговуванні (distributed denial of service / DDoS). Мережеві адміністратори можуть зіткнутися з великими складнощами при відображенні DDoS-атаки, так як відповідний вплив на всі атакуючі комп'ютери може вести і до блокування нормальних авторизованих користувачів (найчастіше в DDoS-атаці беруть участь комп'ютери, на які хакер заздалегідь нелегально встановив відповідне програмне забезпечення для виконання DoS-атаки під єдиним віддаленим керуванням).

Атака «Людина в проміжку» (Man in the middle / MITM): атака типу MITM виникає, коли хакер прослуховує захищену комунікаційну сесію і може бачити, копіювати і контролювати всі дані, якими обмінюються дві частини комунікаційного каналу. Атакуючий має можливість отримувати інформацію, виступаючи і за відправника і за одержувача даних. Для того, щоб атака типу MITM стала успішною, необхідно виконання наступної послідовності дій:

- Хакер повинен отримати доступ до комунікаційної сесії для перехоплення трафіку, коли відправник і одержувач встановлять безпечне з'єднання.

- Хакер повинен мати можливість перехоплення повідомлень, що відправляються між частинами з'єднання, і потім можливість відправляти повідомлення заново, щоб сесія підтримувалася в активному стані.

Існують деякі відкриті криптографічні системи, наприклад, обмін ключами по Diffie-Hellman/DH, які досить слабкі для атак типу MITM. Це пов'язано з тим, що метод DH не використовує аутентифікацію.

Наступні програмні інструменти можуть бути використані для проведення атак типу MITM:

– Dsniff;

– Ettercap;

– Під Windows: Cain & Abel.

Ідентифікація небезпек для бездротових мереж

Атаки прослуховування (Eavesdropping): хакер намагається перехопити трафік, коли він передається між комп'ютером з підтримкою Wi-Fi до Точці Доступу.

Маскування (Masquerading): тут хакер маскується і видає себе за авторизованого користувача бездротової мережі для доступу до мережевих ресурсів і сервісів.

Атаки Відмова в обслуговуванні (Denial of service / DoS): хакер намагається створити ситуацію, коли авторизовані користувачі бездротової мережі не можуть отримувати доступ до мережевих ресурсів, використовуючи передавач для блокування доступних частот (наприклад, це може бути джаммер, що створює широкосмуговий шум, як було описано вище).

Атаки «Людина в проміжку» (Man-in-the-middle/MITM): якщо зловмисник успішно почав атаку типу MITM, то він може отримати можливість відтворити і модифікувати комунікації в бездротової мережі.

Атаки на бездротових клієнтів: атакуючий починає мережеву атаку на працюючий комп'ютер з бездротовим інтерфейсом, який приєднаний до недовірених бездротової мережі.

Для захисту бездротових мереж від мережевих атак можна використовувати наступні стратегії:

Необхідно, щоб усі бездротові комунікації були автентифіковані і зашифровані. Найбільш загальні технології, які використовуються для захисту бездротових мереж від проблем безпеки, - це:

– Wired Equivalent Privacy / WEP (вкрай не рекомендується до використання, оскільки може бути зламана за кілька хвилин);

– Wi-Fi Protected Access / WPA (краще використовувати WPA2 с шифруванням AES);

– IEEE 802.1x.

– оновлення програм і драйверів для бездротових пристроїв.

– Розмістити безпровідну мережу в спеціальній бездротовій демілітаризованій зоні (WDMZ). Маршрутизатор або міжмережевий екран повинні ізолювати WDMZ від захищеної корпоративної мережі. DHCP-служба не повинна використовуватися в WDMZ.

– Для гарантування високого рівня безпеки WLAN всі бездротові пристрої повинні підтримувати 802.1x аутентифікацію з використанням EAP (Extensible Authentication Protocol) і шифрування AES. При цьому важливо використовувати версії EAP с формуванням тунелю, наприклад, EAP-TLS, EAP-TTLS і т.п. (І не використовувати версії EAP, які не формують тунель, наприклад, EAP-MD5 і т.п.).

– В ідеалі, організувати захищений канал комунікацій взаємодії контролера WLAN або точок доступу (при централізованій або автономній архітектурі WLAN відповідно) з AAA-сервером, наприклад, за допомогою IPSec.

– Адміністративні паролі для управління контролера або точки доступу повинні бути складними та довгими.

– У разі використання веб-інтерфейсу для управління контролерами та іншими пристроями використовувати тільки HTTPS (і НЕ використовувати звичайний HTTP).

– У разі використання термінального доступу для управління використовувати SSH (і НЕ використовувуватие telnet).

– SSID не повинен містити назву компанії, адресу компанії або будь-яку іншу ідентифікаційну інформацію.

Для захисту мережі від небезпеки найпростіших способів збору інформації має сенс вимкнути трансляцію SSID. Але це не врятує від досвідченого зломщика.

Визначення вимог до безпеки для різних типів даних

Для визначення вимог до забезпечення безпеки різних типів даних дуже зручно виділити категорії інформації наступним чином:

Відкриті, публічні дані (Public data): ця категорія включає всі дані, які вже публічно доступні на корпоративному веб-сайті компанії або в друкованих виданнях. Так як це відкрита інформація, немає ризику, пов'язаного з тим, що ці дані можуть бути вкрадені. Однак необхідно підтримувати цілісність публічних даних, так як будучи розділеними на частини і вирваними з основного контексту вони можуть істотно спотворити зміст.

Приватна інформація (Private data): дані, які потрапляють в таку категорію, зазвичай добре відомі всередині компанії, але не відомі широкій публіці. Типовий приклад - це дані корпоративного інтранету.

Конфіденційна інформація (Confidential data): дані, які потрапляють в цю категорію, повинні бути захищені від неавторизованого доступу. Організація практично завжди несе втрати, якщо конфіденційна інформація перехоплена зловмисниками.

Секретні дані (Secret data): дані, які більш закриті, ніж конфіденційна інформація. Секретні дані зазвичай включають в себе торгові секрети, інформацію про нові продукти, інформацію по стратегії бізнесу, патентну інформацію. Секретні дані повинні мати вищий рівень забезпечення безпеки.

1.3 Стандартні методи захисту

Парольний захист заснована на тому, що для використання будь-якого ресурсу необхідно задати деяку комбінацію символів (пароль), що відкриває доступ до цього ресурсу. За допомогою паролів захищаються файли, особисті чи корпоративні архіви, програми та окремі комп'ютери. Недоліки такого захисту: слабка захищеність коротких паролів, які за

допомогою спеціальних програм на високопродуктивних комп'ютерах досить швидко розкриваються простим перебором. У мережах паролі використовуються як самостійно, так і в якості основи для різних методів аутентифікації. При виборі паролю потрібно дотримуватися ряду основних вимог:

– в якості пароля не може використовуватися слово з якої б то не було мови;

– довжина пароля не може бути менше 8 символів;

– Один і той же пароль не може бути використаний для доступу до різних ресурсів;

– старий пароль не повинен використовуватися повторно;

– пароль повинен мінятися якомога частіше.

Ідентифікація являє собою процедуру розпізнавання користувача (процесу) за його іменем. Для користувачів мережі вона може бути реалізована програмно або апаратно. Апаратна реалізація заснована на застосуванні для ідентифікації користувачів спеціальних електронних карт, що містять ідентифікаційну конкретного користувача інформацію (подібно банківськими кредитними картками). Системи ідентифікації користувачів, реалізовані апаратно, є більш

надійними, ніж парольний захист.

Розмежування прав доступу користувачів до ресурсів мережі - метод, заснований на використанні таблиць або наборів таблиць, що визначають права користувачів, побудований за правилами «дозволено все, крім" або "дозволено тільки». Таблиці за ідентифікатором або паролі користувача визначають його права доступу до дисків, розділам диска, конкретним файлів або їх групам, операціям запису, читання або копіювання та інших ресурсів мережі. Можливість такого розмежування доступу визначається, як правило, можливостями використовуваної операційної системи та закладені саме в ній. Більшість сучасних

мережевих ОС передбачають розмежування доступу, але в кожній з них ці можливості реалізовані в різному обсязі та різними способами.

Використання закладених в ОС можливостей захисту - це обов'язкове правило. Однак більшість ОС або мають мінімальний захист, або надають можливості її реалізації додатковими засобами.

Міжмережеві екрани

При підключенні корпоративної мережі до відкритих мереж, наприклад до мережі Internet, з'являються загрози несанкціонованого вторгнення в закриту (внутрішню) мережу з відкритої (зовнішньої), а також загрози несанкціонованого доступу із закритої мережі до ресурсів відкритої. Подібний вид загроз характерний також для випадку, коли об'єднуються окремі мережі, орієнтовані на обробку конфіденційної інформації різного рівня секретності.

Через Internet або іншу відкриту зовнішню мережу порушник може вторгнутися у внутрішню мережу підприємства і отримати несанкціонований доступ до конфіденційної інформації і технічних ресурсів, отримати паролі, адреси серверів, а часом і їх вміст, увійти в інформаційну систему підприємства під ім'ям зареєстрованого користувача і т.п. Загрози несанкціонованого доступу в зовнішній мережй з внутрішньої мережі актуальні в разі обмеження дозволеного доступу в зовнішню мережу правилами, встановленими в організації. Боротися з розглянутими загрозами безпеки міжмережевої взаємодії засобами універсальних операційних систем не представляється можливим. Ряд завдань з відбиття найбільш ймовірних загроз для внутрішніх мереж здатні вирішувати міжмережеві екрани (брандмауери, *firewall*). Поза комп'ютерною мережею терміном *firewall* називають стіну, зроблену з негорючих матеріалів що перешкоджає поширенню пожежі. У сфері комп'ютерних мереж міжмережевий екран є бар'єр, що захищає від фігуральної пожежі - спроб зловмисників вторгнутися у внутрішню

мережу. Міжмережевий екран (МЕ) покликаний забезпечити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Міжмережевий екран - це програмна або програмноапаратна система міжмережевого захисту, що дозволяє розділити дві (або більше) взаємодіючі мережі і реалізувати набір правил, що визначають умови проходження пакетів з однієї мережі в іншу.

Рис. 1.4. Схема розташування брандмауера

Для протидії несанкціонованого міжмережевого доступу він повинен розташовуватися між захищаючою мережею організації, що є внутрішньою, і потенційно ворожою зовнішньою мережею (рис. 1.4, хоча подібними екранами можна розділити один від одного внутрішні локальні мережі. Якщо корпоративна мережа складається з ряду віддалених локальних мереж (ЛОМ1, ЛОМ2,...), з'єднаних між собою засобами глобальних мереж, то міжмережеві екрани ставляться в кожній локальної мережі на кордоні з глобальною (рис. 1.5).

Рис. 1.5. Схема захисту ЛОМ корпоративної мережі

Головний аргумент на користь застосування міжмережевих екранів полягає в тому, що без них внутрішня мережа піддається небезпеці з боку мало захищених служб мережі Internet. Міжмережевий екран пропускає через себе весь трафік, приймаючи щодо кожного пакету, рішення - пропускати його або відкинути. Для того щоб МЕ міг здійснити це, йому необхідно визначити набір правил фільтрації відповідно до прийнятої політикою мережевої безпеки.

Політика безпеки включає дві складові: політика доступу до мережевих сервісів і політика реалізації міжмережевих екранів. Відповідно до прийнятої політики доступу до мережевих сервісів визначається список сервісів Internet, до яких користувачі повинні мати обмежений доступ.

Міжмережевий екран може реалізовувати ряд політик доступу до сервісів, проте зазвичай політика заснована на одному з наступних принципів:

– заборонити доступ з Internet у внутрішню мережу і дозволити доступ з внутрішньої мережі в Internet;

– дозволити обмежений доступ у внутрішню мережу з Internet, забезпечуючи роботу тільки окремих «авторизованих» систем, наприклад, інформаційних та поштових серверів.

У відповідності з політикою реалізації міжмережевих екранів визначаються правила доступу до ресурсів внутрішньої мережі. Ці правила повинні базуватися на одному з наступних принципів:

– забороняти все, що не дозволено в явній формі;

– дозволяти все, що не заборонено в явній формі.

Ефективність захисту внутрішньої мережі за допомогою міжмережевих екранів залежить не тільки від обраної політики доступу до мережевих сервісів і ресурсів внутрішньої мережі, але і від раціональності вибору і використання основних компонентів брандмауера.

Функціональні вимоги до міжмережевих екранів включають в себе: вимоги до фільтрації на мережевому, сеансовому та прикладному рівнях моделі OSI/ISO; вимоги з налаштування правил фільтрації та адміністрування; вимоги до засобів мережевої аутентифікації; вимоги щодо впровадження журналів обліку та збору статистики та інші функції.

Міжмережеві екрани можна класифікувати за такими ознаками: місцем їх включення; рівню фільтрації, відповідної еталонної моделі OSI/ISO; вимогам до показників захищеності. За першою ознакою МЕ поділяються на зовнішні і внутрішні. Зовнішні забезпечують захист від зовнішньої мережі, внутрішні розмежовують доступ між сегментами корпоративної мережі.

Робота всіх міжмережевих екранів заснована на використанні інформації різних рівнів еталонної моделі OSI і пятирівневій моделі сімейства протоколів Internet. Як правило, чим вище рівень, на якому міжмережевий екран фільтрує пакети, тим вище ним забезпечується рівень захисту. За рівнем фільтрації моделі OSI міжмережеві екрани поділяють на чотири типи:

- міжмережеві екрани з фільтрацією пакетів (фільтруючі або екрануючі маршрутизатори);
- шлюзи сеансового рівня;

- шлюзи прикладного рівня;
- міжмережеві екрани експертного рівня додатків.

Міжмережеві екрани з фільтрацією пакетів являють собою фільтруючі (екрануючі) маршрутизатори, сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети. Тому такі екрани називають іноді пакетними фільтрами. Фільтрація здійснюється аналізом IP-адреси джерела і приймача, а також портів вхідних TCP-і UDP-пакетів та порівнянням їх з сконфігурованою таблицею правил. Дані системи прості у використанні, дешеві, надають мінімальний вплив на продуктивність мереж. Основним їх недоліком є вразливість для заміни адрес IP.

Шлюзи сеансового рівня контролюють допустимість сеансу зв'язку. Вони стежать за підтвердженням зв'язку між взаємодіючими процесами, визначаючи, чи є викликаний сеанс зв'язку допустимим. При фільтрації пакетів шлюз сеансового рівня грунтується на інформації, що міститься в заголовках пакетів сеансового рівня протоколу TCP.

Шлюзи прикладного рівня перевіряють вміст кожного проходячого через шлюз пакету і можуть фільтрувати окремі види команд або інформації в протоколах прикладного рівня, які їм доручено обслуговувати. Це більш досконалий і надійний тип брандмауера, що використовує програми-посередники прикладного рівня або програми-агенти. Агенти формуються для конкретних служб Internet (HTTP, FTP, Telnet і т.д.) з метою перевірки мережевих пакетів на наявність достовірних даних. Однак шлюзи прикладного рівня знижують продуктивність системи. Міжмережеві екрани експертного рівня поєднують в собі елементи маршрутизаторів, що екранують та прикладних шлюзів. Хоча міжмережевий екран є важливим і досить надійним засобом захисту корпоративної мережі від несанкціонованого доступу, він не може гарантувати повного захисту. Наявність екрану є необхідним, але не достатнім засобом забезпечення безпеки мережі.

Захищені віртуальні мережі VPN

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання глобальних відкритих мереж на початку 90-х років народилася і активно розвивається концепція побудови захищених віртуальних приватних мереж VPN (Virtual Private Networks). В основі концепції лежить досить проста ідея: якщо в глобальній мережі є два вузла, які хочуть обмінятися інформацією, то для забезпечення конфіденційності та цілісності переданої по відкритих мережах інформації між ними необхідно побудувати віртуальний тунель, доступ до якого має бути надзвичайно затруднений всім можливим активним і пасивним зовнішнім спостерігачам. Термін «віртуальний» вказує на те, що з'єднання між двома вузлами мережі не є постійним (жорстким) і існує тільки під час проходження трафіку по мережі.

Переваги таких віртуальних тунелів, полягають, перш за все, в значній економії фінансових коштів. Це пояснюється тим, що відпадає необхідність побудови або оренди дорогих виділених каналів зв'язку, а для створення власних мереж використовуються дешеві Internet-канали, надійність і швидкість передачі яких в більшості своїй сьогодні вже не поступаються виділеним лініям.

