**Безпе́ка мере́жі**

**Безпе́ка мере́жі**  — заходи, які захищають [інформаційну мережу](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) 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 в 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 інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

 

**Концепції мережевої безпеки**

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 трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі.[[2]](https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96#cite_note-2) Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS)[[3]](https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96#cite_note-3).

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

**Як працює система безпеки**

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з 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.

**Ключові елементи захищених мережних служб**

* [**Брандмауери**](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD)**.** Централізовані брандмауери та брандмауери окремих комп'ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.
* [**Антивірусні засоби**](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81)**.** 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 грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

**Стандарти кібербезпеки**

Це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити [кібернетичне середовище](https://uk.wikipedia.org/w/index.php?title=%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B8%D1%87%D0%BD%D0%B5_%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%BE%D0%B2%D0%B8%D1%89%D0%B5&action=edit&redlink=1) користувача чи організації. Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, [програми](https://uk.wikipedia.org/wiki/%D0%A3%D1%82%D0%B8%D0%BB%D1%96%D1%82%D0%B0), служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж. Основна мета — знизити ризики, включаючи попередження або пом'якшення [кібер-атак](https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D0%B0_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

Стандарти [кібербезпеки](https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) існували протягом кількох десятиліть, оскільки користувачі та постачальники співпрацювали на багатьох вітчизняних та міжнародних форумах для здійснення необхідних можливостей, політики та практики — як правило, вони з'являлися з роботи в [Стенфордському](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BD%D1%84%D0%BE%D1%80%D0%B4%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D1%83%D0%BD%D1%96%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D1%82%D0%B5%D1%82) [консорціумі](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%81%D0%BE%D1%80%D1%86%D1%96%D1%83%D0%BC) з досліджень з питань інформаційної безпеки та політики у 1990-х.[[1]](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8#cite_note-1) Також багато завдань, які колись виконувалися вручну, зараз виконуються комп'ютером; тому існує потреба в забезпеченні інформації (ІА) та безпеці.

Американське дослідження 2016 року щодо затвердження рамок безпеки [США](https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D1%96_%D0%A8%D1%82%D0%B0%D1%82%D0%B8_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8) повідомило, що 70 % опитаних організацій вважають [NIST Cybersecurity Framework](https://uk.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&action=edit&redlink=1) найбільш популярним передовим досвідом комп'ютерної безпеки, але багато хто відзначає, що для цього потрібні значні інвестиції.[[2]](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8#cite_note-2)

[Головний службовець](https://uk.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%BE%D0%B2%D0%B5%D1%86%D1%8C) з питань інформаційної безпеки, як правило, покладається на вибір, впровадження та контроль ефективності та ефективності стандартів [кібербезпеки](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) для їх організації.

**Міжнародні стандарти**

* [BS 7799-1: 2005](https://uk.wikipedia.org/w/index.php?title=BS_7799-1:_2005&action=edit&redlink=1) — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ.
* [BS 7799-2: 2005](https://uk.wikipedia.org/w/index.php?title=BS_7799-2:_2005&action=edit&redlink=1) — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУІБ. Друга частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.
* [BS 7799-3: 2006](https://uk.wikipedia.org/w/index.php?title=BS_7799-3:_2006&action=edit&redlink=1) — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки
* [ISO/IEC 17799](https://uk.wikipedia.org/wiki/ISO/IEC_17799): 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005.
* [ISO/IEC 27000](https://uk.wikipedia.org/wiki/ISO/IES_27000) — Словник і визначення.
* [ISO/IEC 27001](https://uk.wikipedia.org/wiki/ISO/IEC_27001) — «Інформаційні технології — Методи забезпечення безпеки — Системи управління інформаційної безпеки — Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005.
* [ISO/IEC 27002](https://uk.wikipedia.org/wiki/ISO/IEC_27002) — Зараз: [ISO/IEC 17799](https://uk.wikipedia.org/wiki/ISO/IEC_17799): 2005. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Дата виходу — 2007 рік.
* [ISO/IEC 27005](https://uk.wikipedia.org/wiki/ISO_/_IEC_27005) — Зараз: [BS 7799-3](https://uk.wikipedia.org/wiki/BS_7799-3): 2006 — Керівництво з управління ризиками ІБ.
* Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій).