ЗМІСТ

ВСТУП

Деякий час назад готельні комплекси надавали, фактично, тільки послуги з проживання та сфер розваг. Зараз, в епоху розвитку інформаційних технологій та Інтернету, клієнтам готельних комплексів необхідні сучасні послуги зв'язку - якісний і економічно привабливий телефонний зв'язок, швидкісний бездротовий Інтернет-доступ і інтерактивні сервіси.

Слід зауважити, що у ряді випадків наявність подібної інфраструктури в готельному комплексі є вирішальним кроком при замовленні номерів, а комерційне надання якісних послуг «Інтернету через Wi-Fi» дозволяє збільшити дохід власника готельного комплексу, повертаючи вкладені інвестиції протягом досить короткого терміну.

Організація Wi-Fi в готелі - це зовсім не привілей найбільш статусних закладів, а обов'язкова міра для забезпечення зручності відвідувачів. Переважаюче число клієнтів готелів - це бізнесмени і туристи. Перші – обирають постійний і безперервний зв'язок з діловими партнерами, другі потребують регулярного обміну новими враженнями і емоціями зі своїми друзями і близькими. Для того, щоб клієнти підтримували контакти з потрібними людьми, а також мали необмежений доступ до інтернет-ресурсів, сучасні готелі організовують безпровідні мережі не лише усередині, але і зовні будівлі. Більше того, нерідко наявність Wi-Fi - це один з основних критеріїв вибору тимчасового місця проживання. Отже, встановити якісне покриття бездротовою мережею - це рішучий крок для підвищення рейтингу закладу.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Інформаційно-технічна революція змінила характер і методи ведення бізнесу. Використання можливостей технічного обміну сьогодні дозволяє легше і швидше створювати і продавати пакети послуг споживачам, вирішувати завдання фінансово-операційного управління, маркетингового планування, підвищувати конкурентоздатність і кількість продажів.

Для швидкого і безпомилкового контролю операцій повноцінного аналізу існуючої ситуації, швидкості і повноти обслуговування гостя у фронт-офісі, тобто для забезпечення високої економічної ефективності та високої якості послуг, неминучим і незамінним стає впровадження автоматизованих інформаційних систем управління.

Інформаційні технології (IT) готельного управління з'явилися у світовій готельній індустрії давно — біля двадцяти п'яти років тому, і пройшли великий шлях розвитку. На українському ринку IT управління готелем присутні відносно недавно. Експерименти з упровадження даних систем у готелях України стали проводиться з середини 90-х років. Кількість впроваджень вимірюється в десятках, а їхня якість найчастіше є предметом суперечок, чуток, домислів і розчарувань по сьогоднішній день.

Коли людина зупиняється в готелі під час відпустки, йому хочеться написати своїм рідним, друзям про сам готель, ресторан і номер, проте якщо у нього немає виходу в Інтернет, то ці повідомлення ніхто не прочитає. Для одних така незручність не має особливого значення, але іншим воно може серйозно зіпсувати враження від готелю, а якщо гість - це бізнесмен, а не турист, то відсутність доступу до Інтернету поставить під питання успіх його поїздки.

На жаль, багато готелів в Західній Європі недооцінюють важливість надання повноцінних сервісів Wi-Fi, хоча в довгостроковій перспективі це

загрожує втратою потенційних клієнтів, які можуть віддати перевагу конкурентам традиційних готелів.

У ZYXEL вирішили з'ясувати, як готельна галузь за допомогою сервісів Wi-Fi задовольняє потреби клієнтів в постійному доступі в Інтернет, і опитали більше 400 готелів, що відповідають за IT менеджерів, з дев'яти європейських країн. До нашого здивування, менеджери готельного бізнесу не рахують Wi-Fi одним з трьох основних критеріїв, по яких мандрівники вибирають готель. На думку менеджерів, цими критеріями є місце, ціна і відгуки (в порядку пріоритетності). Ці дані різко розходяться з результатами нашого попереднього дослідження, проведеного у Великобританії в 2016 році, згідно з яким британські готелі рахують Wi-Fi другим за значимістю критерієм при виборі конкретно.

ZYXEL (Zyxel Communications Corp) - велика міжнародна компанія з штаб-квартирою на Тайвані, відомий виробник мережевого устаткування для середнього і малого бізнесу, промислових підприємств і будинку.

Як бізнесмени, так і туристи розглядають Wi-Fi як стандартний сервіс готелю, включаючи необмежений доступ до Wi-Fi в номері. З цією думкою згідно і переважна більшість (95%) менеджерів європейських готелів, проте у них і їх гостей абсолютно різні поняття про задовільну якість Wi-Fi. Гостям потрібні ті ж сервіси Wi-Fi, якими вони користуються удома, і вони вважають, що часто готелі не надають такі сервіси. Невипадково поганий Wi-Fi є другою найпоширенішою причиною скарг гостей готелю після шуму в номері (рисунок 1.1).

Не варто чекати, що гості готелю, при поганому Wi-Fi, будуть використовувати Інтернет 3G/4G. У багатьох місцях, особливо в сільській місцевості, все ще немає надійного сервісу передачі даних по стільниковій мережі.

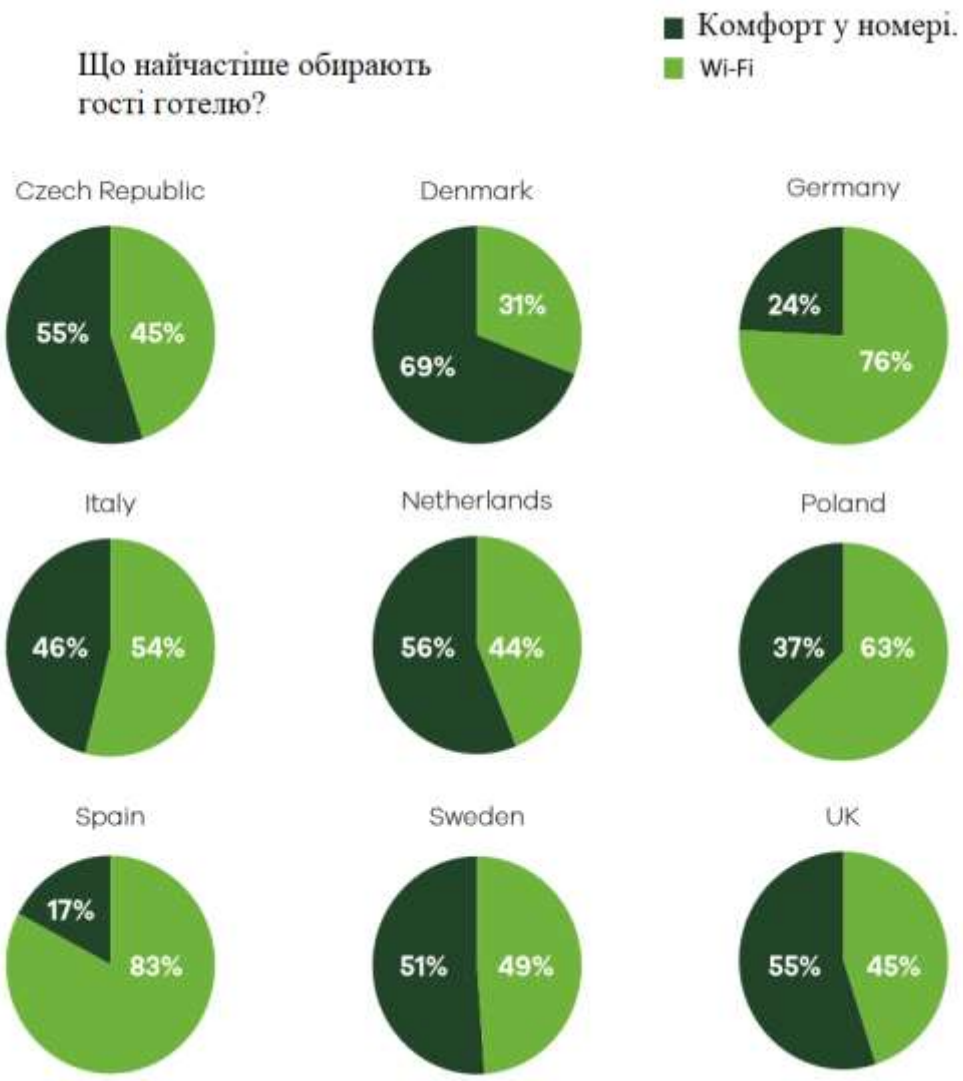

Рисунок 1.1 – Статистика потреб відвідувачів.

Крім того, гості з інших країн часто не можуть використати стільниковий зв'язок із-за високих тарифів на роумінг передачі даних, тому для них Wi-Fi є єдиним прийнятним за ціною варіантом підключення до Інтернету.

Такі часті скарги повинні стати причиною для занепокоєння усієї індустрії, проте майже третина (37 менеджерів готелів заявила, що у них не було жодних проблем зі своїм сервісом Wi-Fi, і тільки 10-ть з них "не дуже задоволені" або "зовсім не задоволені" сервісом Wi-Fi, який їх готель пропонує гостям. Проте більше половини (52 указали, що у них виникають проблеми коли гості намагаються підключити багато пристроїв до

безпровідної мережі, причому 12 із них постійно стикаються з цією проблемою.

Рисунок 1.2 – Статистика скарг відвідувачів.

1.2 Загрози кібербезпеки бездротової мережі у готельному бізнесі

Читаючи в мережі відгуки про готелі, нерідко можна наштовхнутися на наступні скарги постояльців :

- повільно вантажаться сторінки,
- доводиться по кілька разів підключатися до Wi-Fi,
- сильно гальмує при перегляді відео,
- і так далі.

Треба розуміти, що швидкість загального каналу Інтернет (трафік), який надається провайдером для готелю, ділиться між активними абонентами, тобто тими абонентськими пристроями, які в даний момент приймають/передають дані.

При веб-серфінгу навантаження на канал не високе (користувач відкрив сторінку і читає). Але якщо декілька користувачів дивляться on-line відео або використовують торенти, тоді канал "забивається" повністю, швидкість завантаження (передачі) даних падає, і інші користувачі можуть і не отримати доступ в Інтернет взагалі. Частіше, під час переміщення гостей зі своїм мобільним пристроєм усередині будівлі готелю і по прилеглій території з'єднання з мережею Інтернет може уриватися.