Захищеною віртуальної мережею VPN називають з'єднання локальних мереж і окремих комп'ютерів через відкриту зовнішню середу передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку даних. Ефективність віртуальної приватної мережі VPN визначається ступенем захищеності інформації, що циркулює по відкритих каналах зв'язку. Захист інформації в процесі її передачі по відкритих каналах заснована на побудові захищених віртуальних каналах зв'язку, званих тунелями VPN. Тунель VPN представляє собою з'єднання, проведене через відкриту мережу, по якому передаються криптографічно захищені пакети повідомлень віртуальної мережі.

За допомогою цієї методики пакети даних передаються через загальнодоступну мережу як в звичайному двоточковому з'єднанні. Між кожною парою «відправник-одержувач» встановлюється своєрідний тунель - безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

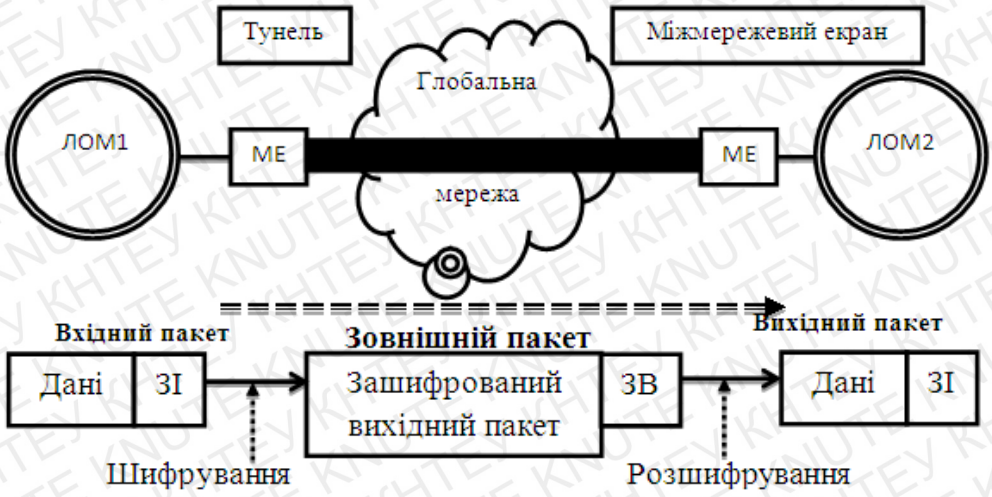


Рис. 1.6 Схема віртуального тунелю

Суть тунелювання полягає в тому, щоб «упакувати» передану порцію даних (разом зі службовими полями) в новий «конверт». Щоб забезпечити конфіденційність переданих даних, відправник шифрує вихідний пакет разом із заголовком, упаковує його в поле даних зовнішнього пакета з новим відкритим IP-заголовком і відправляє по транзитній мережі. Схема віртуального тунелю представлена на малюнку 1.6 (де ЗІ - заголовок вихідного пакета, ЗВ - заголовок зовнішнього пакета). Для транспортування даних по відкритій мережі використовуються відкриті поля заголовка зовнішнього пакета. Для зовнішніх пакетів використовуються адреси прикордонних маршрутизаторів, встановлених на початку і кінці тунелю, а внутрішні адреси кінцевих вузлів містяться у внутрішніх вихідних пакетах в захищеному вигляді. Після прибуття в кінцеву точку захищеного каналу із зовнішнього пакета витягують і розшифровують внутрішній вихідний пакет і використовують його відновлений заголовок для подальшої передачі по внутрішній мережі.

Тунелювання може використовуватися не тільки для забезпечення конфіденційності та цілісності всієї переданої порції даних, але і для організації переходу між мережами з різними протоколами (наприклад, IPv4 і IPv6), а також різними технологіями і системою адресації.

Забезпечення безпеки в бездротових мережах

Питання забезпечення безпеки в бездротових мережах стоїть гостріше, ніж в дротяних. Радіус дії бездротових мереж типу 802.11 може складати сотні метрів, тому зловмисник, охочий перехопити інформацію, може просто приїхати на автомобілі до будівлі, включити в машині ноутбук з прийомопередатчиком і весь трафік, що проходить по локальній мережі всередині будівлі, може бути перехоплений. При використанні бездротових мереж можуть бути наступні види ризиків:

1. Розкрадання послуг. Зловмисник може отримати доступ до Інтернету.

2. Відмова в послугах. Хакер може стати джерелом великої кількості запитів на підключення до мережі, в результаті чого утруднити підключення законних користувачів.

3. Розкрадання або руйнування даних. Зловмисник, підключившись до мережі, може отримати доступ до файлів і папок, а отже отримати можливість копіювання, модифікації і видалення.

4. Перехоплення контролю над мережею. Зловмисник, використовуючи слабкі місця в системі безпеки, може впровадити троянського коня або призначити такі права доступу, які можуть призвести до незахищеності комп'ютера від атак з мережі Інтернет.

Розробкою специфікацій бездротових мереж займається група 802.11x інституту IEEE. Всі технічні деталі стандарту, в тому числі і щодо забезпечення безпеки, поміщаються на web-сайті групи http://www.ieee802.org/11, а також на сайті http://www.wi-fi.org. Стандарт 802.11 описує протокол безпеки рівня передачі даних під назвою WEP

(Wired Equivalent Privacy - таємність, еквівалентна дротовим мережам), призначені для того, щоб убезпечити бездротові ЛОМ так само надійно, як і дротяні. За наявності системи безпеки в мережі 802.11 кожна станція має загальний закритий ключ з базовою станцією. Метод розповсюдження ключів стандартом не обмовляється. Ними можна обмінятися заздалегідь по провідній мережі. При обміні інформацією базова станція, або призначена для користувача машина може випадковим чином вибирати ключ і відсилати його протилежній стороні, попередньо зашифрувавши за допомогою відкритого ключа цю сторону. Після установки ключі можуть залишатися незмінними протягом декількох місяців або навіть років.

При шифруванні за допомогою WEP спочатку перевіряється контрольна сума корисного навантаження пакета. Відкритий текст, переданий алгоритмом шифрування, формується шляхом додавання контрольної суми до корисного навантаження. Отриманий відкритий текст складається по модулю 2 з відрізком ключового потоку і результатом цих перетворень є зашифрований текст. Після отримання пакету приймач витягує з нього зашифровані дані (корисне навантаження) і відновлює відкритий текст. Порівнюючи контрольну суму отриманих даних, можна переконатися в достовірності прийнятої інформації.

Однак протокол має ряд недоліків. По-перше при використанні однакових загальних ключів для всіх користувачів вони можуть запросто читати весь трафік один одного. Але навіть якщо всім користувачам роздати різні ключі, WEP все одно може бути зламаний. Так як ключі не змінюються протягом великих періодів часу, стандарт WEP рекомендує (але не зобов'язує) змінювати вектор ініціалізації при передачі кожного. На жаль, багато мережевих карт стандарту 802.11 для ноутбуків скидають вектор ініціалізації в 0, коли їх вставляють в роз'єм, і збільшують на одиничку з кожним пересланим пакетом. Так як мережеві карти вставляються і виймаються вельми часто, малі числа, що виступають в

якості векторів ініціалізації, - звичайна справа. Якщо зловмисникові вдасться зібрати кілька пакетів, посланих одним і тим же користувачем, з однаковими значеннями вектора ініціалізації (який сам по собі надсилається відкритим текстом разом з пакетом), то він зможе обчислити суму за модулем 2 двох блоків відкритого тексту, що дає можливість зламати шифр. Навіть якщо мережева карта 802.11 підбиратиме значення вектора ініціалізації для кожного пакета випадковим чином, все одно завдяки обмеженій довжині вектора (24 розряду) вектори будуть повторюватися. Алгоритм злому протоколу WEP був опублікований в 2001 році. Друга версія протоколу (WAP-2.0) передбачає можливості захисту на мережному, транспортному і прикладному рівнях, що підвищує надійність захисту. При налаштуванні бездротової мережі слід дотримуватися таких додаткових заходів безпеки:

1. Уникати з'єднання бездротової мережі з провідною ЛОМ. Бездротова точка доступу визначає підключення до маршрутизатора в окремій мережі або до інтерфейсу брандмауера.

2. Для реалізації бездротових з'єднань використовувати віртуальні приватні мережі (VPN).

3. Використовувати інструментальні засоби сканування для перевірки мережі на предмет наявності вразливих місць в системі безпеки.

4. Регулярно перевіряти журнал реєстрації підключень для контролю всіх мережевих підключень [29].

1.4 Безпека Wi-Fi мереж

Як і будь-яка комп'ютерна мережа, Wi-Fi - є джерелом підвищеного ризику несанкціонованого доступу. Крім того, проникнути в бездротову мережу значно простіше, ніж в звичайну, не потрібно підключатися до проводів, досить опинитися в зоні прийому сигналу. Бездротові мережі відрізняються від кабельних тільки на перших двох - фізичному (Phy) і

частково канальному (MAC) - рівнях семирівневій моделі взаємодії відкритих систем. Більш високі рівні реалізуються як в провідних мережах, а реальна безпека мереж забезпечується саме на цих рівнях. Тому різниця в безпеці тих і інших мереж зводиться до різниці в безпеці фізичного і MAC-рівнів.

Хоча сьогодні в захисті Wi-Fi-мереж застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних і контролю цілісності їх передачі, тим не менш, вірогідність доступу до інформації сторонніх осіб є дуже істотною. І якщо налаштуванні мережі не приділити належної уваги зловмисник може:

• роздобути доступ до ресурсів і дискам користувачів Wi-Fi-мережі, а через них і до ресурсів LAN;

• підслуховувати трафік, витягувати з нього конфіденційну інформацію;

• скористатися інтернет-трафіком;

• атакувати ПК користувачів і сервери мережі

• впроваджувати підроблені точки доступу;

• розсилати спам, і здійснювати інші протиправні дії від імені вашої мережі.

Для захисту мереж 802.11 передбачений комплекс заходів безпеки передачі даних. На ранньому етапі використання Wi-Fi мереж таким був пароль SSID (Server Set ID) для доступу в локальну мережу, але згодом виявилося, що дана технологія не може забезпечити надійний захист.

Головним же захистом довгий час було використання цифрових ключів шифрування потоків даних за допомогою функції Wired Equivalent Privacy (WEP). Самі ключі вдають із себе звичайні паролі з довжиною від 5 до 13 символів ASCII. Дані шифруються ключем з розрядністю від 40 до 104 біт. Але це не цілий ключ, а тільки його статична складова. Для посилення захисту застосовується так званий вектор ініціалізації

Initialization Vector (IV), який призначений для рандомізації додаткової частини ключа, що забезпечує різні варіації шифру для різних пакетів даних. Даний вектор є 24-бітовим. Таким чином, в результаті ми отримуємо загальне шифрування з розрядністю від 64 (40 +24) до 128 (104 +24) біт, в результаті при шифруванні ми оперуємо і постійними, і випадково підібраними символами. Але, як виявилося, зламати такий захист можна, відповідні утиліти присутні в Інтернеті (наприклад, AirSnort, WEPcrack). Основне її слабке місце - це вектор ініціалізації. Оскільки ми говоримо про 24 біти, це має на увазі близько 16 мільйонів комбінацій, після використання цієї кількості, ключ починає повторюватися. Хакеру необхідно знайти ці повтори (від 15 хвилин до години для ключа 40 біт) і за секунди зламати решту частини ключа. Після цього він може входити в мережу як звичайний зареєстрований користувач.

Як показав час, WEP теж виявилася не найнадійнішою технологією захисту. Після 2001 року для дротяних і бездротових мереж було запроваджено новий стандарт IEEE 802.1X, який використовує варіант динамічних 128-розрядних ключів шифрування, тобто періодично змінюючі в часі. Таким чином, користувачі мережі працюють сеансами, по завершенні їм надсилається новий ключ. Наприклад, Windows XP підтримує даний стандарт, і за замовчуванням час одного сеансу дорівнює 30 хвилинам. IEEE 802.1X - це новий стандарт, який виявився ключовим для розвитку індустрії бездротових мереж в цілому. За основу узято виправлення недоліків технологій безпеки, вживаних в 802.11, зокрема, можливість злому WEP, залежність від технологій виробника і т. п. 802.1X дозволяє підключати в мережу навіть PDA-пристрої, що дозволяє більш вигідно використовувати саму ідею безпровідного зв'язку. З іншого боку, 802.1X і 802.11 є сумісними стандартами. У 802.1X застосовується той же алгоритм, що і в WEP, а саме - RC4, але з деякими відмінностями. 802.1X базується на протоколі розширеної аутентифікації (EAP), протоколі

захисту транспортного рівня (TLS) і сервері доступу Remote Access Dial-in User Server. Протокол захисту транспортного рівня TLS забезпечують взаємну аутентифікацію і цілісність передачі даних. Всі ключі є 128-розрядними за умовчанням.

В кінці 2003 року був впроваджений стандарт Wi-Fi Protected Access (WPA), який поєднує переваги динамічного оновлення ключів IEEE 802.1X з кодуванням протоколу інтеграції тимчасового ключа TKIP, протоколом розширеної аутентифікації (EAP) і технологією перевірки цілісності повідомлень MIC. WPA - це тимчасовий стандарт, про який домовилися виробники устаткування, поки не набув чинності IEEE 802.11i. По суті, WPA = 802.1X + EAP + TKIP + MIC, де:

• WPA - технологія захищеного доступу до бездротових мереж

• EAP - протокол розширеної аутентифікації (Extensible Authentication Protocol).

• TKIP - протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol).

• MIC - технологія перевірки цілісності повідомлень (Message Integrity Check).

Сьогодні бездротову мережу вважають захищеною, якщо в ній функціонують три основних складових системи безпеки: аутентифікація користувача, конфіденційність і цілісність передачі даних. Для отримання достатнього рівня безпеки необхідно скористатися рядом правил при організації і настройці приватної Wi-Fi-мережі:

• Шифрувати дані шляхом використання різних систем. Максимальний рівень безпеки забезпечить застосування VPN;

• використовувати протокол 802.1X;

• заборонити доступ до налаштувань точки доступу за допомогою бездротового підключення;

• управляти доступом клієнтів по MAC-адресами;

• заборонити трансляцію в ефір ідентифікатора SSID;

• розташовувати антени якнайдалі від вікон, зовнішніх стін будівлі, а також обмежувати потужність радіовипромінювання;

• використовувати максимально довгі ключі;

• змінювати статичні ключі і паролі;

• використовувати метод WEP-аутентификации "Shared Key" оскільки клієнту для входу в мережу необхідно буде знати WEP-ключ;

• користуватися складним паролем для доступу до налаштувань точки доступу;

• по можливості не використовувати в бездротових мережах протокол TCP/IP для організації папок, файлів і принтерів загального доступу. Організація поділюваних ресурсів засобами NetBEUI в даному випадку безпечніше;

•не дозволяти гостьовий доступ до ресурсів загального доступу, використовувати довгі складні паролі;

• не використовувати в бездротовій мережі DHCP. Вручну розподілити статичні IP-адреси між легітимними клієнтами безпечніше;

•на всіх ПК всередині бездротової мережі встановити фаєрвол, не встановлювати точку доступу поза брандмауером, використовувати мінімум протоколів усередині WLAN (наприклад, тільки HTTP і SMTP);

• регулярно досліджувати уразливості мережі за допомогою спеціалізованих сканерів безпеки (наприклад NetStumbler)

• використовувати спеціалізовані мережеві операційні системи такі як, Windows Nt, Windows 2003, Windows Xp.

Так само загрозу мережевій безпеці можуть представляти природні явища і технічні пристрої, проте тільки люди (незадоволені звільнені службовці, хакери, конкуренти) впроваджуються в мережу для навмисного отримання або знищення інформації і саме вони представляють найбільшу загрозу.

