СТАНДАРТ ДЕРЖАВНОЇ МОВИ

ПРОЄКТ

СДМ __.__:2026

Термінологія у сфері кібербезпеки

Видання офіційне

Київ

Національна комісія
зі стандартів державної мови

2026

ЗМІСТ

1. ПЕРЕДМОВА

Стандарт державної мови «Термінологія у сфері кібербезпеки» унормовує 130 термінів та є базовим документом для подальшого розвитку української термінології у сфері кібербезпеки, захисту інформації та інформаційних технологій.

Документ забезпечує однозначне трактування понять з кібербезпеки в нормативно-правових актах, технічній документації та офіційних документах органів державної влади; усуває термінологійну неоднозначність у правозастосуванні, створює єдину мовну базу для розроблення політик безпеки, проведення аудитів, оцінки ризиків та міжвідомчої взаємодії; підвищує ефективність комунікації між фахівцями різних організацій та відомств, що є критично важливим для координації дій у сфері кіберзахисту.

Напрацьований стандарт державної мови може бути використаний у професійній підготовці та підвищенні кваліфікації фахівців з кібербезпеки, створенні навчальних програм та підручників; розробленні технічних регламентів, інструкцій, стандартів операційних процедур у державних установах, силових структурах та організаціях критичної інфраструктури. Документ слугує основою для узгодження національної термінології з глобальними стандартами (ISO/IEC, NIST, ENISA), що полегшує міжнародну співпрацю та обмін досвідом у сфері кібербезпеки.

1. РОЗРОБИЛА Робоча група з напрацювання стандарту державної мови «Термінологія у сфері кібербезпеки» (рішення Національної комісії зі стандартів державної мови від 17.01.2025 № 18 (зі змінами) у складі:

1) Вавіленкової Анастасії – доктора технічних наук, професора, завідувача кафедри кібербезпеки центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України (керівника робочої групи);

2) Ісмайлова Карена – кандидата юридичних наук, доцента, підполковника поліції, начальника 5-го відділу (інформаційних технологій та програмування в південному регіоні) (м. Одеса) 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції Національної поліції України;

3) Бернацької Світлани – кандидата філологічних наук, доцента, заслуженого працівника освіти України, доцента кафедри української мови, літератури та культури факультету лінгвістики Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

4) Безштанька Віталія – кандидата технічних наук, співробітника Адміністрації Державної служби спеціального зв’язку та захисту інформації України;

5) Владімірова Євгена – капітана, директора центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

6) Волошка Сергія – кандидата технічних наук, полковника, старшого наукового співробітника, професора кафедри комунікаційних технологій та кіберзахисту Національного університету оборони України;

7) Довганя Олександра – доктора юридичних наук, професора, заслуженого діяча науки і техніки України, радника при дирекції ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України»;

8) Жиліна Артема – кандидата технічних наук, доцента, співробітника Державної служби спеціального зв'язку та захисту інформації України;

9) Звєрєва Володимира – кандидата технічних наук, старшого наукового співробітника, радника Голови Державної служби спеціального зв'язку та захисту інформації України;

10) Котетунова Віктора – кандидата технічних наук, співробітника Державної служби спеціального зв'язку та захисту інформації України;

11) Ланде Дмитра – доктора технічних наук, професора, завідувача кафедри інформаційної безпеки Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

12) представника Головного управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України;

13) Ткачук Наталії – кандидата юридичних наук, полковника, керівника служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України;

14) Федієнка Олександра – голови підкомітету з питань безпеки у кіберпросторі, урядового зв'язку, криптографічного захисту інформації Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки, народного депутата України.

2. ПРОВЕДЕНО ПУБЛІЧНЕ ГРОМАДСЬКЕ ОБГОВОРЕННЯ з __ _____ 2026 року до __ _____ 2026 року.

3. НАДАНО ПРОПОЗИЦІЇ ТА ВИСНОВКИ:

1) Інституту української мови Національної академії наук України від __ _____ 2026 року;

2) Наукової установи від ___ _____ 2026 року;

3) Закладу вищої освіти від __ _____ 2026 року.

4. ПЕРЕВІРЕНО в апараті Національної комісії зі стандартів державної мови __ _____ 2026 року.

5. УХВАЛЕНО на підставі рішення Національної комісії зі стандартів державної мови від __ _____ 2026 року № ____ «Про затвердження стандарту державної мови „Термінологія у сфері кібербезпеки“» з __ _____ 20__ року.

6. НАДАНО ЧИННОСТІ з __ _____ 2026 року.

7. Цей стандарт державної мови розроблено ВПЕРШЕ.