Причиною подібних неприємностей є, в першу чергу, неправильно спроектована Wi-Fi мережа і відсутність безшовного роумінгу, при якому перемикання абонентських пристроїв між точками доступу повинне відбувається автоматично без втрат даних. Серед головних причин незадовільної якості Wi-Fi доступу :

- недостатня пропускна спроможність загального каналу Інтернет, що надається провайдером,

- неправильний розподіл трафіку між користувачами,

- недостатня кількість точок доступу (погана зона покриття),

- недостатня потужність Wi-Fi устаткування,

- нефахове Wi-Fi устаткування, призначене для домашнього використання,

- Wi-Fi устаткування встановлене в місце, схильний до впливу перешкода.

Гості готелю мають бути упевнені в захищеності інформації, яку вони передають по мережі (наприклад, введення персональних даних, паролів, номерів банківський карт і так далі).

У прагненні залучити клієнтів максимально дешевими послугами готелі не займаються впровадженням систем безпеки, характерних для серйозних компаній, в готелях дуже легко здійснити атаки типу MiM (атака посередника) і MiB (атака через браузер).

Далі, готелі використовують застарілі і неоновлювані Wi-Fi - роутери, що ще більше погіршує ситуацію. Наприклад, в недавньому дослідженні

компанії Cylance відзначалося, що в 277 готелях в 29 країнах світу використовуються роутери ANTLabs InnGate з критичною уразливістю, яка дозволяє зловмисникам зчитувати дані з комп'ютерів користувачів і навіть входити в комп'ютерні системи самого готелю.

У 2015 році з’явилась нова проблема в цій сфері діяльності. До 2015 року більшість готелів залежно від їх розмірів стали жертвами кіберзлочинів. Кіберзлочинці також "поклали" очі на ті компанії, які надають послуги для готелів.

White Lodging керує рядом відомих готелів, таких як Hilton, Marriott, Hyatt, Sheraton і Westin. Хоча вони представляють собою більше компанію з управління готелями, ніж мережу готелів, вони також стали жертвами великої кібер-атаки, про яку стало відомо в 2014 році. У 2013 році в чотирнадцяти їх готелях була скомпрометована інформація про кредитні і дебетові картки клієнтів.

White Lodging - це найбільш швидкозростаюча компанія, що займається розробкою і управлінням готелів в Америці.

Через два роки вони зіткнулися з ще однією атакою на десять своїх готелів (деякі з них були жертвою попередньої атаки). Хакери завдали ще більшої шкоди, вкравши дані за кредитними картками клієнтів: імена власників карток, номери, коди безпеки і терміни дії. За даними White Lodging, ця атака відрізнялася від тієї, що була в 2013 році.

Mandarin Oriental

Розкішний Mandarin Oriental був атакований в березні 2015 року. Шкідлива програма заразила POS-термінали в деяких готелях групи, розташовані в Європі і Америці. Шкідлива програма була спеціально розроблена і направлена на такі типи машинних систем, дозволяючи здійснювати крадіжку інформації про кредитні картки.

Trump Hotels

У період з травня 2014 по червень 2015 було атаковано сім закладів. Як вони самі зізналися, були вкрадені дані кредитних карт клієнтів через

заражені POS-термінали і ПК, розташовані в їх ресторанах, магазинах з сувенірами і т.д. Злочинцям вистачило одного року, щоб отримати величезний обсяг персональної конфіденційної інформації.

Hard Rock Las Vegas

В результаті атаки було заражено кілька POS-терміналів в їх ресторанах, барах і магазинах. Але пристрою в готелі або казино не постраждали. Протягом семи місяців (з вересня 2014 до квітня 2015) Hard Rock Las Vegas зіткнувся з атаками, які привели до крадіжки даних 173 000 банківських карт з їх ресторанів, барів і магазинів. Але вони були не єдиним постраждалим готелем / казино. FireKeepers Casino Hotel в Battle Creek також постраждав в 2015 році.

Hilton Worldwide

У листопаді 2015 року Hilton Worldwide поширив прес-реліз, в якому компанія зізналася, що стала жертвою кібер-атаки. Вони не повідомили докладної інформації про те, що ж сталося, але відомо, що була скомпрометована вся інформація про кредитні картки клієнтів. На щастя, PIN-коди й інша персональна інформація не постраждали.

Starwood

Приблизно в той же самий час, коли була атака на Hilton, Starwood повідомив про те, що вони стали жертвою аналогічної кібер-атаки. Було атаковано 105 готелів в мережі Starwood (Sheraton, St. Regis, Westin, і т.д.), що зробило цю атаку найбільшою атакою на готелі подібного роду на той момент. Вони опублікували список готелів, де були заражені їх POS-термінали.

Hyatt

Рекорд Starwood протримався недовго. Потім сталося те, що ми знаємо як найбільша в історії кібер-атака на готелі. Мережа готелів Hyatt в своєму прес-релізі підтвердила, що були заражені POS-термінали в їх 249 готелях, розташованих в 54 країнах світу. З липня по вересень 2015 року було

заражено їх POS-термінали (знову ж!), Після чого були вкрадені дані кредитних карт всіх їх клієнтів.

Rosen Hotels & Resorts

Найостаннішими жертвами стали Rosen Hotels & Resorts. Поки вони не надали подробиць крадіжки, але вони підтвердили, що їх POS-термінали були заражені шкідливими програмами з вересня 2014 до лютого 2016 року Заразивши їх POS-системи, невідомі особи отримали доступ до даних кредитних карт клієнтів установ Rosen за останні півтора року.

1.3 Аналіз нормативно-правової бази у сфері інформаційної безпеки

У різних технологічно розвинених країнах розроблено і розробляється велика кількість стандартів інформаційної безпеки. Це насамперед міжнародні стандарти оцінки інформаційної безпеки, які використовуються в Україні – ISO 15408, ISO 17799 (BS7799), ISO 27001, BSI; стандарти аудиту, що відображають питання інформаційної безпеки, – COBIT, SAC, COSO, SAS 55/78 і деякі інші.

– BS 7799-1:2005. Information security management. Code of practice for information security management (Практичні правила управління інформаційною безпекою);

– BS 7799-2:2005. Information security management. Specification for information security management systems (Вимоги до систем управління інформаційною безпекою);

– BS 7799-3:2006. Information security management systems. Guidelines for information security risk management (Керівництво з управління ризиками інформаційної безпеки).

– ДСТУ 27001. – Методи захисту систем управління інформ. безпекою.

Впровадження стандарту ДСТУ 27001 в практику увазі наявність в організації як мінімум двох документів: політики ІБ та методології оцінки ризиків ІБ, однак для останнього документа в національній нормативній базі

не відображені питання розробки, форма і зміст. Недолік вітчизняної нормативної бази ІБ полягає у відсутності українського ДСТУ по ризиках.

1.4 Постановка задачі

На підставі аналізу нормативно-правової бази, у сфері захисту інформації, можна зробити висновок, що на підприємствах готельного бізнесу важливо захищати інформацію яка оброблюється, зберігається та циркулює у системі.

На моєму підприємстві ТОВ «ІНТЕР-ГОТЕЛЬ», необхідно вирішити такі питання:

1) Визначити, які загрози кібербезпеки бездротової мережі існують у готельному комплексі.
2) Розглянути, які існують рішення кібербезпеки бездротової мережі у готельному комплексі.
3) Зібрати дані про підприємство, виконати обстеження інформаційного середовища та обстеження обчислювальної системи.
4) Проаналізувати технології моделювання активного обладнання.
5) Визначити який метод шифрування, для передачі даних, встановлений.
6) Зробити висновки.

1.5 Методи рішення проблематики кібербезпеки бездротової мережі у готельному комплексі

Готелі - дуже вигідна мета для кіберзлочинців, оскільки в них зупиняється особливо цікава для них аудиторія: бізнесмени, знаменитості, менеджери компаній. Тому недивно, що цілі хакерські угрупування спеціалізуються на готелях. "Кримінальна група компрометує Wi-Fi - мережі готелю і потім чекає, коли жертва зайде в мережу, щоб змусити її

завантажити що-небудь і встановити програмну закладку, яка заражає пристрій шпигунським ПО".

Інший вид атаки називається "Злий близнюк". Хакери створюють підробну мережу, яка схожа на мережу готелю, і постояльці входять в неї. Тепер хакери можуть легко красти їх логіни і паролі, направляти на фішингові сайти, перехоплювати файли - словом, робити все, що їм заманеться.

Програми типу Mana дозволяють здійснювати такі атаки в напівавтоматичному режимі, і готелі - просто ідеальна сфера їх застосування. Встановивши подібні програми, хакери можуть не зупинитися на зломі ваших паролів. "Вони можуть проаналізувати ваш пристрій і визначити, де ви живете або працюєте", - говорить старший аналітик SensePost Гленн Уилкинсон (Glenn Wilkinson).

Він розробив відому програму Snoopy з метою довести, як легко симулювати Wi-Fi - мережу готелю і змусити постояльців підключатися до підробної мережі. Можна було б подумати, що в дорогих готелях проблема менш актуальна, але на практиці частіше буває навпаки: чим вище клас готелю, тим вище шанси виявитися жертвою хакерів. "

Безпека Wi-Fi мережі забезпечується за допомогою пароля доступу до мережі і алгоритмів шифрування даних (WEP, WPA, WPA2). Не рекомендується використати в готелі постійний пароль для доступу до Wi-Fi, оскільки зловмисники з легкістю можуть заволодіти їм. Уникнути подібної проблеми допоможе функція "Хотспот", яка дозволяє створювати безліч тимчасових паролів для доступу до готельної безпровідної мережі. Наприклад, гостеві, що приїхав на 3 дні дається пароль, який діятиме відповідно 3 дні, а для відвідувачам, які прийшли в конференц-зал готелю, на час конференції.

Сьогодні на ринку Wi-Fi присутні безліч брендів. Різниця між дорогими і дешевими рішеннями для організації готельної Wi-Fi мережі полягає, як правило, у більшій зоні покриття, більшій кількості абонентів, що

підключаються, більш високій мірі захисту (безпеці) і більшій кількості функцій управління.

Сама природа Wi-Fi, коли дані передаються по відкритих радіочастотах, робить його уразливим (в усякому разі без належних систем шифрування), проте готелі особливо виділяються на загальному фоні. Наприклад, у готелях практично ніколи не використовується протокол безпеки WPA.

Це означає, що будь-який пристрій в мережі передає усі дані у вигляді простого тексту, перехопити і прочитати який для зловмисників не складає ніяких труднощів. Для цього навіть не треба спеціальне програмне або апаратне забезпечення - досить дешевого Wi-Fi - адаптера і якої-небудь безкоштовної програми.

1.6 Безпека в мережах Wi-Fi. WEP, WPA, WPA2 шифрування

Серйозною проблемою для усіх безпровідних локальних мереж (і, якщо вже на те пішло, то і усіх дротяних локальних мереж) є безпека. Безпека тут так само важлива, як і для будь-якого користувача мережі Інтернет. Безпека є складним питанням і вимагає постійної уваги. Величезної шкоди може бути завдана користувачеві через те, що він використовує випадкові хот-споты (hot - spot) або відкриті точки доступу Wi-Fi удома або в офісі і не використовує шифрування або VPN (Virtual Private Network - віртуальна приватна мережа). Небезпечно це тим, що користувач вводить свої особисті або професійні дані, а мережа при цьому не захищена від стороннього вторгнення.

WEP

Спочатку було складно забезпечити належну безпеку для безпровідних локальних мереж. Хакери легко здійснювали підключення практично до будь-якій Wi-Fi мережі зламуючи такі первинні версії систем безпеки, як Wired Equivalent Privacy (WEP). Ці події залишили свій слід, і довгий час деякі компанії неохоче впроваджували або зовсім не впроваджували у себе

безпровідні мережі, побоюючись, що дані, що передаються між безпровідними Wi-Fi пристроями і Wi-Fi точками доступу можуть бути перехоплені і розшифровані. Таким чином, ця модель безпеки уповільнювала процес інтеграції безпровідних мереж у бізнес і примушувала нервувати користувачів, які використовують Wi-Fi мережі будинку.

Тоді інститут IEEE, створив робочу групу 802.11i, яка працювала над створенням усеосяжної моделі безпеки для забезпечення 128-бітового AES шифрування і автентифікації для захисту даних. Wi-Fi Альянс представив свій власний проміжний варіант цього специфікації безпеки 802.11i: Wi - Fi захищений доступ (WPA - Wi-Fi Protected Access). Модуль WPA поєднує декілька технологій для вирішення проблем уразливості 802.11 WEP системи. Таким чином, WPA забезпечує надійну автентифікації користувачів з використанням стандарту 802.1x (взаємна автентифікація інкапсуляція даних які передаються між безпровідними клієнтськими пристроями, точками доступу і сервером) і розширюваний протокол автентифікації (EAP).

Також, WPA оснащений тимчасовим модулем для шифрування WEP, 128 - бітового шифрування ключів і використовує часовий протокол цілісності ключів (TKIP). А за допомогою контрольної суми повідомлення (MIC) запобігає зміна або форматування пакетів даних. Таке поєднання технологій захищає конфіденційність і цілісність передачі даних і гарантує забезпечення безпеки шляхом контролю доступу, так щоб тільки авторизовані користувачі отримали доступ до мережі.

WPA

Подальше підвищення безпеки і контролю доступу WPA полягає в створенні нового унікального майстра ключів для взаємодії між кожним призначеним для користувача безпровідним устаткуванням і точками доступу і забезпеченні сесії автентифікації. А також, в створенні генератора випадкових ключів і в процесі формування ключа для кожного пакету. У IEEE стандарт 802.11i, ратифікували в червні 2004 року, значно розширивши

багато можливостей завдяки технології WPA. Wi-Fi Альянс зміцнив свій модуль безпеки в програмі WPA2.

Таким чином, рівень безпеки передачі даних Wi-Fi стандарту 802.11 вийшов на необхідний рівень для впровадження безпровідних рішень і технологій на підприємствах. Одно з істотних змін 802.11i (WPA2) відносно WPA це використання 128-бітового розширеного стандарту шифрування (AES). WPA2 AES використовує у боротьбі з CBC - MAC режимом (режим роботи для блоку шифру, який дозволяє один ключ використати як для шифрування, так і для автентифікації) для забезпечення конфіденційності даних, автентифікації, цілісності і захисту відтворення. У стандарті 802.11i пропонується також кешування ключів і попередньої автентифікації для впорядковування користувачів по точках доступу.

WPA2

Із стандартом 802.11i, увесь ланцюжок модуля безпеки (вхід в систему, обмін повноваженнями, автентифікація і шифрування даних) стає надійнішим і ефективнішим захистом від ненапрямлених і цілеспрямованих атак. Система WPA2 дозволяє адміністраторові Wi-Fi мережі перемкнутися з питань безпеки на управління операціями і пристроями. Стандарт 802.11r є модифікацією стандарту 802.11i. Цей стандарт був ратифікований в липні 2008 року.

Технологія стандарту швидше і надійно передає ключові ієрархії, ґрунтовані на технології Handoff (передача управління) під час переміщення користувача між точками доступу. Стандарт 802.11r є повністю сумісною з Wi-Fi стандартами 802.11a/b/g/n. Також існує стандарт 802.11w, призначений для удосконалення механізму безпеки на основі стандарту 802.11i. Цей стандарт розроблений для захисту пакетів, що управляють. Стандарти 802.11i і 802.11w - механізми захисту мереж Wi-Fi стандарту 802.11n.

1.7 Безпечна передача даних за допомогою VPN – з’єднання

Стрімкий розвиток Інтернету, який ми спостерігаємо впродовж останніх років, відкриває будь-якому власникові комп'ютера доступ до воістину необмежених об'ємів інформації. У зв'язку з цим можливість індивідуального і колективного доступу до корпоративної мережі практично у будь-який час швидко перетворюється на незмінну вимогу ділового світу.

Зміна сфер застосування інформаційних технологій повинна супроводжуватися зміною засадничої мережевої інфраструктури. На зміну традиційному способу встановлення з'єднань між користувачами Інтернету за допомогою модемів і/або виділених ліній приходять віртуальні приватні мережі VPN, що дозволяють користувачам вільно спілкуватися між собою через Інтернет.

Впродовж найближчих років на базі відкритої для усіх глобальний мережі Інтернет можна буде упевнено підтримувати практично усі види трафіку, включаючи обмін даними, мова і відео-зображення. Переваги технології VPN настільки переконливі, що вже сьогодні багато компаній починають будувати свою стратегію з урахуванням використання Інтернету як головного засобу передачі інформації, причому навіть тій, яка є уразливою або життєво-важливою. Різні фахівці по-різному проводять класифікацію VPN. Найчастіше використовуються наступні три ознаки класифікації :

- "робочий" рівень моделі OSI;
- конфігурація структурного технічного рішення;
- спосіб технічної реалізації.

1.7.1 Класифікація VPN за робочим рівнем моделі OSI

Для технологій безпечної передачі даних по загальнодоступній (незахищеній) мережі застосовують узагальнену назву - захищений канал (secure channel). Термін "канал" підкреслює той факт, що захист даних забезпечується між двома вузлами мережі (хостами або шлюзами) уздовж

деякого віртуального шляху, прокладеного в мережі з комутацією пакетів. Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI.

Класифікація VPN по робочому рівню моделі OSI представляє значний інтерес, оскільки від вибраного рівня OSI багато в чому залежить функціональність VPN, що реалізовується, і її сумісність з додатками ІС, а також з іншими методами захисту. За ознакою "робочий" рівень моделі OSI розрізняють наступні групи VPN:

- VPN другого рівня;
- VPN третього (мережевого) рівня;
- VPN п'ятого (сеансового) рівня.

Ймовірно помітили, що VPN будуються на досить низьких рівнях моделі OSI. Причина цього досить проста - чим нижче в стеку реалізовані засоби захищеного каналу, тим простіше їх зробити прозорими для додатків і прикладних протоколів. На мережевому і канальному рівнях залежність додатків від протоколів захисту зникає зовсім. Тому побудувати універсальний і прозорий захист для користувача можливо тільки на нижніх рівнях моделі. Проте тут ми стикаємося з іншою проблемою - залежністю протоколу захисту від конкретної мережевої технології.

Якщо для захисту даних використовується протокол одного з верхніх рівнів (прикладного або представницького), то такий спосіб захисту не залежить від того, які мережі (IP або IPX, Ethernet або ATM) застосовуються для транспортування даних, що можна вважати безперечною гідністю. З іншого боку, додаток при цьому стає залежним від конкретного протоколу захисту, тобто для додатків такий протокол не є прозорим.

Захищеному каналу на найвищому, прикладному рівні притаманний ще один недолік - обмежена зона дії. Протокол захищає тільки цілком певну мережеву службу - файлову, гіпертекстову або поштову. Наприклад, протокол S/MIME захищає виключно повідомлення електронної пошти. Тому для кожної служби необхідно розробляти відповідну захищену версію

протоколу. Слід зазначити, що на верхніх рівнях моделі OSI існує досить жорсткий зв'язок між використовуваним стеком протоколів і додатком.

1.7.1.1 VPN канального рівня

Засоби VPN, використовувані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і більш високих рівнів) і побудову віртуальних тунелів типу точка-точка (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС). До цієї групи відносяться VPN- продукти, які використовують протоколи L2F (Layer 2 Forwarding) і PPTP (Point - to - Point Tunneling Protocol), а також порівняно недавно затверджений стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft.

Протокол захищеного каналу PPTP ґрунтований на протоколі PPP, який широко використовується в з'єднаннях "точка-точка", наприклад при роботі по виділених лініях. Протокол PPTP забезпечує прозорість засобів захисту для додатків і служб прикладного рівня і не залежить від вживаного протоколу мережевого рівня. Зокрема, протокол PPTP може переносити пакети як в мережах IP, так і в мережах, працюючих на основі протоколів IPX, DECnet або NetBEUI. Проте, оскільки протокол PPP використовується далеко не в усіх мережах (у більшості локальних мереж на канальному рівні працює протокол Ethernet, а в глобальних - протоколи ATM, frame relay), то PPTP не можна вважати універсальним засобом. Дійсно, в різних частинах великої складеної мережі, взагалі кажучи, використовуються різні канальні протоколи, тому прокласти захищений канал через це гетерогенне середовище за допомогою єдиного протоколу канального рівня неможливо.

Протокол L2TP, стане, ймовірно, домінуючим рішенням для організації видаленого доступу до ЛВС (оскільки базується в основному на ОС Windows). Між тим рішення другого рівня не набудуть, ймовірно, такого ж значення для взаємодії ЛВС, унаслідок недостатньої масштабованості при необхідності мати декілька тунелів із загальними кінцевими точками.