1.5 Стратегія побудови та забезпечення безпеки мережі Wi-Fi

Все ще нерідко доводиться чути, що мережа бездротового доступу WLAN небезпечна в порівнянні з дротяними рішеннями. На теперішньому етапі розвитку технології Wi-Fi це твердження невірно. Просто безпекою треба займатися (проектувати і підтримувати), як і у випадку провідної мережі. Можна констатувати, що практично найгірша політика зараз - це просто забороняти використання Wi-Fi в компанії. Найчастіше співробітники починають приносити власні дешеві маршрутизатори з Wi-Fi (рівня рішень «для дому) просто тому, що використовувати Wi-Fi - це зручно. А для компанії такий пристрій, встановлене недосвідченим користувачем, - величезна діра в безпеці. Відомі випадки, коли великі компанії, довгий час забороняли будь-яке обладнання Wi-Fi, виявляли після спеціального обстеження, що в їхніх офісах насправді вже працюють тисячі несанкціонованих пристроїв. Тому варто використовувати Wi-Fi, як мінімум, для контролю радіосередовища та виявлення чужих пристроїв. Часто можна чути - як гарантувати те, що сигнал мережі WLAN не вийде за межі будівель компанії? Деякі «фахівці» пропонують використовувати спрямовані антени біля точок, розташованих поблизу зовнішніх стін всередині будівлі або використовувати точки-приманки з антенами, винесеними за межі будівлі, щоб відловлювати хакерів. На жаль, подібні техніки не надають достатнього рівня захисту, так як в реальності просто неможливо передбачити, як будуть поширюватися сигнали усередині будівлі. Наприклад, звичайне відбивання сигналу від металевих шаф з багаторазовим накладенням може призвести до конструктивної інтерференції з підсиленням сигналу, який легко вийде за межі будівлі. Або хакер може використовувати спрямовані антени з великим коефіцієнтом посилення, що дозволяє вловлювати навіть дуже слабкі

сигнали за межами будівлі, як і передавати інформацію в мережу і т.п. Все це говорить про те, що єдиний вірний підхід з бездротовими рішеннями, так само як і з дротяними, це проектувати оборону мережі. Вже давно відомо, що захист будь-якої інфраструктури одними лише методами створення захисного периметра неефективний, тому що найчастіше найбільш небезпечні атаки викликані чинниками всередині мережі, наприклад:

- Власні співробітники

(Що потрапили, скажімо так, під вплив методів соціального інжинірингу);

- Впроваджені шкідливі програми (віруси, трояни, черви, програми введені в мережу через заражені веб-сайти);

- «пир-то-пир» комунікації та впровадження через даний канал;

- Гості компанії, що отримали який-небудь доступ до мережі тощо.

Побудова системи безпеки мережі Wi-Fi має враховувати всі ці фактори, щоб максимально наблизитися до подібного рівня безпеки дротових та бездротових сегментів мережі.

Основні компоненти для побудови системи Безпеки бездротової мережі:

- Контроль доступу.

- Аутентифікація користувачів.

- Шифрування трафіку.

- Система попередження вторгнень в бездротову мережу.

- Система виявлення чужих пристроїв та можливості їх активного придушення.

- Моніторинг радіоінтерференції та DoS-атаки.

- Моніторинг вразливостей в бездротовій мережі та можливості аудиту вразливостей.

- Функції підвищення рівня безпеки інфраструктури бездротової

мережі, наприклад, аутентифікація пристроїв (X.509 і т.п.), захист даних управління - MFP / Management Frame Protection.

Основні завдання при побудові глибокоешелоновій обороні:

1. **Забезпечення контролю доступу** того, хто знаходиться в мережі (аутентифікація), які ресурси користувач може використовувати, застосування політик контролю доступу для трафіку цих користувачів.

2**. Цілісність і надійність** забезпечення того, що сама мережа доступна як ресурс критичний для бізнесу і що виникаючі небезпеки різного роду можуть бути ідентифіковані та знайдені і застосовані шляхи їх обходу.

3. **Забезпечення таємниці** того, що трафік на мережі не доступний для неавторизованих користувачів.

Стратегії безпеки

Стратегія 1: аутентифікації та авторизації всіх користувачів мережі.

Стратегія 2: Конфігурувати VLAN-и для поділу трафіку (наприклад гості/співробітники, високий рівень доступу/низький рівень доступу тощо) та введення первинного, грубого сегментування.

Стратегія 3: Використовувати міжмережеві екрани на рівні портів для формування більш тонкого рівня безпеки.

Стратегія 4: Використовувати шифрування на всій мережі для забезпечення секретності.

Стратегія 5: Визначати небезпеки цілісності мережі і застосовувати методи вирішення цих проблем.

Стратегія 6: Включити забезпечення безпеки кінцевих пристроїв в загальну політику безпеки.

Розглянемо дані стратегії детальніше:

Стратегія 1 / Аутентифікація і Авторизація всіх користувачів мережі Wi-Fi: початковою точкою створення будь-якої інфраструктури з глибокоешелонованим захисто є аутентифікація. Аутентіфкація повинна

застосовуватися на самій ранній початковій точці входу будь-якого користувача або пристрою в мережу на рівні порту ще до отримання IP-адреси. Після позитивного проходження аутентифікації повинна бути пройдена авторизація, яка дає можливість зрозуміти, хто цей аутентіфікований користувач, що він може робити в мережі, куди він може отримувати доступ. Стандарт пропонує використовувати гнучке рішення - 802.1x, яке підтримує велику кількість протоколів аутентифікації від цифрових сертифікатів до методів з логіном/паролем. Також 802.1x підтримується великою кількістю платформ - від дешевих КПК і смартфонів до настільних комп'ютерів і серверів. Модуль 802.1x (суплікант) вбудований в останні версії Windows і MacOS, а також в багато операційних систем для смартфонів, хоча поки і не на 100%. Можна знайти програми-супліканти 802.1x практично для будь-якої популярної операційної системи. 802.1x - це система, стандартизована IEEE і адаптована робочою групою 802.11i для формування контролю доступу с основою на створенні портів. Деякі деталі:

- Процес асоціації 802.11 створює віртуальний порт для кожного клієнта WLAN на ТД;

- ТД блокує всі фрейми даних, які не відповідають трафіку 802.11x;

- 802.1x-фрейми переносять (туннелируют) пакети аутентифікації EAP, які перенаправляються точкою доступу (або контролером WLAN в централізованій архітектурі) до сервера AAA;

- Якщо аутентифікація на базі EAP пройшла успішно, AAA-сервер відправляє до ТД повідомлення успішного завершення (EAP success), потім вже ТД дозволяє трафіку даних від клієнта WLAN пройти через віртуальний порт;

- Ще до відкриття віртуального порту встановлюється шифрування каналу обміну даними між клієнтом WLAN і ТД, щоб гарантувати, що ніякий інший клієнт WLAN не зможе отримати доступ до цього

встановленим віртального порту для даного клієнта, який проходить аутентифікацію. Побудова глибокоешелонованої оборони може бути успішна лише в разі реалізації авторизації користувачів після успішної аутентифікації. Критично важливо, що привілеї користувача на мережі варіюються не тільки на рівні його персональної ідентифікації, а й на таких більш інтелектуальних чинниках, як:

- Ідентифікація пристрою користувача;
- Поточний рівень безпеки цього пристрою;
- Місце розташування користувача;
- Час доби;
- Використовувався метод аутентифікації.

На практиці дуже зручно, коли весь необхідний функціонал аутентифікації, ідентифікації, авторизації і т.п. зібраний в одному пристрої з зручним інтерфейсом управління. Найбільш просунуте рішення має компанія Cisco Systems - це Cisco ISE / Identity Services Engine.

Стратегія 2 / Використання VLAN-ов для розділення трафіку і введення первинного, грубого сегментування для забезпечення безпеки мережі Wi-Fi : VLAN-и (Virtual Local Area Network) за своєю природою - це немаршрутизовані сегменти трафіку. У більшості сучасних будівель доводиться забезпечувати досить великі обсяги маршрутизації IP-трафіку, щоб зв'язати окремі сегменти мережі, побудовані наVLAN-ах. У кампусах роутингом доводиться займатися ще більше. У підсумку з великою кількістю VLAN-ів часто можна спостерігати виникнення проблем з керованістю такої системи. І складності можуть тільки наростати при додаванні мережі WLAN (Wireless Local Area Network) в інфраструктуру. Для спрощення можна використовувати методи підтримки мобільності між різними SSID, а також прагнути зберегти поточну схему IP-адресації. Важливо, щоб вбрання рішення WLAN забезпечувало роботу з безліччю різних VLAN навколо (позаду) одного

SSID. Це дає можливість реалізовувати різні політики безпеки всередині інфраструктури грунтуючись на результатах авторизації користувача не навантажуючи користувача, при цьому, складними правилами. Наприклад щоб отримати доступ до сервісів в зоні-X треба використовувати SSID-X і метод аутентіфкаціі X, а до сервісів в зоні-Y, треба шукати SSID-Y і аутентифікації Y. Всі політики можуть бути реалізовані прозоро і просто для користувача. В даний час це вже досить звичайний функціонал в сучасних централізованих рішеннях вендорів високого рівня.

Стратегії Безпечних VLAN-ів: Ключ до успішного безпечного використання VLAN-ів це динамічне їх призначення. Існує безліч шляхів для динамічного призначення VLAN-ів, наприклад:

- Грунтуючись на аутентифікаційній інформації 802.1x,
- Грунтуючись на інформації з веб-аутентифікації,
- Відповідно до SSID, обраним користувачем в бездротової мережі,
- Грунтуючись на виявленні якого іншого атрибута, як, наприклад, MAC-адресу пристрою, тип пристрою, статус поточного стану безпеки пристрою, місце розташування користувача і т.п.. Введення динамічного призначення VLAN-ів вимагає наявності механізму надання авторизаційної інформації під час аутентіфкаціі. У деяких випадках це може підтримуватися в ручному режимі або використовуючи додаткові можливості, як, наприклад, списки користувачів з інформацією про їх можливості. У разі використання декількох SSID на мережі користувач запитує дозволу на доступ в певну мережу (або сегмент мережі) і потім проходить аутентифікацію. При використанні аутентіфкаціі 802.1x у користувача немає можливості запросити доступ в певний VLAN, що означає, що така інформація (про VLAN-ни куди користувач повинен бути спрямований) повинна бути збережена на сервері, який виконує 802.1x аутентифікацію користувачів (наприклад-якої RADIUS -сервер з відповідним функціоналом). Також, інформація по VLAN-у може бути

модифікована в ході приєднання до мережі WLAN на підставі іншої інформації, наприклад місця розташування користувача і т.п..

Стратегія 3 / Використовувати міжмережеві екрани на рівні портів для формування більш тонкого рівня безпеки мережі Wi-Fi : Використання VLAN-ів може бути достатньо для грубої класифікації користувачів мережі. Але для реального захисту цінних ресурсів до кожного користувача повинні застосовуватися багатосторонні політики керовані мережевою інфраструктурою. Багато мережних інженери прийшли до такого ж висновку і почали використовувати периметральні міжмережеві екрани також і всередині мережі для того щоб застосовувати політики безпеки не тільки в місці виходу в Інтернет. Хоча вже зараз є виробники комутаторів LAN, які виробляють недорогі свічі з підтримкою 802.1x на портах, наприклад Cisco Systems. Хороший робочий підхід полягає в тому, щоб формувати політику безпеки на рівні портів з використанням бездротової мережі доступу. Так як безпека бездротової мережі грунтується на ідентифікації користувача і, при цьому, користувачі не асоціюються більше з фізичними портами. Сучасні рішення для бездротових мереж інтегрують функціонал виконання політик безпеки безпосередньо всередину системи WLAN. Це дозволяє говорити про те, що використання технології Wi-Fi, як основного безпечного, зручного та надійного доступу, логічніше й доцільніше, ніж дротового.

Стратегія 4 / Використовувати шифрування на всій мережі для забезпечення секретності в мережі Wi-Fi : Для бездротових мереж введення забезпечення секретності передачі інформації досить просте завдання. IEEE 802.11i це стандарт для забезпечення безпеки мережі WLAN. Він точно описує як забезпечувати секретність і цілісність даних на мережі WLAN з використанням спеціальних алгоритмів шифрування трафіку і методів аутентіфкаціі, заснованих на 802.1x (див. Стратегію 1). При виникненні завдання забезпечення безпеки і шифрування на

бездротовій мережі починати треба з рішень, побудованих на стандарті 802.11i та володіть високою інтероперабельністю з іншими бездротовими елементами.

Стратегія 5 / Визначати небезпеки цілісності мережі Wi-Fi (Integrity) і застосовувати методи вирішення цих проблем : Існують три основні питання безпеки:

- Контроль доступу,
- Забезпечення секретності (шифрування),
- Забезпечення цілісності.

Найбільш успішні стратегії визначатимуть зони найвищого ризику та спочатку концентруватися саме на них. Це половина шляху у вірному напрямку. Друга половина фокусується на вирішенні таких завдань як боротьба з троянами, вірусами, шкідливим ПЗ і т.п.. Ці небезпеки можуть викликати не тільки деградацію мережі і продуктивність, але і давати доступ до закритої інформації або викликати повну відмову в обслуговуванні. Ризик інфікування дуже високий і ризик для мережі також високий в разі інфікування. Тому в корпораціях вже нормальна практика мати стратегії ідентифікації вірусів та протидії їм. Ті хто поки не додав модулі визначення шкідливого ПЗ або шпигунських програм в антивірусні програми повинні зробити це якомога швидше, тому що ризик надто великий.

Стратегія 6 / Включити забезпечення безпеки кінцевих пристроїв Wi-Fi в загальну політику безпеки : Для використання інформації про статус безпеки кінцевих систем всередині спільних політик безпеки, що враховують стани, визначення кожної політики має включати рівень відповідності статусу безпеки кінцевого пристрою. Хороша практика полягає в зменшенні обсягу аналізу безпеки кінцевої системи і зведення його до зонових визначень, підтримуючи кількість зон наскільки можливо малими - три або чотири зони має бути достатньо для більшості компаній.

Друга хороша практична ідея полягає в тому, що якщо користувач намагається отримати доступ в мережу, але статус безпеки його системи не відповідає політиці просте блокування цього користувача далеко не завжди найкращий вихід. Замість цього користувач повинен отримати з'єднання і повинен бути перенаправлений в карантинну зону мережі, де він може скачати необхідне ПЗ (антивірус, міжмережевий екран і т.п.) або провести оновлення баз даних, щоб вийти на припустимий рівень безпеки персональної системи. Потім вже цей користувач може отримати повний доступ до корпоративних ресурсів.

РОЗДІЛ 2. ТЕХНОЛОГІЯ WI-FI МЕРЕЖ

У всьому світі стрімко зростає потреба в бездротових з'єднаннях, особливо у сфері бізнесу. Користувачі з бездротовим доступом до інформації - завжди і скрізь можуть працювати більш продуктивно і ефективно, ніж їх колеги, прив'язані до дротяних телефонних і комп'ютерних мереж.

Зазвичай бездротові мережеві технології групуються в три типи, що розрізняються за масштабом дії їх радіосистем, але всі успішно застосовуються в бізнесі.

PAN (персональні мережі) - короткодіючі, радіусом до 10 м мережі, які об’єднуть ПК і інші пристрої - КПК, мобільні телефони, принтери. За допомогою таких мереж реалізується проста синхронізація даних, усуваються проблеми з достачею кабелів в офісах, реалізується простий обмін інформацією в невеликих робочих групах. Найбільш перспективний стандарт для PAN - це Bluetooth.

WLAN (бездротові локальні мережі) - радіус дії до 100 м. За їх допомогою реалізується бездротовий доступ до групових ресурсів у будівлі, університетському кампусі і т.д. Зазвичай такі мережі використовуються для продовження дротяних корпоративних локальних мереж. У невеликих компаніях WLAN можуть повністю замінити дротяні з'єднання. Основний стандарт для WLAN - 802.11.

WWAN (бездротові мережі широкої дії) - бездротовий зв'язок, який забезпечує мобільним користувачам доступ до їх корпоративних мереж і Інтернету. Поки тут немає домінуючого стандарту, найбільш активно впроваджується технологія GPRS - найшвидше в Європі і з деяким

відставанням у США.

На сучасному етапі розвитку мережевих технологій, технологія бездротових мереж Wi-Fi є найбільш зручною в умовах, які вимагають мобільності, простості установки і використання. Wi-Fi (від англ. Wireless fidelity - бездротовий зв'язок) - стандарт широкосмугового бездротового зв'язку сімейства 802.11 розроблений у 1997 р. Як правило, технологія Wi-Fi використовується для організації бездротових локальних комп'ютерних мереж, а також для створення так званих гарячих точок високошвидкісного доступу до Інтернету.

2.1 Сценарії проектування та розгортання мережі Wi-Fi (WLAN)

Спочатку необхідно сказати, що існує два великих напрямки розробки і використання архітектур Wi-Fi-рішень:

1. Автономна архітектура.

2. Централізована / керована архітектура.

Саме базуючись на дані архітектур, створюється основна кількість проектів мереж Wi-Fi.

