Best practices for Internet security and safety

Найкращі практики забезпечення безпеки Інтернет

Internet Society
Ukraine Chapter

Safer Internet Day 2025

Моя конфіденційність – Ваша безпека

1. Безпека (safety) і захищеність (security)
2. Право на приватність та безпеку
3. Тренди безпеки та конфіденційність в інтернеті 2025
4. Захист кінцевого користувача в інтернеті

Безпека – умови, в яких перебуває складна система, коли дія зовнішніх та внутрішніх чинників, не призводить до явищ, що вважаються небезпечними.

Безпека – стан "відсутності явної загрози", стан захищеності від шкоди чи іншої можливої небезпеки. Безпека також, може означати усунення визнаних (відомих людству) загроз, для досягнення прийнятного рівня ризику. Тобто гарантувати безпеку неможливо, але можна надати або створити певний рівень безпеки.

Захищеність – комплекс дій спрямований на захист від потенційної загрози, небажаного впливу та спотворення результатів роботи системи та до підвищення стійкості від загроз.

Захищеність – це і відчуття, і стан реальності. Об’єкт – цифровий об’єкт в системі, до яких можна віднести як сутності з якими працюють процеси системи, так само як і самі процеси системи, може відчувати себе захищеним або відчувати себе невпевнено, коли вона (сутність) не захищена.

Право на приватність та безпеку

Приватність є основоположним правом *людини* і має важливе значення для автономії та захисту людської гідності, слугуючи фундаментом, на якому будуються багато інших прав людини. Конфіденційність захищає нас від довільного та необґрунтованого використання влади державами, компаніями та іншими суб'єктами. Вона дозволяє нам регулювати те, що можна знати про нас і робити з нами, водночас захищаючи нас від інших, які можуть бажати контролювати.

Закони про конфіденційність в Інтернеті постійно розвиваються. Уряди по всьому світу впроваджують нові закони та правила для вирішення проблем конфіденційності в Інтернеті. У той же час з'являються нові технології, які викликають нові занепокоєння щодо конфіденційності. Цей розділ містить загальний огляд правового ландшафту

У Сполучених Штатах Федеральна торгова комісія (FTC) відповідає за дотримання законів про конфіденційність в Інтернеті. Основна місія FTC полягає в захисті споживачів від шахрайства та недобросовісної ділової практики. Відповідно до Закону, компанії, які збирають персональні дані, повинні надавати чіткі та лаконічні політики конфіденційності, що пояснюють, як вони збирають і використовують дані, як вони отримають згоду користувача, перш ніж збирати або ділитися своїми персональними даними.

Європейський Союз (ЄС) має одні з найсуворіших законів про конфіденційність в Інтернеті у світі. Загальний регламент про захист даних (GDPR) є основним законом, що регулює захист даних в ЄС. GDPR вимагає, щоб компанії отримували чітку згоду від користувачів, перш ніж збирати їхні персональні дані. Він також вимагає від компаній надати користувачам доступ до своїх даних і право на видалення їхніх даних. GDPR також вимагає, щоб компанії повідомляли про витоки даних протягом 72 годин після їх виявлення

Трансфер права на приватність *людини* – до права на приватність *цифрового об'єкту* в Інтернет

Право на приватність та безпеку

Право на приватність в Україні забезпечується Законом України «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів

- **Захист прав інтелектуальної власності в інтернеті**
- **Захист прав на доменне ім'я**
- **Захист товарного знаку в інтернеті**
- **Захист бренду в мережі Інтернет від контрабанди та паралельного імпорту**
- **Захист бренда в інтернеті**
- **Захист торгівельної марки в інтернеті**
- **Захист від образ та дифамації в інтернеті**

- ***Втручання в роботу комп'ютерних та мережевих систем***
- ***Крадіжка персональних даних***
- ***Крадіжка чужого програмного коду***
- ***Використання в комерційних цілях чужого доменного імені***
- ***Нелегальне копіювання матеріалів інтернет-ресурсів***
- ***Використання чужої інтелектуальної власності на контент***
- ***Поширення недостовірних відомостей***
- ***Несанкціоноване використання торгової марки***
- ***Розміщення на власних сайтах піратських копій аудіо та відеоматеріалів***
- ***...***

Тренди безпеки та конфіденційність в інтернеті 2025

Кібербезпека – це практика захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж та даних від зловмисних атак. Вона також відома як безпека інформаційних технологій або електронна інформаційна безпека.