1.7.1.2 VPN мережевого рівня

VPN- продукти мережевого рівня виконують інкапсуляцію IP в IP. Одним з широко відомих протоколів на цьому рівні є протокол SKIP, який поступово витісняється новим протоколом IPSec (IP Security), призначеним для автентифікації, тунелюванням і шифрування IP- пакетів. Стандартизований консорціумом Internet Engineering Task Force (IETF) протокол IPSec увібрав в себе усі кращі рішення по шифруванню пакетів і повинен увійти в якості обов'язкового компонента в протокол IPv6.

Працюючий на мережевому рівні протокол IPSec є компромісним варіантом. З одного боку, він прозорий для додатків, а з іншої - він може працювати практично в усіх мережах, оскільки ґрунтований на широко поширеному протоколі IP. Нині у світі тільки 1% комп'ютерів не підтримує IP взагалі, інші 99% використовують його або як єдиний протокол, або в якості одного з декількох протоколів.

Протокол IPSec передбачає стандартні методи ідентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні способи використання шифрування кінцевими точками тунелю, а також стандартні методи обміну і управління ключами шифрування між кінцевими точками.

Говорячи про IPSec, необхідно згадати протокол IKE (Internet Key Exchange), що дозволяє захистити інформацію яка передається від стороннього втручання. Він вирішує завдання безпечного управління і обміну криптографічними ключами між видаленими пристроями. Протокол IKE, ґрунтований на алгоритмі шифрування відкритим ключем, автоматизує обмін ключами і встановлює захищене з'єднання, тоді як IPSec кодує і "підписує" пакети. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність інформації яка передається.

1.7.1.3 VPN сеансового рівня

Деякі VPN використовують інший підхід під назвою "посередники каналів" (circuit proxy). Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного пакета окремо. (Сокет IP ідентифікується комбінацією TCP-з'єднання і конкретного порту або заданим портом UDP. Протокол IP не має п'ятого - сеансового - рівня, проте орієнтовані на пакетні операції часто називають операціями сеансового рівня.)

Шифрування інформації, що передається між ініціатором і термінатором тунелю, часто здійснюється за допомогою захисту транспортного рівня TLS (Transport Layer Security). Для стандартизації автентифікованого проходу через міжмережеві екрани консорціум IETF визначив протокол під назвою SOCKS, і нині протокол SOCKS v.5 застосовується для стандартизованої реалізації посередників каналів.

У протоколі SOCKS v.5 клієнтський комп'ютер встановлює автентифікований пакет (чи сеанс) з сервером, що виконує роль посередника (proxy). Цей посередник - єдиний спосіб зв'язку через міжмережевий екран. Посередник, у свою чергу, проводить будь-які операції, що просяться клієнтом. Оскільки посередникові відомо про трафік на рівні пакета, він може здійснювати ретельний контроль, наприклад, блокувати конкретні додатки користувачів, якщо вони не мають необхідних повноважень.

Для порівняння, віртуальні приватні мережі рівнів 2 і 3 зазвичай просто відкривають або закривають канал для усього трафіку по автентифікованому тунелю. Це може представляти проблему, якщо користувач не до кінця довіряє мережі на іншому кінці тунелю.

Мережі VPN з посередником каналу типу IPSec орієнтовані на протокол IP. Між тим якщо IPSec по суті поширює мережу IP на захищений тунель, то продукти на базі протоколу SOCKS розширюють її на кожне застосування і кожен сокет окремо. На відміну від рішень рівня 3 (і рівня 2),

де створені тунелі другого і третього рівня функціонують однаково в обох напрямах, мережі VPN рівня 5 допускають незалежне управління передачею в кожному напрямі. Аналогічно протоколу IPSec і протоколам другого рівня, мережі VPN рівня 5 можна використати з іншими типами віртуальних приватних мереж, оскільки ці технології не є взаємовиключними.

1.7.2 Класифікація VPN за архітектурою технічного рішення

По архітектурі технічного рішення прийнято виділяти три основні види віртуальних приватних мереж :

- VPN з видаленим доступом;
- Внутрішньокорпоративні VPN;
- Міжкорпоративні VPN.

Віртуальні приватні мережі VPN з видаленим доступом (Remote Access VPN) призначені для забезпечення захищеного видаленого доступу до корпоративних інформаційних ресурсів мобільним і/або видаленим (home - office) співробітникам компанії. Принцип їх роботи полягає в наступному: користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі (POP), після чого їх виклики проходять через Інтернет.

Внутрішньо-корпоративні мережі VPN (Intranet VPN) призначені для забезпечення захищеної взаємодії між підрозділами усередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку, включаючи виділені лінії.

Міжкорпоративні мережі VPN (Extranet VPN) призначені для забезпечення захищеного обміну інформацією із стратегічними партнерами по бізнесу, постачальниками, великими замовниками, користувачами, клієнтами і так далі.

Extranet VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і тим самим сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці. У міжкорпоративних мережах

велике значення надається контролю доступу за допомогою міжмережевих екранів і автентифікації користувачів.

Варто відмітити, що останнім часом спостерігається тенденція до конвергенції різних конфігурацій і способів реалізацій VPN. Потім усі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі.

1.7.3 Класифікація VPN за способом технічної реалізації

За способом технічної реалізації розрізняють наступні групи VPN:

- VPN на основі мережевої операційної системи;
- VPN на основі міжмережевих екранів;
- VPN на основі маршрутизаторів;
- VPN на основі програмних рішень;
- VPN на основі спеціалізованих апаратних засобів зі вбудованими шифропроцесорами.

Дуже часто "бюджетні" Wi-Fi рішення не здатні повною мірою забезпечити якісний доступ в Інтернет, і витрати на купівлю дорожчого устаткування будуть невиправданими. Серед недорогих Wi-Fi брендів : Ubiquiti, Miktotik, Engenius. Представники більш високого класу : Ruckus, CISCO, Aruba, Motorola.

Отже переглянувши багато варіантів, представників WI-FI з’єднання я зупинилась на CISCO.

1.7.4 VPN на базі міжмережевих екранів

Ряд фахівців з інформаційної безпеки вважає, що побудова VPN на базі міжмережевих екранів (МЕ) є єдиним оптимальним рішенням з точки зору забезпечення комплексної безпеки корпоративної інформаційної системи від атак з відкритих мереж. Дійсно, об'єднання функцій МЕ і VPN шлюзу в одній точці під контролем єдиної системи управління і аудиту є рішенням не лише технічно грамотним, але і зручним для адміністрування. Як приклад розглянемо типову схему побудови корпоративної VPN на базі популярного

в Росії програмного продукту CheckPoint Firewall - 1/VPN - 1 компанії CheckPoint Software Technologies.

Ця компанія є одним з лідерів в області виробництва продуктів комплексного забезпечення інформаційної безпеки при роботі з Інтернет. Міжмережевий екран CheckPoint Firewall - 1 дозволяє у рамках єдиного комплексу побудувати глубокоэшелонированный рубіж оборони для корпоративних інформаційних ресурсів. До складу такого комплексу входить як сам CheckPoint FW - 1, так і набір продуктів для побудови корпоративної VPN - CheckPoint VPN - 1, засоби виявлення вторгнень RealSecure, засоби управління смугою пропускання FloodGate і так далі.

Підсистема побудови VPN на базі CheckPoint FW - 1 включає програмні продукти VPN - 1 Gateway і VPN - 1 Appliance, призначені для побудови intranet, - VPN; VPN - 1 SecureServer, призначений для захисту виділених серверів, а також VPN - 1 SecuRemote і VPN - 1 SecureClient - для побудови internet/externet/localnet-VPN Для шифрування трафіку в каналах CheckPoint Firewall - 1 використовує відомі криптоалгоритмы DES, CAST, IDEA, FWZ та ін. Увесь продуктный ряд CheckPoint VPN - 1 реалізований на базі відкритих стандартів (IPSec), має розвинену систему аутентифікація користувач, підтримує взаємодія із зовнішній система розподіл відкритий ключ (PKI), дозволяє коштує централізований система управління і аудит і так далі. Тому не дивно, що продукція цієї компанії займає 52% світового ринку VPN згідно з останнім дослідженням Dataquest.

У результаті можна сказати, що побудова VPN на базі ME виглядає цілком збалансованим рішенням. Проте, йому теж властиві деякі недоліки. Передусім, це висока вартість такого рішення в перерахунку на одно робоче місце корпоративної мережі і досить високі вимоги до продуктивності ME навіть при помірній ширині смуги пропускання вихідного каналу зв'язку. Очевидно, що питанню продуктивності ME повинна приділятися підвищена увага при побудові VPN, оскільки фактично усе навантаження по криптообробці трафіку лягає на ME.

1.7.5 VPN та вимоги до законодавства

Одним з невід'ємних і, мабуть, базових елементів будь-якого VPN продукту є наявність в нім засобів (модулів, апаратних пристроїв і так далі), що здійснюють криптографічне перетворення (шифрування) даних.

Питання застосування криптографії в усіх розвинених країнах світу схильні до досить жорсткого законодавчого регулювання з боку держави. Як правило, це регулювання торкається трьох сторін застосування криптографії :

- сертифікація засобів криптографічного захисту інформації (СКЗИ);
- ліцензування діяльності організацій і підприємств, пов'язаної з виробництвом, поширенням, експлуатацією і так далі СКЗІ;
- експортно-імпортні обмеження на СКЗІ.

Мета такого регулювання досить проста: для забезпечення власної безпеки будь-якій державі необхідно в максимальному ступені забезпечити контроль за циркулюючою в комп'ютерних мережах інформацією, причому бажано не лише у своїх національних мережах і не лише своїй інформації.

1.8 Висновки до першого розділу

За всіма кібератаками на готельний бізнес стоїть реальний економічний інтерес. Готельний бізнес став однією з основних цілей для кіберзлочинців. Крім мотивації, варто відзначити і наявність шкідливих програм, спеціально розроблених для збору важливої інформації про кредитні картки через POS-системи. Очевидно, що хакери не збираються йти на спокій в найближчим часом. Ця тривожна ситуація впливає на готельний бізнес не тільки з економічної точки зору, але також підриває його репутацію, викликає паніку серед клієнтів і дестабілізує бізнес.

Шкідливі програми, які заражають POS-термінали для крадіжки даних по кредитних картах, а також цілеспрямовані атаки на IT-системи готелів для крадіжки конфіденційної інформації - це два приклади того, що може

трапитися в результаті кібератаки. Подібні атаки мають негативний вплив на фінансовий стан готелів і їх репутацію.

