КІБЕРБЕЗПЕКА У ВІЙСЬКОВІЙ МЕДИЦИНІ: НОВІТНІ ТЕХНОЛОГІЇ ТА ВИКЛИКИ

Ольга Уразовська
заступник начальника управління –
начальник відділу
УКРНОІВІ, к.ю.н.

IP OFFICE
Український національний офіс інтелектуальної власності та інновацій

АКТУАЛЬНІСТЬ ТЕМИ

Сфера охорони здоров'я – одна із лідерів у світі за зростанням кількості кібератак.
Витоки даних у медичній сфері найдорожчі – у середньому вони обходились медичним закладам західних країн у $10 млн ***(дані CHECK POINT RESEARCH (CPR) TEAM за 2022 рік).***

У сучасних умовах кібербезпека у військовій медицині набуває критичного значення. Військові медичні системи зберігають чутливу інформацію щодо *безпеки медичних персональних даних українських військових, захисту інформаційного поля військової медицини та безпеки і оборони нашої країни в цілому.*

Кібербезпека – це захищеність комп'ютерних інформаційних пристроїв та систем від несанкціонованого доступу, що забезпечує конфіденційність, цілісність, доступність інформації та своєчасне виявлення, запобігання, нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Нормативно-правове регулювання кібербезпеки у військовій медицині

ВРУ 27 березня 2025 року прийняла Закон про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури (реєстр. № 11290).

Законодавство у сфері кібербезпеки, зокрема:

Закон України **«Про державну таємницю»** – регулює порядок охорони інформації, що має статус державної таємниці, в тому числі у сфері військової медицини.

Закон України **«Про інформацію»** – забезпечує основи інформаційного захисту і визначає права та обов'язки стосовно обробки інформації.

Закон України **«Про захист персональних даних»** – регулює обробку і захист персональних даних, що має особливе значення для медичних даних.

Закон України **«Про основні засади забезпечення кібербезпеки України»** – регулює основи кібербезпеки, визначає правові, організаційні та технічні вимоги для захисту інформаційних систем і мереж.

Закон України **«Про захист інформації в інформаційно-комунікаційних системах»** – визначає вимоги до захисту інформації в інформаційних системах, які можуть використовуватись у сфері військової медицини.

Закон України **«Про Державну службу спеціального зв'язку та захисту інформації України»** - визначає правові основи захисту інформації України.

Стратегія забезпечення національної безпеки, Стратегія кібербезпеки України, Стратегія інформаційної безпеки, Стратегія воєнної безпеки України, Стратегія розвитку ОПК, Стратегія розвитку системи охорони здоров'я.

Законодавство у сфері військової медицини, зокрема:

Закон України **«Про військовий обов'язок і військову службу»** – визначає основи організації військової служби, що включають аспект медичної підтримки військових.

Закон України **«Про оборону України»** – включає положення щодо забезпечення національної безпеки, що можуть впливати на управління медичними даними у військових умовах.

Закон України **«Про статус ветеранів війни, гарантії їх соціального захисту»** – забезпечує додаткові права та гарантії для ветеранів війни, включаючи право на безкоштовне медичне обслуговування, санаторно-курортне лікування, реабілітацію та інші види медичної допомоги.

Постанова Кабінету Міністрів України від 5 червня 2000 № 938 **«Про затвердження Положення про медичне забезпечення Збройних Сил України»**.

Накази та постанови Міністерства оборони України – регулюють питання медичної підтримки військових, включаючи організацію медичних закладів і захист медичних даних. **Нормативні документи з охорони здоров'я та медичної допомоги** у військових умовах – можуть включати специфічні вимоги до захисту медичних даних і забезпечення конфіденційності.

Суб’єкти забезпечення кібербезпеки

Президент України
(здійснює координація діяльності у сфері кібербезпеки як складової національної безпеки України)

Раду національної безпеки і оборони України

Національний координаційний центр кібербезпеки

здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення ***Стратегії кібербезпеки України***

Кабінет Міністрів України
(забезпечує формування та реалізацію державної політики у сфері кібербезпеки, боротьбу з кіберзлочинністю тощо)

Суб’єктами, які здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, зокрема є:

- **міністерства та інші ЦОВВ;**
- **місцеві державні адміністрації;**
- **органи місцевого самоврядування;**
- **правоохоронні, розвідувальні і контррозвідувальні органи тощо;**
- **Збройні Сили України, інші військові формування, утворені відповідно до закону;**
- **підприємства, установи, організації, віднесені до об’єктів критичної інфраструктури тощо**

Кібербезпека у військовій медицині – комплексний перетин кількох ключових дисциплін:

Інтелектуальна власність (ІВ)

Трактування ІВ як ключового активу у сфері військової медицини, особливо в контексті розробки нових технологій та інновацій. ***Це можуть бути медичні технології, засоби лікування або профілактики, а також програмне забезпечення, що забезпечує кібербезпеку медичних систем.*** Національна система управління ІВ повинна забезпечувати охорону цих розробок ***шляхом патентування винаходів (корисних моделей), отримання свідоцтва про реєстрацію авторського права, свідоцтва на торговельну марку*** *тощо.*

Кібербезпека

Кібербезпека є важливим елементом у військовій медицині, включає ***захист даних, які зберігаються або передаються в цифровій формі,*** а також ***забезпечення надійної роботи медичних систем у військових умовах.***

Військова медицина

Військова медицина є специфічною сферою, де повинні враховуватись ***особливі вимоги військових структур, такі як оперативність, стійкість до кіберзагроз та захист критичної інфраструктури.***

Розробки в цій сфері можуть мати подвійне призначення – використовуватися як для військових, так і для цивільних потреб.

Об’єкти права інтелектуальної власності у сфері медицини (зокрема і військовій медицині):

Об’єкти авторського права:

- ***наукові твори*** у сфері медицини (лекції, доповіді, книги, науково-медичні статті, дисертації, монографії, довідники, адаптовані переклади тощо);
- ***технологічна і конструкторська документація*** на медичні прилади, інструменти;
- ***аудіовізуальні демонстраційні версії*** оперативних втручань і комп’ютерні версії етапів оперативного втручання (приклад, відео-трансляція унікальних операцій відомого українського кардіохірурга Бориса Тодурова);
- ***фотографічні твори*** (наприклад, демонстраційна версія технології оперативного втручання);
- ***ілюстрації, малюнки, карти*** (наприклад, анатомічний атлас);
- ***комп’ютерні програми*** *тощо.*

Об’єкти промислової власності:

- ***винаходи*** (медична техніка, лікарські препарати, штами мікроорганізмів та ін.);
- ***корисні моделі*** (пристрій: апарат, інструментарій, пристосування тощо);
- ***промислові зразки*** (дизайн приладів, оформлення лікарських засобів та ін.)

З переліку патентноздатних об'єктів вилучено: способи діагностики, лікування, хірургічні методики.

Об’єкти права ІВ, які є позначеннями:

- ***фірмові (комерційні) найменування;***
- ***торговельні марки*** (оригінальна назва лікарських засобів, штамів мікроорганізмів);
- ***географічні зазначення*** (приклад, лікувальні мінеральні і термальні води («Поляна квасова») (межі географічного місця, з яким пов’язуються особливі властивості, певні якості або інші характеристики товару: смт. Поляна Свалявського району Закарпатської області та його околиці)