У разі автономної архітектури рішення являє собою набір незв'язаних точок доступу, кожна з яких конфігурується і обслуговується незалежно. Тому складність обслуговування мережі, побудованої подібним чином, зростає лінійно, а часом і експоненціально, із зростанням кількості пристроїв. Звідси мережі з автономною архітектурою, як правило, давно не проектують великими, зазвичай не більше 3-5 пристроїв. Тут існують деякі винятки, які полегшують створення трохи більше масштабних мереж, наприклад, технологія кластеризації точок доступу. Але це не повноцінно керована архітектура у будь-якому випадку. Також у разі автономної архітектури виникають величезні проблеми з реалізацією системи безпеки бездротової мережі, тому що майже неможливо виконувати корелляцію атаки з урахуванням всіх точок доступу в зоні покриття за відсутності

єдиного центру. Точки доступу незалежні і бачать ефір кожна по своєму, а для повноцінної інтерпретації події як атаки, важливий масштаб сприйняття, розуміння динаміки атаки. Це ж явище спостерігається і при виникненні проблем з інтерференцією, коли неможливо організувати спільне динамічне управління радіоресурсами (RRM-Radio Resource Management) з причини відсутності єдиного центру збору інформації з усіх точок доступу та відповідного прийняття рішень. Варто відзначити, що відомі випадки автономних мереж, що складаються з десятків точок доступу. Але гарантією ефективної роботи такої інфраструктури в нашій практиці була наявність кваліфікованих інженерів з WLAN в IT-службі, які самі писали спеціальні скрипти для масового управління всіма точками доступу, контролю по SNMP та збору статистики і т.д. У будь-якому випадку, це досить нетривіальний підхід, який ще й дуже небезпечний через проблеми з обслуговуванням подібного рішення у разі звільнення інженера-розробника даного ПЗ.

У разі Централізованої архітектури повне управління інфраструктурою мережі радіодоступу виконується контролером WLAN. Наприклад, у Cisco подібна архітектура називається CUWN (Cisco Unified Wireless Network). Контролер у централізованому рішенні управляє завантаженням/зміною ПЗ, змінами конфігурації, RRM (динамічне управління радіоресурсами), управляє зв'язком мережі WLAN із зовнішніми серверами (AAA, DHCP, LDAP і т.п.), управляє аутентифікацією користувачів, управляє профілями якості обслуговування QoS та спеціальними функціями. Більше того, контролери можуть об'єднуватися в групи для забезпечення безшовного роумінгу клієнтів між різними точками доступу в зоні покриття. Наприклад, у рішеннях Cisco Systems можна об'єднати десятки контролерів в один мобільний домен і, відповідно, до декількох десятків тисяч точок доступу. Створення подібних мобільних доменів дозволяє забезпечити безшовні хендоверів (у

термінах Wi-Fi - це роумінг) між точками доступу керованих як одним контролером, так і різними. Існують ефективно працюючі мережі, кількість точок доступу в яких наближається до 100.000. Подібних масштабів можна домогтися тільки в керованій архітектурі рішення. Слід зазначити, що централізовану архітектуру в своїх рішеннях вже пропонують різні виробники.

Для точок доступу або маршрутизаторів з Wi-Fi необхідно орієнтуватися на підтримку 802.11n.

На базі технології Wi-Fi розгортаються різноманітні рішення, наведемо кілька прикладів за напрямами:

- Wi-Fi-доступ для дому (з використанням невеликих домашніх маршрутизаторів з Wi-Fi, наприклад CiscoLinksys, D-Link, Netgear і т.д.).

Найчастіше в квартирі встановлюється один домашній маршрутизатор з Wi-Fi (зазвичай 2.4GHz, але краще, якщо 2.4 +5 GHz), який підключається тим чи іншим проводовим інтерфейсом до мережі провайдера і надає безпровідний доступ домашнім користувачам. Тут має сенс обзавестися хоча б найпростішим програмним забезпеченням типу Wi-FiAnalizer під Android і перевірити, на яких частотних каналах працюють подібні пристрої сусідів. Часто більшість використовує ідентичні канали. Аналіз спектра дозволить налаштувати ваш пристрій на незайняті канали, або канали з найменшим рівнем сигналу. І не забувайте включати WPA2 (зазвичай WPA2-Personal з PSK).

- SOHO/SmallOfficeHomeoffice - Wi-Fi-доступ для невеликого офісу (використовуються невеликі роутери з Wi-Fi, більш продуктивні і багатофункціональні, ніж домашні роутери, наприклад, CiscoWAP, WET, AP, Cisco ISR з Wi-Fi модулями і ряд інших схожих функціонально пристроїв, а також Точки Доступу в Автономному режимі). Тут якраз найчастіше дуже виправдано використання одного багатофункціонального, але продуктивного пристрою. Зона покриття невелика, доступного місця

мало, але навантаження вже може бути істотно вище, ніж у квартирі, і вимоги до стабільності несумірні. Тому краще всього обрати спеціалізований пристрій, спроектований для даних завдань.

- Невеликі корпоративні мережі доступу Wi-Fi (частина поверху, поверх, невелика будівля тощо). Тут дуже добре можуть застосовуватися рішення з централізованою архітектурою, але розраховані на невелику кількість рідко даний рівень вирішення має бути більше 10-20 точок доступу. Тому варто підібрати невеликий сучасний контролер (наприклад, Cisco 2500, Aruba 3000) на базі окремого пристрою або як модуль в багатофункціональний маршрутизатор (наприклад, модуль SRE в маршутізатор CiscoISR).

- Великі корпоративні мережі доступу Wi-Fi (університетські кампуси, корпоративні кампуси, офісні кампуси, заводські території, порти тощо). Для подібних завдань централізована архітектура з потужними та функціональними контролерами - це єдино правильний підхід. Можна використовувати сучасні контролери (наприклад Cisco 5508, ArubaA6000, PCM-сервер у HP), розгорнуті в Датацентрі мережі. Якщо виробник пропонує рішення на модулях для комутаторів або маршрутизаторів (наприклад, CiscoWiSM, WiSM2), то можна їх використовувати і на Кордоні мережі (згадаймо трирівневу модель). Централізована архітектура дозволить забезпечити практично будь-який масштаб мережі та ефективно управляти нею з єдиної точки з мінімальним навантаженням на IT-персонал.

- Так звані «бранчі» (Branches) - Wi-Fi-доступ для маленьких віддалених офісів (об'єднує велику кількість невеликих віддалених офісів під централізованим управлінням, наприклад, широко використовується в банківській сфері для зв'язку штаб-квартири з віддаленими офісами; тут найчастіше зв'язок між віддаленими офісами і центральної штаб-квартирою організовується за орендованим каналом у операторів зв'язку, а

іноді і через супутникові канали).

У даному випадку ключовою проблемою є те, що в силу звичайної практики мінімізації витрат у бізнесі, комунікаційні канали для зв'язку з малими офісами із штаб-квартири рідко бувають виділеними, широкими і надійними. Найчастіше підключення малих віддалених офісів виконується шляхом "підключення до інтернету" через найближчого і дешевого провайдера, а про підписання контракту з SLA (ServiceLevelAgreement) з цим провайдером ніхто й не замислюється (а провайдер, ймовірно, навіть не забезпечує такими послугами). Доступ до корпоративної мережі організовується через VPN. При такому підході дуже часто виникає ситуація, коли канал у віддаленому офісі падає або виникають перевантаження на мережі провайдера або на стику його мережі з мережею провайдера, до якого підключена штаб-квартира, і зв'язок зі штаб-квартирою тимчасово пропадає або стає дуже нестабільним. У будь-якому випадку подібні проблеми не скасовують бажання мати бездротову мережу в віддаленому офісі, але якщо таких офісів багато (як майже в кожному банку), то обслуговування їх стає великою проблемою, оскільки тримати IT-персонал в кожному офісі просто не рентабельно, а посилати інженера з центру при найменших проблемах з мережею довго і дорого. Рішення має забезпечувати:

- Централізоване управління всім конгломератом віддалених Wi-Fi мереж (у віддалених офісах) з центрального сайту. Причому це не повинно залежати від різних характеристик каналів «віддалений офіс - штаб-квартира»; при цьому повинен бути можливий централізований моніторинг, розв'язання проблем та конфігурування віддалених пристроїв.

- Надання послуги Wi-Fi в віддаленому офісі і при тимчасовому зникненні зв'язку з центральним сайтом (з обов'язковою підтримкою аутентифікації і можливістю входу / виходу Wi-Fi-клієнтів),

- Можливість як центральної комутації користувача трафіку

(висновок трафіку з віддаленого сайту в центральний), так і локальної комутації (у віддаленому офісі).

- Зовнішні міські мережі доступу Wi-Fi (точки доступу розташовуються на вулиці і надають сервіс цілий рік поза приміщеннями, наприклад, для міських служб, городян і гостей міста). У даному випадку найбільший інтерес викликають повнозв'язні мережі Wi-Fi (Mesh), де послуга кінцевим користувачам надається через один радіоінтерфейс точки доступу (зазвичай 2.4GHz), а через інший (зазвичай 5GHz) формується транспортний радіоканал з сусідніми точками доступу. У Mesh-мережах зазвичай присутні два типи точок доступу: тип Mesh (MAP у Cisco) і Root (RAP у Cisco), де RAP з'єднується з провідний мережею, а на MAP будується бездротова частина мережі. У мережі Mesh формуються дерева з корінням в RAP, а дерева будуються за допомогою спеціалізованих протоколів (IAPP у Cisco). Гілки дерев, як правило, не повинні перевищувати 8 хопів, але тут все впирається в профілі трафіку на мережі й послуги, а також у конструкцію точок доступу (якщо в 5GHz присутній один радіомодуль, то на кожному хопі пропускна здатність бекхола падає практично в два рази, а якщо є два незалежних радіомодуля 5GHz, то пропускна здатність знижується мінімально). Сама інфраструктура Mesh зазвичай керується Контролером WLAN. Дуже добре, якщо програмне забезпечення контролера WLAN може одночасно керувати і точками доступу в звичайному режимі та в Mesh-режимі, так як це дозволяє гнучко підходити до проектування мережі і пов'язувати як зовнішні домени, так і внутрішні для забезпечення безшовної мобільності на мережі.

Необхідно відзначити, що подібні рішення часто застосовуються і для таких "вуличних/зовнішніх" проектів, як покриття кар'єрів, заводських територій, ліній рейкового транспорту тощо.

Різні рішення для спеціальних випадків (тим не менш, досить широко поширене):

•ангари, склади,

•заводські цехи,

•рішення для залізничного транспорту (надземного і підземного - тут підходи різні),

•рішення для авіаційного транспорту,

•рішення для великих торгових центрів,

•рішення для стадіонів і великих демонстраційних або концертних залів (тут характерна висока щільність користувачів),

•рішення для лікарень і госпіталів і т.п.

У всіх цих випадках централізована архітектура найбільш правильний вибір, а рішення треба розробляти з урахуванням особливостей задачі.

Необхідно відзначити, що для реалізації Wi-Fi-рішень у різних умовах оточеннях розроблені і використовуються Точки Доступу трьох основних типів конструкцій:

1. ТД для використання всередині приміщень/"офісний" варіант

(Часто такі ТД характеризуються привабливим зовнішнім виглядом, інтегрованими антенами і відносно вузьким температурним діапазоном, наприклад, 0 - +40 гр С),

2. ТД для використання всередині приміщень/"ангарного-складський" варіант. (Часто такі точки доступу мають металевий корпус, можливість використання зовнішніх антен і більш широкий температурний діапазон, наприклад, -20 - +55 гр С),

3. Токи доступу для використання поза приміщеннями, на вулиці/"вуличний" варіант (Часто характеризуються посиленим зовнішнім корпусом, зовнішніми, іноді інтегрованими антенами, вологозахищеним корпусом і з'єднаннями, широким температурним діапазоном, наприклад, -40 - +55 грС).

Треба також відзначити, що існують моделі зі спеціальними

корпусами, призначеними для дуже важких оточень, наприклад, для небезпечної атмосфери, як на хімічних або нафтопереробних підприємствах і т.п. Також важливо знати, що існує пропозиція спеціальних термочохлів, що дозволяють використовувати внутрішні точки доступу поза приміщеннями, а також вибухобезпечних кожухів для особливо небезпечних зон, але тут треба дуже акуратно й уважно дослідити питання, перш ніж робити висновки.

2.2 Підходи до планування та проектування розвиненої мережі Wi-Fi

Як показує практика, у типовій російській дійсності до Wi-Fi зазвичай ставляться як до простої і невимогливою технології. І найпоширеніший підхід - це прикинути необхідну кількість точок доступу на око, замовити, а потім розбиратися. На жаль, результати подібного підходу плачевні, і навіть з висококласним устаткуванням можна спостерігати вкрай нестабільні і неякісні за рівнем обслуговування в мережі результати.

З іншого боку, вимоги до бездротового доступу ростуть постійно, зростає набір важких послуг, які вже можна якісно передавати по Wi-Fi або надавати з використанням Wi-Fi. Значна частина проектів вже вимагає розробки «по ємності», а не «по покриттю». Необхідно обслуговувати малопотужні термінали, наприклад смартфони або мітки RFID.

Все це веде до одного - необхідно приділяти серйозну увагу такій важливій частині будь-якого бездротового проекту, як польове радіообстеження об'єкта (SiteSurvey). Зазвичай це не викликає питань для мереж 2G, 3G або WiMAX, а от Wi-Fi - "це просто" і "не варто морочитися", а потім - "упс, мережа працює криво".

Почати необхідно з аналізу своїх поточних побажань та обговорення майбутнього розвитку інфраструктури всередині компанії. Краще, якщо це буде «мозковий штурм» керівників IT-департаменту, маркетингу, операцій

і т.п. Інакше, якщо рішення будуть приймати лише «технарі», то після запуску часто виявляється, що вже через пару місяців керівництво або «продавці», побачивши десь статтю про можливості Wi-Fi, хочуть це мати і в себе, а мережа спроектована під інші вимоги, і все починається спочатку (включаючи нове обстеження об'єкта, проектування, пошук місць і портів під додаткове обладнання тощо). Приклад питань для обговорення:

- На яких частотах буде працювати рішення?

- В яких умовах передбачається розгортання? (План приміщення, особливості будівельних конструкцій, висота стель і т.п.?)

- Чи передбачається робота в складній радіообстановці? (Багато перешкод, наприклад в машинобудівних цехах тощо), хоча це обов'язково для перевірки в ході радіообстеження об'єкта;

- Яка кількість користувачів (з них активних - одноразово споживають послуги) очікується на мережі?

- Як розподілятимуться користувачі по мережі? (Важливо врахувати можливі зони концентрації і очікувана кількість користувачів в цих зонах)

- Які послуги необхідно надавати користувачам при запуску мережі і як це буде розвиватися в осяжній перспективі, наприклад: доступ до Інтернету тощо. Такий інструмент дозволяє побудувати модель, точну рівно на стільки, наскільки точні вхідні дані. Але, на жаль, абсолютної точності вхідних даних не можна забезпечити за визначенням, як і неможливо закласти стан радіосереди та умови для багатопроменевого поширення, загасання сигналів і т.п. Тому до результатів роботи подібного інструментарію треба ставитися обережно.

Відразу виникає питання - тоді навіщо цей крок потрібен? Використання подібного софта дозволяє робити наступне:

1. Формувати досить якісні оцінки необхідної кількості точок доступу і, нерідко, відповідні хороші пропозиції. Але це саме оцінка, а не фінальні значення!

2. Створювати ідеальну модель розміщення точок доступу прямо на карті майбутньої зони покриття реальної мережі. Ці дані можна дуже ефективно використовувати як основу для проведення польового радіообсеження. Можна розміщувати реальні точки доступу прямо в місця, зазначені в попередньому дизайні на карті, знімати поточні показання та тюнить ідеальну модель до реальної.

Подібний програмний модуль вбудований, наприклад, у відомі системи управління WLAN від Cisco: WCS / Wireless Control System і нову Cisco Prime NCS/Network Control System. До речі, ці системи є в демо-версіях (повноцінна система), доступних на протязі 30 днів. Можна завантажити з сайту Cisco.

Тут вже можна обговорювати питання топології транспортної інфраструктури для підтримки передбачуваної топології Бездротової мережі Wi-Fi, а також наявності портів мережі передачі даних (краще з підтримкою 803.3af/PoE-PoweroverEthernet) в зоні покриття і розеток 220В, якщо не всюди доступні порти з PoE.

