Урок №10. **Тема.** **Керування механізмами захисту. Виявлення атак. Захист периметра комп'ютерних мереж. Міжнародні стандарти інформаційної безпеки.**

**IV. Вивчення нового матеріалу**

 *4.* **Безпека мережі** (*Network security*) — заходи, які захищають інформаційну мережу від [несанкціонованого доступу](https://uk.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D1%96%D0%BE%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF), випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів.

Безпека [інформаційної мережі](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0) включає захист обладнання, [програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F), даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних у мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та в закладах інших типів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або «ключ», кредитну картку або мобільний телефон, при трифакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

 *5.* Безпека мережі включає:

* захист обладнання;
* захист персоналу;
* захист ПЗ;
* захист даних від несанкціонованого доступу.

 *6.* Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить із ладу, решта продовжує захищати дані вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.Система безпеки мережі:

* захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином;
* забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації;
* контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями;
* забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

 *7.* Ключові елементи захищених мережних служб

● **Брандмауери.** Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

● **Антивірусні засоби.** Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

● **Знаряддя, які відстежують стан мережі**, грають важливу роль під час визначення мережних загроз.

● **Захищений віддалений доступ і обмін даними**. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу відіграє важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

 *9.* Захист в Wi-Fi мережах . Існує два основних варіанти пристрою бездротової мережі:

 **– Ad-hoc** - передача безпосередньо між пристроями;

**– Hot-spot -** передача здійснюється через точку доступу; В Hot-spot мережах присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але і доступ до зовнішніх мереж. Hot-spot представляє найбільший інтерес з точки зору захисту інформації, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених в даній бездротовій мережі.

 *9.* **Методи обмеження доступу**

* + Фільтрація MAC-адреси.
	+ Режим прихованого ідентифікатора SSID.
	+ Методи аутентифікації.
	+ Методи шифрування.

 *12.* **Фільтрація MAC-адреси:**

Даний метод не входить в стандарт IEEE 802.11. Фільтрацію можна здійснювати трьома способами:

 – точка доступу дозволяє отримати доступ станціям з будь-якою MAC-адресою;

– точка доступу дозволяє отримати доступ тільки станціям, чиї MAC-адреси знаходяться в довірчому списку;

– точка доступу забороняє доступ станціям, чиї MAC-адреси знаходяться в «чорному списку»;

 Найбільш надійним із точки зору безпеки є другий варіант, хоча він не розрахований на підміну MAC-адреси, що легко здійснити зловмисникові.

 *11.* **Режим прихованого SSID** . Для свого виявлення точка доступу періодично розсилає кадри-маячки (англ. beacon frames). Кожен такий кадр містить службову інформацію для підключення і, зокрема, присутній SSID (ідентифікатор бездротової мережі). У разі прихованого SSID це поле порожнє, тобто неможливо виявлення вашої бездротової мережі і не можна до неї підключитися, не знаючи значення SSID. Але всі станції в мережі, підключені до точки доступу, знають SSID і при підключенні, коли розсилають Probe Request запити, вказують ідентифікатори мереж, наявні в їх профілях підключень. Прослуховуючи робочий трафік, з легкістю можна отримати значення SSID, необхідне для підключення до бажаної точки доступу.

 *12. Методи аутентифікації*

Аутентифікація - видача певних прав доступу абоненту на основі наявного в нього ідентифікатора.

IEEE 802.11 передбачає два методи аутентифікації:

Відкрита аутентифікація (англ. Open Authentication):

Робоча станція робить запит аутентифікації, у якому присутня тільки MAC-адреса клієнта. Точка доступу відповідає або відмовою, або підтвердженням аутентифікації. Рішення ухвалює на основі MAC-фільтрації, тобто це захист на основі обмеження доступу, що не є безпечним.

