АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 349
DOI https://doi.org/10.32782/TNU-2707-0581/2023.1/07

Гнедюк В.Л.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В УКРАЇНІ СЬОГОДНІ

Стаття є дослідженням особливостей правового забезпечення кіберзахисту в Україні. Кіберзахист – це комплекс заходів, які мають на меті забезпечити безпеку інформаційних технологій та електронних систем від зловживань, злому, витоку даних, вірусів, кібершпигунства та інших кіберзагроз. Це важлива галузь, яка стає все більш актуальною з розвитком цифрової економіки та збільшенням кількості кібератак. Кіберзахист передбачає застосування технічних, організаційних та правових засобів для забезпечення безпеки інформаційних систем та даних. Він є необхідним для захисту важливих інформаційних ресурсів, що використовуються в державному управлінні, фінансових установах, медичній галузі, освітніх та наукових закладах, а також для захисту конфіденційних даних індивідуальних користувачів. Розглянуто питання захисту критично важливих інфраструктур (електромереж, транспортних систем, банківських систем тощо) від кібератак, проаналізовано існуючі заходи та необхідність їхнього покращення. Досліджено процес регулювання діяльності провайдерів інтернет-послуг: аналіз законодавства, яке регулює діяльність провайдерів інтернет-послуг в Україні. Охарактеризовано Національну стратегію кібербезпеки. Зазначено, що Стратегія 2021 року визначає три пріоритети: безпечний кіберпростір, захист прав громадян у цифровому просторі та європейську і євроатлантичну інтеграції. У статті також досліджено питання кіберзахисту державних установ: аналіз проблем кібербезпеки, з якими стикаються державні установи в Україні, надано оцінку загрозам та ризикам. Здійснено аналіз видів кіберзлочинності, що відбуваються в Україні, надано оцінку ризиків та шляхів боротьби з кіберзлочинністю. Основними видами кіберзлочинності в Україні є: фішинг, віруси, черви та троянські коні, крадіжка ідентифікаторів, кібершантаж, кібершпигунство, кібертероризм. Звернено увагу на те, що одним з найважливіших аспектів правового забезпечення кіберзахисту є застосування новітніх технологій, серед яких основною є штучний інтелект. Також зосереджено увагу на аспектах міжнародного співробітництва в галузі кібербезпеки.

Ключові слова: *кіберзахист, кібербезпека, штучний інтелект, кіберзлочинність, законодавство, інтернет-послуги, кібератаки.*

Постановка проблеми. Кіберзахист є однією з найбільш актуальних тем сучасної інформаційної ери. Швидкий розвиток технологій і зростання кількості цифрових сервісів призвели до збільшення загроз кібербезпеці інформації та даних, що стали об'єктом атак з боку кіберзлочинців.

Україна, як країна, що розвивається, не залишається осторонь цих проблем. У відповідь на це, національна влада прийняла ряд правових документів та законів, які регулюють сферу кіберзахисту в Україні.

Однак, не зважаючи на наявність законодавчої бази, проблеми кібербезпеки залишаються досить актуальними в Україні. За даними наукових досліджень, кібератаки на компанії та установи зростають з кожним роком, що створює загрозу для національної економіки та інформаційної безпеки держави.

Тому, вирішення проблем кібербезпеки є надзвичайно важливим завданням для України, і вимагає постійного вдосконалення і удосконалення законодавчої бази, а також застосування сучасних технологій і методів захисту від кібератак.

Аналіз останніх досліджень і публікацій. Дослідження ґрунтується на аналізі законодавства України, науково-методичної літератури,

наукових статей, періодичних видань та напрацювань сучасних та попередніх вчених і дослідників, серед яких: О.М. Ляшенко, І.О. Полякова, І.В. Матвієнко, В.І. Котенко, В. Старовойт, О. Гончаренко тощо.

Мета статті:

– аналіз нормативно-правових актів, що регулюють питання правового забезпечення кіберзахисту в Україні;

– охарактеризувати процес захисту критично важливих інфраструктур (електромереж, транспортних систем, банківських систем тощо) від кібератак;

– окреслити види кіберзлочинності, що відбуваються в Україні, надання оцінки ризиків та шляхів боротьби з кіберзлочинністю;

– описати новітні технології у сфері правового забезпечення кіберзахисту та описати важливість міжнародного співробітництва в галузі кібербезпеки.