ЗАТВЕРДЖЕНО
Рішення Національної комісії
зі стандартів державної мови
__ _____ 20__ року № ___

2. СТАНДАРТ ДЕРЖАВНОЇ МОВИ «ТЕРМІНОЛОГІЯ У СФЕРІ КІБЕРБЕЗПЕКИ»

2.1. СФЕРА ЗАСТОСУВАННЯ

Цей Стандарт застосовують у всіх сферах суспільного життя, визначених у законодавстві.

2.2. НОРМАТИВНІ ПОКЛИКАННЯ

Підставою для цього Стандарту є такі документи:

Закон України від 25 квітня 2019 року № 2704-VIII «Про забезпечення функціонування української мови як державної»;

Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України»;

Закон України від 05 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах»;

Указ Президента України від 26 серпня 2021 року № 447/2021 «Про Стратегію кібербезпеки України»;

постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури»;

постанова Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»;

постанова Кабінету Міністрів України від 06 листопада 2019 року № 911 «Про затвердження Положення про Національну комісію зі стандартів державної мови»;

рішення Національної комісії зі стандартів державної мови від 16 листопада 2023 року № 421, зареєстроване в Міністерстві юстиції України 04 грудня 2023 року за № 2107/41163 «Про затвердження Порядку напрацювання, затвердження, уведення в дію, перегляду стандартів державної мови та внесення змін до них»;

рішення Національної комісії зі стандартів державної мови від 17 січня 2025 року № 18 «Про напрацювання проєкту стандарту державної мови “Термінологія у сфері кібербезпеки”» (зі змінами);

пункт 4 Програми робіт із напрацювання, затвердження, перегляду стандартів державної мови чи внесення змін до них, затвердженої рішенням Національної комісії зі стандартів державної мови від 14 лютого 2024 року № 34 (зі змінами);

ДСТУ 3966:2009 «Термінологічна робота. Засади і правила розроблення стандартів на терміни та визначення понять».

2.3. ЗАГАЛЬНЕ ПОЯСНЕННЯ

Стандарт охоплює широкий спектр термінів – від базових понять кібербезпеки до термінів, що використовуються в національному та міжнародному законодавстві, директивах Європейського Союзу. Документ містить термінологію, пов’язану з побудовою стратегій забезпечення стійкості до кібератак, реагуванням на кіберінциденти, відновленням після кібератак, веденням війни у кіберпросторі, цифровою експертизою, тестуванням безпеки мереж тощо.

Для кожного поняття встановлено один застандартизований термін, поданий напівгрубим шрифтом. До окремих термінів (за наявності) дібрано синоніми, подані світлим курсивом з великої літери.

У документі наведено абетковий покажчик установлених цим Стандартом українських термінів із кібербезпеки.

Як довідкові подані англійські терміни-відповідники, узяті з міжнародних стандартів і фахових словників.

Завдання Стандарту:

унормувати однозначно зрозумілі й логічно несуперечливі терміни у сфері кібербезпеки в майбутніх лексикографічних працях, науковій, довідковій і навчально-методичній літературі;

сприяти перекладу українською мовою термінології у сфері кібербезпеки;

привести національне законодавство у сфері кібербезпеки до єдиної вживаної термінології;

сприяти підвищенню рівня технічної освіти в Україні;

сприяти подальшому розвиткові української професійної мови у сфері кібербезпеки та кіберзахисту;

забезпечити взаємодію між суб’єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом і НАТО.

2.4. ОСНОВНИЙ ЗМІСТ

2.4.1 автентифікація
Електронний процес, що дає змогу підтвердити цифрову ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних.

2.4.2 автоматизований кіберзахист
Використання програмно-апаратних спеціалізованих комплексів, що в автоматичному або напівавтоматичному режимі виконують функції виявлення, запобігання та реагування на кіберзагрози без участі оператора або з його мінімальною участю.

2.4.3 авторизація
Надавання автентифікованому суб’єкту дозволу на доступ до інформаційних ресурсів та/або виконання визначених операцій відповідно до встановлених політик безпеки.
Авторизація з безпеки.

2.4.4 акредитація з безпеки
Процедура офіційного підтвердження відповідності інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи або її окремих елементів, об’єкта критичної інформаційної інфраструктури до вимог законодавства, національних стандартів та нормативних документів у сферах технічного захисту, криптографічного захисту та кіберзахисту, що передбачає оцінку впроваджених заходів захисту інформації, щоб гарантувати прийнятний рівень ризику та надійність роботи з чутливими даними.