Термін «кібербезпека» застосовується в різних контекстах, від бізнесу до мережевих та пов'язаних з ними обчислень.

- **Мережева безпека – це практика захисту комп'ютерної мережі від зловмисників, будь то цілеспрямовані зловмисники або опортуністичний шкідливий програмний забезпечення**
- **Безпека додатків зосереджена на захисті програмного забезпечення та пристроїв від загроз. Скомпрометована програма може надати доступ до даних, для захисту яких вона призначена. Успішна безпека починається на етапі проектування, задовго до розгортання програми або пристрою**
- **Інформаційна безпека захищає цілісність і конфіденційність даних, як при зберіганні, так і при передачі.**
- **Операційна безпека включає процеси та рішення щодо обробки та захисту активів даних. Дозволи, які користувачі мають під час доступу до мережі, а також процедури, які визначають, як і де можуть зберігатися або ділитися даними, підпадають під цю парасольку..**
- **Аварійне відновлення та безперервність роботи визначають, як організація реагує на інцидент кібербезпеки або будь-яку іншу подію, що спричиняє втрату операцій або даних. Політика аварійного відновлення визначає, як організація відновлює свої операції та інформацію, щоб повернутися до тієї ж операційної потужності, що й до події. Безперервність роботи – це план (DRP), до якого організація повертається, намагаючись працювати без певних ресурсів.**
- **Освіта кінцевих користувачів стосується найбільш непередбачуваного фактора кібербезпеки: людей. Будь-хто може випадково занести вірус у безпечну систему, не дотримуючись належних методів безпеки. Навчити користувачів видаляти підозрілі вкладення електронної пошти, не підключати неідентифіковані USB-накопичувачі та різні інші важливі уроки є життєво важливими для безпеки будь-якої організації**

Кібербезпека і захист даних

Кібербезпека – фокусується на захисті цифрових систем, мереж та інфраструктури від атак, загроз та несанкціонованого доступу.

Захист даних – спрямовано на захист самих даних незалежно від середовища їх зберігання та передачі та від втрати, модифікації, крадіжки чи витоку.

Аспект	Кібербезпека	Захист даних
Фокус	Забезпечення безпеки мереж, серверів, пристроїв, програм	Забезпечення конфіденційності, цілісності та доступності даних
Об’єкт захисту	Інфраструктура (мережі, сервери, пристрої, IoT)	Дані (файли, бази даних, облікові записи)
Методи захисту	Мережі екрани (Firewall), IDS/IPS, VPN, MFA, антивіруси	Шифрування, контроль доступу, резервне копіювання, DLP-системи
Типи загроз	Кібератаки, зломи, DDoS, шкідливе ПЗ, фішинг	Витіки даних, внутрішні загрози, крадіжка інформації
Ключові технології	SIEM, SOC, Zero Trust Security, AI для кібербезпеки	AES/RSA шифрування, блокчейн, DRM, політики керування доступом

Тренди безпеки та конфіденційність в інтернеті 2025

Аспекти кіберзагроз:

1. **Кіберзлочинність включає окремих суб'єктів або групи, які націлені на системи з метою отримання фінансової вигоди або з метою спричинення збоїв.**
2. **Кібератака часто пов'язана зі збором фінансової, технологічної, економічної або політично вмотивованої інформації.**
3. **Кібертероризм має на меті підірвати електронні системи, викликати паніку чи страх.**

Шкідливе програмне забезпечення

- **Вірус – самовідтворювана програма, яка прикріплюється до чистого файлу та поширюється по всій комп'ютерній системі, заражаючи файли шкідливим кодом**
- **Трояни – тип зловмисного програмного забезпечення, яке маскується під законне програмне забезпечення. Кіберзлочинці обманом змушують користувачів завантажувати трояни на свій комп'ютер, де вони завдають шкоди або збирають дані**
- **Шпигунські програми – програма, яка таємно записує, що робить користувач, щоб кіберзлочинці могли скористатися цією інформацією. Наприклад, шпигунське програмне забезпечення може заволодіти даними кредитної картки**
- **Програми-вимагачі – зловмисне програмне забезпечення, яке блокує файли та дані користувача з погрозою видалити їх, якщо не буде сплачено викуп.**
- **Рекламне програмне забезпечення – рекламне програмне забезпечення, яке може використовуватися для розповсюдження шкідливого програмного забезпечення**
- **Ботнети – мережі комп'ютерів, заражених шкідливим програмним забезпеченням, які кіберзлочинці використовують для виконання завдань в Інтернеті без дозволу користувача**