Виклад основного матеріалу. Законодавство в сфері кібербезпеки в Україні складається з ряду законів та нормативно-правових актів, які регулюють захист інформації та даних в електронному вигляді від кібератак. Основними законами, що стосуються кібербезпеки в Україні, є Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист персональних даних», Закон України «Про інформацію».

Закон України « Про основні засади забезпечення кібербезпеки України « був прийнятий у 2017 році та регулює діяльність в галузі кібербезпеки в Україні. Він містить визначення понять, пов'язаних з кібербезпекою, встановлює правові засади захисту критично важливих об'єктів інформаційної інфраструктури, а також встановлює механізми взаємодії між органами державної влади та операторами критично важливих об'єктів [1].

Закон України «Про захист персональних даних» прийнятий у 2010 році та регулює захист персональних даних громадян в електронному вигляді. Він встановлює вимоги до збору, зберігання та обробки персональних даних, права громадян на захист своїх персональних даних та відповідальність за їх порушення [2].

Однак, незважаючи на існуючу законодавчу базу, проблеми кібербезпеки залишаються досить актуальними в Україні. Один із причин полягає в тому, що інформаційні технології розвиваються дуже швидко, тому існуючі закони можуть бути неефективними у боротьбі з новими загрозами.

Також в Україні відсутні спеціальні закони, які б регулювали діяльність провайдерів інтернет-послуг, забезпечення безпеки мереж та інтернет-трафіку, а також захисту персональних даних користувачів в мережі Інтернет. Це може призвести до порушення конституційних прав та свобод громадян від інформаційних злочинів.

Захист критично важливих інфраструктур від кібератак є однією з найбільш актуальних проблем у сфері кібербезпеки в Україні. Критично важливі об'єкти – це об'єкти інфраструктури, які забезпечують життєдіяльність нації та безпеку держави, такі як енергетичні мережі, транспортні системи, банківські системи, телекомунікаційні мережі тощо.

Для захисту критично важливих інфраструктур від кібератак необхідно вживати комплексних заходів, які включають технічні, організаційні та правові засоби. Технічні засоби включають захисні програмні та апаратні засоби, які дозволяють виявляти та блокувати кібератаки. Організаційні заходи включають встановлення процедур та правил щодо захисту інформації, регулярне навчання персоналу, встановлення правил доступу до інформації та інші заходи, що забезпечують безпеку критично важливих об'єктів. Правові заходи включають встановлення відповідальності за порушення кібербезпеки та відшкодування збитків від кібератак [6, с. 82].

Україна вже вживає заходів для захисту критично важливих інфраструктур від кібератак, але необхідність покращення і доповнення таких заходів залишається дуже високою. У зв'язку з тим, що кіберзлочинці постійно удосконалюють свої методи та атаки, необхідно встановлювати нові стандарти та норми безпеки, вдосконалювати наявні технічні та організаційні заходи та проводити регулярні навчання персоналу з питань кібербезпеки.

Крім того, необхідно розробити та впровадити систему моніторингу та реагування на кібератаки на критично важливих об'єктах. Ця система повинна дозволити виявляти та аналізувати кібератаки в режимі реального часу, а також реагувати на них швидко та ефективно.

Також важливо враховувати те, що захист критично важливих інфраструктур не може бути здійснений окремою організацією чи установою. Це повинна бути системна діяльність, що передбачає взаємодію між державними та приватними структурами, включаючи провайдерів телекомунікаційних та інтернет-послуг, операторів електромереж, представників банківської та іншої сфер [8, с. 85].

Регулювання діяльності провайдерів інтернет-послуг є важливою складовою сфери кібербезпеки в Україні. Провайдери інтернет-послуг –

це компанії, які забезпечують доступ користувачів до мережі Інтернет, тому вони несуть велику відповідальність за забезпечення безпеки та конфіденційності даних користувачів.

Законодавство, яке регулює діяльність провайдерів інтернет-послуг в Україні, включає ряд нормативно-правових актів, серед яких можна виділити Закон України «Про електронні комунікації», Закон України «Про захист персональних даних», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Постанова КМУ «Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану».

Згідно із законодавством, провайдери інтернет-послуг мають забезпечувати безпеку мережі та інтернет-трафіку, захищати персональні дані користувачів від несанкціонованого доступу, забезпечувати захист від кібератак та інших загроз. Провайдери повинні вести журнали з подій, пов'язаних з безпекою мережі та інтернет-трафіку, а також забезпечувати доступ до цих журналів відповідним органам влади [4, с. 14].