Далі, вже достатньо підготовленими, можна переходити до польового радіообстеження. Тут, крім описаної інформації, необхідно використовувати аналізатор спектру для розглянутого частотної ділянки і спеціальний інструментарій (ПЗ + радіоблок з антеною) для виконання радіообстеження. Вкрай важливо виконувати не просто пасивне обстеження (PassiveSiteSurvey) зі збором інформації про рівень сигналу, а робити активне обстеження (ActiveSiteSurvey), при якому постійно передається трафік даних і знімаються свідчення 'сигнал + реально досяжна швидкість передачі даних 'у великій кількості точок зони покриття. Для генерації тестового трафіку часто використовується iPerf. Таким чином виходить реальна картина швидкостей незалежно від рівня сигналу, що дуже добре, тому що далеко не завжди працює лінійна залежність - чим вище рівень сигналу і SNR, тим більше MCS

(Modulation&CodingSchema) і тим вище досяжна швидкість передачі для кінцевих користувачів.

Інструментарій для обстеження виробляє багато компаній, наприклад AirMagnet (поглинений FlukeNetworks), Ekahau тощо.

Важливі нюанси:

- При радіообстеженні важливо використовувати саме ті точки доступу і антени (якщо із зовнішніми антенами), які будуть використані на реальній мережі,

- При радіообстеженні важливо виконувати тести з використанням найгіршого користувацького пристрою (по радіо-характеристикам), яке очікується побачити і обслуговувати на даній мережі. Часто це смартфони або мітки RFID. Після завершення радіообстеження виконується:

- Остаточний дизайн Бездротової мережі,

- Остаточний дизайн транспортної інфраструктури,

- Остаточний дизайн (або доробки) центрального сайту всієї мережі,

- Аналіз та дизайн інтеграції розроблюваного рішення з існуючими системами,

- Рекомендації до майбутнього розгортання рішення,

- Уточнюється кількість необхідного обладнання, після цього можна переходити до замовленням.

2.3 Радіообстеження зони покриття мережі Wi-Fi

Проект бездротової мережі Wi-Fi завжди повинен включати в себе радіообстеження об'єкта на стадії проектних робіт і до початку інсталяції обладнання. Це єдина дійсно реальна можливість, при правильному проведенні, отримати достатньо підстав для створення працездатного рішення бездротової мережі з передбачуваними характеристиками.

У бездротових системах дуже складно передбачити поширення радіохвиль і визначити наявність інтерференції без використання

тестового обладнання. Навіть якщо ви використовуєте всенаправлені омні-антени, в дійсності радіохвилі не поширюються на однакову відстань у всіх напрямках. Замість цього різні перешкоди, як, наприклад, стіни, двері, ліфтові шахти, люди саричиняють різний рівень загасання сигналу, що є причиною того, що діаграма спрямованості радіо стає неоднозначною і непередбачуваною. У результаті, часто необхідно виконувати радіообстеження зони покриття Wi-Fi-мережі (SiteSurvey) для повноцінного розуміння поведінки та поширення радіосигналів до початку розгортання точок доступу бездротової мережі.

Основна мета радіообстеження (SiteSurvey) - це отримання достатнього обсягу інформації, щоб визначити кількість і позиції точок доступу для надання необхідного покриття всередині всієї цільової зони. У більшості випадків потрібне покриття визначається забезпеченням мінімальної швидкості передачі даних (datarate). Радіообстеження також визначає присутність інтерференції, яке йде від інших джерел, яка може знизити продуктивність WLAN.

Вимоги та складність радіообстеження об'єкта будуть змінюватись в залежності від самого об'єкта і його характеристик. Наприклад, невеликий офіс, що складається з декількох кімнат відкритого типу, може взагалі не вимагати радіообстеження. Хоча інтерференцію, тим не менш, перевірити варто. Цей сценарій, ймовірно, може бути реалізований шляхом установки однієї точки доступу десь в офісі, і можна очікувати, що покриття для загальних завдань буде адекватним. Якщо ж точка доступу зіткнеться з інтерференцією від ЛОМ сусіднього офісу, то, найімовірніше, перехід на сусідній канал, який не перекривається, може вирішити проблему. Радіообстеження ніколи не треба заміщати кабінетною аналітикою навіть у разі проектування невеликих мереж.

Великі приміщення, такі великі офіси, житлові будинки, лікарні, ангари, цехи зазвичай вимагають детального радіообстеження. Без

обстеження користувачі зіткнуться з недостатнім покриттям і будуть відчувати проблеми з продуктивністю мережі (пропускною здатністю) у деяких зонах. Навряд чи захочеться заново міняти місця встановлення кількох десятків точок доступу, а також всі їх підключення, якщо проблема вимагає редизайну радіопідсистеми вже після розгортання.

При проведенні радіообстеження об'єкта для Wi-Fi необхідно зробити наступні кроки:

1. Отримати план приміщення

До початку радіообстеження отримайте план всієї території майбутньої мережі, включаючи поверхові плани всіх приміщень, де передбачається покриття. Якщо немає нічого доступного, то намалюйте свій план з розмірами і вкажіть положення всіх стін, переходів, вікон, ліфтів тощо.

2. Візуально оглянути весь об'єкт

До початку будь-яких тестів пройдіть по всьому об'єкту і перевірте точність планів приміщень. Це також хороший момент для виявлення потенційних перешкод, які можуть впливати на поширення радіосигналів. Наприклад, візуальне обстеження допоможе виявити такі перешкоди для радіосигналу, як металеві шафи та перегородки, яких зазвичай немає на плані приміщення.

3. Визначити місця знаходження майбутніх користувачів WLAN

На плані приміщення відзначте зони знаходження користувачів з провідним і бездротовим з'єднанням. Додатково проілюструйте де може знадобитися роумінг для бездротових / мобільних користувачів, а також куди вони не ходять. Можливо вдасться обійтися меншою кількістю точок доступу, якщо вдасться обмежити зони роумінгу або взагалі перейти до моделі організації «гарячих зон» Wi-Fi, а не суцільного покриття.

4. Визначити тип і модель точок доступу в майбутньої мережі.

Виходячи з первинного повного обстеження об'єкту і зібраної

інформації необхідно визначитися з типами точок доступу, антен для майбутньої мережі. Це може залежати від великої кількості факторів, наприклад: необхідність використання інтегрованих антен, коли є вимоги з естетики; високі стелі, відповідно до рішення із зовнішніми антенами; зони високої щільності користувачів, необхідне збільшення ємності шляхом формування вузьких осередків, відповідно точки із зовнішніми антенами з вузькою діаграмою спрямованості.

5. Визначити попередні місця встановлення точок доступу.

Попередньо можна оцінити місце розташування і кількість точок доступу для забезпечення адекватного покриття необхідної зони шляхом аналізу місць положення користувачів WLAN, очікуваної зони покриття і величини осередків, сервісів на мережі і самих елементів радіопідсистеми. Для забезпечення суцільного покриття необхідно планувати деяке перекриття осередків суміжних точок доступу, але треба пам'ятати, що при призначенні каналів для точок доступу (при ручному конфігуруванні або при попередньому плануванні) Крапка з ідентичним частотним каналом повинна бути досить далеко від даної, або була мінімальною інтерференція від випромінювання через сусідню крапку доступу. Пам'ятайте, що в спектрі 2.4GHz у нас доступні лише три частотних каналу 1, 6 і 11, які не перекриваються. Також варто додати, що достатнім рівнем перекриття осередків можна вважати:

- Перекриття порядку 10-15% при наданні сервісу передачі даних, як основної послуги,

- Перекриття порядку 20%, коли на мережі надаються голосові послуги VoIP через Wi-Fi,

Гарною підмогою в справі попереднього і обгрунтованого визначення положення точок доступу може стати спеціальний програмний модуль для планування мережі Wi-Fi. Подібний програмний модуль вбудований, наприклад, у відомі системи управління WLAN від Cisco:

WCS/Wireless Control System і нову Cisco Prime NCS/Network Control System. До речі, ці системи є в демо-версіях (повноцінна система з обмеженим терміном дії), доступних на протязі 30 днів. Можна завантажити з сайту Cisco.

Але це тільки полегшує проведення радіообстеження, не заміщаючи його. З оцінкою розташування точок доступу на плані приміщення необхідно проводити обстеження, перевіряти і коригувати рекомендовані положення.

Необхідно виявити відповідні монтажні позиції для інсталяції антен, кабелів передачі даних і кабелів живлення. Також враховуйте необхідність застосування різних типів антен, коли приймаєте рішення щодо позиції точки доступу. Наприклад, якщо передбачається монтувати точку доступу поруч із зовнішньою стіною будівлі, то в цьому випадку можливий і кращий підхід - це використання спрямованої панельної антени з відносно високим посиленням всередині будівлі. Якщо передбачається використовувати точки доступу з інтегрованими антенами, то вони часто мають діаграму спрямованості таку, що найбільш правильно їх розташовувати на стелі (обов'язково виступаючими всередину приміщення). У даному випадку висота стелі повинна бути звичайною для офісів. Для приміщення з високими стелями або в цехах / ангарах використовуйте точки доступу з направленими антенами.

6. Перевірка місць положення точок доступу і реального рівня параметрів мережі.

Це відбувається на початку реальних тестів. Зазвичай розміщується кілька точок доступу в попередньо сплановані позиції на об'єкті і проводяться натурні тести з використанням спеціалізованих інструментів для проведення радіообстеження, наприклад Ekahau, Fluk / AirMagnet і т.п. Дуже важливо використовувати при обстеженні саме ті моделі точок доступу та антен, які згодом будуть на реальній мережі, а також

виконувати тести з урахуванням найгірших за радіохарактерістіками користувача пристроїв, які Ви очікуєте побачити на своїй мережі. Також дуже важливо проводити не просто пасивні тести знімаючи характеристики саме радіомережі, а треба робити Активні тести з формуванням реального навантаження від трафіку (зазвичай є вбудовані механізми в інструменти з активним функціоналом радіообстеження), тому що тільки це покаже реальну картину майбутньої поведінки мережі.

Дуже корисно також мати в арсеналі аналізатор спектру для частотних діапазонів 2.4GHz і 5GHz. Це дозволить виявити і точно уявляти собі інтерференційну картину в зоні покриття.

Діаграми спрямованості основних типів антен для Wi-Fi

- **Омні-антена (всеспрямована)** діаграма спрямованості виглядає як Тор (у західних джерелах часто можна бачити назву Donut, відомий,як пончик), з точкою доступу або її антенами в центрі.

Найбільш часто така діаграма зустрічається у точок доступу з інтегрованими антенами, у точок доступу із зовнішніми антенами типу Диполь, Монополь, із зовнішніми багатоелементними Омні-антенами з рознесенням випромінюючих елементів для підтримки MIMO. Специфіка випромінювання антени такого типу завжди накладає свої умови на розміщення в зоні покриття. Треба бути дуже акуратними з розміщенням поблизу металевих стін і конструкцій (стіна ангара, мет. шафи, ліфтові шахти, силові конструкції будівель тощо), щоб не отримати потужне відбиття і багатопроменеве поширення власних сигналів (multipath), що призведе до інтерференції і деградації продуктивності.

- Спрямована антена діаграма спрямованості виглядає як груша з точок доступу у вузькій частині цієї "груші".

Найчастіше, як "спрямована", використовується Панельна (Patch), хоча є маса інших типів, наприклад Яги. Якщо точка доступу підтримує 802.11n, то вона повинна підтримувати MIMO. Сучасні точки доступу

підтримують MIMO аж до 4x4, що означає наявність чотирьох передавачів і чотирьох приймачів. Для максимальної ефективності системи та використання можливостей рознесення (diversity) краще використовувати рекомендовані виробником антени (це стосується і випадку з Omni).

Антени спрямованого типу широко застосовуються для забезпечення покриття в приміщеннях з високими стеля (при монтажі точок доступу на стелі або в Пленумі), в дизайнах WLAN з високою щільністю користувачів, де необхідно створювати вузькі комірки і підвищувати загальну ємність мережі.

РОЗДІЛ 3. СТВОРЕННЯ БЕЗДРОТОВОЇ КОРПОРАТИВНОЇ МЕРЕЖІ WI-FI ТА ЇЇ ЗАХИСТ

Даний розділ слугує реалізацією теоретичного матеріалу на практиці, а саме створення безпровідної корпоративної мережі на базі технології WiFi. Дійсно КНТЕУ вже використовує у своїй діяльності бездротову мережу WiFi для підключення користувачів переносних комп'ютерів до локальної обчислювальної мережі, доступом до корпоративних ресурсів, та Інтернет. У силу особливостей діяльності замовника, а також конфігурації приміщень, було скрутно забезпечити всіх потенційних користувачів проводовим підключенням. Розгорнута бездротова мережа (на обладнанні ASUS і D-Link), однак, не цілком задовольняла потребам замовника а саме:

- Слабкі можливості управління (були потрібні індивідуальні налаштування кожної точки доступу).
- Слабкі можливості моніторингу (неможливо визначити, де знаходиться клієнт, параметри його підключення, статистика з'єднань).
- Низькою безпеки (використовувався метод авторизації за відомим всім паролю, WPA-PSK).
- Відсутність підтримки безперервного мобільного підключення (роумінгу).
- Необхідність вручну займатися радіочастотним плануванням, ідентифікувати проблемні місця та «нелегальні» підключення.

У зв'язку цим виникло завдання побудови надійної, сучасної та безпечної бездротової інфраструктури. Яке було успішно мною вирішене на основі поєднання уніфікованої бездротової інфраструктури (CUWN)

Cisco, і доменної інфраструктури Microsoft.

Принципова схема побудованого рішення наведена на рис. 3.1

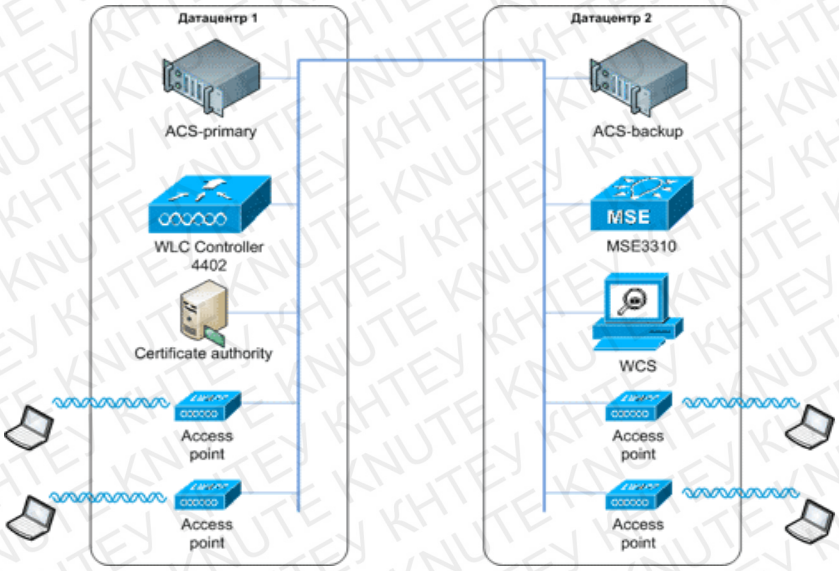


Рис.3.1 Інфраструктура на основі нового обладнання.

Мережа розподілена на два корпуси, кожен з яких має невеликий дата-центр. Об'єднавши корпуси захищеним каналом пропускною здатністю 10 Гігабіт/с використовуючи обладнання Cisco Catalyst в локальній мережі. В одному з корпусів потрібно встановити контролер бездротових точок доступу Cisco WLC4402, що підтримує до 12 «легких» точок доступу. Ці пристрої, моделей LAP-1131 і LAP-1121, розподілемо по приміщеннях замовника які здійснюють безпосереднє обслуговування бездротових клієнтів (ноутбуків), яких у мережі одночасно може нараховуватися до ста. Для авторизації і контролю доступу користувачів бездротової мережі точок доступу, разом з контролером, використав протокол 802.1x. При цьому в якості механізму авторизації застосовував EAP-TLS, з авторизацією по доменних сертифікатах служб каталогів Windows. Кожен користувач бездротової мережі має обліковий запис у службі каталогів наявного домену Windows. На базі облікового запису в службі сертифікатів домену створюється сертифікат, який встановлюється на ноутбук користувача і використовується при його авторизації. В якості

серверів авторизації (RADIUS) виступають пристрої Cisco ACS 5.2 (2 штуки в різних дата-центрах, для відмовостійкості) робоче вікно пристрою на рис. 3.2..