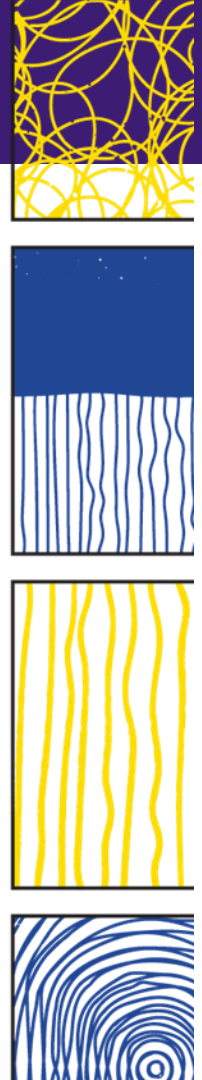
Організація медичного забезпечення:

Медична служба Збройних Сил України –
основна структура, що забезпечує медичну допомогу військовослужбовцям, включає: військові госпіталі, медичні роти, санітарно-епідеміологічні підрозділи та інші медичні заклади

Санітарна евакуація –
є ключовим елементом системи медичного забезпечення військовослужбовців, включає евакуацію поранених та хворих з поля бою до медичних закладів, а також організацію медичної допомоги на різних етапах евакуації

Реабілітація та відновлення –
заходи для військовослужбовців включають фізичну, психологічну та соціальну реабілітацію. Вони здійснюються в спеціалізованих центрах реабілітації, санаторіях та інших медичних закладах

Розробка і застосування медичних технологій
(військова медицина активно займається розробкою нових медичних технологій, які можуть бути застосовані у бойових умовах, таких як новітні системи для моніторингу здоров'я та термінової медичної допомоги)



Аспекти кібербезпеки у медичних даних:

Медичні сили

Збройних Сил України

Конфіденційність медичних даних - передбачає захист особистої інформації пацієнтів від несанкціонованого доступу. Наприклад, шифрування (може включати використання паролів, біометричних даних або двофакторної аутентифікації), аудит і моніторинг (регулярний моніторинг і перевірка доступу до медичних даних для виявлення і запобігання можливим порушенням безпеки)

Цілісність даних. Методи забезпечення цілісності включають: цифрові підписи, контроль, резервне копіювання, захист від атак тощо

Захист медичних інформаційних систем. Медичні інформаційні системи, такі як електронні медичні картки (ЕМК), медичні бази даних і клінічні інформаційні системи, потребують особливого захисту: антивірусний захист тощо

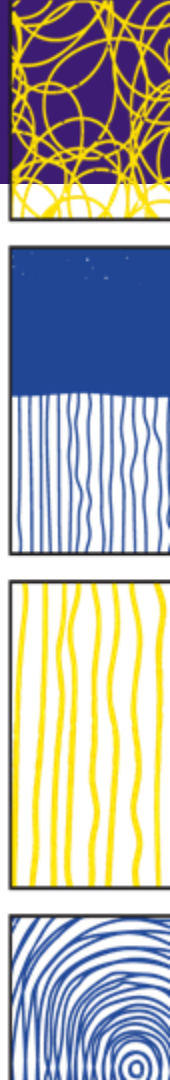
Основні виклики кібербезпеки у сфері військової медицини:

Цілеспрямовані кібератаки – хакери можуть здійснювати атаки на медичну інфраструктуру задля отримання даних або виведення з ладу обладнання

Низький рівень цифрової підготовки персоналу – медичні працівники не завжди навчені належно реагувати на кіберзагрози

Застаріле програмне забезпечення – багато медичних пристроїв використовують застарілі операційні системи, які легко зламати

Проблеми з мобільністю та хмарними технологіями – використання мобільних пристроїв і віддаленого доступу створює нові вразливості



Новітні технології кібербезпеки у сфері військової медицини

Штучний інтелект (AI):
Використовуються для моніторингу мережевої активності та виявлення кібератаки ще до того, як вона завдасть шкоди.

Шифрування даних:
Використання сучасних протоколів шифрування для захисту персональних та операційних медичних даних.

Блокчейн-технології:
Забезпечують прозорий і незмінний облік медичних даних. Доступ можливий лише для авторизованих осіб, що унеможливлює підробку або несанкціонований перегляд.