У разі порушення провайдерами вимог законодавства з кібербезпеки, вони можуть нести відповідальність перед законом, включаючи штрафні санкції та судові розбіжності.

Проте, в Україні відсутні спеціальні закони, які б регулювали діяльність провайдерів інтернет-послуг у сфері кібербезпеки. Це ставить під загрозу безпеку користувачів та може спричинити різноманітні кібератаки на їхні пристрої та системи. Тому потрібно удосконалювати законодавство з кібербезпеки та включати в нього нові положення, які б забезпечували безпеку та конфіденційність даних користувачів від кіберзлочинців.

Також важливо проводити регулярні перевірки провайдерів інтернет-послуг з метою виявлення та усунення можливих вразливостей в їхніх мережах та системах, а також навчати персонал провайдерів правильному реагуванню на кібератаки [5, с. 190].

Крім того, для забезпечення кібербезпеки важливо встановлювати міжнародні стандарти та норми безпеки, які визначають мінімальні вимоги до захисту мереж та інформації. Україна може брати участь у міжнародних проектах з кібербезпеки та відповідно впроваджувати міжнародні стандарти в національну практику.

1 лютого 2022 року було підписано указ Президентом України Володимиром Зеленським щодо введення в дію рішення Ради національної безпеки і оборони України про «Про План реалізації Стратегії кібербезпеки України», який було затверджено в серпні 2021 року. Нова стратегія має свої особливості порівняно з попередньою і включає досягнення ряду цілей. Вона також пов'язана з Європейською стратегією на цифровим століттям [3, с. 74].

У 2016 році була прийнята перша Стратегія кібербезпеки України, проте документ мав декілька прогалин, які негативно вплинули на її ефективність. У ній не були чітко визначені пріоритети державної політики в кіберсекторі, увага була акцентована на діяльність органів безпеки та оборони без пропозиції моделей державно-приватної співпраці та залучення академічних кіл та громадськості. Крім того, не було розроблено систему індикаторів виконання стратегії як засобу оцінки стану кібербезпеки.

Стратегія 2021 року визначає три пріоритети: безпечний кіберпростір, захист прав громадян у цифровому просторі та європейську і євроатлантичну інтеграції, а також передбачає досягнення важливих цілей, як-то:

– Дієва кібероборона. Для цього в структурі Міноборони заплановане створення кібервійська в першому півріччі 2023 року.

– Протидія розвідувально-підривній діяльності та кібертероризму.

– Протидія кіберзлочинності шляхом завершення імплементації в українське законодавство положень Конвенції про кіберзлочинність та залучення відповідних практик США.

– Розвиток асиметричних інструментів стримування.

– Національна кіберготовність та надійний кіберзахист (таким чином документ обіцяє створення національної системи управління інцидентами).

– Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки.

– Безпечні цифрові послуги.

– Зміцнення системи координації.

– Формування нової моделі відносин у сфері кібербезпеки, де за державою закріплюватиметься роль партнера.

– Прагматичне міжнародне співробітництво [9].

Слід також звернути увагу на захист державних установ від кібератак. Цей процес є одним з найважливіших завдань у галузі кібербезпеки. У зв'язку зі зростаючими загрозами від кіберзлочинців, державні установи повинні розглядати кібербезпеку як пріоритетний напрямок діяльності та приділяти достатню увагу захисту своїх інформаційних систем.

Основні проблеми кібербезпеки, з якими стикаються державні установи в Україні, включають:

– Недостатня кваліфікація та обізнаність персоналу з питань кібербезпеки.

– Використання застарілих технологій та програмного забезпечення.

– Недостатня увага до захисту від соціальної інженерії та фішингу.

– Відсутність ефективних механізмів моніторингу та виявлення кіберзагроз.

– Недостатня увага до захисту конфіденційної інформації та персональних даних.

– Відсутність ефективної системи управління кібербезпекою та відповідальних осіб за захист інформації [7, с. 48].

Для забезпечення кібербезпеки в державних установах необхідно застосовувати комплексні заходи, включаючи:

– Організацію навчання та підвищення кваліфікації персоналу з питань кібербезпеки.