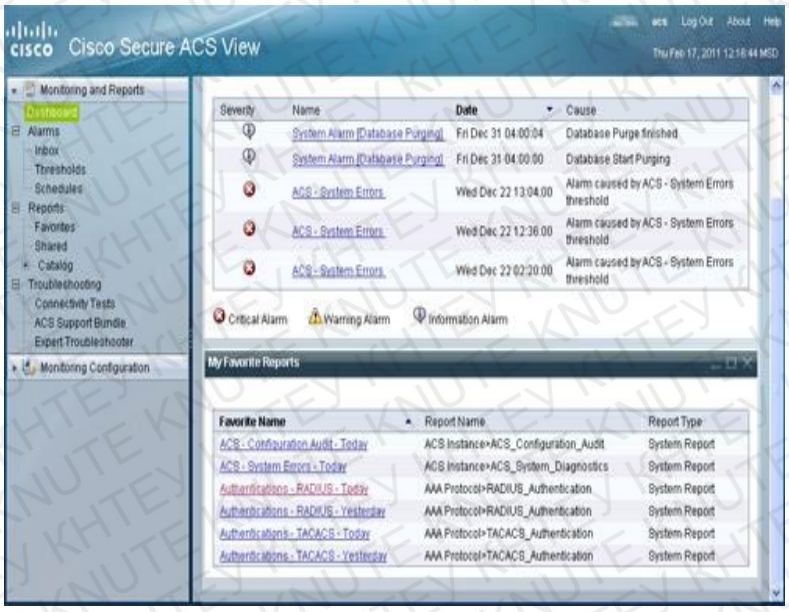


Рис. 3.2 Моніторинг користувачів

Для більш точного позиціонування працюючих бездротових клієнтів на карті-плані приміщення в мережі встановив додатковий контролер, Mobility Services Engine, безперервно обробляючий інформацію від бездротових точок доступу, та контролера.

Для централізованого управління мережею, перегляду статистики, налаштування, візуалізації застосовував програмне забезпечення Cisco Wireless Control System.

Для скорочення витрат з обслуговування апаратної інфраструктури «пристрою» MSE, ACS, WCS, служби каталогу та сертифікати домену виконуються в віртуальних машинах VMware.

Таким чином, шляхом побудови сучасної бездротової мережі були успішно вирішені наступні завдання замовника:

- Безпечне та надійне підключення користувачів до бездротової

мережі, що використовує існуючий механізм домену Windows.

•Централізоване управління, моніторинг, обслуговування безпровідних пристроїв та супутніх систем.

•Автоматичний контроль над радіо-обстановкою, роумінгом, визначенням положення легітимних і несанкціонованих клієнтів.

•Підтримка декількох бездротових мереж на базі єдиної фізичної інфраструктури з різними політиками безпеки (департаменти, гостьовий доступ).

•Додаванням контролерів і точок доступу, бездротова мережа може бути масштабирована в десятки разів, у тому числі і на віддалені майданчики, без будь-яких змін в її конфігурації.

На рис. 3.3 зображене вирівнювання сигналу за допомогою CISCO WCS Home.

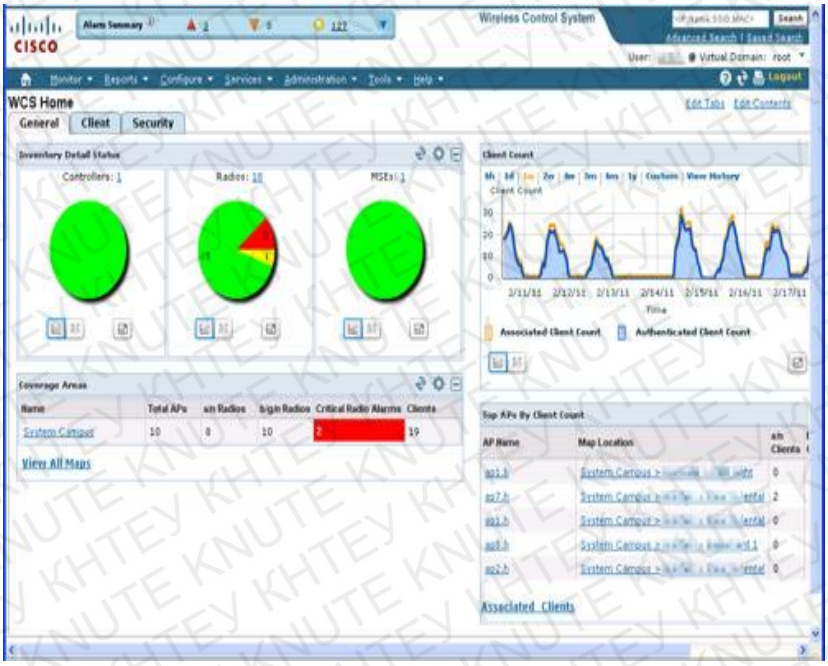


Рис. 3.3. WCS Home

3.1 Налаштування Wi-Fi контролера Cisco

Я обрав контролер wi-fi виробництва Cisco, та ще декілька нових точок доступу, для налаштування, отже, навіщо потрібен контролер? Не сильно вдаючись у подробиці, точки доступу і контролер спільно надають доступ бездротовим клієнтам до решти (дротових) частини мережі. Половину завдань, пов'язаних з доступом до радіо-середовища, генерацією beacon-фреймів, шифрування, виконує сама точка доступу. Іншу половину, в основному асоціацію та авторизацію, обслуговує контролер. Це називається Split-MAC архітектурою рис.3.4.

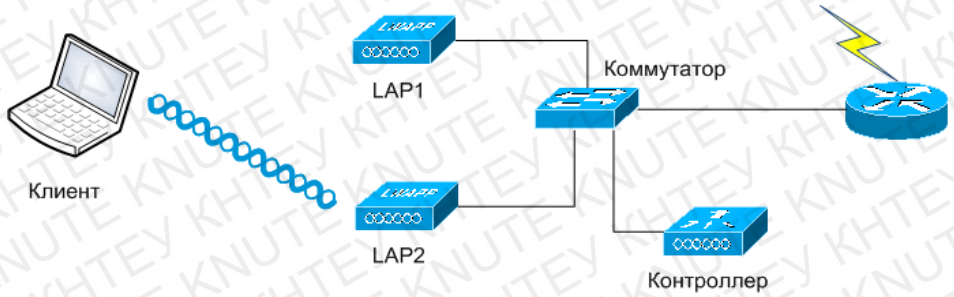


Рис.3.4 Split-MAC архітектура

До контролера через локальну комутовану мережу підключені точки доступу (звичайно виробництва Cisco, навіть коли протокол взаємодії CAPWAP відкритий). Їх може бути до сотень на контролер, залежно від його продуктивності. Кілька контролерів можна об'єднати в групи, при цьому забезпечується скоординована робота контролерів, і самих точок, згідно загальних налаштувань. Переваги такого підходу очевидні: централізоване управління, гнучкість налаштувань, відмовостійкість, балансування навантаження, інтелектуальні функції безшовного роумінгу, управління частотним ресурсом, потужністю, якістю обслуговування, авторизацією.

На точках доступу, підключених до контролера, так званих

«Легковагих» (lightweighted) працює практично такий же образ IOS (AIR-LAP-xxx), що і на звичайних (standalone, AIR-AP-xxx). Різниця у відсутності режиму «conf t», так як точки налаштовуються контролером централізовано. Прошивки між standalone lightweighted можливо змінювати в ручну. «туди і назад».

При старті точка доступу виробляє пошук кращого з доступних контролерів за досить складною схемою, авторизується, викачує прошивку (якщо потрібно), налаштування, і починає обслуговувати клієнтів. Між точкою і контролером організував канал управління (UDP порт 5246), і канал даних (UDP порт 5247). Користувальницькі дані инкапсулюються в UDP пакети незалежно від номера клієнтського WLAN/VLAN, що дозволяє розміщувати точки доступу де завгодно в мережі (на access портах комутаторів), та централізовано керувати безпекою на рівні VLAN на стороні контролера. Для випадку «віддаленого доступу», де немає контролера, передбачений режим з локальним свічингом трафіку клієнтів рис. 3.5.

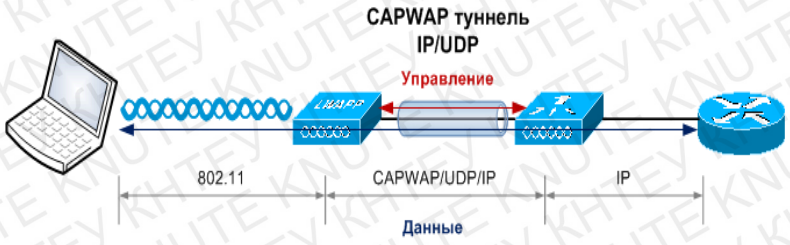


Рис.3.5 Керування безпекою VLAN на стороні контролера

Контролер архітектурно являє собою спеціалізований комп'ютер (різної апаратної архітектури та розрядністю, залежно від моделі) з досить старою версією MontaVista Linux всередині. До ядра додано декілька модулів, іноді драйвери для «заліза», що займається апаратним прискоренням шифрування або пересилання пакетів. Всі дії, пов'язані з життєдіяльністю контролера, виконує великий монолітний процес,

оформлений як user-додаток.

Підключивши контролер до електроживлення, COM-порту (9600/8/N/1) та локальної мережі, провів первинне налаштування. Нижче наведена процедура початкового налаштування контролера NME-AIR-WLC (модуль для маршрутизатора ISR), в моєму випадку успішно віртуалізованого та запущеного у віртуальній машині:

Cryptographic library self-test....passed!

XML config selected

Validating XML configuration

Cisco is a trademark of Cisco Systems, Inc.

Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 7.0.220.0

Initializing OS Services: ok

Initializing Serial Services: ok

Initializing Network Services: ok

Starting ARP Services: ok

Starting Trap Manager: ok

Starting Network Interface Management Services: ok

Starting System Services: ok

Starting Fastpath Hardware Acceleration: ok

Starting Switching Services: ok

Starting QoS Services: ok

Starting Policy Manager: ok

Starting Data Transport Link Layer: ok

Starting Access Control List Services: ok

Starting System Interfaces: ok

Starting Client Troubleshooting Service: ok

Starting Management Frame Protection: ok

Starting Certificate Database: ok

Starting VPN Services: ok

Starting LWAPP: ok

Starting CAPWAP: ok

Starting LOCP: ok

Starting Security Services: ok

Starting Policy Manager: ok

Starting Authentication Engine: ok

Starting Mobility Management: ok

Starting Virtual AP Services: ok

Starting AireWave Director: ok

Starting Network Time Services: ok

Starting Cisco Discovery Protocol: ok

Starting Broadcast Services: ok

Starting Logging Services: ok

Starting DHCP Server: ok

Starting IDS Signature Manager: ok

Starting RFID Tag Tracking: ok

Starting RBCP: ok

Starting Mesh Services: ok

Starting TSM: ok

Starting CIDS Services: ok

Starting Ethernet-over-IP: ok

Starting DTLS server: enabled in CAPWAP

Starting CleanAir: ok

Starting WIPS: ok

Starting SSHPM LSC PROV LIST: ok

Starting RRC Services: ok

Starting FMC HS: ok

Starting Management Services:

Web Server: ok

CLI: ok

Secure Web: Web Authentication Certificate not found (error). If you cannot access management interface via HTTPS please reconfig

Secure Web: Web Authentication Certificate not found (error). If you cannot access management interface via HTTPS please reconfigure Virtual Interface.

(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

Зупинив дію autoinstall. Вона дозволяє контролеру автоматично завантажити по TFTP заздалегідь приготований конфіг-файл. Таким чином, можна розгорнути в мережі дуже багато контролерів, не вдаючись до ручного налаштування кожного. Корисно, якщо працює система управління WCS.

Would you like to terminate autoinstall? [Yes]: yes

AUTO-INSTALL: process terminated - no configuration loaded

Встановив ім'я контролера (пропоноване генеруватись з MAC-адреси), логін і пароль адміністратора:

System Name [Cisco_bb: bb: 40] (31 characters max): **wlc4.xxx.xxx.net**

Enter Administrative User Name (24 characters max): **Artem**

Enter Administrative Password (3 to 24 characters): *************

Re-enter Administrative Password: *************

Налаштував адресацію інтерфейсу управління. Це логічний інтерфейс, через який контролер «спілкується» із зовнішнім світом (окрім точок доступу).

Звичайна практика така, що всі фізичні интерфейси контролера об'єднуються в EtherChannel групу (можна зробити це пізніше), в такому загальному каналі налаштував скільки потрібно логічних інтерфейсів,

кожен у своєму VLAN-і. У даному прикладі між комутатором і контролером створений trunk-порт, а обслуговування ведеться через VLAN 310. Для access-порту, або якщо застосовувати native VLAN, вказав номер 0. Адреса DHCP-сервера потрібна для пересилання тих клієнтських DHCP-запитів, якщо ті налаштовані. Контролер буде DHCP-Релеєм (хоча також може виконувати роль DHCP-сервера).

Management Interface IP Address: **xx.xx.145.10**

Management Interface Netmask: **255.255.255.128**

Management Interface Default Router: **xx.xx.145.1**

Management Interface VLAN Identifier (0 = untagged): **310**

Management Interface Port Num [1]:

Management Interface DHCP Server IP Address**: xx.xx.145.9**

Усі контролери, окрім моделі 5508, використовують окремий логічний інтерфейс ap-manager для спілкування з точками доступу. Таким чином Я налаштував його адресу з тієї ж мережі:

AP Manager Interface IP Address: **xx.xx.145.14**

AP-Manager is on Management subnet, using same values

AP Manager Interface DHCP Server (xx.xx.145.9):

Останній логічний інтерфейс - віртуальний. Він використовується для передачі DHCP-запитів клієнтам, веб-авторизації, роумінгу. На нього прописав адресу, яка не використовується ніде в мережі та немаршрутизаторах, зазвичай це 1.1.1.1 : він повинен бути однаковий для декількох контролерів, між якими передбачається роумінг клієнтів.

Virtual Gateway IP Address: **1.1.1.1**

Для цілей роумінгу клієнтів контролери об'єднав в групи мобільності (mobility group), ім'я яких і пропонується задати. Також пропонується задати ім'я групи контролерів, сукупно забезпечуючих управління радіоресурсом (частотний план і потужність, rf group). Хоча це можуть бути різні групи з набору пристроїв та імені, тут вказується загальне ім'я

(його можна змінити пізніше):

Mobility / RF Group Name: WLAB

Візард пропонує створити одну бездротову мережу (WLAN).

Network Name (SSID): test

також дозволив роботу бездротовим клієнтам, у яких IP-адреса прописана статично. Реально ця опція включає кешування ARP на контролері, що корисно.

Allow Static IP Addresses [YES] [no]:

Для цілей авторизації клієнтів (а також доступу до контролера, і деяких інших специфік) використав зовнішній RADIUS-сервер, який налаштував пізніше через веб-інтерфейс.

Configure a RADIUS Server now? [YES] [no]: **no**

Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.

Кожна точка доступу та контролер, мають код країни, в якій вони працюють. Насправді country code визначає дозволений набір частот (каналів) і граничних потужностей, що впливає на роботу алгоритмів автоматичного вибору частоти і т.д. Рекомендую, щоб у всій мережі список кодів країн був налаштований одноманітно.

Enter Country Code list (enter 'help' for a list of countries) [US]: **RU**

Контролер пропонує включити мережі 2.4 і 5 ГГц (11b/g/n і 11a/n відповідно). Насправді ці парамери передаються на асоційовані з контролером точки доступу, на яких власне і встановлено радіо. Було виявлено що включати радіо через веб-інтерфейс потрібно вже після того, як налаштовані всі інші параметри.

Enable 802.11b Network [YES] [no]: **no**

Enable 802.11a Network [YES] [no]: **no**

Запит на включення корисних алгоритмів динамічного управління частотним ресурсом та потужностями, те про що говорив раніше.

Enable Auto-RF [YES] [no]:

Налаштування часу (сервер часу, і статстично заданий час/часовий пояс) важливі не тільки для правильності тегів в лог-файлах, але і для роботи авторизації точок доступу за сертифікатами (вони використовують CAPWAP, заснований на DTLS, заснований на сертифікатах з відомими перевірками термінів валідності).

Configure a NTP server now? [YES] [no]: **no**

Configure the system time now? [YES] [no]: **no**

Warning! No AP will come up unless the time is set.

Please see documentation for more details.

Нарешті, коли все готово, контролер зберігає конфігурацію, та перезапускається:

Configuration correct? If yes, system will save it and reset. [Yes] [NO]: **yes**

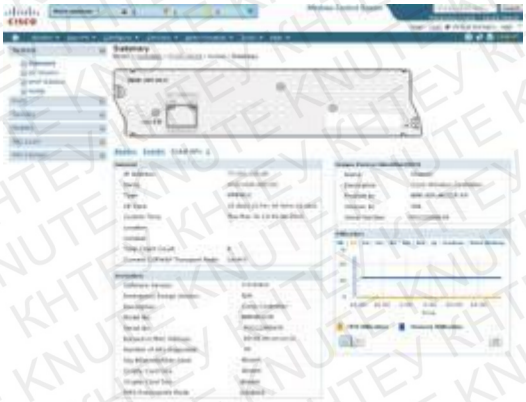
Configuration saved!

