УДК 342.9:355.4:004.056
DOI https://doi.org/10.32782/2227-796X.2026.1.03

ЗАБЕЗПЕЧЕННЯ КІБЕРІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІЙСЬКОВИХ ЧАСТИНАХ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

Метою статті *є комплексний аналіз чинного адміністративно-правового механізму забезпечення кіберінформаційної безпеки у військових частинах, визначення особливостей правового регулювання діяльності суб'єктів кіберзахисту у військовій сфері, а також формування пропозицій щодо вдосконалення відповідної системи з урахуванням сучасних кіберзагроз та євроатлантичних стандартів.*

Методологічну основу дослідження *становлять загальнонаукові та спеціально-юридичні методи пізнання, зокрема: діалектичний метод – для з'ясування сутності та змісту кіберінформаційної безпеки у військових частинах; формально-юридичний метод – для аналізу норм адміністративного законодавства у сфері кібербезпеки; системно-структурний метод – для визначення місця адміністративно-правових механізмів у загальній системі національної безпеки; порівняльно-правовий метод – для зіставлення національних підходів із міжнародною та європейською практикою; логіко-юридичний метод – для формулювання узагальнень та висновків.*

Результати дослідження *полягають у встановленні, що адміністративно-правове забезпечення кіберінформаційної безпеки у військових частинах характеризується фрагментарністю нормативного регулювання, значною кількістю підзаконних актів та відсутністю спеціалізованого комплексного законодавчого акта, який би чітко визначав правовий статус, повноваження та відповідальність суб'єктів кіберзахисту у військовій сфері. Обґрунтовано необхідність посилення адміністративного контролю, удосконалення процедур міжвідомчої координації, а також нормативного закріплення спеціальних вимог до організації кібербезпеки у військових частинах з урахуванням стандартів НАТО та Європейського Союзу.*

Висновки *зводяться до того, що ефективне забезпечення кіберінформаційної безпеки у військових частинах неможливе без формування цілісної адміністративно-правової моделі, яка поєднує стратегічне планування, чітке нормативне регулювання, належну систему адміністративної відповідальності та професійну підготовку кадрів. Запропоновано напрями вдосконалення адміністративного законодавства у сфері кібербезпеки військових формувань як важливого елементу зміцнення національної безпеки України.*

Ключові слова: кіберінформаційна безпека; кібербезпека; військові частини; адміністративно-правове забезпечення; національна безпека; інформаційні системи; державне управління; суб'єкти кіберзахисту; адміністративний контроль; правове регулювання.

Нашинець-Наумова Анфіса,
доктор юридичних наук, професор, академік Академії адміністративно-правових наук, заступник декана з науково-методичної та навчальної роботи факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка
orcid.org/0000-0002-5811-7733
a.nashynets-naumova@kubg.edu.ua

1. Вступ

У сучасних умовах розвитку інформаційно-комунікаційних технологій та загострення глобального протистояння у кіберпросторі роль кіберінформаційної безпеки (кібербезпеки) у системі національної безпеки держави невпинно зростає. Особливо актуальним це питання є для воєнних структур, де захист інформації та інформаційних систем має не лише організаційне, але й життєво-стратегічне значення.

Кібербезпека військових частин – це складовий елемент безпеки держави, котрий включає правові, організаційні, технічні та кадрові засади, спрямовані на запобігання, виявлення та реагування на кібер-загрози. У 2026 році цей феномен набуває нових рис через активне впровадження цифрових технологій у бойову діяльність, управління військами, логістику та розвідку. Під поняттям кіберінформаційної безпеки розуміють комплекс заходів, спрямованих на захист інформаційних та інформаційно-технічних систем від несанкціонованого доступу, порушення цілісності, доступності або конфіденційності інформації. У військовому середовищі ці заходи мають підвищені вимоги через національну та стратегічну важливість даних і комунікацій. Особливості кібербезпеки в армії пов'язані із захистом систем управління військами, автоматизованих баз даних, технічних засобів розвідки, комунікаційних мереж та засобів логістичного забезпечення.

