IZDEVNIECĪBA
BALTIJA
PUBLISHING

INNOVATIONS IN SCIENCE: CURRENT RESEARCH AND ADVANCED TECHNOLOGIES

Scientific monograph

Part 2

Riga, Latvia
2025

UDK 001(08)
IN570

Title: Innovations in science: current research and advanced technologies

Subtitle: Scientific monograph

Scientific editor and project director: Anita Jankovska

Authors: Yuri Bandazheuski, Nataliia Dubovaya, Olena Grishyna, Olena Menkus, Anatoliy Shchelkunov, Irina Dobronravova, Anatoliy Shchelkunov, Mane Iskandaryan, Tetiana Biliak, Tatiana Hulyk, Kateryna Kraus, Yuliia Meish, Maria Meish, Liudmyla Nechyporuk, Oleksandra Kocherhina, Dariia Smolych, Nataliia Turlo, Elena Litvin, Natalia Fedorova, Olena Shumkova, Viktoriia Musiienko, Tatiana Hrekul-Kovalyk, Nataliia Korogod, Olha Urazovska, Oleksandr Panasiuk, Olena Perunova, Yuliia Volynets, Nadiia Stadnik, Olha Dienichieva, Hanna Ivaniuk, Olha Oleksiuk, Oksana Kravchenko, Andrii Dzyhovskyi, Nadiya Novoselska, Solomia-Liliia Komarnytska, Tetiana Ponomarenko, Kuzina Oksana, Daryna Mudryk

Publisher: Publishing House "Baltija Publishing", Riga, Latvia

Available from: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/572

Year of issue: 2025

Innovations in science: current research and advanced technologies : Scientific monograph. Part 2. Riga, Latvia : Baltija Publishing, 2025. 664 p.

ISBN: 978-9934-26-531-0

DOI: https://doi.org/10.30525/978-9934-26-531-0

The scientific monograph presents theoretical and practical aspects of the development of science, technology, and innovation in the context of the global transformation of society. It covers general issues of medical sciences, economics and law sciences, pedagogical and philological sciences. The publication is intended for scientists, educators, postgraduate students and undergraduates, as well as the general readership.

Table of Contents

CHAPTER «LAW SCIENCES»

DIGITALIZATION AND SECURITY: THE LATEST SOLUTIONS IN MILITARY MEDICINE

ЦИФРОВІЗАЦІЯ ТА БЕЗПЕКА: НОВІТНІ РІШЕННЯ У ВІЙСЬКОВІЙ МЕДИЦИНІ

Nataliia Korogod[1]
Olha Urazovska[2]

DOI: https://doi.org/10.30525/978-9934-26-531-0-37

Abstract. Modern military conflicts and global challenges require innovative approaches to preserving the lives and health of military personnel. Military medicine is developing rapidly due to the introduction of advanced technologies, including digital solutions and cybersecurity. Automation of medical processes, use of artificial intelligence, telemedicine and secure databases play a key role in improving the efficiency of medical care on the battlefield. Reliable guarantees for the acquisition, exercise, protection and enforcement of intellectual property rights are an essential attribute of the statehood of every civilized country. A modern system of legal protection of intellectual property contributes to the development of the national economy, preservation and enrichment of the scientific and technical potential of the state, development of international trade, and attraction of foreign investments into the country's economy, in particular in the form of state-of-the-art technologies. *The purpose* of the article is to identify the latest solutions in military medicine by studying the development of digital transformation and security (cybersecurity). *Methodology* of the study is based on general research methods of analysis and synthesis, induction and deduction, observation and abstraction. *The results* of the study showed international experience shows a high level of integration of the latest

[1] Candidate of Pedagogical Sciences, Professor,
Professor of the Department of Intellectual Property and Projects Management,
Ukrainian State University of Science and Technologies, Ukraine
ORCID: https://orcid.org/0000-0002-0242-5497
[2] Candidate of Legal Sciences,
Deputy Head of the Intellectual Property and Innovations Department
of National IP Office of Ukraine, Ukraine
ORCID: https://orcid.org/0009-0004-4136-7711

technologies and solutions, while in Ukraine there is a need for further development and implementation of these technologies. Recommendations including increased funding, integration with international standards, and professional development can help Ukraine achieve a higher level of cybersecurity in military medicine. *Practical implications.* Effective management of intellectual property in the field of military medicine cybersecurity is crucial to protecting innovative developments, ensuring national security and maintaining technological progress in the field of military medicine.

1. Вступ

Сучасні військові конфлікти та глобальні виклики вимагають інноваційних підходів до збереження життя та здоров'я військовослужбовців. Військова медицина стрімко розвивається за рахунок впровадження передових технологій, зокрема цифрових рішень та системи кібербезпеки. Автоматизація медичних процесів, використання штучного інтелекту, телемедицина та захищені бази даних виконують ключову роль у підвищенні ефективності медичного забезпечення на полі бою.

Однак цифровізація медичних послуг несе і нові виклики, зокрема загрози кіберзлочинності, які можуть поставити під ризик як особисті дані за рахунок, так і функціонування критично важливих медичних систем. Тому розвиток військової медицини сьогодні неможливий без належного рівня кіберзахисту.

Хакери постійно намагаються викрасти дані для кібератак та інформаційних кампаній. Тому країнам необхідно приділяти особливу увагу питанням кібербзепеки на стратегічному, організаційному та технічному рівнях. Адже будь-хто в державному та приватному секторах може стати елементом атаки на ланцюг постачання. За останні роки цифровізація охорони здоров'я стрімко зростає, розробляються і впроваджуються відповідні «дорожні карти» цифрових проєктів, з-поміж яких важливе місце займають кібербезпека та заходи, що вживаються для підвищення її рівня.