Resetting system with new configuration...

Тепер налаштував пристрій через веб-інтерфейс управління, який доступний через пару хвилин за адресою: https :/ / xx.xx.145.10. Щоб уникнути непотрібних питань про валідності сайту, контролеру виписав сертифікат для роботи SSL рис 3.6.

Рис.3.6 Інформація по контролеру

Потім впровадив за допомогою керівництва налаштування контролера вкрай зручний централізований засіб управління бездротовою мережею NCS/WCS, скриншот якого наведено нижче:



3.2 Підключення точок доступу до контролера Cisco

Користуючись описаним вище методом налаштував та підключив до локальної мережі контролер бездротових точок доступу Cisco WLC. Доступ до нього є, але «Wi-Fi-я кокристувачам» ще немає. Наступним кроком стало - підключити до контролера наявні точки доступу, які і будуть обслуговувати радіо-клієнтів. Незважаючи на відкритість CAPWAP протоколу, контролер буде працювати тільки з точками виробництва Cisco, про що прямо і заявляє виробник.

Далі, точки доступу з «автономного світу» (AIR-AP-xxx), переконвертував в світ контролерів (AIR-LAP-xx). Всі точки доступу підтримують дану операцію. Для проведення була потрібна сама точка доступу, доступна по мережі (з прописаним IP-адресою і відомими правами доступу), та або спеціальна безкоштовна утиліта, або ПЗ керування WCS або NCS, в якому присутній необхідний інструмент. Вся препрошивка, за великим рахунком в мене звилася до наступних операцій:

- переписуванню (TFTP) спеціального recovery-образу на точку доступу

- видаленню старого конфіг-файлу

- видаленню наявного автономного софта

- синхронізації годин

- генерації сертифіката точки доступу

Сертифікат мені потрібен тому, що протокол спілкування точки доступу з контролером, CAPWAP, в основі має протокол Datagram TLS, фактично захищений через сертифікати UDP-транспорт. Конвертована мною точка доступу перезавантажується, та «шукає» свій контролер. Процес пошуку включає в себе отримання IP-адреси пристроєм, і так само отримання списку контролерів, перевірки наявності, доступності та навантаженості кожного з них, і власне реєстрація обраного.

Точка доступу може або отримати IP-адресу у DHCP-сервера (будь-якого виробника: Cisco IOS, Miscosoft, Unix ISC-DHCP), або скористатися статично налаштованою IP-адресою. Залежно від обставин можна скористатися будь-яким методом. У моєму випадку для «ручної» установки точки доступу мені було потрібно підключитися до консолі (9600/8/N/1). При завантаженні точка доступу потрапляє в режим отримання адреси, і пошуку контролера. Типово, логін і пароль "Cisco" (з великої літери), enable пароль такий же. При деякій кількості невдалих спроб точка перезавантажується, і продовжує процес вічно. Для запобігання перезавантажень мені необхідно скасувати їх наступною недокументованою командою:

debug capwap client no-reload

Далі явно встановив точці адресу:

capwap ap ip address <ip_address> <subnet mask> capwap ap ip default-gateway <gw_address>

Далі встановив точці адреси контролерів:

capwap ap primary-base <controller_name> <wlc_mgmt_ip> capwap ap secondary-base <controller_name> <wlc_mgmt_ip>

Далі вказав адресу саме *management*-інтерфейс контролера. Та подивився на результат налаштування командою **show capwap client config:**

configMagicMark 0xF1E2D3C4

chkSumV2 47358

chkSumV1 27913

swVer 7.0.220.0

adminState ADMIN_ENABLED (1)

name ap2.wlab

location KorpusXX

group name ApGg1

mwarName wlc2.xxx.xxx.nxx

mwarIPAddress xx.xx.xx.3

mwarName

mwarIPAddress 0.0.0.0

mwarName

mwarIPAddress 0.0.0.0

ssh status Enabled

Telnet status Disabled

...

Для автоматичного налаштування IP-адреси точки доступу по DHCP задав необхідну опцію, номер 43, яка повідомляє точці про доступні їй адреси контролерів. Трюк полягає в тому, щоб передати в параметрах опції 43 адреси моїх контролерів. Значення параметра (в HEX вигляді) має формат TLV, наприклад, *f108c0a80a05c0a80a14*, де 0xf1 (241) - номер параметра опції, 0x08 (довжина даних, два рази по 4 байти октету IP адреси), 0xc0a80a05 переводиться в 192.168.10.5 і 0xc0a80a14 в

192.168.10.20. Точка доступу може отримати адреси контролерів також через запит по DNS, або від сусідів «по повітрю». Все, що точці доступу потрібно, це IP-зв'язність з контролером. Досить просто підключити її в access-порт (порт доступу) нашої локальної мережі, нарівні з іншими комп'ютерами.

Встановивши точку в локальній мережі спостерігаю, як вона намагається підключитися до контролера (Monitor-AP Join) рис.3.7:

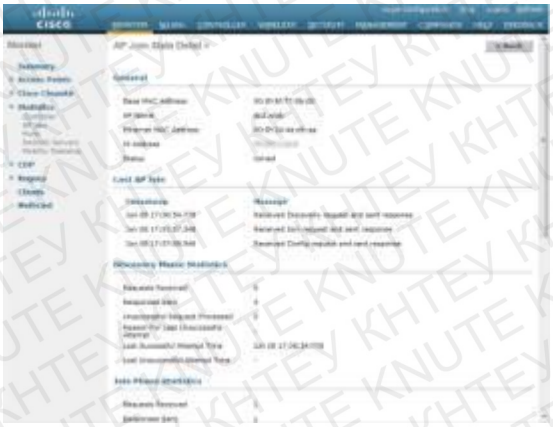


Рис. 3.7 Monitor-AP Join

Далі встановлюю політику безпеки, яка налаштував в меню "Security-AAA-AP Policies". Майже всі політики так чи інакше пов'язані з сертифікатами. Як було сказано, через деталі роботи CAPWAP дані між точкою і контролером зашифровані за допомогою сертифікатів. Контролер поставлявся з уже встановленими сертифікатами Cisco Systems (кореневим, та його похідними), може нести додаткові сертифікати для веб-авторизації і локального RADIUS-сервера рис.3.8.

Рис. 3.8 Вікно RADIUS-сервера для перевірки валідності MAC-адреси

Додатково застосував RADIUS-сервер для перевірки валідності MAC-адреси точки доступу рис 3.8. Також явно задав MAC-адресу точки, яка застосовує MIC-сертифікат (auth-list). Однак для SSC сертифікатів був зушений внести кожен з них у список, при цьому вказавши не тільки MAC-адресу Ethernet-інтерфейсу точки доступу, але також хеш (hash) сертифікат, для цього в контролері дозволив налагодження процесу перевірки сертифікатів:

(Cisco Controller)> debug pm pki enable

* SpamReceiveTask: Jun 10 21:49:39.450: sshpmGetCID: called to evaluate cscoDefaultIdCert

* SpamReceiveTask: Jun 10 21:49:39.450: sshpmGetCID: comparing to row 0, CA cert bsnOldDefaultCaCert

* SpamReceiveTask: Jun 10 21:49:39.450: sshpmGetCID: comparing to row 1, CA cert bsnDefaultRootCaCert

* SpamReceiveTask: Jun 10 21:49:39.450: sshpmGetCID: comparing to row 2, CA cert bsnDefaultCaCert

...

* SpamReceiveTask: Jun 10 21:49:39.731: sshpmGetIssuerHandles: subject L = San Jose, ST = California, C = US, O = Cisco Systems, MAILTO = support@cisco.com, CN = C1100-000f244ed6aa

* SpamReceiveTask: Jun 10 21:49:39.731: sshpmGetIssuerHandles: issuer L = San Jose, ST = California, C = US, O = Cisco Systems, MAILTO = support@cisco.com, CN = C1100-000f244ed6aa

* SpamReceiveTask: Jun 10 21:49:39.732: sshpmGetIssuerHandles: Mac Address in subject is 00:0 f: 24:4 e: d6: aa

* SpamReceiveTask: Jun 10 21:49:39.732: sshpmGetIssuerHandles: Cert Name in subject is C1100-000f244ed6aa

* SpamReceiveTask: Jun 10 21:49:39.732: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.

* SpamReceiveTask: Jun 10 21:49:39.741: ssphmSsUserCertVerify: self-signed user cert verfied.

...

* SpamReceiveTask: Jun 10 21:49:39.752: sshpmGetIssuerHandles: SSC Key Hash is d886bcaf0d22398538ccdef3f53d6ec7893463b8

* SpamReceiveTask: Jun 10 21:49:39.755: sshpmFreePublicKeyHandle: called with 0xf2de114

Далі вибрав пункт Add, тип SSC, скопіював MAC-адресу та хеш у відповідні поля, Apply, зачекав перезавантаження точки, вимкнув (debug disable-all), і точка підключена рис.3.9:

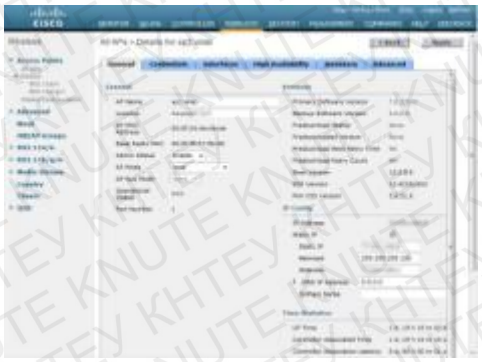


Рис.3.9 Додавання точки доступу

Додати хеш сертифіката можна також і вручну:

config auth-list ap-policy ssc enable config auth-list add ssc 00:0 f: 24:4 e: d6: aa d886bcaf0d22398538ccdef3f53d6ec7893463b8

Тепер, коли точки доступу підключені, можна включити радіо-інтерфейси (Wireless - 802.11a/n, 802.11b/g/n), режими-g,-n, та перейти до налаштування бездротових мереж (SSID).

3.3 Налаштування бездротової мережі та реалізація захисту на контролері Cisco

Користуючись керівництвом з первісного налаштування та підключення точок доступу до Wi-Fi контролера Cisco WLC, в мене побудована необхідна інфраструктура бездротової мережі. Тепер потрібно налаштувати самі мережі (WLAN, SSID), для надання послуг зв'язку користувачам.

Рис. 3.10 Меню WLANs

Хоча контролер управляється через командний рядок (консоль, ssh), було виявлено що майже всі операції з налаштування краще (швидше і зручніше) робити через веб-інтерфейс. Контролер доступний через HTTP (за умовчанням; краще перевести на HTTPS) з логіном-паролем, заданими при установці.

Всі налаштування провів в меню WLANs рис.3.10. Для створення нової мережі вибрав пункт меню «Create new» рис.3.11, та задав базові параметри:

Рис.3.11 Створення нової мережі в пункті Create new

Обрав тип мережі: WLAN (бездротова), тому що контролер може також працювати як Captive Portal для провідної мережі (Guest LAN).

Створивши нову мережу, я потрапив у вікно з закладками, в якому і вказав всі параметри її роботи рис.3.12:

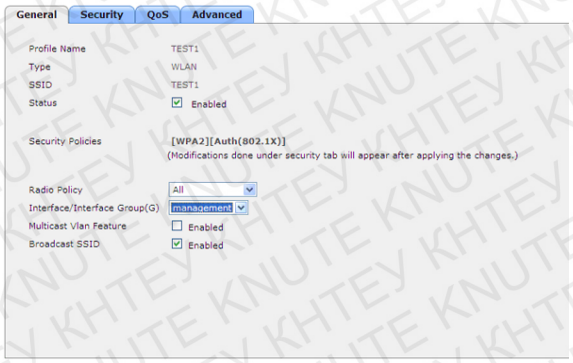


Рис.3.12 Меню для заданням параметрів нової мережі

– Enable включає/виключає обслуговування мережі точками доступу.

– Security policy оповіщатиме мене про поточний набір політик безпеки мережі, які налаштовуватиму далі.

– Radio policy вибираю всі дозволені діапазони та швидкості в яких працюватиме мережа.

– Interface визначає, на який провідний мережевий (саб-) інтерфейс (VLAN) контролера за замовчуванням буде підключення бездротових клієнтів. Мною створено кілька так званих «динамічних інтерфейсів», кожен зі своїм VLAN ID, що дозволяє розподіляти

користувачів в залежності від того, до якої мережі вони підключилися.

– Multicast VLAN визначає, куди у випадку кількох груп інтерфейсів буде йти мультикаст трафік.

Останній параметр Broadcast SSID визначає, чи буде ім'я мережі відображатися в beacon (анонсах) пакетів, що періодично розсилатимуться точкою доступу. Інакше це називається «відкрита/закрита мережа». Наступна закладка, Security, викликала в мене найбільший інтерес, рис.3.13.

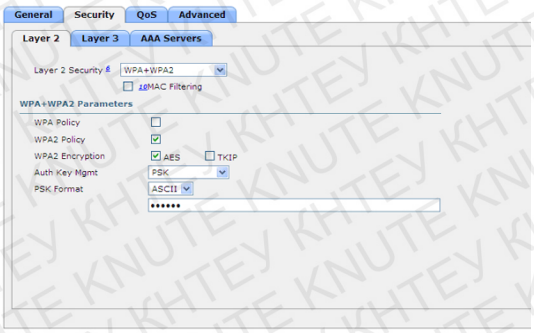


Рис.3.13 Налаштування безпеки

Безпека бездротової мережі будується з трьох компонентів:

– Авторизація

– Шифрування

– Веб-політика (опціонально)

Перші дві політики працюють на 2 рівні OSI, тому їх логічно назвали Layer 2. Авторизація в мене буде відповідати за те, кого пускати в мережу, та як. Шифрування визначатиме сам алгоритм шифрування пакетів в радіо-середовищі. Веб-політика дозволятиме загортати клієнтську HTTP-сесію на вбудований веб-сервер контролера, та запитувати підтвердження/логін-пароль через форму.

Мені доступні параметри безпеки 2-го рівня:

None - авторизація та шифрування трафіку не застосовуються («небезпечна мережа»). Використовується для гостьового доступу, в

хотспоти. Найчастіше комбінується з веб-політикою, при якій мені вдасться без питань підключитися до бездротової мережі, але при спробі кудись вийти веб-браузером сесія перехоплюється контролером, і мене змушать ввести логін-пароль, погодитися з умовами і т.п..

WPA + WPA2 – дозволяє мені вибрати політику WPA або WPA2 (або обидві), тип шифрування TKIP або AES (чи обидва). Дані параметри просто анонсуються клієнтам у beacon пакетах. Не всі клієнтські адаптери (особливо старі) здатні зрозуміти сучасні стандарти. Якщо всі клієнти - нові, найбільш оптимальним для мене буде використання WPA2/AES. Додатково пропонується вказати, як буде утворюватися ключ для шифрування:

802.1X - індивідуальний ключ для кожного клієнта буде генеруватися RADIUS-сервером у момент авторизації. Найбільш безпечний варіант, також іменований WPA (2) Enterprise.

CCKM - використовується власний механізм Cisco генерації ключів, підходить тільки для Cisco Wi-Fi телефонів.

PSK - загальний (pre-shared) ключ, пароль на мережу, іменовану в такому випадку WPA (2) Personal.

802.1x + CCKM - гібрид CCKM і RADIUS-ключа (для Cisco-телефонів).

802.1X - індивідуальний ключ для кожного клієнта буде генеруватися RADIUS-сервером у момент авторизації.

Static WEP - статичний WEP-ключ.

Static WEP +802.1 X - гібрид двох попередніх.

CKIP - пропрієтарний аналог WEP для Cisco телефонів.

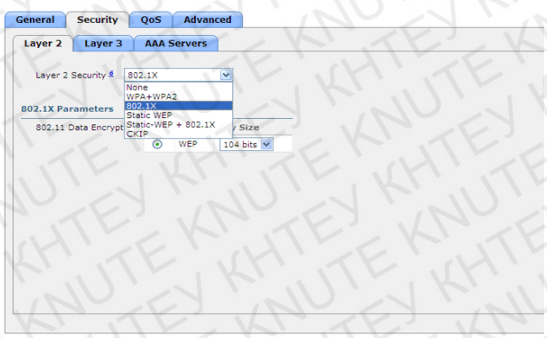


Рис.3.14 Вибір рівня безпеки

Проаналізувавши дані варіанти мені довелося робити вибір між:

1. Відсутністю шифрування/авторизації (гостьовий доступ).
2. WPA2 (AES) PSK aka «WPA2 Personal» для доступу в мережу по загальному паролю.
3. WPA2 (AES) + 802.1X aka «WPA2 Enterprise» для доступу в мережу через авторизацію на RADIUS-сервері (EAP: по доменному аккаунту, сертифікатом і т.п.).