Аутентифікація із загальним ключем (англ. Shared Key Authentication):

Необхідно налаштувати статичний ключ шифрування алгоритму WEP (англ. Wired Equivalent Privacy). Клієнт робить запит у точки доступу на аутентифікацію, на що отримує підтвердження, яке містить 128 байт випадкової інформації. Станція шифрує отримані дані алгоритмом WEP (виконується побітове додавання з модулем 2 даних повідомлення з послідовністю ключа) і надсилає зашифрований текст разом із запитом на асоціацію. Точка доступу розшифровує текст і порівнює з початковими даними. У разі збігу надсилає підтвердження асоціації, і клієнт вважається підключеним до мережі. Схема аутентифікації із загальним ключем вразлива до атак «Man in the middle». Алгоритм шифрування WEP — це проста XOR-послідовність з корисною інформацією, отже, прослухавши трафік між станцією і точкою доступу, можна відновити частину ключа. IEEE почав розробки нового стандарту IEEE 802.11i, але через труднощі затвердження, організація WECA (англ. Wi-Fi Alliance) спільно з IEEE анонсували стандарт WPA (англ. Wi-Fi Protected Access). У WPA використовується TKIP (англ. Temporal Key Integrity Protocol, протокол перевірки цілісності ключа), який використовує вдосконалений спосіб керування ключами та покадрову зміну ключа.

WPA також використовує два способи аутентифікації:

Аутентифікація за допомогою наданого ключа WPA-PSK (англ. Pre-Shared Key) (Enterprise Autentification);

Аутентифікація за допомогою RADIUS-сервера (англ. Remote Access Dial-in User Service)

###  *13.* Методи шифрування

### WEP-шифрування (англ. Wired Equivalent Privacy):

### Аналог шифрування трафіку в провідних мережах. Використовується симетричний потоковий шифр RC4 (англ. Rivest Cipher 4), який досить швидко функціонує. На сьогоднішній день WEP і RC4 не вважаються криптостійкими.

### Є два основних протоколи WEP:

### 40-бітний WEP (довжина ключа 64 біта, 24 з яких — це вектор ініціалізації, який передається відкритим текстом);

### 104-бітний WEP (довжина ключа 128 біт, 24 з яких — це теж вектор ініціалізації); Вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності алгоритму.

### TKIP-шифрування (англ. Temporal Key Integrity Protocol):

### Використовується той же симетричний потоковий шифр RC4, але є більш криптостійким. Вектор ініціалізації становить 48 біт. Враховані основні атаки на WEP. Використовується протокол Message Integrity Check для перевірки цілісності повідомлень, який блокує станцію на 60 секунд, якщо послані протягом 60 секунд два повідомлення не пройшли перевірку цілісності. З урахуванням всіх доопрацювань і удосконалень TKIP все одно не вважається криптостійким.

### CKIP-шифрування (англ. Cisco Key Integrity Protocol):

### Має подібності з протоколом TKIP. Створений компанією Cisco. Використовується протокол CMIC (англ. Cisco Message Integrity Check) для перевірки цілісності повідомлень.

### WPA-шифрування:

### Замість уразливого RC4, використовується криптостійкий алгоритм шифрування AES (англ. Advanced Encryption Standard). Можливе використання EAP (англ. Extensible Authentication Protocol, розширюваний протокол автентифікації).

### Є два режими:

### Pre-Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі;

### Enterprise - перевірка здійснюється серверами RADIUS;

### WPA2-шифрування (IEEE 802.11i):

### Прийнятий у 2004 році, з 2006 року WPA2 повинна підтримувати все вироблене Wi-Fi обладнання. В даному протоколі застосовується RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Спочатку в WPA2 використовувався протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника). Основою є алгоритм AES. Для сумісності зі старим обладнанням є підтримка TKIP і EAP (англ. Extensible Authentication Protocol) з деякими його доповненнями. Як і в WPA є два режими роботи: Pre-Shared Key і Enterprise.

###  *14.* Віддалена мережева атака — інформаційний руйнівний вплив на розподілену обчислювальну систему , що здійснюється програмно по каналах зв'язку.

###  *15.* Види мережевих атак:

### атака листами;

### віруси, троянські коні;

### мережева розвідка;

### Man-in-the-Middle;

### сніффінг пакетів;

### IP-спуфінг;

### соціальна інженерія;

### відмова в обслуговуванні (DoS );

### ін’єкція.

###  *16.* Атаки настільки ж різноманітні, як різноманітні системи, проти яких вони спрямовані.

### Атака листами. Вважається найстарішим методом атак, хоча суть його проста й примітивна: велика кількість листів унеможливлюють роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Цій атаці складно запобігти, тому що провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.