Готелям необхідно посилити заходи безпеки в своїх мережах, на пристроях і в системах, а також знати, як вибрати найбільш відповідне рішення для захисту їх IT-систем. Чи не будь-яка система захисту підходить для готельних мереж, тому що кожна з них пропонує різні рівні безпеки, і не кожна здатна захистити їх в будь-який цифровий екосистемі або оточенні.

Використання інформаційних технологій в підприємницькій діяльності значно підвищує ефективність процесів, зменшує затрати на їх проведення, проте в той же час зумовлює виникнення нових загроз для функціонування підприємства. Тому, за результатами проведеного дослідження визначено, що необхідним є створення системи аналізу можливих інформаційних загроз, розробка методики оцінки інформаційних ризиків, вживання заходів для забезпечення економічного захисту інформаційної безпеки, адже інформаційна безпека фактично відображається у ступені захищеності важливої для підприємства інформації від впливу дій випадкового або навмисного характеру, які можуть завдати збитків підприємству.

Доведено, що підприємствам необхідно завчасно виявляти проблеми, та вживати заходи, що спрямовані для запобігання загроз інформаційній безпеці.

Отже, можно зробити висновки, що використання VPN мережі у готелі буде надійніше. Адже використання бездротової мережі без паролів, та кодів доступу можуть бути загрозою для гостей готелю.

РОЗДІЛ 2. ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Загальні відомості про готельний комплекс

ТОВ «ІНТЕР-ГОТЕЛЬ» («Business & Relax Hotel GoodZone») знаходиться за адресою: вул. Чкалова 70, с Піщанка, 49000.

У зв'язку з необхідністю проведення бездротової мережі на території «Business & Relax Hotel GoodZone», проведені заходи по обстеженню умов, що сприяють розробці бездротової мережі, а також виявлення негативних факторів. Об'єктом є готельний комплекс.

Штат співробітників: (режим роботи співробітників)

Генеральний директор

- організовує і забезпечує ефективну діяльність готелю;

- здійснює контроль над якістю обслуговування клієнтів відповідно до класу готелю;

- вживає заходів до зміцнення та розширення матеріально-технічної бази готелю, підвищенню рівня її комфортабельності.

керівник служби прийому і розміщення

- вживає заходів щодо забезпечення готелю кваліфікованим персоналом;

- здійснює заходи щодо впровадження прогресивних форм організації обслуговування.

- спрямовує роботу персоналу і служб готелю на забезпечення схоронності і утримання приміщень та майна в справному стані відповідно до правил і норм експлуатації, безперебійної роботи устаткування, зовнішнього благоустрою, дотримання санітарно-технічних і протипожежних правил;

- розглядає претензії, пов'язані з незадовільним обслуговуванням клієнтів і проводить відповідні організаційно-технічні заходи.

Старший адміністратор

- організовує роботу з профілактичного огляду житлових номерів, підсобних та інших приміщень готелю, по проведенню капітального і поточного ремонту;

- забезпечує надання клієнтам інформації про послуги, що надаються;

- забезпечує роботу з ефективного і культурного обслуговування клієнтів, створенню для них комфортних умов;

- здійснює контроль над своєчасною підготовкою номерів до прийому прибувають в готель, дотриманням чистоти в готелі, регулярною зміною білизни в номерах, збереженням майна і устаткування;

- контролює дотримання працівниками організації трудової і виробничої дисципліни, правил і норм охорони праці, техніки безпеки, вимог виробничої санітарії і гігієни;

- розглядає претензії, пов'язані з незадовільним обслуговуванням клієнтів і проводить відповідні організаційно-технічні заходи;

- інформує керівництво організації про наявні недоліки в обслуговуванні клієнтів, вживає заходів до їх ліквідації.

Адміністратори

- інформує проживають в готелі про надавані додаткові платні послуги, приймає замовлення на їх виконання і контролює їх виконання;

- дає усні довідки, що стосуються готелю, розташування міських визначних пам'яток, видовищних, спортивних споруд і т.д;

- приймає і оформляє необхідні документи;

- вживає заходів до вирішення конфліктів, що виникають при обслуговуванні проживаючих.

IT - фахівець

- виконують всі поставлені завдання від керівництва;

- виконують роботу з покращення системи.

2.2 Об’єкт інформаційної діяльності

На територій 4 корпуси, у кожному корпусі по 15 номерів. Також є лісові котеджі – 20 номерів. Річні котеджі – 16 номерів. Особисті вілли – 20 будинків. На територій розташовано міні-готель для співробітників – 50 номерів. Біля комплексу протікає річка Самара.

На ситуаційному плані (рис 2.1) відображено положення ОІД щодо об'єктів місцевості.

Сусідні будівлі:

З північної сторони - в 700м, лісова зона.

З південного боку - в 100м, лісова зона.

Із західного боку - в 100м, річка Самара (протяжність 3 км).

Зі східного боку - в 100м, лісова зона (протяжністю 4 км).

Поряд з ОІД знаходиться:

З північної сторони – в 700м, знаходиться міні-готель для співробітників.

З південного боку - в 300м, лісні будинки.

Із західного боку - в 200м, озеро(протяжність 900м)

Зі східного боку - в 600м, місце для розваг.

На ситуаційному плані позначено:

- усі споруди;
- місця для розваг;
- озеро та річка;
- місце для зупинки транспорту;
- ОІД знаходиться у готелі №1;
- лісову частину.

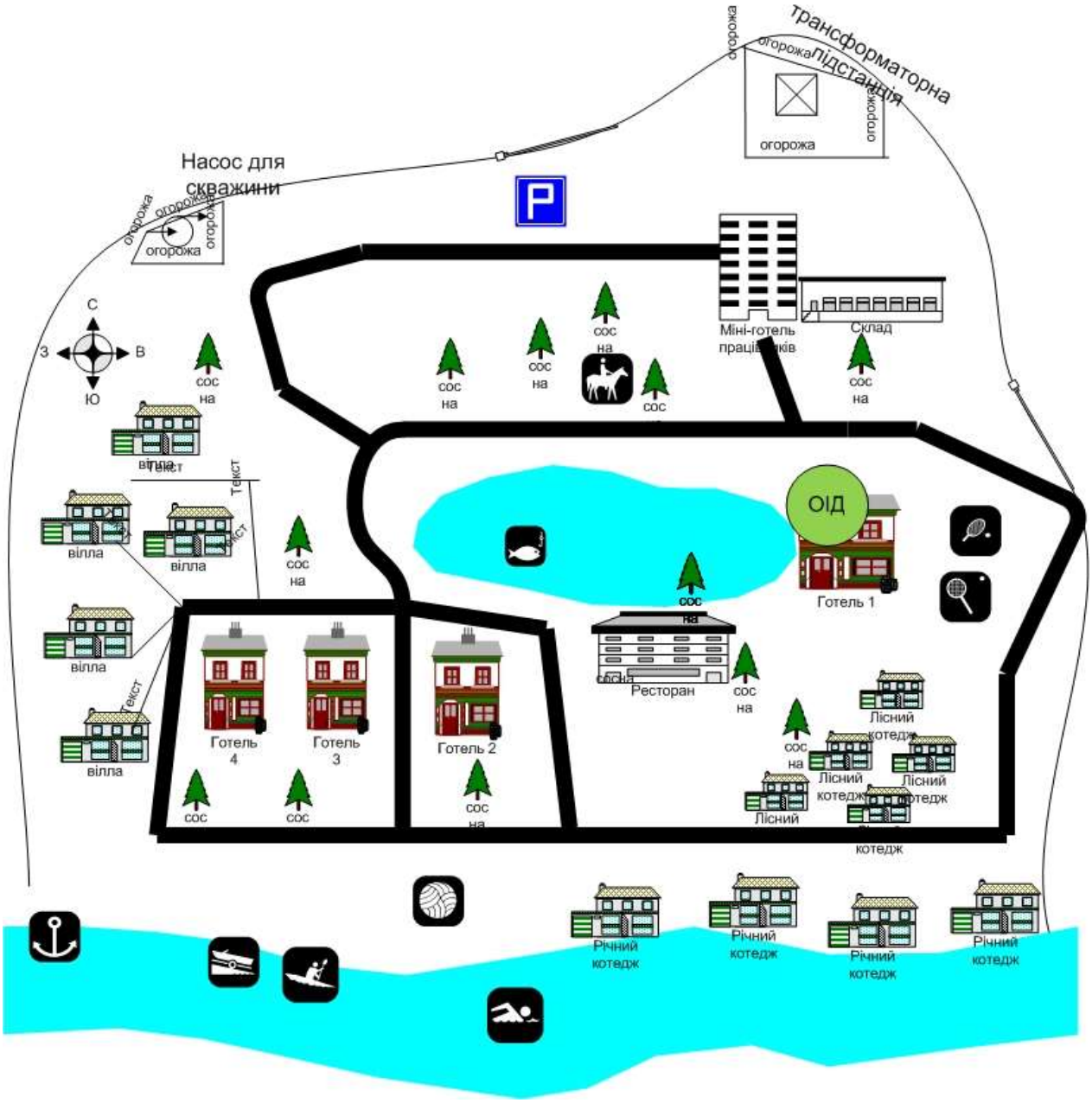

Рисунок 2.1 – Ситуаційний план

Таблиця 2.1 - Опис фізичного середовища

Система комунікації	Пояснення
Система електропостачання	Підключена до трансформаторної станції, яка знаходиться за межами КЗ, але в межах території.
Система опалення	Автономна, особиста система яка знаходитися за межами КЗ, але в межах території.
Система каналізації	Особиста система за межами КЗ.

Продовження таблиці 2.1

Система комунікації	Пояснення
Система водопостачання	Підключена до водоканалу, за межами КЗ, але в межах території.
Система заземлення	Всі прилади, комп'ютери заземлені до загального контуру заземлення, який замкнутий і виходить за межі КЗ.
Телефонна Лінія і Інтернет	Інтернет StarLink. Підключений за допомогою супутникової мережі. Телефонна мережа корпоративна, оператор Київстар.
Система вентиляції	Приточно-витяжна.
Система сигналізації	Складається з датчиків відкриття, датчиків руху і системи кабелів.
Система кондиціонування	Спліт-система, яка складається з двох блоків: внутрішній і зовнішній.
Система відеоспостереження	Складається з більш 40 камер, системи кабелів, квадратура з моніторів, плати відео-захоплення і відео-реєстратора, на якому зберігається знята інформація. Відео-реєстратор знаходиться в межах КЗ.
Протипожежна безпека	Складається з системи оповіщення і датчиків, дані з яких обробляються протипожежним приймально-контрольним пристроєм, який знаходиться в межах КЗ.

