ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ

Рисунок А.1

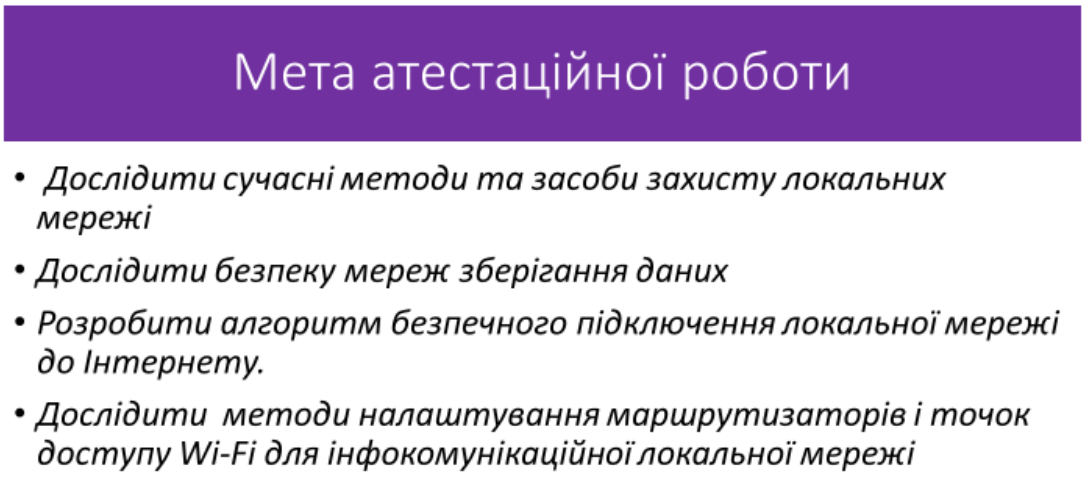


Рисунок А.2

Інформаційні ризики локальних мереж

Таблиця 1.1 – Порушення регламентів ІБ

Вид атаки	%
Застосування протоколів LLMNR і NetBios	69
Застосування ПЗ для віддаленого доступу	67
Використання незахищених протоколів передачі даних	64
Використання BitTorrent	36
Завантаження та встановлення потенційно небезпечного стороннього ПЗ	10

Таблиця 1.2 – Підозріла мережева активність (частки компаній)

Активність	%
Приховування трафіка (тунелювання, проксірування)	59
Отримання даних з контролера домену	36
Численні, невдалі спроби автентифікації	31
Запуск інструментів для адміністрування та проведення атак	31
Сканування внутрішньої мережі	23
Спроби підключення до внутрішніх вузлів	21
Підозрілі підключення по протоколам віддаленого доступу	18
Спроби віддаленого запуску процесів	18

Таблиця 1.3 – Найпопулярніше ШПЗ 2020 року

Вид шкідливого програмного забезпечення	%
ШПЗ для віддаленого доступу	29
Майнери	27
Шифрувальник	24
Рекламне ПЗ	12
Банківський троян	12
Завантажувач	10
Шпигунське ПЗ	10

Рисунок А.3

Стандартні засоби безпеки в ЛІКМ

Методи захисту

- . організаційні;
- технічні або апаратні;
- програмні;
- апаратно-програмні.

Основні бар'єри для зловмисників

- фізичне перешкода, що виключає можливість дотику третьої особи з елементами мережі;
- система контролю і управління доступом, яка регламентує рівні прав користувачів;
- використання криптографічних засобів захисту інформації (шифрування даних);
- регламентація дій персоналу;

Рисунок А.4

Таблиця 1.4 – Карти – ідентифікатори користувачів [6]

Тип	Характеристика
Безконтактні радіочастотні (PROXIMITY) карти	Найбільш перспективний і вживаний зараз тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціювання, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність системи. Зчитувач генерує електромагнітне випромінювання певної частоти і, при внесенні карти до зони дії зчитувача, це випромінювання через вбудовану в карті антену живить чіп картки. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти.
Магнітні картки	менш поширений варіант, володіє декількома недоліками - малий термін служби, необхідність чіткого позиціонування. Існують карти з низько коерцитивною і високо коерцитивною магнітною смугою і з записом на різні доріжки. Використовуються як правило для ідентифікаторів з дуже обмеженим терміном дії.
Карти Вігана	названі по імені вченого, який відкрив магнітний сплав, що володіє прямокутною петлею гістерезису. Всередині карти розташовані відрізки дроту з цього сплаву, які, при переміщенні повз них голівки, що зчитує, дозволяють отримувати інформацію. Ці карти довговічніші, ніж магнітні, але й дорожчі. Один з недоліків - те, що код в карту заноситься при виготовленні раз і назавжди.
Штрих-кодові карти	на карту наноситься штрихований код. Існує складніший варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області спектру.