###  *17.* Віруси, троянські коні, поштові черв'яки, сніффери, Rootkit-и і інші спеціальні програми.

### Наступний вид атаки є більш витонченим методом отримання доступу до закритої інформації - це використання спеціальних програм для ведення роботи на комп'ютері жертви, а також подальшого розповсюдження (це віруси і черв'яки). Принципи дії цих програм різні.

###  *18.* Сніффінг пакетів

### Також досить поширений вид атаки, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. У такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальним додатком, який називається сніффер, для обробки. У результаті зловмисник може отримати велику кількість службової інформації: хто звідки куди передавав пакети, через які адреси ці пакети проходили.

###  *19*. IP-спуфінг

### Теж поширений вид атаки в недостатньо захищених мережах, коли зловмисник видає себе за санкціонованого користувача, перебуваючи у самій організації, або за її межами. Така атака можлива, якщо система безпеки дозволяє ідентифікацію користувача тільки за IP-адресою і не вимагає додаткових підтверджень.

###  *20.* Соціальна інженерія

### Соціальна інженерія (від англ. Social Engineering) - використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації. Як говорить стара приказка, «Найслабша ланка системи безпеки - людина».

### Основною метою соціальної інженерії є: дослідження причин тої чи іншої поведінки людини; обставин та середовища, що впливають на формування системи цінностей індивіду, і як наслідок - їх поведінки.

###  *21.* Відмова в обслуговуванні

### DoS (від англ. Denial of Service - відмова в обслуговуванні) - атака, яка має на меті змусити сервер не відповідати на запити

###  *22.* Мережева розвідка

### У ході такої атаки крекер власне не робить ніяких деструктивних дій, але в результаті він може отримати закриту інформацію про побудову та принципи функціонування обчислювальної системи жертви. У ході такої розвідки зловмисник може виробляти сканування портів, запити DNS, луна-тестування відкритих портів, наявність і захищеність проксі-серверів.

### Man-in-the-Middle

### З англ. «Людина посередині». Коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. Мета такої атаки - крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Тому в чисто технічному плані убезпечити себе можна лише шляхом криптошифрування переданих даних.

###  23. Програмно-апаратні засоби захисту мереж

### Міжмережеві екрани

### Біометричний захист інформації

### Віртуальна приватна мережа

### Антивірус

### Криптографічний захист

### МЕ можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по ІР-адресах (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів ТСР і прапорців, що містяться в пакетах (наприклад, запити на встановлення з’єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

### Віртуальна приватна мережа створюється на базі загальнодоступної мережі Інтернет. І якщо зв’язок через Інтернет має свої недоліки, головним з яких є те, що вона схильна до потенційних порушень захисту та конфіденційності, то VPN можуть гарантувати, що направляється через Інтернет трафік так само захищений, як і передача всередині локальної мережі. У той же час віртуальні мережі забезпечують істотну економію витрат у порівнянні з вмістом власної мережі глобального масштабу.

### Антивірус – програмний засіб, призначений для боротьби з вірусами. Виходячи з визначення, основними завданнями антивірусу є:

### перешкоджання проникненню вірусів у комп’ютерну систему;

### виявлення наявності вірусів у комп’ютерній системі;

### усунення вірусів з комп’ютерної системи без нанесення ушкоджень іншим об’єктам системи;

### мінімізація збитку від дій вірусів;

### технології виявлення вірусів.

### Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

 *24.*VPN **–** це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об’єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв’язку між ними непідконтрольних каналів.

Технологія VPN створює віртуальні канали зв’язку через загальнодоступні мережі, так звані «VPN**-**тунелі». Трафік, що проходить через тунелі, які зв’язують віддалені філії, шифрується. Зловмисник, що перехопив шифровану інформацію, не зможе переглянути її, оскільки не має ключа для розшифровки.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол**-**IP (такий спосіб використовує реалізація PPTP-Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Технологія VPN останнім часом використовується не тільки для створення власне приватних мереж, але і деякими провайдерами для надання виходу в Інтернет складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути кілька, і «зовнішня» мережа, по якій проходить інкапсульоване з’єднання (зазвичай використовується Інтернет). Можливо також підключення до віртуальної мережі окремого комп’ютера. Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступної) мережі. При підключенні віддаленого користувача (або при установці з’єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (дистанційна мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації. Класифікувати VPN рішення можна за кількома основними параметрами.