Структура обчислювальної системи

Складовими структури є: 3 персональних комп'ютери з'єднані локальною мережею (з виходом в Інтернет), зовнішній модем.

Технічні засоби прийому, обробки, передачі та зберігання інформації: системний телефон, телефакс, сканер, принтер.

Допоміжні технічні засоби і системи (ВТСС): лінії пожежної сигналізації, лінії Інтернет, кабелі телефонного зв'язку, лінії мережі електроживлення, відведена телефонна лінія між усіма співробітниками готелю, 5 ламп денного світла.

Таблиця 2.2 - Робочі станції

Положення	Тип	Назва
Робочі станції	Операційна система	Windows 7 SP1 enterprise.
	ОС для роботи сервера	DiskStation Manager (DSM)
	ПЗ для роботи з документами	Microsoft Office 2016 SERVIO 2017 Adobe Reader
	Веб-браузер	Google Chrome
	ПЗ для забезпечення бухгалтерського звіту	1С:Бухгалтерія 8.1 клієнт
	Антивірус	ESET SmartSecurity 6

Таблиця 2.3 - Склад обчислювальної техніки

Назва	Характеристика	Кількість	Підпис
Принтер-сканер	Модель: HP Deskjet 2545	1	Принтер
ADSL модем	Модель: TP-LINK DI-304	3	Модем
Робоча станція	Everest Home & Office 1005 (1005_2504): Intel Celeron (2.4 ГГц) / RAM 4 ГБ / HDD 500 ГБ / Intel HD Graphics	3	PC -1 PC – 2 PC - 3
POS-термінал	ТМ «Екселлио DP-45», підключене через wi-fi.	1	POS -термінал
Файловий сервер	Synology DS216J	1	Файловий сервер

Робота з POS - терміналом здійснюється гостями, при оплаті наданих послуг. Дана інформація переходить в банк, а оплата надходить на відкритий рахунок. Зняттям або переказом коштів займається Генеральний директор.

Доступ до робочих станцій здійснюється при вході в систему під своїм логіном і паролем. Доступ у адміністраторів обмежений, а старший адміністратор має більше повноважень. Кожен день, при закінченні зміни,

необхідно скласти звіт про завантаження готелю, заселенням гостей і додаткової інформації. Звіт складає працівник рецепції - адміністратор.

Компанія ExpertSolution надає готелю ПЗ, SERVIO 2017. Кожен день автоматично здійснюється відправка даних в базу даних компанії. Компанія ExpertSolution, знаходиться в Києві, тому звіт надсилається через мережу Інтернет.

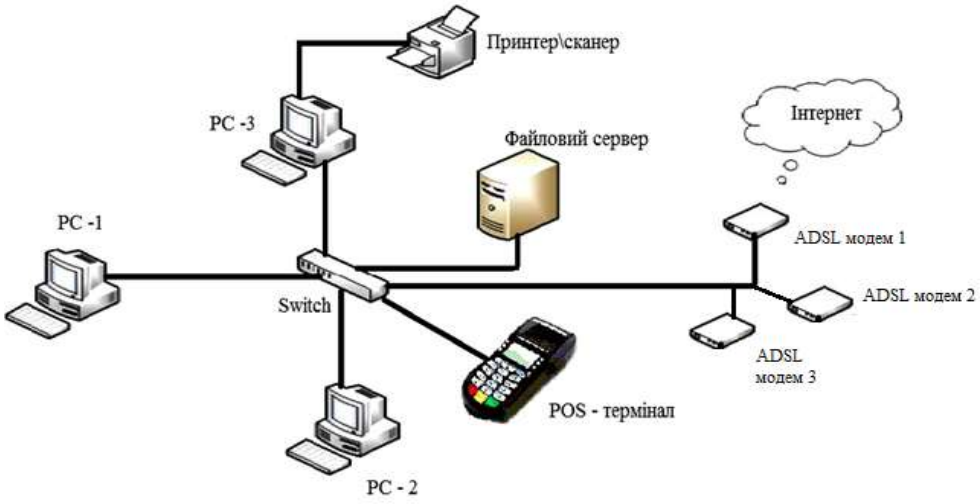

Рисунок 2.2 – Схема обчислювальної мережі

2.3 Характеристика обчислювальної техніки бездротової мережі

Сьогодні наявність Wi-Fi в готелі це вже норма, а його відсутність вказує на те, що це готель низького рівня з мінімальним набором послуг. Створення Wi-Fi мережі в готелі значно підвищує її рівень. Також слід зазначити, що багато власників перед придбанням Wi-Fi роутера для готелю відносяться недбало, купують в магазині звичайний Wi-Fi роутер, а потім виникає безліч проблем, які виливаються в негативні відгуки про готель в інтернеті, а це зменшення кількості відвідувачів і додаткова робота по нейтралізації таких відгуків.

Нижче розглянемо характеристики існуючого обладнання, та на що необхідно звернути увагу при виборі Wi-Fi роутера для готелю і зупинимося

на додаткових можливостях, які можна отримати при використанні таких пристроїв.

У готелі використовується: маршрутизатор, модель TP-LINK DI-304.

Таблиця 2.4 – Характеристика обчислювальної техніки

Порт	4 порта RJ-45 10/100 Ethernet (IP-адресація для кожного інтерфейса обмежена класом С)
	1 консольний порт
Локальна мережа	Стандарт IEEE 802.3 10BASE-T Ethernet
	Мережевий протокол CSMA/CD
	Швидкість передачі даних 10/100 Мбит/с
Функції ISDN	Стандартний PPP/Multi-link PPP
	Стиснення даних Hi/f ?LZS (Stac)
	Стискування: 4 до 1
ISDN(Integrated Services Digital Network)	Швидкість ISDN BRI: до 128,000 біт
	ISDN інтерфейс BRI S/T
	1 порт ISDN BRI: 64Кб по каналу B x 2
	16Кбод по каналу D x 1
Функції маршрутизатора	Маршрутизація пакетів IP: RIP-1 и RIP-2; статистична маршрутизація
Безпека	PAP, CHAP
	Міжмережевий екран
	RADIUS

Маршрутизатор TP-LINK DI-304

Маршрутизатор з інтегрованим комутатором і термінальним адаптером ISDN призначений для використання в малих офісах і дозволяє передавати/ приймати дані із швидкістю 64Кбит/сік або 128Кбіт\сек.

Вбудований комутатор

Цей маршрутизатор має вбудований 4-портовий комутатор 10/100 Ethernet, що є ідеальним рішенням для використання в умовах малого або домашнього офісу. За допомогою вбудованого комутатора можна

підключити до ISDN лінії чотирьох або більше за користувачів, уникнувши при цьому витрат засобів і часу на купівлю і установку окремого комутатора.

Транслятор мережевих адрес (NAT)

Маршрутизатор підтримує перетворення мережевих, що дозволяє декільком користувачам підключатися до глобальної мережі з використанням одного IP- адреси для зниження витрат і поліпшення безпеки.

Безпека

Підтримуються такі системи безпеки, як захист паролем внутрішньої системи управління маршрутизатором PAP ,CHAP протоколи для видалених користувачів. Мережевий екран, що настроюється, забезпечує контроль за доступом в/з глобальної мережі. Підтримується до восьми паролів системних адміністраторів, які можуть контролювати роботу пристрою. Протокол RADIUS забезпечує централізовану перевірку паролів видалених користувачів.

Сама природа Wi-Fi, коли дані передаються по відкритих радіочастотах, робить його уразливим (в усякому разі без належних систем шифрування), проте готелі особливо виділяються на загальному фоні. Наприклад, у готелях практично ніколи не використовується протокол безпеки WPA.

2.4 Типова схема побудови корпоративної VPN на базі маршрутизаторів Cisco

Відносно недавно з'явився новий продукт компанії - Cisco VPN client, який дозволяє коштувати захищені з'єднання "точка-точка" між робочими станціями (у тому числі і видаленими) і маршрутизаторами Cisco, що робить можливою побудову internet - і localnet - VPN. Для організації VPN тунелів маршрутизатори компанії Cisco нині використовують протокол канального рівня L2TP (створений на базі фірмових протоколів L2F (Cisco Systems) і PPTP (Microsoft Co.)) і протокол мережевого рівня IPSec, розроблений асоціацією IETF (Internet Engineers Task Force). Не вдаючись до серйозного

аналізу згаданих протоколів, відмітимо лише найцікавіші сторони їх практичного використання.

Протокол L2TP забезпечує інкапсулювання протоколів мережевого рівня (IP, IPX, NetBEUI та ін.) в пакети канального рівня (PPP), які і передаються по мережах, що підтримують доставку дейтаграмм в каналах "точка-точка". Хоча цей протокол і претендує на рішення проблем безпеки в VPN, він ніяк не специфікує процедури шифрування, автентифікації (процедура автентифікації відбувається один раз на початку сесії) і перевірки цілісності кожного переданого по відкритій мережі пакету, а також процедури управління криптографічними ключами.

Інкапсуляція — один з трьох основних механізмів об'єктно-орієнтованого програмування. Йдеться про те, що об'єкт вміщує не тільки дані, але і правила їх обробки, оформлені в вигляді виконуваних фрагментів (методів).

Перевагою L2TP є його незалежність від транспортного рівня, що дозволяє використати його в гетерогенних мережах. Досить важливою якістю L2TP є його підтримка в ОС Windows 2000, що в принципі дозволяє будувати комбіновані VPN на базі продуктів Microsoft і Cisco. Проте, "канальна природа" L2TP протоколу є причиною його істотного недоліку : для гарантованої передачі захищеного пакету через складені мережі усі проміжні маршрутизатори повинні підтримувати цей протокол, що, очевидно, досить важко гарантувати. Мабуть з цієї причини компанія Cisco сьогодні кинула пильніший погляд на просування сучаснішого VPN протоколу - IPSec.

На сьогодні IPSec є одним з Інтернет-протоколів, що самих, що пропрацювали і досконалих, в плані безпеки. Зокрема, IPSec забезпечує автентифікацію, перевірку цілісності і шифрування повідомлень на рівні кожного пакету (для управління криптографічними ключами IPSec використовує протокол IKE, що добре зарекомендував себе у своїй більше ранній версії Oakley). Крім того, робота протоколу на мережевому рівні є однією із стратегічних переваг IPSec, оскільки VPN на його базі працюють

повністю прозоро як для усіх без виключення застосувань і мережевих сервісів, так і для мереж передачі даних канального рівня. Також IPSec дозволяє маршрутизувати зашифровані пакети мережам без додаткового налаштування проміжних маршрутизаторів, оскільки зберігає стандартний IP- заголовок, прийнятий в IPv4. А той факт, що IPSec включений в якості невід'ємної частини в майбутній Інтернет-протокол IPv6, робить його ще привабливішим для організації корпоративних VPN.

На жаль, IPSec властиві і деякі недоліки: підтримка тільки стека TCP/IP і досить великий об'єм службової інформації, який може викликати істотне зниження швидкості обміну даними на низькошвидкісних каналах зв'язки, до яких доки, на жаль, можна сміливо віднести більшість з існуючих каналів.

Повертаючись до побудови корпоративних VPN на базі маршрутизаторів, відмітимо, що основним завданням цих пристроїв є маршрутизація трафіку, а значить криптообробка пакетів є деякою додатковою функцією, що вимагає, очевидно, додаткових обчислювальних ресурсів. Іншими словами, якщо ваш маршрутизатор має досить великий запас по продуктивності, то йому цілком можна "доручити" і формування VPN. Проте, якщо маршрутизатор працює "на межі", він навряд чи впорається з цим завданням не порушуючи загальної функціональності своєї роботи.

У випадку побудови VPN на базі маршрутизаторів необхідно пам'ятати ще і про те, що сам по собі такий підхід не вирішує проблему забезпечення загальної інформаційної безпеки компанії, оскільки усі внутрішні інформаційні ресурси все одно залишаються відкритими для атак ззовні. Для захисту цих ресурсів, як правило, застосовуються міжмережеві екрани (МЕ), які розташовуються за пограничними маршрутизаторами, а значить на каналі від маршрутизатора до МЕ і далі уся конфіденційна інформація йде в "відкритому" виді. Це, зокрема, означає, що маршрутизатор необхідно ставити як можна "ближче" до МЕ, бажано в загальному приміщенні, що охороняється.

Одним з істотних недоліків побудови VPN на базі маршрутизаторів є те, що в цьому випадку рішення єдиної задачі захисту інформаційних ресурсів компанії від атак ззовні розподіляється по декількох функціонально незалежних пристроях (наприклад, маршрутизатор і МЕ). Такий підхід може привести до серйозних організаційних і технічних проблем у випадках, наприклад, визначення відповідальності за порушення інформаційної безпеки мережі.

2.5 Обґрунтування вибору маршрутизаторів CISCO

Адекватність і реалії цінової політики. Так, продукцію Cisco ні в якому разі не можна віднести до бюджетного цінового сегменту, її вартість на порядок вища за розробки багатьох конкуруючих брендів. Проте, вивчивши комплекс її характеристик, розумієш, що за їх рахунок вона набагато швидше окупається і має великий ККД.

Можливості вибору. Компанія Cisco може похвалитися надзвичайно широким асортиментом WAP, серед яких знайдуться моделі, оптимально відповідні для використання практично у будь-яких умовах. Крім того, модельний ряд устаткування регулярно удосконалюється і поповнюється функціональними новинками.

Забезпечення швидкості передачі даних, спочатку заявленої виробником. Ні для кого не секрет, що бюджетні роутери трохи (а іноді і досить помітно) "халтурять" у цьому питанні, чого не можна сказати про точки доступу Cisco.

Максимальний рівень безпеки. Один з найвагоміших плюсів безпровідного устаткування Cisco полягає в тому, що управління їм здійснюється за допомогою використання власної ОС. Цей факт свідчить про гнучкість установки параметрів пристроїв і їх захищеності від хакерських атак і витівок зломщиків.

Можливість відновлення даних, постраждалих від яких-небудь збоїв в роботі. Ця перевага безпосередньо пов'язана з попередньою, оскільки діє воно тільки завдяки унікальним функціональним особливостям ОС Cisco.

Таблиця 2.5 – Характеристика маршрутизатора Cisco RV320 VPN Router

Опис	Характеристика
Розміри маршрутизатора	RV320: 206 x 132 x 44 мм
Кількість LAN-портів	LAN: 4 x 10/100/1000 RJ-45 WAN: 1 x 10/100/1000 RJ-45; 1 x 10/100/1000 RJ-45/DMZ USB x 2
Джерело живлення	RV320: 12 В 1,5 А
Вага	RV320: 1,385 кг
Стандарти	802.3, 802.3u, IPv4 (RFC 791), IPv6 (RFC 2460)
Пропускна здатність IPsec VPN	100 Мбіт
Пропускна здатність SSL VPN	20 Мбіт
VLAN	802.1Q VLAN Підтримуються 7 віртуальних локальних мереж Фільтрація контенту охоплює 27+ мільярдів URL-адрес
PPTP	10 PPTP тунелів для віддаленого доступу
Кількість одночасних з’єднань	20000
Протоколи управління	Веб-браузер (HTTP / HTTPS) Прости протокол управляння мережею (SNMP) v1, v2c, и v3 Bonjour

2.6 Висновок до другої частини

Безпровідна мережа з хорошим покриттям і стабільним доступом до інтернету відкриває перед готелем масу можливостей. Наприклад, вона дозволяє у будь-якій точці використати мобільні термінали оплати послуг, встановити банкомати або інші термінали самообслуговування. Крім того, з'являється можливість впровадити IT- інструменти автоматизації бізнесу через смартфони і планшети для персоналу, що дозволяє спростити управління окремими службами.

Великі світові готельні мережі вже тестують різні форми мобільних застосувань для самих гостей, пропонуючи інструменти задоволення своїх потреб при мінімальному контакті з персоналом, які стають доступними при підключенні до інтернету або Wi-Fi мережі готелю, що особливо зручно для гостей з інших міст або країн.

Також існують багато загроз, з якими може зіштовхнутись гість комплексу при підключенні до мережі Wi-Fi.

Найпопулярніша це: передача паролів, кодів, або іншої цінної інформації хакеру. Так як у готельному комплексі не було встановлено VPN мережі, за для автентифікації у мережу.

Розглянувши багато маршрутизаторів, їх характеристики та описи, було прийнято рішення який саме буде рекомендований до встановлення у готелі.

Маршрутизатор - Cisco RV320 VPN Router

Переваги:

- максимальний рівень безпеки;
- забезпечення швидкості передачі даних;
- адекватність та реалії цінової політики.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Визначення витрат на проектування та експлуатацію систем інформаційної безпеки

Мета: обґрунтування економічної доцільності. Впровадження бездротової мережі у готельний комплекс.

В економічній частині дипломного проекту виконано:

Розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення (далі об’єкт проектування).

1. Розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування.
2. Визначення річного економічного ефекту від впровадження об'єкта проектування.
3. Визначення та аналіз показників економічної ефективності запропонованого в дипломному проекті проектного рішення.
4. Висновок про економічну доцільність проектного рішення.

Основою для визначення витрат на створення систем інформаційної безпеки є концепція сукупної вартості володіння.

3.1.2 Розрахунок (фіксованих) капітальних витрат

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

До фіксованих (капітальних) варто відносити наступні витрати:

- вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);
- витрати на залучення зовнішніх консультантів;
- вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему визначаються у відсотках до сумарної вартості обладнання та програмного забезпечення. (7-8%)

Методика розрахунку витрат на створення програмного забезпечення наведена далі.

3.1.3 Визначення витрат на створення програмного засобів захисту інформації

При виконанні дипломних проектів, спрямованих на розробку і використання програмного забезпечення (ПЗ) в системах інформаційної безпеки, техніко-економічні розрахунки мають містити:

- визначення трудомісткості розробки та опрацювання ПЗ;
- розрахунок витрат на створення програмного продукту;
- оцінку швидкодії та надійності роботи програмного продукту.

3.1.4 Визначення трудомісткості розробки та опрацювання програмного продукту

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин,}$$

$$t = 0,5 + 0,45 + 0,96 + 0,96 + 7,2 + 2,1 = 12,1 \quad (3.1)$$

де: $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті **Q** (з урахуванням можливих уточнень у процесі роботи над алгоритмом і програмою).

Умовна кількість операторів у програмі:

$$Q = q \cdot c\,(1 + p), \text{ штук,}$$

$$Q = 2 * 2\,(1 + 5) = 24 \text{ штук,} \quad (3.2)$$

Де: q = 2 – очікувана кількість операторів;

c = 2 – коефіцієнт складності програми;

p = 5 – коефіцієнт корекції програми в процесі її опрацювання.

Коефіцієнт складності програми **c** визначає відносну складність програми щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25...2,0.

Коефіцієнт корекції програми **p** визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму внаслідок уточнення технічного завдання. Його величина знаходиться в межах 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5-10% готової програми.