Додатковим чинником зростання ролі кіберінформаційної безпеки у військових частинах є трансформація характеру сучасних воєнних конфліктів, у яких кіберпростір розглядається як окремий театр воєнних дій поряд із сушею, морем, повітряним та космічним просторами. Кібероперації здатні завдавати значної шкоди без застосування традиційних видів озброєння, впливаючи на системи управління, зв'язку та прийняття рішень у військових структурах.

В умовах постійного зростання кількості та складності кібератак особливого значення набуває формування ефективної системи управління кібербезпекою у військових частинах. Така система має ґрунтуватися на чіткому розмежуванні повноважень,

нормативно-правовому регулюванні, впровадженні сучасних технічних засобів захисту інформації, а також на підготовці висококваліфікованого особового складу, здатного оперативно реагувати на кіберінциденти.

Водночас забезпечення кіберінформаційної безпеки у військовій сфері потребує системного та комплексного підходу, що поєднує превентивні, захисні та відновлювальні заходи. Ефективна реалізація такого підходу сприяє підвищенню стійкості військових інформаційних систем, зниженню ризиків втрати критично важливих даних та забезпеченню безперервності управління військами в умовах гібридних загроз і кіберпротистояння.

Метою наукової статті є комплексний аналіз кіберінформаційної безпеки військових частин як складової системи національної безпеки держави, визначення її основних особливостей в умовах сучасних кіберзагроз, а також обґрунтування ключових напрямів удосконалення організаційних, правових і технічних механізмів забезпечення кібербезпеки у військовій сфері.

Аналіз останніх досліджень і публікацій. У сучасній науковій і професійній літературі питання кібербезпеки військових структур розглядається в широкому міждисциплінарному контексті, що включає як технічні аспекти захисту інформаційних систем, так і організаційно-управлінські механізми реагування на кіберзагрози. Зокрема, в зарубіжних та вітчизняних фахових виданнях з кібербезпеки опубліковано низку актуальних робіт, які присвячені використанню штучного інтелекту, цифровій суверенності та оцінюванню зрілості кібербезпеки організацій (Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест, 2025).

Одне з сучасних досліджень пропонує рамкову модель цифрового суверенітету для військових AI-орієнтованих систем кібербезпеки, яка зосереджена на збереженні контролю над критично важливими цифровими активами – від даних до AI-моделей – та захисті від загроз несанкціонованого доступу і атак ланцюга поставок. Такий підхід підкреслює важливість міждисциплінарного бачення та стратегії взаємодії з технологіями наступного покоління в оборонному контексті (Стоцький І. В. та ін., 2025)

У вітчизняних наукових журналах, зокрема в серії «Кібербезпека: освіта, наука, техніка», окремі публікації 2025 року присвячені дослідженням адаптивних алгоритмів та моделей захисту інформаційних систем, використанню хмарних технологій та методів штучного інтелекту для підвищення кіберстійкості критичних об’єктів, а також оцінюванню кіберзрілості організацій відповідно до міжнародних стандартів (NIST CSF 2.0, ISO/IEC 27001 та ін.) (Шевченко С. та ін., 2025).

Також у спеціалізованих виданнях розглядається методологія підвищення ефективності ведення кіберборотьби у Збройних Силах, де аналізуються фактори, що впливають на здатність військових структур протистояти кібератакам в умовах реальних операцій. Ці роботи підкреслюють значення комплексного підходу до організації кібербезпеки, що включає не лише

технічні засоби, а й підготовку персоналу та оптимізацію процесів реагування (Гук О. М. та ін., 2024; Горгуленко В. А., Коломієць Б. І., 2025; Воєнні інновації в сучасних війнах, 2025).