– Використання сучасних технологій та програмного забезпечення з відповідними механізмами захисту.

– Застосування механізмів захисту від соціальної інженерії та фішингу.

– Впровадження ефективних механізмів моніторингу та виявлення кіберзагроз.

– Використання захисту конфіденційної інформації та персональних даних згідно з вимогами законодавства.

– Встановлення ефективної системи управління кібербезпекою та призначення відповідальних осіб за захист інформації.

– Регулярні аудити та тестування систем захисту на наявність вразливостей та можливих атак.

– Укладення угод та контрактів з постачальниками послуг з кібербезпеки для забезпечення додаткового захисту [8, с. 89].

Для успішного захисту державних установ від кібератак, необхідно також створити ефективну систему взаємодії між різними державними структурами, включаючи правоохоронні органи, інформаційно-аналітичні центри, провайдерів послуг та інших зацікавлених сторін.

Правове забезпечення кіберзахисту передбачає встановлення правил та норм, які регулюють взаємодію між державними органами, бізнесом та громадськістю в галузі кібербезпеки. Вони визначають відповідальність сторін за дотримання правил та процедур, що сприяють захисту від кіберзлочинності. Крім того, правове забезпечення кіберзахисту передбачає створення спеціальних органів та структур, які забезпечують здійснення заходів з кіберзахисту, розслідування та припинення кіберзлочинів.

Кіберзлочинність та правове забезпечення кіберзахисту пов'язані між собою. З одного боку, кіберзлочинність є загрозою для кібербезпеки і вимагає застосування різноманітних технічних та правових заходів для її запобігання та протидії. З іншого боку, правове забезпечення кіберзахисту визначає правові механізми, що регулюють діяльність у галузі кібербезпеки та забезпечують належний рівень захисту від кіберзлочинності.

Кіберзлочинність – це будь-яке злочинне діяння, яке виконується з використанням комп'ютерних технологій та мережі Інтернет. Такі дії можуть бути спрямовані на викрадення конфіденційної інформації, пошкодження комп'ютерних систем, шахрайство та інші злочинні дії [7, с. 50].

Основні види кіберзлочинності, які відбуваються в Україні, включають:

Фішинг – спроби шахрайства шляхом використання електронної пошти або соціальних мереж.

Віруси, черви та троянські коні – шкідливі програми, які можуть завдати шкоди комп'ютерній системі, вкрасти конфіденційну інформацію та інші дії.

Крадіжка ідентифікаторів – використання чужих паролів для отримання доступу до конфіденційної інформації.

Кібершантаж – вимагання грошової винагороди в обмін на забезпечення безпеки даних або відновлення доступу до комп'ютерної системи.

Кібершпигунство – незаконне збирання конфіденційної інформації через інтернет.

Кібертероризм – використання комп'ютерних технологій для терористичних актів [3, с. 76].

Оцінка ризиків та шляхів боротьби з кіберзлочинністю передбачає використання комплексу заходів, які мають на меті зменшення ризику кіберзлочинності. До таких заходів можуть належати:

– Забезпечення безпеки комп'ютерних систем шляхом встановлення сучасного антивірусного програмного забезпечення.

– Регулярні апдейти програмного забезпечення та операційних систем для виправлення виявлених проблем.

– Використання сильних паролів та двофакторної автентифікації для захисту від крадіжки ідентифікаторів.

– Використання шифрування та інших методів захисту конфіденційної інформації.

– Співпраця з провайдерами послуг з кібербезпеки для забезпечення додаткового захисту.

– Систематичний аналіз та оцінка потенційних загроз та ризиків для розробки ефективних стратегій боротьби з кіберзлочинністю.

– Регулярна перевірка внутрішніх процесів та систем захисту на виявлення можливих проблем.

– Забезпечення кібербезпеки є надзвичайно важливою задачею для української влади, оскільки кіберзлочинність може завдати значних матеріальних та моральних збитків як окремим громадянам, так і державі в цілому, особливо під час повномасштабної війни [4, с. 16].

Слід також звернути увагу на те, що одним з найважливіших аспектів правового забезпечення кіберзахисту є застосування новітніх технологій. У зв'язку зі стрімким розвитком кіберзлочинності, захист від неї стає все складнішим і потребує використання новітніх технологій.

Сьогодні українські законодавці активно працюють над введенням нових технологій в правове забезпечення кіберзахисту. Одним з прикладів може бути використання штучного інтелекту (AI) у виявленні та запобіганні кібератакам. Такі системи AI можуть аналізувати великі обсяги даних та розпізнавати зразки атак для швидкого виявлення та запобігання їм.

За допомогою штучного інтелекту можна створювати програмні засоби для аналізу законодавчих актів, які регулюють кібербезпеку. Такі засоби допомагають забезпечити виконання вимог щодо захисту інформації, які містяться в законодавстві. Також вони можуть допомогти управляти правилами доступу до конфіденційної інформації та захисту персональних даних.

Штучний інтелект може бути використаний і для виявлення та аналізу потенційних загроз кібербезпеці. Він допомагає виявити аномальну поведінку користувачів та незвичайні зміни в системі безпеки, що можуть свідчити про кібератаку. За допомогою машинного навчання, системи можуть вчиться розпізнавати нові загрози та адаптуватися до них [5, с. 190].

Окрім того, штучний інтелект може допомогти автоматизувати процес реагування на кібератаки, що забезпечує швидкий та ефективний захист від нових загроз. Наприклад, системи моніторингу можуть виявляти небезпеку та самостійно зупиняти атаки до того, як вони завдають шкоди.

Окрім штучного інтелекту, існує безліч інших новітніх технологій, які використовуються для підвищення рівня кіберзахисту. Деякі з них:

Blockchain – технологія, що дозволяє забезпечити безпеку транзакцій та зберігання даних шляхом розподіленого зберігання на кількох вузлах.

Квантова криптографія – технологія, яка використовує квантові властивості для захисту інформації.

IoT Security – технології, спрямовані на забезпечення безпеки Інтернету речей, включаючи захист від кібератак та захист даних.

Cloud Security – технології, які забезпечують безпеку даних та захист від кібератак в хмарних сервісах.

Identity and Access Management (IAM) – технології, що дозволяють забезпечувати безпеку доступу до систем та ресурсів шляхом автентифікації користувачів та контролю доступу.

Threat Intelligence – технології, що дозволяють забезпечувати аналіз потенційних загроз та виявлення кібератак.

Security Information and Event Management (SIEM) – технології, що дозволяють забезпечувати моніторинг та аналіз подій, які відбуваються в системах, з метою виявлення кіберзагроз [6, с. 87].

Ці технології допомагають підвищити рівень кіберзахисту та зменшити ризики вразливості перед кібератаками. Однак, їх використання не може бути єдиним рішенням, оскільки кіберзагрози постійно еволюціонують, тому необхідно постійно вдосконалювати та розширювати застосовувані технології.

Міжнародне співробітництво в галузі кібербезпеки є надзвичайно важливим з метою запобігання кібератакам, збереження стабільності мереж та інформаційних систем, а також захисту від кіберзлочинності. Україна активно співпрацює з іншими країнами в цій галузі, укладає міжнародні договори та угоди, взаємодіє з міжнародними організаціями з кібербезпеки.

Одним з найважливіших міжнародних документів в галузі кібербезпеки є Конвенція про кіберзлочинність Ради Європи. Україна є стороною цієї Конвенції та зобов'язана дотримуватися її вимог щодо криміналізації кіберзлочинів, захисту даних користувачів, співпраці з іншими країнами у розслідуванні кіберзлочинів тощо.

Україна також активно співпрацює з іншими країнами в рамках програми НАТО з кібербезпеки, взаємодіє з міжнародними організаціями з кібербезпеки, такими як Європейський центр кібербезпеки (ЕС3), Міжнародний союз з телекомунікацій (ITU), Організація з безпеки та співробітництва в Європі (OSCE) тощо [5, с. 193].

Одним з головних напрямів міжнародної співпраці в галузі кібербезпеки є обмін досвідом та інформацією про кіберзагрози та заходи їхнього

запобігання. Україна відкрита для співпраці з іншими країнами у цьому питанні, проводить регулярні зустрічі та конференції з кібербезпеки, на яких представники різних країн обговорюють актуальні питання та шляхи співпраці.