Оцінка тривалості складання технічного завдання на розробку ПЗ $\mathbf{t_{тз}}$ залежить від конкретних умов і визначається дипломником на підставі експертних оцінок за узгодженням із керівником проекту.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікації програміста можливо оцінити за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \quad \text{годин},$$

$$t_B = \frac{24*1,5}{(80*1)} = 0,45 \qquad (3.3)$$

Де: В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом:

- від 2 до 3 років – 1,0;

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25) \cdot k}, \text{ годин.}$$

$$t_a = \frac{24}{25*1} = 0,96 \qquad (3.4)$$

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25) \cdot k}, \text{ годин.}$$

$$t_{пр} = \frac{24}{25} = 0,96 \qquad (3.5)$$

Тривалість опрацювання програми на ПК:

$$topr = \frac{1{,}5Q}{(4...5)\cdot k},\ \text{годин.}$$

$$t_{\text{опр}} = \frac{1{,}5*24}{5*1} = 7,\ 2 \qquad (3.6)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_{\text{Д}} = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)} \cdot 0{,}75$$

$$t_{\text{д}} = \frac{24}{20} + \frac{24}{20} * 0{,}75 = 2{,}1 \qquad (3.7)$$

3.1.4.1. Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту **Кпз** складаються з витрат на заробітну плату виконавця програмного забезпечення **Ззп** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК **Змч**:

$$К_{\text{пз}} = З_{\text{зп}} + З_{\text{мч}}$$

$$К_{\text{пз}} = 726 + 7490 = 8216 \qquad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{\text{ЗП}} = \text{t} \cdot З_{\text{пр}},\ \ \text{грн,}$$

$$З_{\text{зп}} = 12{,}1 * 60 = 726 \qquad (3.9)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр = 60 грн/год – средньогодинна заробітна плата програміста з нарахуваннями.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot C_{мч} + t_д \text{ , грн,}$$

$$З_{мч} = 7{,}2 * 1040 + 2{,}1 = 7490 \quad (3.10)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,}$$

$$C_{мч} = 0{,}14 * 3 * 2{,}74 + \frac{1000*399}{1920} + \frac{2000*799}{1920} = 1040 \quad (3.11)$$

Де:

P – встановлена потужність ПК, кВт;

$C_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р = 1920$.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н},$$

$$К=10000+7000+8216+9000+10000+2000= 37217 \quad (3.12)$$

Де: $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.1.5 Розрахунок поточних (експлуатаційних) витрат

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

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad \text{тис. грн.}$$

$$С=0,7+2089+0,15=208985 \quad (3.13)$$

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С = С_{н} + С_{а} + С_{з} + С_{єв} + С_{е} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

$$С = 10000+0,15+194400+736,5+736,5+2000+1116=2089 \quad (3.14)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) (табл. Додатка).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}\text{ , грн.}$$

$$С_з = 18000 + 14400 = 194400 \qquad (3.15)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е\text{ , грн,}$$

$$С_{ед} = 0{,}14 * 1920 * 2{,}74 = 736{,}5 \qquad (3.16)$$

Де: Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації.

$С_{тос}$ - визначається за даними організації або у відсотках від вартості капітальних витрат (1-3%).

3.2 Оцінка можливого збиту від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку застосуємо наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

І – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$
$$U = 408+2737+201, 9 = 3346 \quad (3.17)$$

Де: $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad П_п = \frac{\sum Зс}{F} \cdot t_п,$$
$$П_п = \frac{1800}{176} * 4 = 408{,}8 \quad (3.2)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

$$П_в = 1022 + 715 + 1000 = 2737 \quad (3.18)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі.

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}$$

$$П_{ви} = \frac{1800}{176} * 10 = 1022 \quad (3.19)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньо-годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в$$

$$П_{пв} = \frac{1800}{176} * 7 = 715 \quad (3.20)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{20000}{2080} * (4 + 7 + 10) = 201{,}9 \quad (3.21)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U.$$

$$B = 3346*3346 = 11195716 \quad (3.22)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C,$$

$$E = 11195716*0{,}15 - 208985 = 14703 \quad (3.23)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій $Т_о$.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

$$\text{ROSI} = \frac{14703}{37216} = 0{,}39 \qquad (3.24)$$

Де: Е – загальний ефект від впровадження системи інформаційної безпеки (розділ 3.2 методичних вказівок, формула 3.8), тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій $Т_р$.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \quad \text{років}$$

$$T_o = \frac{37216}{14703} = \frac{1}{0{,}39} \qquad (3.28)$$

2, 5=2, 5

Якщо варіанти економічно рівноцінні, то приймається варіант, що забезпечує більш високу надійність, поліпшення умов праці.

3.4 Висновки до третьої частини

У дипломному проекті було визначені такі показники:

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

К = 37217 грн;

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки та становить:

Е = 14703 грн;

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

С = 208985

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

То - термін окупності капітальних інвестицій.

$$T_o = \frac{37216}{14703} = \frac{1}{0{,}39}$$

2, 5=2, 5

Можем зробити висновок, що показники капітальних витрат та загальний ефект від впровадження системи інформаційної безпеки – рівноцінні. Отже, вони забезпечують більш високу надійність, поліпшення умов праці на даному підприємстві.

ВИСНОВКИ

У дипломній роботі розв’язано завдання щодо забезпечення безпеки бездротової мережі у ТОВ «ІНТЕР - ГОТЕЛЬ». Перелік поставлених задач було виконано повною мірою.

Розглянуті загрози кібербезпеки, бездротової мережі, на прикладі готельного комплексу товариства з обмеженою відповідальність «ІНТЕР-ГОТЕЛЬ».

Розглянуті методи рішення проблематики кібербезпеки бездротової мережі, у готельному комплексі. Та можемо підкреслити, що більшість відвідувачів готельного комплексу, користуються бездротовою мережею, а отже наражають себе на ризик проникнення хакерів.

Проаналізовано обстеження об’єкта інформаційної діяльності підприємства.

Складена характеристика обчислювальної техніки бездротової мережі. Визначено, що на підприємстві було використано, застарілу техніку. Отже зловмисник міг спокійно проникнути у мережу, та зняти необхідну йому інформацію.

В економічній частині визначено та проаналізовано показники економічної ефективності системи інформаційної безпеки. За отриманими результатами, можемо зробили висновок, що показники капітальних витрат та загальний ефект від впровадження системи інформаційної безпеки – рівноцінні. Отже, вони забезпечують більш високу надійність, поліпшення умов праці на даному підприємстві.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».
2. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу».
3. НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».
4. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215».
5. НД ТЗІ 1.6-003-04 «Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації».
6. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
7. НД ТЗІ 3.3-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації».
8. Закон України «Про інформацію».
9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
10. Закон України «Про захист персональних даних».
11. Закон України «Про телекомунікації».
12. Закон України «Про Державну службу спеціального зв’язку та захисту інформації України».

13. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».
14. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт».
15. ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».
16. Міжнародний стандарт ISO / IEC 27001 до: 2013 «Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки - Вимоги».
17. ISO 27002:2013 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою».
18. http://proline.biz.ua/articles/wifi-router-for-hotel
19. https://habr.com/company/tp_link_russia/blog/331342/
20. https://studfiles.net/preview/299334/page:5/
21. https://nv.ua/techno/it-industry/rossijskij-stsenarij-mogut-li-v-ukraine-zapretit-vpn-servisy-i-chem-eto-grozit-2093951.html

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст	2	
3	А4	Вступ	1	
4	А4	1 Розділ	23	
5	А4	2 Розділ	14	
6	А4	3 Розділ	15	
7	А4	Висновки	1	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Відгук керівника економічного розділу

Керівник : _____ к.е.н.,доц. Пілова Д.П.

(підпис)

ДОДАТОК В. ВІДГУК

на дипломний проект магістра

студентки групи 125М-17-2

Чиркіної Влади Віталіївни

з теми: «Забезпечення кібербезпеки бездротовії мережі у публічних місцях, на прикладі готельного комплексу Товариство з обмеженою відповідальністю «ІНТЕР ГОТЕЛЬ»»

Метою дипломного проекту є забезпечення кібербезпеки бездротової мережі ТОВ «ІНТЕР-ГОТЕЛЬ».

Тема дипломного проекту безпосередньо пов’язана з об’єктом діяльності магістра фаху 6.125 «Кібербезпека». Для досягнення поставленої мети в дипломному проекті вирішуються наступні задачі: визначити, які загрози кібербезпеки бездротової мережі існують у готельному комплексі. Розглянути, які існують рішення кібербезпеки бездротової мережі у готельному комплексі. Зібрати дані про підприємство, виконати обстеження інформаційного середовища та обстеження обчислювальної системи. Проаналізувати технології моделювання активного обладнання. Визначити який метод шифрування, для передачі даних, встановлений. Зробити висновки. Практичне значення результатів дипломного проекту полягає в можливості їх використання у ТОВ «ІНТЕР-ГОТЕЛЬ».

Перевагою дипломного проекту є розробка інструкцій які дозволяють встановити більш надійне апаратне забезпечення.

Оформлення пояснювальної записки до дипломної роботи виконано з деякими відхиленнями від стандартів.

За час дипломування Чиркіна В.В. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі.

Оцінка роботи_____

Керівник дипломної роботи,
д.т.н., проф. Корнієнко В.І.

Керівник спец. розділу,
ст. викл. кафедри БІТ Галушко С.О.

ДОДАТОК Г. Перелік файлів на електронному носії

1. Дипломний проект Чиркіна В.В. 125М-17-2 – Пояснювальна записка.
2. Чиркіна В.В.pttx – Презентація.

ДОДАТОК Д. Групи основних засобів та інших необоротних активів і мінімально допустимі строки їх амортизації

Групи	Мінімально допустимі строки корисного використання, років
група 4 – машини та обладнання з них: електронно-обчислювальні машини, інші машини для автоматичного оброблення інформації, пов’язані з ними засоби зчитування або друку інформації, пов’язані з ними комп’ютерні програми (крім програм, витрати на придбання яких визнаються роялті, та/або програм, які визнаються нематеріальним активом), інші інформаційні системи, комутатори, маршрутизатори, модулі, модеми, джерела безперебійного живлення та засоби їх підключення до телекомунікаційних мереж, телефони (в тому числі стільникові), мікрофони і рації, вартість яких перевищує 2500 гривень	5 2

ДОДАТОК Е . Строки амортизації нематеріальних активів

Групи	Строк дії права користування
група 5 – авторське право та суміжні з ним права (право на комп’ютерні програми, програми для електронно-обчислювальних машин, компіляції даних (бази даних), крім тих, витрати на придбання яких визнаються роялті;	відповідно до правовстановлюючого документа, але не менш як 2 роки

WPA

Дальнейшее повышение безопасности и контроля доступа WPA заключается в создании нового уникального мастера ключей для взаимодействия между каждым пользовательским беспроводным оборудованием и точками доступа и обеспечении сессии аутентификации. А также, в создании генератора случайных ключей и в процессе формирования ключа для каждого пакета.

WPA3

окрема, буде посилено безпеку навіть якщо користувачі обирають «слабкий» пароль мережі, а також буде спрощено налаштування приладів без дисплеїв. Також буде посилено захист приватних даних користувачів у відкритих мережах шляхом індивідуальних налаштувань алгоритмів шифрування.

WPA	- полягає у створенні нового унікального майстра - у створенні генератора випадкових ключів і в процесі форм кожного пакету.
WPA2	- дозволяє адміністраторові Wi - Fi мережі перемкнутися з управління операціями і пристроями.
WPA3	- посилення безпеки навіть якщо користувачі обирають «слаб також спрощено налаштування приладів без дисплеїв. Також посил даних користувачів у відкритих мережах шляхом індивідуальних на шифрування (8 січня 2018 рік).