В окремих публікаціях також розглядаються аспекти застосування штучного інтелекту у військовій сфері в контексті кібербезпеки, що відповідають сучасним викликам цифрової трансформації оборонних систем. Це підтверджує, що наукова спільнота активно реагує на потребу інтеграції передових технологій в інфраструктуру захисту державних і військових інформаційних систем (Гриндей А. О., 2024; Трофименко О., 2024; Когут Ю. І.,2024; Сушинська А. М. і Родигін К. М., 2024)

У статті використано такі **методи дослідження:** аналіз і синтез – для узагальнення наукових підходів до розуміння сутності та особливостей кіберінформаційної безпеки у військовій сфері; системно-структурний метод – для дослідження кібербезпеки військових частин як складової системи національної безпеки; порівняльно-правовий метод – для аналізу вітчизняного та міжнародного досвіду забезпечення кібербезпеки у воєнних структурах; формально-логічний метод – для уточнення понятійно-категоріального апарату дослідження; метод узагальнення – для формування висновків та визначення перспективних напрямів удосконалення системи кіберінформаційної безпеки.

2. Комплексний аналіз чинного адміністративно-правового механізму забезпечення кіберінформаційної безпеки у військових частинах

Як видається, формування сучасної системи забезпечення кібербезпеки в Україні ґрунтується на комплексі нормативно-правових актів, ключове місце серед яких посідає Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, що діє в оновленій редакції станом на 19 жовтня 2025 року. Саме зазначений закон, на нашу думку, закладає базові правові та організаційні підвалини функціонування системи кібербезпеки, визначаючи її цілі, принципи, суб’єктний склад та об’єкти правового захисту.

Слід зазначити, що вказаний закон має рамковий характер і спрямований насамперед на регламентацію принципів захисту кіберпростору та критичної інформаційної інфраструктури, визначення повноважень органів публічної влади, а також створення національної системи реагування на кіберінциденти. Водночас правове регулювання цієї сфери не обмежується лише спеціальним законом, а доповнюється нормами адміністративного, кримінального та інформаційного законодавства, що, у сукупності, формує комплексний міжгалузевий правовий механізм.

Аналіз чинного законодавства дає підстави стверджувати, що забезпечення кібербезпеки в Україні здійснюється в межах багаторівневої системи публічного управління з чітко розмежованими компетенціями. Так, стратегічне планування у сфері національної безпеки, у тому числі кібербезпеки, покладено на Раду національної безпеки і оборони України

(https://rnbo.gov.ua/), яка виконує координаційну та дорадчу функції.

Кабінет Міністрів України (https://www.kmu.gov.ua/), у свою чергу, забезпечує реалізацію державної політики у сфері кібербезпеки, організовує міжвідомчу взаємодію та здійснює нормативно-правове регулювання у межах своєї компетенції. Важливу роль відіграє Служба безпеки України (https://ssu.gov.ua/), яка, з огляду на свій спеціальний статус, уповноважена здійснювати превентивні та контррозвідувальні заходи, а також розслідувати кіберінциденти, що становлять загрозу національній безпеці.

Окремої уваги заслуговує діяльність Державної служби спеціального зв'язку та захисту інформації України (https://cip.gov.ua/), зокрема в частині організації технічного захисту інформації та функціонування урядової команди реагування на комп'ютерні надзвичайні події. Міністерство цифрової трансформації України (https://thedigital.gov.ua/), як вбачається, доповнює зазначену систему, забезпечуючи розвиток цифрової інфраструктури та впровадження сучасних управлінських і технологічних рішень.

З огляду на те, що військові частини належать до об'єктів критичної інфраструктури, вони підпадають під дію загальнодержавного механізму забезпечення кібербезпеки. Закон України № 2163-VIII, як видається, закріплює адміністративно-правові обов'язки суб'єктів забезпечення кібербезпеки, у тому числі щодо визначення відповідальних посадових осіб та встановлення процедур взаємодії між органами військового управління й цивільними кіберструктурами.

Водночас реалізація зазначених положень на практиці потребує належного організаційно-технічного забезпечення, яке регламентується підзаконними нормативними актами та галузевими стандартами. Йдеться, зокрема, про вимоги до захисту інформаційно-телекомунікаційних систем, проведення аудитів інформаційної безпеки, впровадження засобів контролю доступу та систем моніторингу кіберзагроз.

Необхідно підкреслити, що ефективність адміністративно-правового механізму значною мірою залежить від налагодженості процедур реагування на кіберінциденти, які реалізуються за участю CERT-UA (https://cert.gov.ua/) та відповідних підрозділів сектору безпеки і оборони.

Важливим елементом адміністративно-правового регулювання є інститут державного контролю. Так, у грудні 2025 року було затверджено Порядок державного контролю за дотриманням вимог законодавства у сфері кіберзахисту [14], який деталізує процедурні аспекти здійснення перевірок та визначає підстави притягнення винних осіб до юридичної відповідальності.

Слід зауважити, що чинне законодавство передбачає як адміністративну, так і кримінальну відповідальність за порушення вимог щодо захисту інформації, неналежне забезпечення кіберзахисту об'єктів критичної інфраструктури, а також бездіяльність посадових осіб. У цьому контексті вбачається, що командири та інші посадові особи військових частин

можуть бути суб'єктами відповідальності за недотримання встановлених адміністративно-правових вимог.

Узагальнення нормативного матеріалу дозволяє виокремити низку позитивних аспектів чинного механізму, зокрема наявність системного законодавчого регулювання, інституційно закріплений розподіл повноважень та функціонування механізмів контролю і відповідальності. Водночас, на нашу думку, існують і певні проблемні моменти.

По-перше, рамковий характер Закону України № 2163-VIII зумовлює необхідність подальшої деталізації його положень у підзаконних актах. По-друге, у практичній діяльності військових частин можуть виникати труднощі координації між органами військового управління та цивільними суб'єктами кібербезпеки. По-третє, актуальним залишається питання гармонізації національного законодавства зі стандартами НАТО та Європейського Союзу.

У зв'язку з цим у наукових колах обґрунтовується доцільність удосконалення адміністративно-правового регулювання шляхом уточнення компетенції органів публічної влади, посилення вимог до технічних стандартів та підвищення рівня професійної підготовки персоналу військових частин у сфері кібербезпеки.

3. Визначення особливостей правового регулювання діяльності суб'єктів кіберзахисту у військовій сфері

Правове регулювання діяльності суб'єктів кіберзахисту у військовій сфері є одним із найактуальніших напрямів забезпечення національної безпеки. Насамперед, слід зазначити, що діяльність таких суб'єктів охоплює комплекс заходів із запобігання, виявлення та нейтралізації кіберзагроз, що можуть мати критичний вплив на оборонні системи держави. При цьому, правове регулювання цієї сфери характеризується певними специфічними особливостями, які відрізняють його від традиційних норм цивільного чи адміністративного права. Так, за словами Мазепи С. існує необхідність розробки спеціальних норм, які будуть враховувати особливості кібероперацій під час збройного конфлікту та забезпечувати адекватну правову відповідь на гібридні загрози [15].

Необхідно виділити особливу роль міжнародно-правових актів та стандартів, які, фактично, визначають рамки діяльності суб'єктів кіберзахисту у військовій сфері. Зокрема, конвенції та резолюції ООН щодо кібербезпеки, а також положення НАТО про захист інформаційних систем, створюють базис, який імплементується у національне законодавство. Так, резолюція ООН № 75/240 (2020) визначає, що держави мають «вживати всіх можливих заходів для запобігання кіберзагрозам критично важливих об'єктів» [16]. Аналогічно, стандарти НАТО з кібероборони (NATO Cyber Defence Policy, 2021) закріплюють принципи координації між союзниками та розмежування цивільних і військових функцій [17].

Водночас, як показує аналіз сучасної практики, внутрішні нормативно-правові акти (зокрема закони про національну безпеку та оборону, акти щодо захисту інформації) містять низку спеціальних положень, що регламентують повноваження військових кіберпідрозділів, права та обов'язки їх персоналу, а також порядок взаємодії з іншими державними органами.

Слід враховувати, що діяльність суб'єктів кіберзахисту у військовій сфері здійснюється в умовах підвищеної секретності. Це, безпосередньо, зумовлює необхідність специфічного правового режиму доступу до інформації, а також запровадження механізмів контролю за її використанням. У науковій літературі (зокрема в працях сучасних юристів та експертів із кібербезпеки) підкреслюється, що така регламентація є надзвичайно важливою для запобігання внутрішнім загрозам, зокрема несанкціонованому розголошенню військових даних.

Варто відзначити, що правове регулювання кіберзахисту у військовій сфері передбачає інтеграцію цивільних та військових норм. Іншими словами, суб'єкти, які здійснюють кіберзахист (таблиця 1), повинні діяти у межах військового законодавства, але при цьому враховувати й положення законів про інформаційні технології, захист персональних даних та критичної інфраструктури. Такий підхід, фактично, забезпечує баланс між безпековими потребами держави та правами і свободами громадян, що є однією з ключових ознак сучасного правового регулювання.

Нижче наведена узагальнена таблиця основних суб'єктів, які здійснюють ківберзахист та їх функції.

Таблиця 1

Категорія суб'єкта	**Основні функції**	**Юридична база**	**Рівень секретності**
1	2	3	4
Війська зв'язку та кібербезпеки Збройних Сил України	Планування та забезпечення розгортання/згортання, функціонування системи зв'язку та інформаційних систем, систем бойового управління та оповіщення, їх нарощування в мирний час, в особливий період, в умовах надзвичайного та воєнного стану з метою вирішення завдань забезпечення управління військами (силами) Збройних Сил України, а також здійснення заходів	1. Закон України «Про основні засади забезпечення кібербезпеки України» 2. Проєкт Закону України про Кіберсили Збройних Сил України (реєстр. № 12349)	Високий

Продовження таблиці 1

1	2	3	4
	з функціонування національної системи кібербезпеки та відбиття воєнної агресії у кіберпросторі (кібероборони) тощо.		
Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)	Формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, активної протидії агресії у кіберпросторі; Координування діяльності CERT-UA як державного центру реагування на кіберінциденти в Україні тощо.	1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» 2. Спільний наказ Служби безпеки України та Адміністрації Держспецзв'язку від 19 грудня 2024 р. № 627/772 «Деякі питання розробки, затвердження та погодження планів захисту об'єктів критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» 3. Постанова Кабінету Міністрів України від 26 листопада 2025 р. № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» 4. Постанова Кабінету Міністрів України від 13 листопада 2025 р. № 1471 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування	Середній/ Високий

Продовження таблиці 1

1	2	3	4
		на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності» 5. Постанова Кабінету Міністрів України від 03 грудня 2025 р. № 1580 «Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах»	
CERT-UA (Computer Emergency Response Team of Ukraine)	Накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту тощо.	1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» 2. Закон України «Про основні засади забезпечення кібербезпеки України» 3. Закон України «Про телекомунікації»	Інформація закрита або обмежена

Продовження таблиці 1

Цивільні постачальники послуг кібербезпеки	Захист мереж, серверів, хмарних середовищ і кінцевих пристроїв. Аудит та оцінка безпеки. Реагування на інциденти: виявлення та аналіз кібератак; локалізація та мінімізація наслідків; відновлення після інцидентів. Консалтинг та навчання. Взаємодія з державою тощо.	1. Закон України «Про основні засади забезпечення кібербезпеки України» 2. Закон України «Про інформацію» 3. Закон України «Про захист інформації в інформаційно-комунікаційних системах» 4. Закон України «Про захист персональних даних» 5. Цивільний кодекс України 6. Підзаконні акти КМУ 7. Міжнародні стандарти (добровільні або договірні)	Низький або обмежений

Джерело: розроблено автором

Таким чином, аналіз сучасного стану правового регулювання діяльності суб'єктів кіберзахисту у військовій сфері дає підстави стверджувати, що воно характеризується комплексністю, багаторівневістю та високим рівнем спеціалізації. Визначальними особливостями цього регулювання є підпорядкованість нормам міжнародного права, поєднання військових і цивільних правових режимів, підвищені вимоги до режиму секретності інформації, а також спеціальний порядок контролю та нагляду за діяльністю суб'єктів кіберзахисту. Водночас наукова дискусія щодо оптимізації адміністративно-правових механізмів у цій сфері триває, що зумовлено стрімким розвитком цифрових технологій та зростанням ролі кібербезпеки в системі національної й колективної оборони.

До основних проблем забезпечення кіберінформаційної безпеки у військових частинах України належать:

– відсутність єдиного комплексного законодавчого акта, який би чітко визначав адміністративно-правовий статус системи кібербезпеки у військових частинах, повноваження відповідних суб'єктів та юридичну відповідальність за порушення у цій сфері;

– фрагментарність і розпорошеність нормативно-правової бази, що поєднує акти загального та спеціального характеру, унаслідок чого ускладнюється їх практичне застосування;

– відставання технічних і організаційних стандартів кіберзахисту від динаміки сучасних кіберзагроз, що негативно впливає на рівень стійкості військових інформаційних систем.

4. Висновки

Адміністративно-правове забезпечення кіберінформаційної безпеки у військових частинах України є складним, динамічним та багаторівневим процесом, що ґрунтується на взаємодії норм законодавства, державної політики у сфері національної безпеки та практики функціонування Збройних Сил України. Незважаючи на наявність низки системних проблем, правова база у сфері кібербезпеки перебуває у стані активного розвитку та адаптації до сучасних викликів, зумовлених глобалізацією цифрового простору та зростанням кількості кіберзагроз військового характеру.

Перспективними напрямами подальшого вдосконалення адміністративно-правового регулювання у цій сфері є гармонізація національного законодавства з європейськими та стандартами НАТО у сфері кібербезпеки, прийняття спеціалізованого нормативно-правового акта, спрямованого на регулювання кібербезпеки у військовому секторі, а також розвиток системи кіберосвіти й профільної підготовки військових фахівців як ключового елемента ефективного кіберзахисту.

Список використаних джерел:

1. 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. Київ, 2025. № 10. 166 с.

2. Використання алгоритмів AI для виявлення та блокування кібератак на військові інформаційні системи / І. В. Стоцький, В. П. Костенко, Г. І. Налісний. *ВІСНИК ХНТУ*. 2025. № 3 (94). Ч. 2. С. 443–447.

3. Шевченко С., Жданова Ю., Кія О. Напівавтоматизований інструмент багато-стандартної оцінки кіберзрілості організації на основі NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 TA CIS CONTROLS V8. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2025. Том 3. № 31. С. 43–60. URL: https://doi.org/10.28925/2663-4023.2025.31.1004 (дата звернення: 05.02.2026).

4. Гук О. М., Мурасов Р. К., Фараон С. І., Толмачов І. В. Стратегії кібербезпеки для захисту критичної інфраструктури: виклики та перспективи. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення* : Міжнародна науково-практична інтернет-конференція, 12–13.03.2024. Вип. 86. URL: http://www.konferenciaonline.org.ua/ua/article/id-1649/ (дата звернення: 05.02.2026).

5. Горгуленко В. А., Коломієць Б. І. Фактори впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. Том 53. № 2.С. 51-59.

6. Воєнні інновації в сучасних війнах : Збірник анотацій Міжнародного академічного форуму / Центральний науково-дослідний інститут Збройних Сил України. Київ : 7БЦ, 2025. 390 с.

7. Гриндей А. О. Використання штучного інтелекту в оборонній сфері. *Вчені записки ТНУ імені В. І. Вернадського*. *Серія: Публічне управління та адміністрування.* 2024. Том 35 (74) № 6. С. 120–123.

8. Трофименко О., Логінова Н., Соколов А., Чикунов П. Штучний інтелект у військовій сфері. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2024 1 (25), С. 161–176. URL: https://doi.org/10.28925/2663-4023.2024.25.161176 (дата звернення: 07.02.2026).

9. Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research. URL: https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By2025-Zion-Market-Research.html (дата звернення: 04.02.2026).

10. Когут Ю. І. Штучний інтелект і безпека: практичний посібник / за ред. док-ра тех. наук, проф. А. С. Довгопологого. Київ : Консалтингова компанія «СІДКОН» ; ВД Дакор, 2024. 294 с.

11. Сушинська А. М., Родигін К. М. Штучний інтелект як інструмент дезінформації. Прикладні аспекти сучасних міждисциплінарних досліджень. 2024. С. 274–276.

12. Фабрика брехні. Як штучний інтелект допомагає в інформаційній війні проти України. URL: https://novynarnia.com/2024/08/13/fabryka-brehniyak-shtuchnyj-intelekt-dopomagaye-v-informaczijnij-vijni-proty-ukrayiny/ (дата звернення: 29.01.2026).

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Стаття 403. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 14.01.2026).

14. Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту : Постанова Кабінету Міністрів України від 17 грудня 2025 р. № 1668. URL: https://zakon.rada.gov.ua/go/1668-2025-%D0%BF (дата звернення: 29.01.2026).

15. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*. 2025. 2 (42). С 164–171.

16. Резолюція Генеральної Асамблеї ООН. Досягнення в сфері інформатизації та телекомунікацій у контексті міжнародної безпеки: резолюція, прийнята Генеральною Асамблеєю 31 грудня 2020 [за доповіддю Першого комітету (A/75/394, пункт 17)] / Генеральна Асамблея Організації Об'єднаних Націй. Нью-Йорк: ООН, 2020. Док. A/RES/75/240. 2 с.

17. NATO Cyber Defence Policy, 2021 : політика кібероборони НАТО. Comprehensive Cyber Defence Policy endorsed at the 2021 Brussels Summit / North Atlantic Treaty Organization (NATO). Брюссель: NATO, 2021. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (дата звернення: 15.01.2026).

References:

1. Dovhan, O. (Ed.). (2025). Cybersecurity in the information society: Information and analytical digest (№ 10). Kyiv: Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine; V. I. Vernadskyi National Library of Ukraine.

2. Stotskyi, I. V., Kostenko, V. P., Nalisnyi, H. I. (2025). The use of AI algorithms for detecting and blocking cyberattacks on military information systems. *Visnyk of KhNTU*, 3 (94), Part 2, 443–447.

3. Shevchenko, S., Zhdanova, Yu., Kiia, O. (2025). A semi-automated tool for multi-standard cybersecurity maturity assessment based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, and CIS Controls v8. Cybersecurity: Education, Science, Technology, 3 (31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004

4. Huk, O. M., Murasov, R. K., Pharaoh, S. I., Tolmachov, I. V. (2024). Cybersecurity strategies for critical infrastructure protection: Challenges and prospects. In Information society: *Technological, economic and technical aspects of development* (Issue 86). https://www.konferenciaonline.org.ua/ua/article/id-1649/

5. Horhulianko, V. A., Kolomiiets, B. I. (2025). Factors influencing the effectiveness of cyber warfare in the interests of the armed forces. *Modern Information Technologies in the Sphere of Security and Defence*, 53 (2), 51-59.

6. Military innovations in modern wars. (2025). Kyiv: Central Research Institute of the Armed Forces of Ukraine.

7. Hryndei, A. O. (2024). The use of artificial intelligence in the defense sector. Scientific Notes of V. I. Vernadsky Taurida National University. Series: *Public Administration*, 35 (74), 6, 120–123.