Тренди безпеки та конфіденційність в інтернеті 2025

SQL-ін’єкції

- Ін’єкція SQL (structured language query) – це тип кібератаки, який використовується для отримання контролю та крадіжки даних із бази даних. Кіберзлочинці використовують вразливості в програмах на основі даних, щоб вставити шкідливий код у базу даних за допомогою шкідливого SQL-виразу. Це дає їм доступ до конфіденційної інформації, що міститься в базі даних

Фішинг

- Фішинг – це коли кіберзлочинці націлюються на жертв за допомогою електронних листів, які виглядають як від законної компанії, яка просить конфіденційну інформацію. Фішингові атаки часто використовуються для того, щоб обманом змусити людей передати дані кредитних карток та іншу особисту інформацію

Атака “man-in-the-middle"

- Атака "людина посередині" – це тип кіберзагрози, коли кіберзлочинець перехоплює спілкування між двома особами з метою крадіжки даних. Наприклад, у незахищеній мережі Wi-Fi зловмисник може перехопити дані, які передаються з пристрою жертви та мережі

Атака типу «denial-of-service»

- Атака "відмова в обслуговуванні" – це коли кіберзлочинці перешкоджають комп’ютерній системі виконувати законні запити, перевантажуючи мережі та сервери трафіком. Це робить систему непридатною для використання, заважаючи організації виконувати життєво важливі функції

Захист кінцевого користувача в інтернеті

Захист кінцевих користувачів або безпека кінцевих точок є важливим аспектом кібербезпеки. Зрештою, часто це фізична особа (кінцевий користувач), яка випадково завантажує шкідливе програмне забезпечення або іншу форму кіберзагрози на свій настільний комп'ютер, ноутбук або мобільний пристрій.

Як заходи кібербезпеки захищають кінцевих користувачів і системи?

1. Кібербезпека ґрунтується на криптографічних протоколах для шифрування електронних листів, файлів та інших критично важливих даних. Це не тільки захищає інформацію під час передачі, але й захищає від втрати або крадіжки.
2. Захисне програмне забезпечення кінцевого користувача сканує комп'ютери на наявність фрагментів шкідливого коду, поміщає цей код у карантин, а потім видаляє його з комп'ютера. Захисні програми можуть навіть виявляти та видаляти шкідливий код, прихований у первинному завантажувальному записі, і призначені для шифрування або стирання даних з жорсткого диска комп'ютера.
3. Електронні протоколи безпеки зосереджені на виявленні шкідливого програмного забезпечення в режимі реального часу. Багато хто використовує евристичний і поведінковий аналіз для моніторингу поведінки програми та її коду для захисту від вірусів або троянів, які змінюють свою форму з кожним виконанням (поліморфні та метаморфічні шкідливі програми). Програми безпеки можуть обмежувати потенційно шкідливі програми віртуальною бульбашкою, окремою від мережі користувача, щоб аналізувати їхню поведінку та вчитися краще виявляти нові інфекції.

Програми безпеки продовжують розвивати нові засоби захисту, оскільки фахівці з кібербезпеки виявляють нові загрози та нові способи боротьби з ними. Щоб отримати максимальну віддачу від програмного забезпечення безпеки кінцевих користувачів, співробітники повинні бути проінструктовані щодо його використання. Важливо підтримувати його в робочому стані та часто оновлювати, що гарантує, що він може захистити користувачів від новітніх кіберзагроз.

Захист кінцевого користувача в інтернеті

Найкращі практики дотримання безпеки в Інтернеті

- Використовуйте надійні, унікальні паролі
- Увімкніть двофакторну автентифікацію (2FA)
- Регулярно оновлюйте програмне забезпечення
- Остерігайтеся фішингового шахрайства
- Використовуйте безпечне інтернет-з’єднання
- Встановіть антивірусне програмне забезпечення
- Регулярно створюйте резервні копії даних
- Будьте обережні з особистою інформацією
- Захистить свою робочу або домашню мережу
- Освітлюйте себе та свою сім’ю

Safer Internet Day 2025

День безпечного Інтернету 2025

Internet Society GIGABIT CHAPTER 2025

Internet Society Ukraine Chapter

ISOC Ukraine Chapter

Зроби крок до всесвітньої спільноти, знайди себе у світі Інтернет

Приєднуйся до наших лав

https://www.isoc-ua.org/about/