Вибір теми дослідження зумовлюється зростаючою роллю охорони та захисту прав інтелектуальної власності у сфері військової медицини; кіберзахисту, як комплексу процесів, практичних порад,

технологічних рішень, які допомагають захистити важливі системи і дані у військовій медицині від несанкціонованого доступу, особливо це актуально під час війни.

Проблематика питань до цього часу ще не отримала належного теоретичного осмислення та не була досліджена повною мірою. Все це визначає актуальність нашого дослідження, мета якого полягає в аналізі сучасних цифрових технологій та засобів кібербезпеки у військовій медицині, їх вплив на ефективність медичного забезпечення військовослужбовців, а також оцінка ризиків.

Мета роботи: дослідити розвиток новітніх рішень у військовій медицині через призму цифровізації та безпеки.

Застосовані методи: емпіричні методи дослідження (порівняння та дослідження), методи аналізу та синтезу, структурно-функціональний, порівняльно-правовий.

Дослідження подаємо через розкриття таких питань: сучасні тенденції захисту інтелектуальної власності в умовах кібербезпеки військової медицини; основні нормативно-правові акти у сфері сучасних цифрових технологій та засобів кібербезпеки у військовій медицині; ІТ-технології та штучний інтелект (ШІ) у військовій медицині тощо.

2. Сучасні тенденції захисту інтелектуальної власності в умовах кібербезпеки військової медицини

Важливою віхою у становленні права інтелектуальної власності стало підписання у 1967 р. у Стокгольмі Конвенції, якою засновувалася Всесвітня організація інтелектуальної власності (далі – ВОІВ). Відповідно до ст. 2 цієї Конвенції на міжнародному рівні вводиться термін «інтелектуальна власність» та дається визначення цього терміну – це права щодо конкретних результатів творчої діяльності у виробничій, науковій та художній сферах [1].

Основною характеристикою інтелектуальної власності є те, що тільки власник інтелектуальної власності, і насамперед автор, має в своєму розпорядженні виняткові права на її використання, а так само те, що ніяка інша особа не може яким-небудь чином використовувати інтелектуальну власність без його дозволу.

Інтелектуальна власність включає: об'єкти промислової власності, об'єкти авторського права і суміжних прав, засоби індивідуалізації,

так звані «нетрадиційні» об'єкти інтелектуальної власності, в число яких входять комерційна таємниця, секрети виробництва (ноу-хау).

Промислова власність як об'єкт інтелектуальної власності включає патенти на винаходи, корисні моделі, промислові зразки, товарні знаки і знаки обслуговування, фірмові найменування і найменування місць походження товару.

До об'єктів авторського права відносять – твори науки, літератури і мистецтва, комп'ютерні програми, бази даних та інші.

Надійні гарантії набуття, здійснення, охорони та захисту права інтелектуальної власності є невід'ємним атрибутом державності кожної цивілізованої країни. Наявність сучасної системи правової охорони інтелектуальної власності сприяє розвитку національної економіки, збереженню і збагаченню науково-технічного потенціалу держави, розвитку міжнародної торгівлі, залученню в економіку країни іноземних інвестицій, зокрема у вигляді найсучасніших технологій, входженню України як рівноправного партнера до світового ринку інтелектуальної власності. Водночас, кожна галузь, і військова медицина в цьому не є виключенням, має свої особливості і специфіку щодо формування системи права інтелектуальної власності.

Теоретичні підходи до трактування управління інтелектуальною власністю у сфері кібербезпеки військової медицини стосуються комплексного перетину кількох ключових дисциплін, ґрунтується на поняттях інтелектуальної власності (ІВ), кібербезпеки та військової медицини.

Інтелектуальна власність виступає ключовим активом у сфері військової медицини, особливо в контексті розробки нових технологій та інновацій. Це можуть бути медичні технології, засоби лікування, діагностики 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. Важливим є правовий підхід: національні закони щодо ІВ (патенти, свідоцтва на авторські права тощо) та міжнародні угоди (наприклад, Договір про патентну кооперацію [2], Угоди ТРІПС [3]) визначають основні механізми захисту інтелектуальної власності.

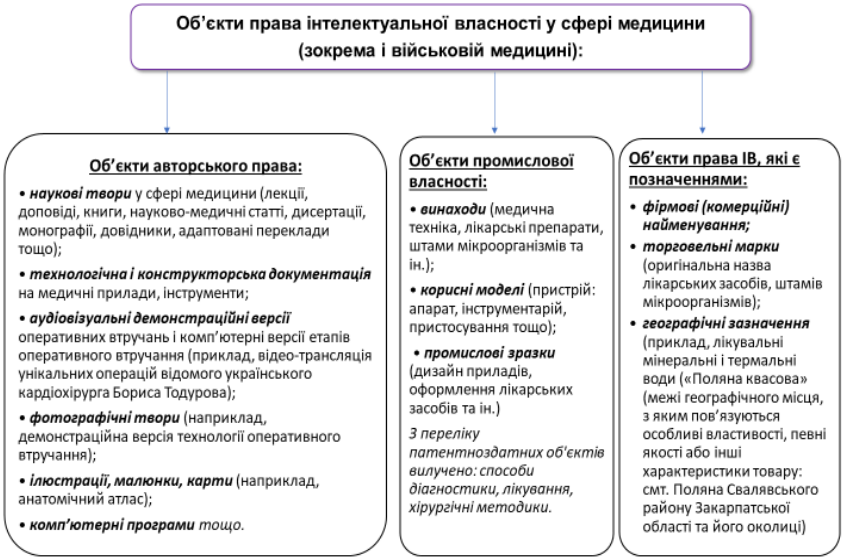

Рис. 1. Об'єкти права інтелектуальної власності у сфері медицини (зокрема і військовій медицині)