8. Trofymenko, O., Lohinova, N., Sokolov, A., Chykunov, P. (2024). Artificial intelligence in the military sphere. Cybersecurity: *Education, Science, Technology*, 1 (25), 161–176. https://doi.org/10.28925/2663-4023.2024.25.161176

9. Artificial intelligence (AI) in cyber security market will reach USD 30.9 billion by 2025. (2019). Zion Market Research. https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By2025-Zion-Market-Research.html

10. Kohut, Yu. I. (2024). Artificial intelligence and security: A practical guide. Kyiv: SIDCON Consulting Company; Dakor Publishing House.

11. Sushynska, A. M., Rodyhin, K. M. (2024). Artificial intelligence as a tool of disinformation. *Applied Aspects of Modern Interdisciplinary Research*, 274–276.

12. The factory of lies: How artificial intelligence supports the information war against Ukraine. (2024). https://novynarnia.com/2024/08/13/fabryka-brehniyak-shtuchnyj-intelekt-dopomagaye-v-informaczijnij-vijni-proty-ukrayiny/

13. Law of Ukraine On the Basic Principles of Ensuring Cybersecurity of Ukraine. (2017). https://zakon.rada.gov.ua/go/2163-19

14. Cabinet of Ministers of Ukraine. (2025). Resolution No. 1668 on approval of the procedure for state control over compliance with legislation in the field of cyber protection. https://zakon.rada.gov.ua/go/1668-2025-%D0%BF

15. Mazepa, S. (2025). Cybersecurity in Ukraine: Current challenges and ways to improve legislative regulation. *Actual Problems of Law*, 2 (42), 164–171.

16. United Nations General Assembly. (2020). Developments in the field of information and telecommunications in the context of international security (A/RES/75/240). New York: United Nations.

17. North Atlantic Treaty Organization. (2021). NATO Cyber Defence Policy. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

ENSURING CYBER INFORMATION SECURITY IN MILITARY UNITS: ADMINISTRATIVE AND LEGAL ASPECT

Anfisa Nashynets-Naumova,
Doctor of Law, Professor, Academician of the Academy of Administrative and Legal Sciences,
Deputy Dean of the Faculty of Law and International Relations
Borys Grinchenko Kyiv Metropolitan University
orcid.org/0000-0002-5811-7733
a.nashynets-naumova@kubg.edu.ua

The purpose *of the article is a comprehensive analysis of the current administrative and legal mechanism for ensuring cyber-information security in military units, determining the features of the legal regulation of the activities of cyber-defense subjects in the military sphere, as well as the formation of proposals for improving the relevant system, taking into account modern cyber threats and Euro-Atlantic standards.*
The methodological basis *of the study is made up of general scientific and special legal methods of cognition, in particular: the dialectical method – to clarify the essence and content of cyber-information security in military units; the formal-legal method – to analyze the norms of administrative legislation in the field of cybersecurity; the systemic-structural method – to determine the place of administrative and legal mechanisms in the general system of national security; the comparative-legal method – to compare national approaches with international and European practice; the logical-legal method – to formulate generalizations and conclusions.*
The results *of the study are that the administrative and legal support of cyber information security in military units is characterized by the fragmentation of regulatory regulation, a significant number of by-laws and the absence of a specialized comprehensive legislative act that would clearly define the legal status, powers and responsibilities of cyber protection subjects in the military sphere. The need for strengthening administrative control, improving interdepartmental coordination procedures, as well as regulatory consolidation of special requirements for the organization of cybersecurity in military units, taking into account NATO and European Union standards, is substantiated.*
The conclusions *are that effective provision of cyber information security in military units is impossible without the formation of a holistic administrative and legal model that combines strategic planning, clear regulatory regulation, an appropriate system of administrative responsibility and professional training of personnel. Directions for improving administrative legislation in the field of cybersecurity of military formations as an important element of strengthening the national security of Ukraine are proposed.*
Key words: cyber information security; cybersecurity; military units; administrative and legal support; national security; information systems; public administration; cyber defense entities; administrative control; legal regulation.

Дата першого надходження статті до видання: 12.03.2026
Дата прийняття статті до друку після рецензування: 16.04.2026
Дата публікації (оприлюднення) статті: 08.05.2026