Висновки. Забезпечення кібербезпеки стає все більш актуальною проблемою як для окремих користувачів, так і для держави в цілому. В Україні вже прийнято Національну стратегію кібербезпеки, яка визначає ключові напрямки розвитку кібербезпеки та заходи для її підвищення. Однак, кіберзлочинність постійно еволюціонує, тому важливо продовжувати здійснювати моніторинг та вдосконалювати заходи для захисту від кібератак. Також, співпраця з іншими країнами в галузі кібербезпеки та використання сучасних технологій, таких як штучний інтелект та машинне навчання, можуть допомогти у підвищенні ефективності боротьби з кіберзлочинністю. Кожен користувач, державна установа та компанія має приділяти увагу забезпеченню своєї кібербезпеки, щоб уникнути можливих збитків та наслідків, що можуть бути дуже серйозними.

Список літератури:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017, № 2470-IX: веб-сайт. URL: https://zakon.rada.gov.ua/ (дата звернення: 19.03.2023).

2. Про захист персональних даних: Закон України від 01.06.2010, № 2438-IX: веб-сайт. URL: https://zakon.rada.gov.ua/ (дата звернення: 19.03.2023).

3. Логвіненко О., Домбровський Н. Проблеми та перспективи розвитку кібербезпеки в Україні. *Наукові праці Державної служби спеціального зв'язку та захисту інформації України.* 2021. № 2. С. 71–80.

4. Ляшенко О. М., Полякова І. О. Аналіз сучасного стану кібербезпеки в Україні. *Східноєвропейський журнал передових технологій*. 2020. № 3(106). С. 11–16.

5. Матвієнко І. В., Котенко В. І. Механізми забезпечення кібербезпеки в Україні. *Вісник Придніпровської державної академії будівництва та архітектури*. 2020. Вип. 35. С. 187–194.

6. Петрова М. Кібербезпека в Україні: актуальні проблеми та шляхи їх вирішення. *Науковий вісник Мелітопольського державного педагогічного університету імені Богдана Хмельницького. Сер. : Філософія. Педагогіка. Психологія.* 2020. Вип. 2. С. 80–88.

7. Старовойт В., Гончаренко О. Кібербезпека: проблеми інформаційної безпеки в Україні. *Правова доктрина.* 2020. № 1. С. 44–52.

8. Холоденко А., Шимко С. Аналіз загроз кібербезпеці та методи захисту інформаційних ресурсів в Україні. *Науковий вісник Херсонського державного університету. Сер. : Економічні науки.* 2020. Вип. 39. С. 85–91.

9. Нова стратегія кібербезпеки: як Україна захищатиметься в кіберпросторі?: веб-сайт. URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori (дата звернення: 21.03.2023).

Gnediuk V.L. LEGAL ASSURANCE OF CYBERSECURITY IN UKRAINE TODAY

This article is a study of the features of legal assurance of cybersecurity in Ukraine. Cybersecurity is a set of measures aimed at ensuring the safety of information technologies and electronic systems from abuses, hacking, data leaks, viruses, cyber espionage, and other cyber threats. It is an important area that becomes more relevant with the development of the digital economy and the increasing number of cyberattacks. Cybersecurity involves the use of technical, organizational, and legal means to ensure the security of information systems and data. It is necessary to protect vital information resources used in public administration, financial institutions, medical industry, educational and scientific institutions, as well as to protect the confidential data of individual users. The protection of critical infrastructure (power grids, transport systems, banking systems, etc.) from cyberattacks is discussed, existing measures and the need for their improvement are analyzed. The process of regulating the activities of Internet service providers is investigated: an analysis of the legislation regulating the activities of Internet service providers in Ukraine. The National Cybersecurity Strategy is characterized. It is noted that the 2021 Strategy identifies three priorities: a secure cyberspace, protection of citizens' rights in the digital space, and European and Euro-Atlantic integration. The article also explores the issue of cybersecurity of public institutions: an analysis of the cybersecurity problems faced by public institutions in Ukraine, an assessment of threats and risks is provided. An analysis of the types of cybercrime occurring in Ukraine is carried out, an assessment of risks and ways to combat cybercrime is provided. The main types of cybercrime in Ukraine are: phishing, viruses, worms and Trojan horses, identity theft, cyber extortion, cyber espionage, cyber terrorism. Attention is drawn to the fact that one of the most important aspects of legal assurance of cybersecurity is the application of the latest technologies, among which the main one is artificial intelligence. Also, attention is focused on aspects of international cooperation in the field of cybersecurity.

Key words: *cybersecurity, cyber safety, artificial intelligence, cybercrime, legislation, internet services, cyberattacks.*