Щодо особливостей управління інтелектуальною власністю у сфері кібербезпеки, зазначимо, що кібербезпека є важливим елементом захисту інформації, пов'язаної з інтелектуальною власністю у військовій медицині. Це включає захист даних, які зберігаються або передаються в цифровій формі, а також забезпечення надійної роботи медичних систем у військових умовах. Технології, пов'язані з кібербезпекою, самі по собі можуть бути предметом ІВ, і водночас повинні бути захищені від несанкціонованого доступу. Тому в управлінні даною сферою використовують інформаційно-технологічний підхід: цей підхід акцентує увагу на управлінні та захисті даних, використовуючи системи кібербезпеки, шифрування, управління доступом та інші технології для захисту інтелектуальної власності. Він також вивчає ризики, пов'язані з витоком даних та кібератаками.

Військова медицина є специфічною сферою, де національні системи управління ІВ повинні враховувати особливі вимоги військових

структур, таких 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. Військова медицина – це спеціалізована галузь медицини, яка займається охороною здоров'я і наданням медичної допомоги особам, що перебувають на військовій службі, а також цивільному населенню під час воєнних конфліктів, гуманітарних криз та інших екстремальних ситуацій. Вона охоплює широкий спектр медичних, оперативних та адміністративних аспектів, які відповідають специфічним умовам військової діяльності [4].

Отже, важливою складовою Збройних Сил будь-якої держави є військово-медична служба. Вона забезпечує найбільш повну реалізацію можливостей особового складу військ шляхом постійного зміцнення його здоров'я, сприяючи тим самим успішній діяльності Збройних Сил. У воєнний час медична служба виконує відповідальні функції медичного забезпечення бойових дій військ, надання ефективної кваліфікованої допомоги пораненим та хворим.

Завдання Медичних сил та заходи, що ними виконуються, визначаються: станом здоров'я, фізичним розвитком, рівнем і характером захворюваності особового складу; умовами бойової підготовки та побуту військ (сил); порядком та характером їх застосування; санітарно-епідемічним станом та клімато-географічними умовами розташування військ (сил) [5]. Аналізуючи складові військової медицини зауважимо також на таких аспектах:

– медична підтримка військових операцій включає як медичну допомогу на місці подій, так і стаціонарне лікування;

– організація і координація медичної евакуації поранених з поля бою до медичних установ для подальшого лікування;

– медична підтримка підрозділів включає забезпечення медичних засобів, обладнання і персоналу для підтримки здоров'я військових у зоні бойових дій;

– профілактика і гігієна здійснюється через вакцинацію (проведення вакцинацій для запобігання інфекційним захворюванням, які можуть загрожувати військовим) та управління санітарними умовами у військових таборах і зонах бойових дій для запобігання епідеміям та забезпечення здорових умов для особового складу;

– психологічна підтримка надається як допомога військовим, які можуть страждати від стресу, травмування, посттравматичного стресового розладу (ПТСР) та інших психологічних проблем, а також з метою адаптації до бойових умов (підготовка військових до можливих психологічних навантажень і стресів, що виникають під час служби);

– психологічна допомога надає психологічну підтримку військовим, які можуть страждати від стресу, травмування, посттравматичного стресового розладу (ПТСР) та інших психологічних проблем;

– військова епідеміологія ґрунтується на моніторингу і контролі інфекцій, а саме на вивченні і контролю епідемічних загроз, що можуть вплинути на військових у різних регіонах, особливо в зонах епідемій або ендемічних захворювань;

– організація медичних закладів включає створення і управління військовими лікарнями, поліклініками та іншими медичними установами;

– розробка медичних стратегій та їх впровадження повинні відповідати специфічним умовам військових операцій.

– розробка і застосування медичних технологій ґрунтується на інноваціях. 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.

Медичні служби (медичні центри, управління, відділи, групи) видів, родів військ (сил) ЗСУ (далі – органи управління медичним забезпеченням ЗСУ) призначені для планування, організації та управління медичним забезпеченням застосування військ (сил) в особливий період, забезпечення високої бойової та мобілізаційної готовності підпорядкованої медичної служби, здійснення контролю за бойовою та спеціальною підготовкою особового складу медичної служби та керівництва медичними службами підпорядкованих військових частин і установ з повноваженнями надавати вказівки, розпорядження і роз'яснення з питань медичного забезпечення [5]. Основу медичної служби військової частини становлять медичні підрозділи або особовий склад медичної служби у військових підрозділах. Кожна військова частина або військовий підрозділ мають у своєму складі такі відповідні елементи медичної служби: поліклініка або медичний пункт – у вищих

військових навчальних закладах; медична рота або медичний пункт – у бригаді; медичний пункт – у полку, батальйоні (дивізіоні); старший бойовий медик – у роті (батареї); бойовий медик – у взводі [5].

Наступним підходом до управління інтелектуальною власністю у сфері кібербезпеки військової медицини є системний підхід: національна система управління ІВ у військовій медицині повинна функціонувати як інтегрована система, яка враховує різні аспекти: правовий захист, технологічні виклики, взаємодію з іншими національними та міжнародними структурами.

Ще раз наголосимо, що надзвичайно важливими в сучасному світі є кібербезпека та захист медичних даних є, оскільки медичні дані часто містять чутливу інформацію, яка потребує високого рівня захисту від несанкціонованого доступу, витоку або атак. Сфера кібербезпеки у медичній галузі зосереджена на забезпеченні конфіденційності, цілісності та доступності медичних даних, а також на захисті медичних інформаційних систем. У контексті військової медицини надзвичайно важливо забезпечити кіберзахист медичних даних, як-от дані про стан здоров'я військовослужбовців. При розробленні відповідного програмного забезпечення мають бути дотримані суворі правила щодо забезпечення конфіденційності даних, які обробляються в медичних інформаційних системах. Питання захищеності інфраструктури збору, зберігання і передачі медичних даних насамперед полягає в обмеженні доступу та створенні надійної електронної бази медичної інформації [6].

Проаналізувавши літературу, наприклад наукові дослідження О. Г. Трофименко, Я. В. Дубової, Н. І. Логінової, Ю. В. Прокоп, О. В. Задерейко можна виділити й іншу систематизацію особливих аспектів кібербезпеки у медичних даних [6]. Так, конфіденційність медичних даних – передбачає захист особистої інформації пацієнтів від несанкціонованого доступу. Наприклад, шифрування (використання криптографічних методів для захисту медичних даних під час зберігання і передачі. Шифрування гарантує, що дані можуть бути прочитані лише авторизованими особами), контроль доступу (впровадження систем управління доступом, які забезпечують, що тільки уповноважені користувачі мають доступ до чутливих даних. Це може включати використання паролів, біометричних даних або двофактор-

ної аутентифікації), аудит і моніторинг (регулярний моніторинг і перевірка доступу до медичних даних для виявлення і запобігання можливим порушенням безпеки) [7].

Цілісність медичних даних забезпечує, щоб інформація не була змінена або пошкоджена під час зберігання або передачі. Методи забезпечення цілісності включають: цифрові підписи (використання цифрових підписів для підтвердження, що дані не були змінені після їх створення або обробки), контроль версій (зберігання та моніторинг різних версій медичних даних для відновлення початкових даних у разі пошкодження), доступність даних (доступність медичних даних забезпечує, щоб дані були доступні для авторизованих користувачів у будь-який час, коли це необхідно.

Основні заходи для забезпечення доступності включають: резервне копіювання – регулярне створення резервних копій медичних даних для відновлення інформації у разі втрати або пошкодження), захист від атак (захист інформаційних систем від атак, таких як DDoS-атаки (розподілені атаки на відмову в обслуговуванні), які можуть перешкоджати доступу до медичних даних) [8].

Захист медичних інформаційних систем включає використання медичних інформаційних систем, таких як електронні медичні картки (ЕМК), медичні бази даних і клінічні інформаційні системи, потребують особливого захисту: антивірусний захист (використання антивірусного програмного забезпечення для запобігання шкідливому програмному забезпеченню, яке може загрожувати медичним даним) [9].

Наступний підхід – управління ризиками: зосереджується на ідентифікації ризиків для медичних даних і відповідному управлінні ними. Він також включає розвиток політик і протоколів для реагування на кіберзагрози та захисту від кібератак.

Також сфера військової медицини та кібербезпеки потребує дотримання міжнародних стандартів та участі в глобальних ініціативах щодо захисту ІВ та кіберзахисту. Важливим є вивчення глобальних тенденцій та стандартів щодо захисту ІВ у контексті військової медицини і кібербезпеки. Це також включає аналіз міжнародних договорів та угод щодо координації між країнами в цій сфері [10]. Сфера кібербезпеки є особливою областю, де інтелектуальна власність має специфічні особливості та виклики. Військова медицина є високоспеціалізо-

ваною областю, де управління інтелектуальною власністю стикається з певними викликами.

Таблиця 1

Прийняття управлінських рішень у сфері ІВ військової медицини

Виклики	Рішення
Конфіденційність і безпека	Розробки у сфері військової медицини часто є секретними і потребують підвищеного захисту. Управління ІВ має забезпечувати захист цих розробок від несанкціонованого доступу і використання.
Права і відповідальність	Військова медицина часто пов'язана з державною власністю, де права на інтелектуальну власність можуть бути обмежені державними інтересами і законодавством. 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. Це вимагає адаптації управлінських підходів до ІВ для підтримки інноваційного процесу.
Технічні інновації	Розробки в сфері кібербезпеки, такі як новітні алгоритми шифрування, програмні засоби для захисту від кіберзагроз, вимагають патентного захисту і захисту авторських прав. 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. Управління ІВ має враховувати ці аспекти для запобігання витоку або несанкціонованого доступу.

Підсумовуючи, зазначимо, що військова медицина є критично важливою для забезпечення ефективності військових операцій і захисту здоров'я військових і цивільного населення у випадках конфліктів і надзвичайних ситуацій. Вона інтегрує медичні знання і технології з специфічними вимогами військової служби, сприяючи не лише лікуванню, але і профілактиці захворювань і травм, психологічній підтримці і загальному забезпеченню медичної безпеки. Теоретичні підходи до трактування системи управління ІВ у сфері кібербезпеки військової медицини показують важливість інтеграції правових, адміністративних і економічних аспектів для ефективного захисту і використання інновацій.

3. Основні нормативно-правові акти у сфері сучасних цифрових технологій та засобів кібербезпеки у військовій медицині

Теоретичне трактування системи управління інтелектуальною власністю у сфері кібербезпеки військової медицини базується на кількох ключових підходах: правовому, інформаційно-технологічному, системному та підході до управління ризиками.

Щодо безпосередньо до теми нашого дослідження, захист інформації в контексті кібербезпеки визначається низкою законодавчих актів і нормативних документів. Першочергово зупинимось на Законі України «Про основні засади забезпечення кібербезпеки України» [11], що регулює основи кібербезпеки, визначає правові, організаційні та технічні вимоги для захисту інформаційних систем і мереж. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. В статті 1 даного закону даються важливі для теми нашого дослідження визначення, зокрема:

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Кібер-шпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури.

Згідно цього закону об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору [11].

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів ЄС та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій. Забезпечення кібербезпеки в Україні ґрунтується на встановлених принципах, також законодавчо визначених [11].

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [11]. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні, покладені на них завдання.

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також

з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

Інший важливий закон – Закон України «Про захист інформації в інформаційно-комунікаційних системах» – визначає вимоги до захисту інформації в інформаційних системах, які можуть використовуватись у сфері військової медицини [12]. Відповідно цього закону об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації, порушення цілісності та режиму доступу до інформації [12].

Також, важливу роль у сфері кібербезпеки військової медицини відіграють Стратегії розвитку. Так, Стратегія розвитку інновацій [13] – це проєкт Мінцифри з детально розписаними напрямками та кроками до 2030-го. «Україна вже майже 10 років перебуває у стані перманентної кібервійни», – наголошується в документі. Мета – створити умови для розробки кіберпродуктів. Наприклад, залучати фінансових партнерів, розробити регулювання штучного інтелекту (ШІ) в контексті кібербезпеки та налагодити співпрацю приватного сектора з оборонними відомствами.

Для галузі кібербезпеки Мінцифри пропонує два проєкти. Перший – «Кіберстійка нація». Це має бути екосистема для заохочення цивільних брати участь у «кіберщиті». Другий – перетворення держави на кібербренд за аналогією з Ізраїлем [14].

При проведенні наукового дослідження було взято до уваги Стратегію кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 р. № 447 [15]. Стратегія кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Негативною ознакою технологічного розвитку, пов'язаного із всеохоплюючим поширенням цифрових технологій, розширенням Інтернетсередовища, є критично зростаючий технічний рівень інструментарію реалізації кіберзагроз, від чого ландшафт таких загроз охоплює все більше

сфер життєдіяльності. Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критично важливій інфраструктурі. Зловмисники зосереджують зусилля на пошуку вразливостей активів (систем управління) і розробляють для цього унікальні за своїми властивостями: багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети, що здійснюють розподілені атаки (DDoS) на операційні мережі, виробничі системи, які використовують хмарні сервіси, атаки на ланцюги поставок.

Відповідно Національній економічній стратегії на період до 2030 року, Постанова Кабінету Міністрів України від 03.03.2021 № 179 (http://surl.li/wesruo) [16], вказана візія напряму: цифрові технології – основа добробуту України; світ, де створюються наші нові можливості; сфера, що визначає суть трансформацій у країні для кращого життя. Аналіз цифрової економіки: низький рівень розвитку цифрових інфраструктур стримує зростання цифрової економіки в Україні.

Таким чином, проведений нами аналіз нормативно-правової бази показує, що в Україні існує ряд добре розроблених законодавчих і нормативних актів, які охоплюють різні аспекти захисту кібербезпеки та медичних даних.

Проте існують певні проблеми і виклики:

– існує потреба в синхронізації законодавчих актів, які регулюють захист інтелектуальної власності і кібербезпеки, щоб забезпечити єдиний підхід до управління і захисту даних;

– нормативно-правова база повинна бути оновлена відповідно до швидкого розвитку технологій у сфері кібербезпеки та військової медицини;

– важливим аспектом є інтеграція національних норм з міжнародними стандартами і угодами для забезпечення ефективного захисту інтелектуальної власності та медичних даних на міжнародному рівні;

– необхідно підвищити рівень правової прозорості і забезпечити чіткість у питаннях захисту прав ІВ у сфері медичних інновацій і кібербезпеки.

Підсумовуючи, зазначимо, що управління інтелектуальною власністю (ІВ) у сфері кібербезпеки військової медицини є складним процесом, який включає захист технологічних інновацій, програмного

забезпечення, медичних даних та інші аспекти, що мають критичне значення для безпеки національних інтересів і здоров'я військових.

Для подолання зазначеної проблематики необхідно: оновлення законодавства (потребує актуалізації національних законів і нормативно-правових актів з урахуванням швидкого розвитку технологій та міжнародних стандартів); інвестування в технології та кадри (збільшення фінансування для розробки і впровадження нових технологій, а також навчання і підготовки фахівців); захист конфіденційності (розробка комплексних стратегій для забезпечення конфіденційності медичних даних і зменшення ризиків витоку інформації), міжнародна співпраця (розширення співпраці з міжнародними організаціями для покращення обміну інформацією і впровадження передових практик у сфері управління ІВ). Це дозволить забезпечити ефективну охорону й захист інтелектуальної власності та підвищити безпеку медичних даних у військовій медицині. Розглянуті теоретичні та законодавчо-нормативні аспекти дозволять нам розробити конкретні практичні заходи з підвищення ефективності досліджуваної сфери діяльності.

4. ІТ-технології та штучний інтелект (ШІ) у військовій медицині

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі [15].

Економічно розвинені держави постійно шукають можливості для залучення інноваційних ідей у виробництво та повсякденне життя своїх громадян, тим паче у такі пріоритетні сфери життя, як військова медицина. Це створює можливості покращувати якість та зберегти життя населення. На жаль, в Україні впровадження таких ідей та проектів здійснюється неефективно, але саме від них залежить її майбутнє: економічне зростання чи стагнація.

Слід зазначити, що сучасна кібербезпека військової медицини все більше покладається на ІТ-технології та технології штучного інтелекту

(ШІ) для забезпечення безпеки медичних даних, систем і процесів. З метою порівняння застосування цих технологій у різних країнах, а також в Україні, важливо розглянути, як міжнародний досвід співвідноситься з практиками, що реалізуються на національному рівні.

Сьогодні кіберзагрози постали не тільки перед нашою державою, а і перед всією світовою системою безпеки в цілому. Питома вага кіберзагроз зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів.

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [17].

Боротьба ведеться не тільки на полі бою, але й в мережі Інтернет. Нині, у сучасному цифровому світі, де кіберзагрози стають все більш складними і високотехнологічними, захист від кібератак вимагає не лише традиційних методів, а й впровадження новітніх технологій. Запобігання кіберзлочинності та захист цифрових систем від атак ворога вимагають поєднання винахідливості, ефективних стратегій та доступу до передових технологій. Одними з таких технологій безумовно є технології штучного інтелекту (ШІ).

Штучний інтелект (ШІ) сприяє управлінню та попередженню небезпек, своєчасному виявленню загроз та реагуванню на них у реальному часі, визначенню пріоритетів серед потенційних ризиків, а також виявленню можливостей та ресурсів для реагування на реальні та потенційні загрози. Це свідчить про значний потенціал штучного інтелекту у збільшенні рівня кібербезпеки. Крім того, технології ШІ

можуть використовуватися для визначення вразливостей та слабких місць у системах та мережах, що дозволяє попереджувати та вчасно усувати їх [18].

ШІ відіграє ключову роль у забезпеченні безпеки в сфері кібербезпеки, дозволяючи залишатися крок попереду від потенційних кіберзагроз. Одним із основних способів застосування ШІ в цій сфері є розробка передових алгоритмів, що допомагають виявляти та запобігати кібератакам. Ці алгоритми призначені для аналізу великих обсягів даних та виявлення закономірностей, які можуть вказувати на реальну або потенційну загрозу.

Штучний інтелект забезпечує можливість обробки цієї інформації зі швидкістю та масштабами, недосяжними для людини, що дозволяє системам оперативно виявляти потенційні та реальні кіберзагрози та надавати належну реакцію на них. Однак в контексті використання ШІ важливо розуміти і про дотримання прав ІВ. Сам по собі ШІ як такий – це комп'ютерна програма, тому правовий режим ШІ регулюється законодавством про авторське право. Охорона комп'ютерної програми поширюється на комп'ютерні програми, виражені у вихідному або об'єктному кодах, якщо вони є оригінальними. Охорона надається формі вираження комп'ютерної програми. Графічний інтерфейс користувача, набір виконуваних функцій, формат файлів даних, які використовуються у комп'ютерній програмі для експлуатації її функцій, не є формами вираження комп'ютерної програми. Ідеї та принципи, на яких ґрунтується будь-який елемент комп'ютерної програми, зокрема ті, на яких ґрунтується її інтерфейс, логічні схеми, алгоритми та мови програмування, не охороняються авторським правом. Слід відмітити, що неоригінальні об'єкти, створені програмою, є тими, що відрізняються від існуючих і утворюються без прямого втручання людини. Суб'єктами цього права можуть бути автори програми, їх спадкоємці або особи з правом на її використання. Створенням такого об'єкта не виникають особисті немайнові права, а сам обсяг прав визначається відповідно до законодавства. Якщо неоригінальний об'єкт, створений комп'ютерною програмою, використовує матеріали з авторським або суміжним правом, суб'єкт має право на цей об'єкт за умови дотримання прав власників цих матеріалів.

Щоб ширше розкрити тематику нашого дослідження звернемося до міжнародного досвіду щодо ІТ-технологій у кібербезпеці військової медицини. Так, Сполучені штати Америки (США): активно впроваджують ІТ-технології у військову медицину через системи електронних медичних записів (EMR), які інтегровані з платформами для моніторингу здоров'я в реальному часі. Наприклад, система Defense Health Agency (DHA) забезпечує централізоване управління медичними даними та їх захист на рівні всіх військових медичних закладів [19]. Defense Health Agency (DHA) – Агентство охорони здоров'я оборони є об'єднаним інтегрованим Агентством бойової підтримки, яке дозволяє медичним службам армії, флоту та повітряних сил надавати медичні сили бойовим командуванням як у мирний, так і у воєнний час. DHA використовує принципи Ready Reliable Care для просування практики високої надійності в системі військової охорони здоров'я шляхом вдосконалення роботи системи, впровадження інноваційних рішень і культивування культури безпеки [20]. США є лідером із запровадження кібербезпеки в аерокосмічній, оборонній та безпековій галузях, маючи найбільшу кількість патентів, вакансій і угод, пов'язаних із кібербезпекою. Тим часом Велика Британія, Греція, Німеччина та Японія також зберігають значні позиції щодо впровадження кібербезпеки в аерокосмічній, оборонній та безпековій галузях [21].

Країни ЄС застосовують інтегровані платформи для обміну медичними даними та забезпечення безпеки цих даних. У Німеччині, наприклад, використовуються системи для моніторингу і захисту даних військових медичних установ, які інтегровані з національними системами безпеки [22].

Сьогодні в багатьох провідних країнах світу вже сформовані загальнодержавні системи кібербезпеки – як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [23]. За таких умов актуальним та своєчасним є висвітлення прогресивного досвіду держави Ізраїль щодо організаційно-правового забезпечення побудови національної системи кібербезпеки, враховуючи також провідні позиції цієї країни у світових рейтингах. Ізраїльські військові медичні системи використовують розгорнуті ІТ-рішення для забезпечення безпеки даних, включаючи шифрування і

контроль доступу. Країна також застосовує системи для прогнозування і моніторингу медичних ризиків. Слід зазначити, що на даний час Ізраїль є другим у світі після США експортером програмного забезпечення. Отже, з постачальника стартапів Ізраїль поступово перетворюється на міжнародний центр високих технологій і, насамперед, одного з провідних світових лідерів в галузі кібербезпеки [23]. В Ізраїлі активно застосовуються принципи конверсії та трансферу технологій.