Таблиця 1.5 - Контролери СКУД

Тип	Характеристика
Автономні	Призначені для обслуговування, як правило, однієї точки проходу. Зустрічаються найрізноманітніші варіації: контролери, суміщені зі зчитувачем, контролери, вбудовані в електромагнітний замок і так далі. Автономні контролери розраховані на застосування різних типів зчитувачів. Розраховані на обслуговування невеликої кількості користувачів, зазвичайно до п'ятисот.
Мережеві	Працюють під управлінням комп'ютера з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери застосовуються для створення СКУД будь-якого ступеня складності. При цьому адміністрація одержує величезну кількість додаткових можливостей: дозволу або заборони проходу; отримання звіту про наявність чи відсутність співробітників на роботі; миттєво дізнатися, де конкретно знаходиться співробітник; вести автоматичний табель обліку робочого часу; отримати звіт про те, хто і куди ходив практично за будь-який період часу; сформувати часовий графік проходу співробітників, тобто хто, куди і в який час може ходити; можливість ведення бази даних співробітників (електронної картотеки
Комбіновані	Поєднують в собі функції мережних і автономних контролерів. При наявності зв'язку з керуючим комп'ютером (пр. Ліра) контролери працюють як мережний пристрій, при відсутності зв'язку - як автономні. Найкраще рішення для сучасних інтегрованих систем безпеки, дозволяють побудувати відмовостійку на гнучку СКУД.

Рисунок А.5

Таблиця 1.8 – Методи та технології захисту канального рівня

Метод захисту	Загрози, яким протидіють	Наслідки дії методу
Функція Portsecurity	Внутрішні загрози несанкціонованого підключення до мережі або зміни MAC- адреси	При несанкціонованому підключенні вузла порт блокується або відкидаються кадри з недозволеною MAC-адресою відправника
Функція DHCP Snooping	Внутрішні загрози додавання несанкціонованого DHCP-серверу, DoS-атаки на DHCP-сервер.	Автоматичне створення прив'язок IP-MAC-порт з подальшим відкиданням кадрів від вузлів, які не відповідають прив'язкам
Функція Dynamic ARP Inspection	Внутрішні загрози, пов'язані з підміною MAC-адрес в ARP-записах (атака ARP-spoofing)	Відкидання кадрів з незаконними ARP-повідомленнями
Функція IP SourceGuard	Внутрішні загрози, пов'язані з підміною IP-адрес	Відкидання кадрів від вузлів, які не відповідають прив'язці IP-MAC-порт
Сегментація на VLAN	Внутрішні загрози широкомовних штормів та НСД до вузлів та інформації	Передача кадрів з будь-якими MAC-адресами отримувача тільки між вузлами окремих VLAN
Авторизація по протоколу 802.1x	Внутрішні загрози несанкціонованого підключення вузлів до мережі та доступу до сервісів та інформації	Передача кадрів від вузла тільки після проходження автентифікації та авторизації кінцевого пристрою або користувача

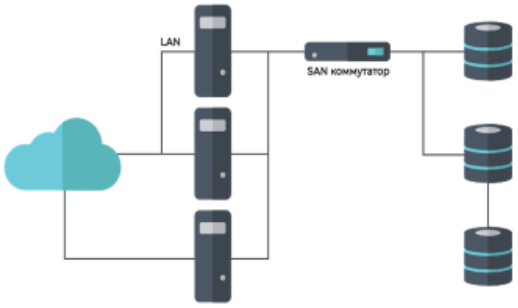
Рисунок А.6

Апаратно-програмні засоби захисту ЛІКМ

- апаратні засоби контролю доступу (електронні замки, пристрої ідентифікаційних ознак);
- спеціалізовані мережі зберігання (SAN - Storage Area Network). Вони призначені для консолідації дискового простору на спеціально виділених зовнішніх дискових сховищах, що збільшує продуктивність системи;
- дискові сховища даних, наприклад, RAID-масиви;
- стрічкові накопичувачі, для резервного зберігання даних, що, захищає їх від втрати.