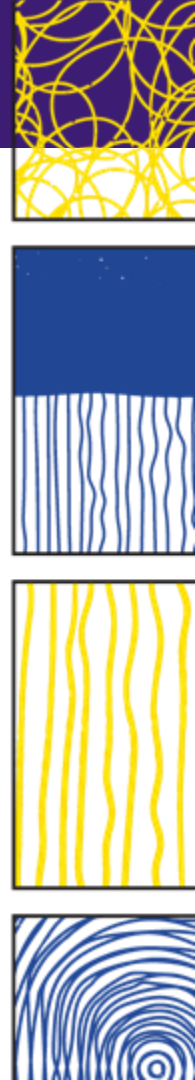
Інтегровані системи реагування на інциденти SIEM (Security Information and Event Management): *Автоматизовані платформи для збору, аналізу та реагування на інциденти в мережі. Допомагають швидко і точно ідентифікувати загрози.*

Багатофакторна автентифікація (MFA):
Підвищує безпеку доступу до медичних систем, комбінуючи паролі з біометрією або смс-кодами.

Кіберполігони та тренажери:
Спеціальні симуляційні середовища для навчання персоналу реагувати на кібератаки, без шкоди для реальних систем.

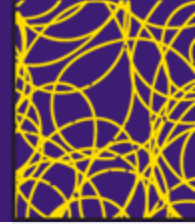
Хмарні захищені платформи:
Використання спеціалізованих військових або сертифікованих хмарних середовищ для зберігання і обробки медичних даних.

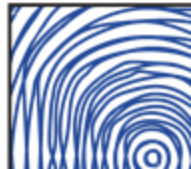
Інтелектуальні системи доступу:
Контроль за рівнями доступу персоналу до чутливої інформації та її використання.



ВИКЛИКИ і РІШЕННЯ щодо інновацій у сфері кібербезпеки військової медицини

Виклики	Рішення
Конфіденційність і безпека	*Розробки у сфері військової медицини часто є секретними і потребують підвищеного захисту від несанкціонованого доступу і використання.*
Права і відповідальність	*Важливо чітко визначити права і обов'язки винахідників, замовників і користувачів таких технологій.*
Інновації і адаптація	*Військова медицина потребує швидкого впровадження новітніх технологій для покращення ефективності медичних рішень.*
Технічні інновації	*Особливу увагу слід приділяти захисту технологій, що забезпечують національну безпеку.*
Класифікація інформації	*У військовій медицині і кібербезпеці існує потреба в особливій класифікації і захисті інформації, яка може мати стратегічне або тактичне значення.*



Порівняльний аналіз щодо використання ІТ-технологій та технологій Штучного Інтелекту, через призму кібербезпеки військової медицини, в країнах світу та в Україні

ІТ-технології

США: система Defense Health Agency (DHA) забезпечує централізоване управління медичними даними та їх захист на рівні всіх військових медичних закладів.

Німеччина: використовуються системи для моніторингу і захисту даних військових медичних установ, які інтегровані з національними системами безпеки.

Ізраїль: Національне управління кібербезпеки (The National Cyber Bureau) як координаційний орган, діяльність якого спрямована на посилення цифрового захисту.

Технології Штучного Інтелекту (ШІ)

США: активно використовують ШІ для виявлення і запобігання кіберзагрозам у медичних системах. Платформи, як-от IBM Watson for Cyber Security, застосовуються для виявлення нових видів загроз і швидкого реагування.

Великобританія: у Великобританії використовуються алгоритми ШІ для покращення безпеки медичних даних, включаючи системи для автоматизованого виявлення вразливостей та моніторинг загроз.

Використання ШІ в **Україні** у сфері кібербезпеки військової медицини лише починається.

Дякую за увагу!

IP OFFICE
Український національний офіс інтелектуальної власності та інновацій

olha.urazovska@nipo.gov.ua

+ вул. Годзенка, 1,
Kyiv, Ukraine