Щодо вітчизняної військової медичної системи, в Україні існує кілька ІТ-рішень для управління медичними даними у військових медичних установах. Впровадження електронних медичних карток і систем для обробки медичних записів відбувається, проте масштабність і інтеграція таких систем на рівні всіх військових медичних закладів потребують подальшого розвитку. Основними викликами для України в цьому плані є недостатнє фінансування, старіння інфраструктури та недостатня інтеграція з міжнародними системами, що обмежує ефективність кібербезпеки.

Зауважимо, що використання ШІ в Україні у сфері кібербезпеки військової медицини лише починається. Є кілька розробок в області автоматизованого виявлення загроз і аналізу ризиків, проте їх масштабування і інтеграція на рівні всієї системи поки що обмежена.

У підсумку на основі результатів порівняльного аналізу стану сфери кібербезпеки військової медицини, зробимо висновок, що в розвинених країнах спостерігається висока інтеграція ІТ-рішень і ШІ у військову медицину, що забезпечує ефективний захист і управління медичними даними. В Україні, хоча й є певні досягнення, інфраструктура та інтеграція знаходяться на етапі розвитку і потребують значних поліпшень. Розвинені країни активно впроваджують новітні технології, розроблені з використанням інтелектуальної власності для вдосконалення кібербезпеки у військовій медицині. В Україні технологічний розвиток у цій сфері обмежений, і більшість рішень базуються на вже існуючих ІТ-технологіях.

Враховуючи вищевикладене можна надати такі рекомендації для подолання зазначених вище викликів і проблем:

– на державному рівці необхідне збільшення фінансування для розробки і впровадження передових ІТ-рішень і технологій ШІ у сфері військової медицини;

– покращити інтеграцію з міжнародними стандартами: адаптація національних рішень до міжнародних стандартів і практик для покращення кібербезпеки;

– здійснювати сучасне підвищення кваліфікації та підготовку фахівців у сфері кібербезпеки і ШІ для забезпечення ефективного впровадження нових технологій;

– розширення співпраці з міжнародними організаціями і країнами для обміну досвідом і передовими практиками.

Отже, використання інтелектуальної власності, ІТ-технологій та технологій ШІ у кібербезпеці військової медицини має важливе значення для захисту медичних даних і систем. Міжнародний досвід показує високий рівень інтеграції новітніх технологій і рішень, в той час як в Україні існує потреба в подальшому розвитку і впровадженні цих технологій. Україні необхідно досягти більш високого рівня кібербезпеки у військовій медицині. Окремі практичні підходи до визначення ролі управління інтелектуальною власністю представимо в наступному підрозділі даної роботи.

5. Висновки

Військова медицина є критично важливою для забезпечення ефективності військових операцій і захисту здоров'я військових і цивільного населення у випадках конфліктів і надзвичайних ситуацій. Вона інтегрує медичні знання і технології з специфічними вимогами військової служби, сприяючи не лише лікуванню, але і профілактиці захворювань і травм, психологічній підтримці і загальному забезпеченню медичної безпеки.

Чинна нормативно-правова база національної системи управління інтелектуальною власністю у сфері кібербезпеки військової медицини є комплексною і охоплює різні аспекти захисту медичних даних та інтелектуальних досягнень. Однак для підвищення ефективності управління і захисту даних необхідно продовжувати вдосконалення законодавства, адаптацію до нових технологій та забезпечення інтеграції з міжнародними стандартами.

Міжнародний досвід показує високий рівень інтеграції новітніх технологій і рішень, в той час як в Україні існує потреба в подальшому розвитку і впровадженні цих технологій. Рекомендації, що включають

збільшення фінансування, інтеграцію з міжнародними стандартами і підвищення кваліфікації, можуть допомогти Україні досягти більш високого рівня кібербезпеки у військовій медицині.

Ефективне управління інтелектуальною власністю у сфері кібербезпеки військової медицини має вирішальне значення для захисту інноваційних розробок, забезпечення національної безпеки та підтримки технологічного прогресу в галузі військової медицини.

Список літератури:

1. Право інтелектуальної власності: Акад. курс: Підруч. для студ. вищих навч. П68 закладів / О. П. Орлюк, Г. О. Андрощук, О. Б. Бутнік-Сіверський та ін.; За ред. О. П. Орлюк, О. Д. Святоцького. К.: Видавничий Дім «Ін Юре», 2007. 696 с.

2. Договір про патентну кооперацію. URL: https://zakon.rada.gov.ua/laws/show/895_001#Text

3. Угода про торговельні аспекти прав інтелектуальної власності. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text

4. Енциклопедія. Військова медицина. URL: https://esu.com.ua/article-34457

5. Доктрина «Медичні сили Збройних Сил України». URL: https://sprotyvg7.com.ua

6. Трофименко О. Г., Дубовой Я. В., Логінова Н. І., Прокоп Ю. В., Задерейко О. В. Аналіз проблеми забезпечення кібербезпеки медичних комп'ютерних систем. *Захист інформації.* Київ :Національний авіаційний університет. 2021. Т. 23. № 1. С. 30–39. DOI: 10.18372/2410-7840.23.15153

7. Конфіденційність медичних даних. URL:

8. Як захищені персональні та медичні дані пацієнтів в е-системі охорони здоров'я. Юридична газета. URL: https://yur-gazeta.com/golovna/yak-zahishcheni-personalni-ta-medichni-dani-pacientiv-v-esistemi-ohoroni-zdorovya.html

9. Безпека електронної системи охорони здоров'я. URL: https://ehealth.gov.ua/2022/07/19/bezpeka-elektronnoyi-systemy-ohorony-zdorov-ya

10. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

11. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

12. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

13. ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC

27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100059

14. Стратегія розвитку інновацій. URL: https://forbes.ua/innovations/krediti-oboronnim-startapam-fabrika-chipiv-rinok-rozminuvannya-ta-kombayni-droni-forbes-oznayomivsya-iz-povnoyu-s

15. Стратегія кібербезпеки України : Указ Президента України від 15.03.16 р. № 96. *Офіційний вісник України*. 2016. № 23. –Ст. 899.