Мій вибір зупинився на останньому варіанті так як він враховує політики безпеки перших 2-х, плюс йому доступні високі швидкості.

Також для того щоб забезпечити надійнішу безпеку мною було вирішено додати політику L3 рис.3.15, яка полягає в перехопленні клієнтської веб-сесії:

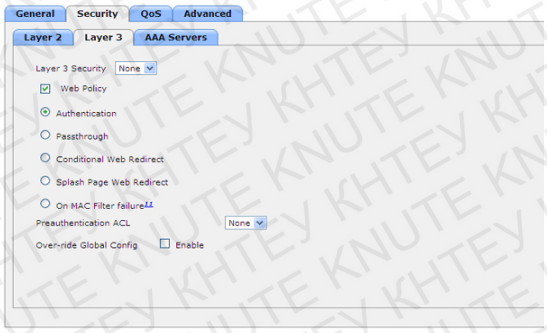


Рис.3.15 Вікно додаткових налаштувань безпеки

В даному вікні мені доступні наступні параметри:

Authentication - користувач бачить вікно введення логіна-пароля, які потім перевіряються на контролері (у його локальній базі), або на RADIUS-сервері.

Passthrough - користувач бачить вікно привітання, де у нього можуть опціонально запитати його e-mail адресу (далі ніде не використовується і не перевіряється).

Conditional Web Redirect - дозволяє редирект сесію користувача на зазначену у RADIUS-відповіді сторінку після авторизації. Наприклад, на сторінку поповнення балансу. Після редиректу користувач повинен авторизуватися.

Splash Page Web Redirect - те ж саме, але з доступом в мережу відразу.

On MAC Filter failure - редирект відбувається при блокуванні користувача MAC-фільтром.

Додатково вказав ACL (список доступу) для користувачів, які не пройшли авторизацію (наприклад, для DNS-сервера або зовнішнього веб-сервера з логотипом). Також вибрав, яку сторінку (форму) показувати користувачеві при авторизації (стандартну).

У разі використання RADIUS-сервера мені необхідно зробити додаткові налаштування. Перш за все, задати сам сервер авторизації в меню Security - RADIUS - AAA – Authentication рис.3.16:

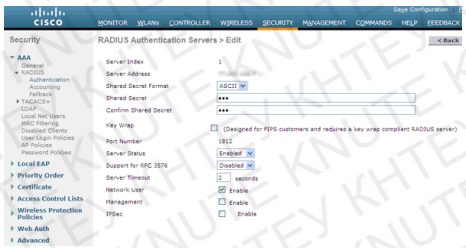


Рис.3.16 Меню захисту RADIUS-сервера

Де мені довелося вказати наступні параметри:

– IP-адресу сервера.

– Shared secret (ключ радіус-сервера).

– Network user - щоб сервер підтримував авторизацію користувачів Wi-Fi мережі.

– Management - щоб сервер підтримував авторизацію адміністраторів самого контролера. Інші параметри інтересу не представляють.

Потрібно також задати той же сервер для цілей обліку (Accounting). В параметрах налаштування безпеки бездротової мережі натиснув вкладку AAA серверів рис.3.17, де все вказане за замовчуванням, забезпечує роботу всіх зареєстрованих на контролері RADIUS-сервері.

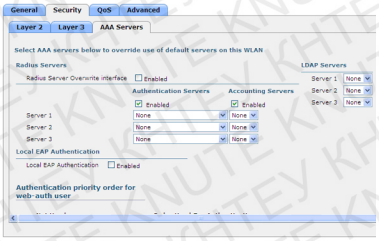


Рис.3.17 Налаштування AAA серверів

Закладка QoS відповідає за параметри якості обслуговування в мережі, даючи пріоритети різним типам трафіку та користувачам. В даному вікні проставив всі відмітки тому що в моїй бездротовій мережі широко використовується голос, відео, багато гостьових користувачів при великому навантаженні рис.3.18.

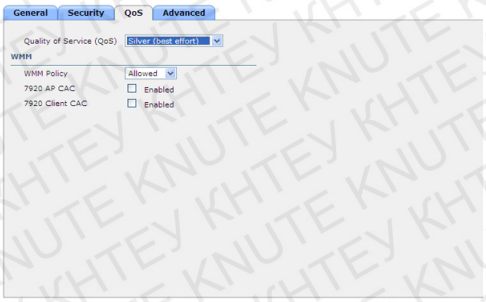


Рис.3.18 Надання пріоритету різним типам трафіку

Остання закладка, Advanced, рис.3.19., описує різні «додаткові параметри» моєї бездротової мережі, яких досить багато.

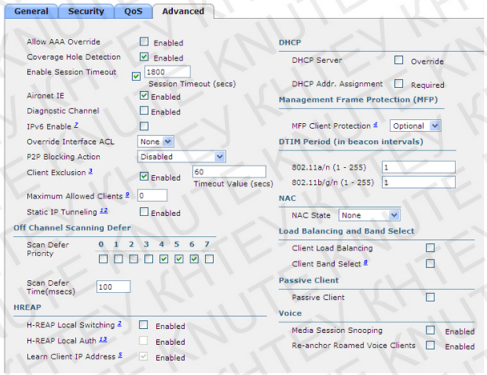


Рис.3.19 Додавання додаткових параметрів безпеки

Allow AAA Override - дозволяє передати додаткові параметри від RADIUS-сервера в момент успішної авторизації клієнта, та застосувати їх до даного клієнта індивідуально. Такими параметрами можуть бути номер VLAN, ім'я локального інтерфейсу, список доступу (ACL), URL для редиректу, QoS політика і т.п.

Coverage Hole Detection - управляє механізмом визначення та компенсації зони недостатнього покриття для клієнтів даної бездротової мережі. Рекомендую відключати для гостьових WLAN.

Enable Session Timeout, Session Timeout (secs) - включає і визначає тайм-аут сесії клієнта при веб-авторизації.

Aironet IE - включає специфічні для Cisco розширення параметрів beacon кадру. Розумні клієнтські адаптери у такому випадку працюють краще (роумінг, енергозбереження).

Diagnostic Channel - активує додатковий логічний канал діагностики для CCX5-сумісних клієнтських адаптерів.

IPv6 - в реальності тільки дозволяє IPv6 трафік для веб-авторизації.

Override Interface ACL - дозволяє задати альтернативний список

доступу (ACL) замість зазначеного на дротовому VLAN (management, dynamic) інтерфейсі контролера.

P2P Blocking Action - визначає політику пропускання трафіку між бездротовими клієнтами (в межах контролера). Допустимі значення: Disabled (пропускати), Drop (не пропускати), Forward-UpStream (відправляти на роутер, нехай він вирішує).

Client Exclusion, Timeout Value (secs) - включає і задає тайм-аут винятку (тимчасового блокування) клієнта, авторизація якого в бездротовой мережі закінчилася невдало.

Maximum Allowed Clients - задає максимальне число одночасних асоціацій з даною мережею.

Static IP Tunneling - дозволяє роумінг між контролерами клієнтів зі статичною IP-адресою.

Off Channel Scanning Defer, Scan Defer Priority - кожна точка іноді «зіскакує» зі свого робочого каналу (частоти) і слухає інші канали на предмет сусідніх мереж, чистоти спектру, «поганих» абонентів і т.п. При цьому таке «зіскакування» може негативно позначитися на голосовому трафіку, переданому даною крапкою. Якщо точка «бачить» пакети зі значенням 802.1p поля, зазначеного галочкою (0 1 2 3 4 5 6 7), то зіскок з робочою састоти буде відкладений.

Scan Defer Time (msecs) - на скільки мілісекунд відкладений.

H-REAP Local Switching - дозволяє точці доступу, яка знаходиться в режимі H-REAP (віддалений офіс) при обслуговуванні даної бездротової мережі «замикати» трафік абонентів локально, а не передавати в CAPWAP-тунелі на контролер.

H-REAP Local Auth - дозволяє точці доступу, яка знаходиться в режимі H-REAP (віддалений офіс) при обслуговуванні даної бездротової мережі проводити авторизацію локально, а не на контролері.

Learn Client IP Address - в режимі H-REAP точка буде рапортувати

IP-адресу клієнта на контролер, якщо той доступний.

DHCP Server Override, DHCP Server IP Addr - використовувати вказані IP-адреса DHCP-сервера замість того, який прописаний в налаштуваннях проводового інтерфейсу контролера, на яких «замикається» трафік бездротових клієнтів.

DHCP Addr. Assignment - вимагати використання DHCP-сервера клієнтами даної бездротової мережі (статично налаштовані клієнти працювати не будуть).

MFP Client Protection - включати і вимагати захист клієнтських фреймів, варіанти Disabled (немає), Optional (за наявності можливості) і Required (обов'язково, і всі ваші клієнти повинні підтримувати CCX5).

DTIM Period (in beacon intervals) - як часто передавати broadcast / multicast кадри, впливає на енергоефективність клієнтів.

NAC State - вибирає режим роботи спільно з пристроєм NAC.

Client Load Balancing - дозволяє балансування клієнтів між точками доступу згідно з їх завантаженості.

Client Band Select - дозволяє «виштовхування» клієнтів в діапазон 5ГГц, який більш кращий в силу меншої його завантаженості.

Passive Client - дозволяє роботу клієнтських пристроїв, які «мало говорять» (на кшталт Wi-Fi ваг).

Media Session Snooping - дозволяє «підглядати» в телефонні SIP-сесії.

Re-anchor Roamed Voice Clients - дозволяє примусово переноситись між контролерами голосових клієнтів, які перебувають у роумінгу.

Налаштувавши параметри мережі, натиснувши на кнопочку Apply і не забувши зберегти конфігурацію контролера, підключаюся до захищеної мережі.

ВИСНОВКИ

В даній дипломній роботі, а саме в першому розділі було розглянуто основні поняття: корпоративна мережа, безпека корпоративної мережі, атаки на мережу Wi-Fi, стандартні методи захисту, стратегія побудови та забезпечення безпеки мережі Wi-Fi. Другий розділ присвячений: технологіям WI-FI мереж, сценарію проектування та розгортання мережі Wi-Fi (WLAN), підходам до планування та проектування розвиненої мережі Wi-Fi, радіообстеження зони покриття мережі Wi-Fi. Отже будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи пов'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес-процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вона не займалася - для урядової установи, банку, промислового підприємства, комерційної фірми.

Такий загальний погляд на організацію, дозволяє сформулювати деякі загальні принципи побудови бездротових корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації.

Також було з’ясовано, що безпровідна територіально розподілена корпоративна мережа - це система що забезпечує передачу інформації між різними додатками, які використовуються в системі корпорації.

Корпоративна мережа являє собою мережу окремої організації. Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP та використовує комунікаційні стандарти Інтернету, а також сервісні додатки, що забезпечують доставку даних користувачам мережі.

Були обговорені питання що до захисту інформації від несанкціонованого доступу, а також наведені кілька стратегій безпеки які можна застосувати для захисту інформації в бездротовій мережі Wi-Fi та їх розгортання.

Виявлені проблеми безпеки з якими може зіткнутися створена мережа.

В третьому розділі було розроблено бездротову локальну мережу (WLAN – wireless LAN) на основі поєднання уніфікованої бездротової інфраструктури (CUWN) Cisco, і доменної інфраструктури Microsoft, яка використовується в офісах для підключення мобільних співробітників у місцях перебування значної кількості користувачів. Проведено налаштування бездротової мережі та реалізації захисту на контролері фірми Cisco, яке і використовувалось для створення всієї корпоративної мережі.

Слід звернути увагу, що правильно налаштована безпровідна мережа являє собою нездоланний бар’єр для зловмисника, звичайно, до відомої границі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яковлев М, 2012. – С.328.
2. Ботт Э. Эффективная работа: Безопасность Windows / Э. ботт, К. Зихерт, 2013. – С.682.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации / Л. В. Бройдо, 2015. – С.688.
4. О. С. Муранов Апаратні та програмні засоби персональних комп'ютерів : конспект лекцій для студ. спец. "Радіотехніка" / О. С. Муранов ; Одес. нац. політехн. ун-т. - О. : Наука і техніка, 2016. – С.135. : рис., табл. - Бібліогр.: с. 133. – 100 экз.
5. Воройский Ф.С. Основы проектирования автоматизированных библиотечно-информационных систем: Справочное пособие / Ф.С. Воройский - М.: ФИЗМАТЛИТ, 2015. – С.384.
6. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин - М.: ДМК Пресс, 2014. – С.616.
7. Телекоммуникации и сети: тез. докл. науч.-практ. конф. (окт. 2013) / отв. ред. В.А. Галкин М.: МГТУ им. Н.Э. Баумана, 2013. – С.608.
8. Аппаратные средства локальных сетей. М.Гуки – С.576.
9. Камышников В.В. Основы сетевой архитектуры Internet. [Текст] / В.В. Камышников - Самара: Издательство «Самарский университет», 2011. – С.107.
10. Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта /А.А. Корниенко, В.В. М. Кулыгин Технологии корпоративных сетей: Энциклопедия. / М.

Кулыгин, 2017. – С.704.
11. Курило А.П. Обеспечение информационной безопасности бизнеса. / А.П. Курило – М.: ВДС-пресс, 2015. – С.512.
12. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 2-е изд. / В.Г.Олифер, Н.А. Олифер, 2014. – С.864.
13. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко А.А. Под ред. Пятибратова А.П.- М.: Финансы и статистика, 2016. – С.512.
14. Родичев Ю.А. Принципы проектирования корпоративных информационных сетей образовательных учреждений. / Ю.А. Родичев, К.В. Чарковский // Журн.Вестник СамГТУ. Серия: Физико-математические науки. 2016, выпуск 19 С.150-155.
15. Родичев А.Ю. Системная модель защиты информации информационных систем распределенного типа. /А.Ю. Родичев, Ю.А. Родичев // Журн. Вестник Самарского гос. ун-та. 2013. – № 2 – С.15-20.
16. Родичев Ю.А. Элементы теории корпоративных информационных систем сферы подготовки и развития интеллекта. / Ю.А. Родичев // Журн. Вестник Самарского гос. ун-та. 2014. – № 2, – С. 176-187.
17. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. А.В.Соколов, В.Ф. Шаньгин– М.: ДМК Пресс, 2012. – С. 656.
18. Танненбаум Э. Компьютерные сети. 4-е изд. / Э.Танненбаум-МПб, 2013. – С. 992.
19. Титоренко Г.А. Методы и средства построения систем информационной безопасности. Их структура. 2-е издание, дополненное / Г.А. Титоренко – М., 2013. – С. 205.
20. Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта /В.В. Яковлев, А.А. Корниенко М, 2012. – С. 328.

21. Олифер В.Г. Новые технологии и оборудование IP-сетей / В.Г. Олифер, Н.А. Олифер – 2011.
22. Самардак А.С. Корпоративные информационные системы / А.С. Самардак – 2011.
23. Просис Д. Руководство по TCP/IP для начинающих / Д. Просис // Журн. PC Magazine. – 2010 р. – № 3. – С.58-67.
24. Семенов Ю.А. Протоколы и ресурсы Internet / Ю.А. Семенов. – 2012. С.420.
25. Комплексные решения по построению инфраструктуры предприятия. [Электронный ресурс] : - Режим доступа : www/ URL: http:// www.lankey.ru. Загл. с екрану. – 2013.
26. Кутыркин С. Б. Повышение качества предприятия с помощью информационных систем класса ERP / С.Б. Кутыркин, С.А.Волчков, И.В. Балахонов. – 2015 С. 348.
27. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы 4 издание / В.Г. Олифер, Н.А. Олифер. – 2013 – С. 916.
28. Plunkett, Jack, Balan, Andreea, Brison, Brandon , Jordan, Daniel P,Kolber, Maria, Plunkett's Wireless, Wi-Fi, RFID and Cellular Industry Almanac, Plunkett Research Ltd 2018. – 461 p.
29. Michelle Bornstein,Wifi Hotspot: Advantages and Disadvantages of Wifi Hotspots, 2015. – 17 p.