Переваги VPN очевидні. Надавши користувачам можливість з’єднуватися через Інтернет, масштабованість досягається в основному збільшенням пропускної здатності каналу зв’язку, коли мережа стає перевантаженою. VPN допомагає заощадити на телефонних витратах, оскільки вам не потрібно мати справу з пулом модемів. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які в звичайній ситуації адміністратори змушені виносити на зовнішнє з’єднання.

**Отже, VPN забезпечує:**

* захищені канали зв’язку за ціною доступу в Інтернет, що в кілька разів дешевше від виділених ліній;
* при установці VPN не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів **–** все це значна економія;
* забезпечується масштабування, оскільки VPN не створює проблем росту і зберігає зроблені інвестиції;
* незалежність від криптографії та можливість використання модулів криптографії будь-яких виробників у відповідності з національними стандартами тієї чи іншої країни;
* відкриті інтерфейси дозволяють інтегрувати вашу мережу з іншими програмними продуктами та бізнес-додатками.

До недоліків VPN можна віднести порівняно низьку надійність. У порівнянні з виділеними лініями та мережами на основі Frame relay віртуальні приватні мережі менш надійні, проте в 5**-**10, а іноді і в 20 разів дешевші. На думку аналітиків, це не зупинить VPN, це не суттєво для більшості користувачів.

###  *25.* Міжмережевий екран (МЕ) - це локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему і/або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall (англ. вогняна стіна).

### МЕ служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп’ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, спливаючі вікна та інше, не надсилати іншим «чужим» серверам інформацію про ваш комп’ютер, знешкоджує роботу програм-троянів і засобів віддаленого адміністрування. Робота МЕ полягає в аналізі структури і вмісту інформаційних пакетів, що надходять зі зовнішньої мережі, і в залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує. Ефективність роботи МЕ, що працює під управлінням Windows, зумовлена тим, що він повністю заміщує реалізований стек протоколів TCP\IP, і тому порушення його роботи хакерами з допомогою спотворення протоколів зовнішньої мережі є неможливим.

### МЕ виконують такі функції:

### фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв’язку;

### багатоетапну ідентифікацію запитів, що надходять в мережу;

### перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;

### реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;

### контроль цілісності програмного забезпечення і даних;

### економію адресного простору мережі;

### приховування IP-адреси внутрішніх серверів з метою захисту від хакерів.

### Розрізняють два типи МЕ: апаратний і програмний. Апаратний являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп’ютер. Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп’ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип реалізації МЕ.

### МЕ можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів за ІР-адресами (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів ТСР і прапорців, що містяться в пакетах (наприклад, запити на встановлення з’єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

### Переваги серверів прикладного рівня: локальна мережа стає невидимою з мережі Internet; при порушенні працездатності міжмережевого екрана пакети перестають проходити через нього, тим самим не виникає загрози для захисту локальної мережі; захист серверів прикладного рівня дозволяє здійснювати велику кількість додаткових перевірок, знижуючи тим самим імовірність злому з використанням дірок у програмному забезпеченні; за допомогою аутентифікації на рівні користувача може бути реалізована система негайного попередження про спробу злому.

### Недоліки: більш висока вартість, продуктивність нижча, ніж у пакетних фільтрів; неможливість використання протоколів RPC і UDP.

 *26.*Засоби захисту периметру

**Периметр** - це укріплена границя корпоративної мережі, що може включати:

* маршрутизатори (routers);
* брандмауери (firewalls);
* проксі-сервери; (proxy-servers)
* систему виявлення вторгнень (IDS);
* пристрої віртуальних приватних мереж (VPN);
* засоби антивірусного захисту;
* демілітаризовану зону (DMZ) і екрановані підмережі.

Маршрутизатори (routers) – це пристрої, які здійснюють керування трафіком, що надходить у мережу, чи виходить із мережі або трафіком усередині самої мережі. Прикордонний маршрутизатор (border router) є останнім маршрутизатором, що контролює безпосередньо вхід/вихід в Інтернет. Оскільки весь Інтернет-трафік організації проходить через цей маршрутизатор, останній часто функціонує в ролі першої й останньої лінії захисту мережі, забезпечуючи фільтрацію вхідного й вихідного трафіку.