16. Національна економічна стратегії на період до 2030 року, Постанова КМУ від 03.03.2021 № 179. URL: http://surl.li/wesruo

17. Hurzhii S. The special features of using the artificial intelligence in the matters of cybersecurity. *INFORMATION AND LAW*. 2023. №4(47). С. 207-216.

18. Звіт компанії OpenAI. URL: https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

19. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu

20. URL: https://www.health.mil/About-MHS/OASDHA/Defense-Health-Agency

21. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №9 (вересень). – 351 с. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf

22. Європейська інтеграція та трансформація публічного врядування в Україні: матер. наук.-практ. конф. (19 квітня 2024 р., м. Львів) / упорядн.: Буник М. З., Бліщук К. М., Федорчак О. В, Худоба О. В. – Львів: НУ «Львівська політехніка», 2024. 279 с.

23. Досвід Ізраїлю у сфері забезпечення кібербезпеки. URL: https://ippi.org.ua/sites/default/files/6_9.pdf

References:

1. Intellectual property law: Academic course: Textbook for students of higher education institutions / O. P. Orliuk, H. O. Androshchuk, O. B. Butnik-Siverskyi and others; Edited by O. P. Orliuk, O. D. Sviatotskyi Kyiv: In Yure Publishing House, 2007. 696 p. (in Ukrainian)

2. Patent Cooperation Treaty. URL: https://zakon.rada.gov.ua/laws/show/895_001#Text

3. Agreement on Trade-Related Aspects of Intellectual Property Rights. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text

4. Encyclopedia. Military medicine. URL: https://esu.com.ua/article-34457

5. Doctrine “Medical Forces of the Armed Forces of Ukraine”. URL: https://sprotyvg7.com.ua (in Ukrainian)

6. Trofymenko O. , Dubovoi Y., Loginova N., Prokop Y., Zadeiko O. (2021) Analysis of the problem of ensuring the cybersecurity of medical computer

systems. *Information Protection.* Kyiv: National Aviation University. Vol. 23. No. 1. P. 30–39. DOI: 10.18372/2410-7840.23.15153. (in Ukrainian)

7. Confidentiality of medical data. URL: https://medplatforma.com.ua/article/946-dotrimannya-konfdentsynost-nformats-pro-patsnta (in Ukrainian)

8. How personal and medical data of patients are protected in the eHealth system. Yurydychna gazeta. URL: https://yur-gazeta.com/golovna/yak-zahishcheni-personalni-ta-medichni-dani-pacientiv-v-esistemi-ohoroni-zdorovya.html (in Ukrainian)

9. Security of the electronic healthcare system. URL: https://ehealth.gov.ua/2022/07/19/bezpeka-elektronnoyi-systemy-ohorony-zdorov-ya

10. Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine" of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (in Ukrainian)

11. Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian)

12. Law of Ukraine "On Protection of Information in Information and Communication Systems". URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (in Ukrainian)

13. DSTU EN ISO/IEC 27001:2022 Information technology. Methods of protection. Information security management systems. Requirements (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100059 (in Ukrainian)

14. Strategy of innovation development. URL: https://forbes.ua/innovations/krediti-oboronnim-startapam-fabrika-chipiv-rinok-rozminuvannya-ta-kombayni-droni-forbes-oznayomivsya-iz-povnoyu-s (in Ukrainian)

15. Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine dated 15.03.16, No. 96. *Official Gazette of Ukraine.* 2016. No. 23. P. 899. (in Ukrainian)

16. National Economic Strategy for the period up to 2030, Resolution of the Cabinet of Ministers of Ukraine No. 179 of 03.03.2021. URL: http://surl.li/wesruo (in Ukrainian)

17. Hurzhii S. The special features of using the artificial intelligence in the matters of cybersecurity. *INFORMATION AND LAW*. 2023. №4(47). P. 207-216.

18. OpenAI report. URL: https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

19. Army of Cyberwarriors: International Legal Experience in Combating Cybercrime. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu

20. URL: https://www.health.mil/About-MHS/OASDHA/Defense-Health-Agency

21. Cybersecurity in the Information Society: Information and Analytical Digest / edited by O. Dovhan; compiled by. O. Dovhan, L. Lytvynova, S. Dorohykh; State Scientific Institution "Institute of Information, Security and Law of the National Academy of Sciences of Ukraine"; Vernadsky National Library of Ukraine. K.,

2023. No. 9 (September). 351 p. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf (in Ukrainian)

22. European integration and transformation of public governance in Ukraine: materials of the scientific and practical conference (April 19, 2024, Lviv) / compiled by: Bunyk M. Z., Blishchuk K. M., Fedorchak O. V., Khudoba O. V. Lviv: Lviv Polytechnic National University, 2024. 279 p. (in Ukrainian)

23. Israeli experience in the field of cybersecurity. URL: https://ippi.org.ua/sites/default/files/6_9.pdf

Izdevniecība “Baltija Publishing”
Valdeķu iela 62 – 156, Rīga, LV-1058
E-mail: office@baltijapublishing.lv

Iespiests tipogrāfijā SIA “Izdevniecība “Baltija Publishing”
Parakstīts iespiešanai: 2025. gada 27. februāris
Tirāža 300 eks.