Рисунок А.7

Мережа зберігання даних



Таблиця 2.1 – Характеристика мереж

Мережі	Характеристика
SAN	Високопродуктивна мережа, яка добре масштабується, та з'єднує хости із загальним пулом пристроїв зберігання даних на рівні блоків.
NAS	Підключається до одного хосту і керується ним. Сховище складається з дисків в хості і / або зовнішніх дискових полицях, які безпосередньо підключені до контролерів в хості.
DAS	Сховище із загальним доступом, яке зберігає і дозволяє спільно використовувати файли за стандартними протоколами - в основному, за протоколами Network File System і Server Message Block - по IP-мереж.

Рисунок А.8

Інформаційні ризики мереж зберігання даних

Загрози	Вразливі місця
• фізичне знищення; • розкрадання; • несанкціоноване спотворення даних; • порушення автентичності даних; • підміна даних; • блокування доступу до масиву даних.	• елементи архітектури; • протоколи обміну; • інтерфейси; • апаратні платформи; • системне програмне забезпечення; • умови експлуатації; • територіальне розміщення вузлів мережі зберігання

Рисунок А.9

Рівні, на яких відбувається захист

- рівень пристроїв;
- рівень даних;
- рівень мережевої взаємодії;
- рівень управління і контролю.

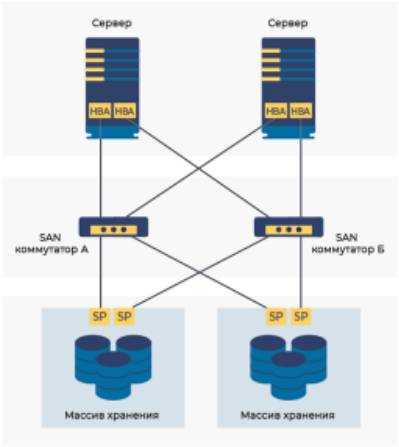


Рисунок А.10

Для організації та підтримки даних можливостей при розробці архітектури використані наступні технології

- *Standard Cisco IPSec, що забезпечує VPN з'єднання між офісами підприємства; динамічна маршрутизація на основі протоколу OSPFv2.*
- *технологія PAT для трансляції приватних IP-адрес в публічний IP-адреса.* PAT (Port Address Translation)
- *списки доступу ACL для обмеження доступу до ресурсів мережі підприємства*. ACL (Access Control List)
- *технологія VLAN для розмежування доступу всередині широкомовного домену локальної мережі.*
- *контроль доступу до мережевих пристроїв на основі парольної аутентифікації з використанням списку привілеїв.*
- *віддзеркалення трафіку на комутуючі пристрої для контролю активності мережі*
- віддалене управління мережевими пристроями на основі захищеного протоколу SSH

Рисунок А.11

Характеристики запропонованих сервісів

Сервіс	Характеристика
Контроль додавання пристроїв	Реалізується за рахунок налаштування безпеки портів на комутаторах доступу. Кожному інтерфейсу комутатора ставиться у відповідність MAC-адреса дозволеного для цього інтерфейсу мережевого адаптера. Дане рішення також здатне захистити локальну мережу від атак типу «відмова в обслуговуванні», які реалізуються з допомогою переповнення таблиці MAC-адрес.
Конфігурація VLAN	Кожен підрозділ прив'язаний до свого комутатора доступу і знаходиться у власній VPN, інтерфейси даних комутаторів асоціюються з номером цієї віртуальної мережі. Інтерфейси комутаторів, які повинні передавати трафік декількох VPN, позначаються як trunk-інтерфейси; на прикордонному маршрутизаторі виділяються кілька підінтерфейсів для кожного VLAN.
Віддзеркалення трафіку на центральному комутаторі	Використовується для контролю, приходить з мережі інтернет трафіку за допомогою IDS або анализатора трафіку, який встановлений на робочої станції, контрольованої системним адміністратором. З використанням віддзеркалення здійснюється приховування контролю трафіку для звичайних користувачів мережі і зловмисників.