Брандмауер або міжмережевий екран (firewall) - це пристрій, що аналізує трафік з використанням набору правил, які дозволяють визначити, чи можна передавати цей трафік мережею. Область дії брандмауера починається там, де закінчується область дії прикордонного маршрутизатора. Він виконує набагато більшу, ретельну перевірку пакетів при фільтрації трафіку. Існує кілька різних типів брандмауерів, до яких відносяться статичні пакетні фільтри (static packet filters), брандмауери експертного рівня (stateful-брандмауери), а також проксі-брандмауери (proxy firewalls).

 Для блокування доступу до підмережі можна використовувати, приміром, вбудований статичний пакетний фільтр маршрутизатора Nortel Accellar, для контролю за дозволеними сервісами - брандмауери експертного рівня, наприклад Cisco PIX, а для контролю за вмістом (content) - проксі-брандмауер, наприклад, Secure Computing's Sidewinder. Брандмауери зможуть заблокувати все, що їм зазначено блокувати, і дозволити все, що їм дозволено.

Проксі-сервер (proxy-server) – це проміжний комп’ютер, який є посередником між комп’ютером (або мережею комп’ютерів) та Internet. Через нього проходять всі звернення до Internet, проксі-сервер обробляє їх, надає користувачу, та зберігає дані, які пройшли через нього. За рахунок цього підвищується швидкість доступу до інформації, яка потрібна іншим користувачам і яка вже збережена в пам’яті проксі. Дуже зручно, коли на всіх комп’ютерах встановлено однакові операційні системи та/або програмне забезпечення, оновлення компонентів яких буде відбуватися швидше. (Наприклад, оновлення системи безпеки Windows XP, оновлення для антивірусних програм, персональних брандмауерів тощо). При зверненні в Internet, проксі-сервер надає свою ІР-адресу, а не адресу користувача. Це дозволяє залишатися непомітним в глобальній мережі.

 IDS (Intrusion Detection System — система виявлення вторгнень) - це система, що використовується для виявлення й повідомлення про всі вторгнення й потенційно небезпечні події у корпоративній мережі. Система може містити велику кількість детекторів різного типу, розміщених у стратегічних точках мережі. Існує два основних типи систем виявлення вторгнень: система виявлення вторгнень на рівні мережі (Network-based IDS, NIDS) і система виявлення вторгнень на рівні хоста (Host-based IDS, HIDS).

Детектори NIDS являють собою пристрої, що виконують спостереження за мережевим трафіком і фіксують будь-яку підозрілу активність. Детектори NIDS часто розміщуються в підмережах, які безпосередньо з'єднані із брандмауером, а також у критичних точках внутрішньої мережі. Детектори HIDS функціонують на окремих хостах. Загалом кажучи, детектори IDS шукають заздалегідь задані сигнатури небажаних подій і можуть виконувати статистичний аналіз і аналіз аномальних подій. У випадку виявлення небажаних подій детектори IDS сповіщають адміністратора різними способами: використовуючи електронну пошту, пейджинговий зв'язок або розміщаючи запис в log-файлі. Детектори IDS можуть складати звіт для центральної бази даних, що корелює інформацію, яка від них надходить.

 *28.* **Стандарти інформаційної безпеки —** це стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем оброблення інформації. Основна мета — знизити ризики, включаючи попередження або пом'якшення кібер-атак.

Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

 *29.* **Загальні рекомендації щодо захисту мережі (від Microsoft)**

* Постійно інсталюйте останні оновлення для комп'ютера
* Використання брандмауера
* Запуск антивірусного програмного забезпечення на кожному комп'ютері.
* Використання маршрутизатора для спільного доступу до Інтернету
* Не входьте до системи як адміністратор
* Намагайтеся охороняти свою приватність.

**VII. Підведення підсумків уроку**

* ***Бесіда за питаннями*** *( 35)*
1. Що включає безпека інформаційної мережі?
2. Безпека мережі - це…
3. Що таке мережева атака?
4. Які є види мережевих атак?
5. Які механізми захисту ви знаєте?
6. Що таке міжнародні стандарти безпеки? Яка їх мета?