**Нзарій Ющишин**

**(Рівне, Україна)**

**КІБЕРБЕЗПЕКА У СУЧАСНОМУ СВІТІ**

У сучасному світі кібербезпека є однією з найбільш актуальних проблем, оскільки цифрові технології переплітаються зі всіма аспектами нашого життя, від економіки та політики до соціальних мереж та особистих даних. Розширення цифрового простору також призводить до збільшення кількості кібератак та кіберзлочинів, які можуть стати загрозою для безпеки людей та організацій. Особливо важливо забезпечити кібербезпеку в таких галузях, як банківський сектор, медицина, енергетика та транспорт, де порушення безпеки можуть мати серйозні наслідки. У цій науковій роботі будуть розглянуті актуальні проблеми кібербезпеки у сучасному світі та запропоновані практичні рекомендації щодо забезпечення безпеки в цифровому просторі.

У сучасному цифровому світі кібербезпека стала однією з найбільш актуальних та важливих тем. З кожним днем все більше людей та компаній використовують Інтернет та інформаційні технології для своїх потреб. Однак разом з цим зростають ризики порушення безпеки інформації та вразливості до кібератак.

Кібербезпека охоплює безпеку комп’ютерів, мереж, пристроїв, програм та даних, що знаходяться в цифровому середовищі. Вона має на меті захистити інформацію від несанкціонованого доступу, розголошення, зміни, втрати та втручання.

Загрози кібербезпеці можуть походити з різних джерел, включаючи зловмисники, які можуть проводити кібератаки з метою отримання конфіденційної інформації, пошкодження системи, зміни даних або вимагання викупу. Окрім того, вирішальну роль у кібербезпеці відіграють люди, які можуть бути неправильно навчені, що може призвести до вразливості системи.

Для захисту від кібератак існує безліч заходів та стратегій. Одним з найважливіших є забезпечення безпеки мережі та даних. Це може бути досягнуто шляхом встановлення паролів, шифрування даних, аутентифікації користувачів та використання захищеного з’єднання. Для забезпечення безпеки програм можна використовувати антивірусні програми та програми для виявлення вразливостей. Однак важливо пам’ятати, що кібербезпека це не тільки технічні засоби, але й управління ризиками та культура безпеки в цілому.

***Управління ризиками*** - це підхід до кібербезпеки, який полягає у виявленні потенційних загроз, їх оцінці та прийнятті заходів для зменшення ризиків. Цей підхід дозволяє компаніям та організаціям оцінити потенційні загрози та ризики для їх бізнесу та прийняти належні заходи для забезпечення безпеки. Наприклад, встановлення регулярних оновлень програмного забезпечення та забезпечення резервного копіювання даних можуть зменшити ризик втрати даних через кібератаки.

***Культура безпеки*** - це усвідомлення людьми необхідності забезпечення безпеки в цифровому середовищі. Вона полягає в навчанні та популяризації знань про кібербезпеку та правильної поведінки в Інтернеті. Це може включати навчання користувачів, як правильно встановлювати та використовувати паролі, не надсилати конфіденційну інформацію на запит, використання захищеного з’єднання та багато іншого.

Забезпечення кібербезпеки має важливе значення не тільки для користувачів, але й для компаній та організацій. Недостатній рівень кібербезпеки може призвести до втрати конфіденційної інформації, порушення законодавства, падіння репутації та фінансових втрат. Це може вплинути на бізнес-процеси та загрожувати існуванню компанії.

Користувачі повинні усвідомлювати необхідність забезпечення своєї кібербезпеки та використовувати заходи захисту, такі як паролі, двофакторна аутентифікація та антивірусне програмне забезпечення. Крім того, важливо пам’ятати про небезпеки фішингу, шахрайства та інших видів кібератак.

Компанії та організації повинні включати кібербезпеку у свою стратегію та плани, забезпечувати свої системи захисту та відповідати за безпеку даних своїх клієнтів та співробітників. Важливо відзначити, що кібербезпека не є одноразовою задачею, а має бути постійною увагою і розвитком.

Кібербезпека у медицині є дуже важливим питанням, оскільки медичні установи містять велику кількість чутливої інформації про пацієнтів, такі як медичні картки, результати тестів, інформація про стан здоров’я та інші конфіденційні дані. Ці дані можуть стати об’єктом крадіжки та зловживання, якщо за ними не буде належного контролю.

*Нижче наведено деякі рекомендації, які можуть допомогти у забезпеченні кібербезпеки в медицині:*

1. Забезпечити захист даних: Медичні установи повинні використовувати захищені системи зберігання даних та шифрування інформації, щоб запобігти несанкціонованому доступу до чутливих даних.
2. Оновлювати програмне забезпечення: Медичні установи повинні регулярно оновлювати програмне забезпечення своїх комп’ютерів та серверів, щоб запобігти вразливостям у системах, які можуть бути використані зловмисниками для атаки.
3. Тренувати персонал: Працівники медичних установ повинні бути навчені про правила безпеки та ризики кібератак, щоб уникнути потенційних проблем.
4. Застосовувати багатофакторну аутентифікацію: Медичні установи повинні використовувати багатофакторну аутентифікацію для доступу до систем, щоб запобігти несанкціонованому доступу
5. Аудит безпеки: Медичні установи повинні регулярно проводити аудит безпеки, щоб виявити можливі вразливості та вжити заходи щодо їх усунення.
6. Використовувати захист від вірусів: Медичні установи повинні використовувати антисептичні засоби та противірусні препарати, захисні маски тощо.

*Основні принципи кібербезпеки у медицині включають наступне:*

1. Забезпечення безпеки мережі: це означає використання захисних механізмів для захисту медичних пристроїв та мережі від кібератак. До таких механізмів належать, наприклад, мережеві брандмауери та антивірусні програми.
2. Захист медичної інформації: це означає використання шифрування та інших технологій для захисту конфіденційної медичної інформації від несанкціонованого доступу.
3. Забезпечення безпеки медичних пристроїв: це означає використання захисних механізмів та програмного забезпечення для захисту медичних пристроїв від кібератак та зловживання.
4. Своєчасне оновлення програмного забезпечення та патчів безпеки: це означає регулярне оновлення програмного забезпечення та патчів безпеки для медичних пристроїв та систем управління медичними даними.
5. Навчання персоналу: це означає надання персоналу медичних закладів необхідної освіти та навичок, які дозволяють забезпечити кібербезпеку у медицині.
6. Систематичні аудити та тестування на проникнення: це означає проведення регулярних аудитів та тестування на проникнення для виявлення потенційних ризиків та вразливостей у медичних системах та пристроях.

**Висновок**

Отже, кібербезпека є важливою складовою цифрового світу, яка потребуєвсебічного підходу та уваги як соціальних аспектів, так і технічних. Це означає, що кібербезпека має бути відповідальністю кожного користувача Інтернету, а також компаній та організацій.

**Література:**

1. Андрєєв В.В., Як організувати діловодство на підприємстві [Текст] / В.В. Андрєєв. Андрєєв. - М.ІНФРА-М, 2009. - 94с.
2. Основні напрями досліджень, що ґрунтуються на семантичному аналізі текстів [Електронний ресурс] / СГ держ. ун-т, фак. прикладної математики - процесів управління.
3. Пошукова система Google Search: [http:://google.com](https://www.google.com/)

**Науковий керівник:**

спеціаліст вищої категорії, викладач Черняк Тетяна Григорівна.