Налаштування списків доступу ACL.	Основними є списки доступу до загальних ресурсів мережі - серверів. Дані списки частково виконують функції брандмауера, оскільки здатні фільтрувати трафік за адресою призначення, джерела, типу протоколу. Внаслідок того, що контроль адрес здійснюється на прикордонному маршрутизаторі, завданням для списків доступу до серверів є контроль допустимих для використання портів.
Реалізація VPN-з'єднання між віддаленими офісами.	Налаштування прикордонних маршрутизаторів характеризується методом обміну ключами (ISAK.MP), методом шифрування (AES), алгоритмом хешування (SHA-1), методом аутентифікації (обмін ключами при Ви створюєте з'єднання), обміни ключами методом Діффі-Хеллмана другої групи (1024 біта).
Налаштування PAT	ускладнюються використанням технології VPN для правильної конфігурації, який необхідно виключення з транслювання трафіку між віддаленими офісами, так як протокол IPSec вже виробляє трансляцію для зазначеного в його списках доступу трафіку.
Перевірка працездатності і захищеності мережі	Перевірка працездатності і захищеності мережі, реалізованої за допомогою запропонованого алгоритму, проводиться поетапно. Першим етапом є перевірка працездатності та захищеності мережевого обладнання локальної мережі. другим етапом вважається перевірка працездатності та захищеності доступу в інтернет і взаємодії з віддаленими офісами.

Рисунок А.12

Рисунок А.13

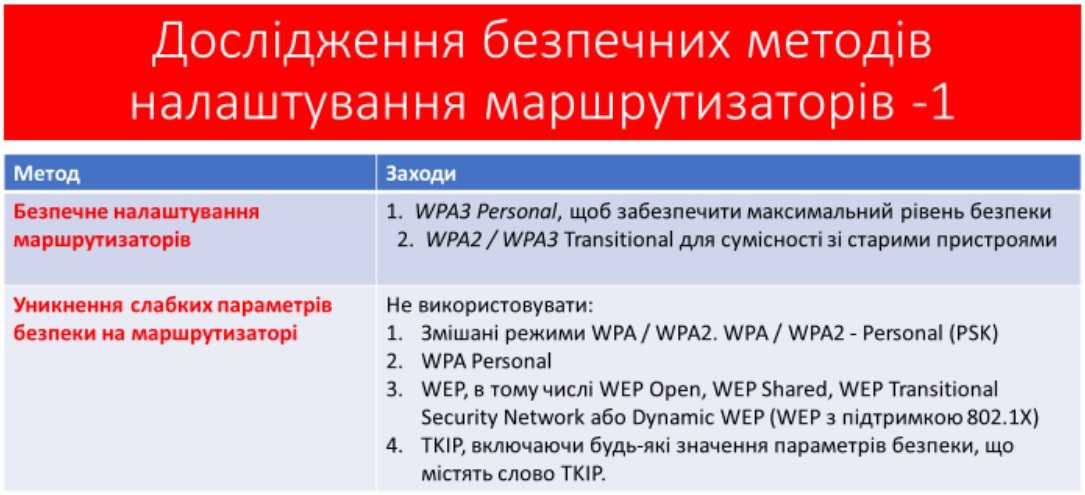


Рисунок А.14

Дослідження безпечних методів налаштування маршрутизаторів -2

Метод	Заходи
Ім'я мережі	Задайте єдине, унікальне ім'я (з урахуванням регістру)
Прихована мережа	Використовувати відповідні налаштування безпеки.
Фільтрація MAC-адрес, аутентифікація, контроль доступу	задавати значення: «Відключено»
Автоматичне оновлення прошивки	задайте значення: «Включено»
Радіорежим	Задайте значення: «Все» (рекомендується), або «Wi-Fi 2 - Wi-Fi 6» (802.11a / g / n / ac / ax).
Діапазони	Додайте всі діапазони, підтримувані вашим маршрутизатором

Рисунок А.15

Дослідження безпечних методів налаштування маршрутизаторів -3

Метод	Заходи
Канал	**Задайте значення: «Авто».**
Ширина каналу	**Задайте значення: «20 МГц» для діапазону 2,4 ГГц**
DHCP (протокол динамічної конфігурації хоста	Задайте значення: «Включено», якщо ваш маршрутизатор є єдиним DHCP-сервером в мережі
Час оренди DHCP	Задайте значення: «8 годин" для домашніх або офісних мереж; «1 + час» для точок доступу або гостьових мереж
NAT (**перетворення мережевих адрес**)	Задайте значення: «Включено», якщо ваш маршрутизатор є єдиним пристроєм, що реалізує функцію NAT в мережі
WMM	Задайте значення: «Включено»

Рисунок А.16

Таблиця 4.1 – Переваги та недоліки NAT [30]

Переваги	Недоліки
1. NAT допомагає зберегти адресний простір IPv4, коли користувач використовує NAT перевантаження 2. NAT підвищує надійність та гнучкість взаємозв'язків із глобальною мережею шляхом розгортання декількох пулів джерел, пулу балансування навантажень та резервних пулів. 3. NAT має відомий метод мережевої адресації. Якщо є використання глобальної IP-адреси, то адресний простір повинен бути належним чином призначений. Тому що при розбудові мережі може знадобитися багато IP-адрес 4. NAT надає додатковий рівень безпеки в мережі, тому що хост, вбудований в мережу NAT, недоступний для інших мережевих пристроїв відповідно до уподобань користувача.	1. Коли запрошення гостя на віддалений доступ, він повторно перевірить, чи належать з'єднання від маршрутизатора до NAT. Але деякі гості встановили з'єднання з іншим хостом, якщо конкретний користувач не відповість на правильний хост, то він отримає запит, інший хост. Цей критерій призведе до погіршення продуктивності мережі 2. Якщо існує декілька додатків і протоколів, на які покладаються цілі функції, то мережа користувача не може бути доступною для інших користувачів. Оскільки хост вбудований всередині мережі NAT, як я надоступна, як обговорювалося вище 3. Якщо є необхідність усунення неполадок у мережі з віддалених районів, то усунення несправностей буде важким і призводить до втрати відстеження від кінця до кінця. 4. Застосування протоколів тунелювання створює більше ускладнень через значення перекладених NAT у заголовках IP, а також перериває перевірку цілісності, проблеми IPsec та лікими протоколами тунелювання. 5. Послуги, для яких потрібні з'єднання з встановленим UDP або TCP з глобальної сторони, можуть бути порушені та, можливо, часом недоступні.

Таблиця 4.2 - Переваги та недоліки WMM [31]

Переваги	Недоліки
1. Все сучасне мережеве обладнання працює за стандартом WMM. 2. Ефективно працює для медіа (IPTV) і голосового (VoIP) трафіку. 3. За її рахунок акумулятори мобільних пристроїв економлять до 30% заряду.	1. Пріоритет ставить на голос і відео, і вибрати тільки між ними не можна. 2. Старі пристрої не працюють з даним стандартом.

Рисунок А.17

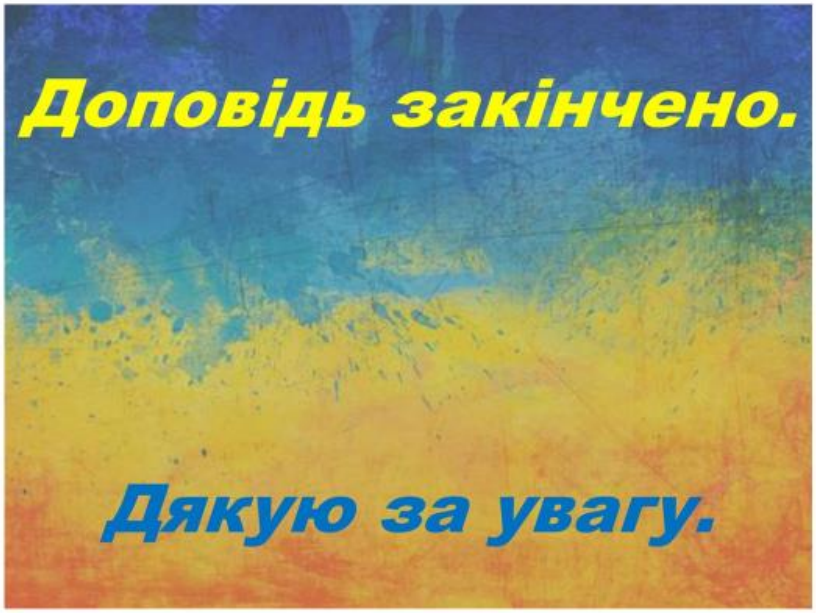


Рисунок А.18

Позначення	Найменування	Дод. відомості
	Текстові документи	
1.	Пояснювальна записка	94 с.
	Графічні документи	
2.	Слайди презентації	18

Змін.	Арк.	Номер докум.	Підпис	Дата	Дослідження методів апаратно-технічного захисту локальної мережі	Літ.	Аркуш	Аркушів
						У	1	1
Розробив		Діль				ХНУРЕ кафедра ІМІ		
Перевір.		Золотарьов						
Н. контр.		Золотарьов						
Затв.		Безрук						