2.4.5 акредитована з безпеки система
Інформаційна, електронна комунікаційна, інформаційно-комунікаційна, технологічна система або її окремі елементи, об’єкт критичної інформаційної інфраструктури, у якій запроваджені заходи та/або встановлені системи безпеки інформації, що пройшли акредитацію з безпеки.

2.4.6 анонімізація
Обробка даних, яка унеможливлює цифрову ідентифікацію особи завдяки видаленню, зміні чи приховуванню інформації, що може її ідентифікувати.

2.4.7 антивірусне програмне забезпечення
Спеціалізовані програмні засоби, призначені для виявлення, блокування та видалення шкідливого програмного забезпечення, а також запобігання його виконанню в інформаційній системі.

2.4.8 антиспам

Програмні засоби або функції інформаційних систем, призначені для виявлення, фільтрації та блокування небажаних електронних повідомлень.

2.4.9 атрибуція кібератаки

Процес визначення джерела кібератаки.

Примітка. Атрибуція кібератаки допомагає встановити її мотиви та цілі, інші потенційні та/або реальні кіберзагрози, розробити відповідні заходи кіберзахисту та реагування на кібератаки чи кіберінциденти.

2.4.10 багатофакторна автентифікація

Електронний процес, що вимагає підтвердження особи для доступу до облікового запису чи системи з використанням щонайменше двох факторів автентифікації, які належать до різних груп.

2.4.11 базовий профіль безпеки системи

Мінімально необхідний набір вимог і заходів із захисту інформації, визначений для інформаційних систем певного типу або категорії та застосовуваний як обов'язкова норма для їх захисту.

Примітка. Базовий профіль є основою для подальшого формування цільового профілю безпеки системи.

2.4.12 безпека мережевого порту

Комплекс технічних і організаційних заходів, спрямований на контроль доступу до портів мережевого обладнання через обмеження кількості підключених пристроїв та ідентифікації їхніх MAC-адрес із метою запобігання несанкціонованому підключенню та мережевим атакам на переповнення таблиці комутації.

Примітка. Функцію контролю за підключеннями пристроїв до окремого виконує мережевий комутатор.

2.4.13 біометрична автентифікація

Метод автентифікації, що здійснюється на основі порівняння біометричних характеристик особи з відповідними збереженими в довідковій базі еталонними біометричними даними.

Примітка. Біометричні характеристики можуть належати до фізіологічних або поведінкових ознак.

2.4.14 блокування облікового запису

Тимчасове або постійне припинення можливості використання облікового запису з метою запобігання несанкціонованому доступу або реагування на підозрілі дії.

Примітка. Повідомлення від небажаної особи під час її блокування автоматично приховуються.

2.4.15 бот

Автоматизована програма, що виконує заздалегідь визначені дії через стандартні інтерфейси користувача без його безпосередньої участі, імітуючи людську поведінку, призначена для автоматизації повторюваних завдань або виконання віддалених команд.

Примітка. Бот може функціонувати як легітимно (пошукові боти, чат-боти, торгові боти), так і зловмисно (боти у складі ботнетів для несанкціонованих дій на інфікованих пристроях).

2.4.16 ботнет

Мережа скомпрометованих пристроїв, якими керує кіберзловмисник та використовує для виконання скоординованих шкідливих дій.

Примітка. Ботнет використовують для здійснення розподілених кібератак, викрадення даних, розповсюдження шкідливого програмного забезпечення та інших несанкціонованих дій.

2.4.17 відкритість кіберпростору

Принцип забезпечення вільного, недискримінаційного та доступного користування цифровими ресурсами й сервісами.

2.4.18 віртуальна приватна мережа

Технологія створення захищеного зашифрованого з'єднання (тунелю) поверх мереж електронних комунікацій для забезпечення конфіденційності, цілісності даних та безпечного доступу до віддалених мережевих ресурсів.

2.4.19 вразливість

Недолік у проєктуванні, створенні, налаштуванні чи експлуатації інформаційно-комунікаційних систем, програмного забезпечення або процесу, який створює можливість для реалізації кіберзагрози.

Примітка. Джерелами кіберзагроз можуть бути кіберзловмисники, внутрішні порушники, помилки користувачів, відмови обладнання, недоліки процесів або природні явища.

2.4.20 галузевий профіль безпеки системи

Визначений набір вимог щодо заходів із захисту інформації та кіберзахисту для інформаційних та інформаційно-комунікаційних систем окремої галузі, сформований з урахуванням базового профілю, галузевих стандартів, політик безпеки та особливостей функціонування таких систем.

2.4.21 демілітаризована зона

Мережевий сегмент між зовнішньою (ненадійною) та внутрішньою (довіреною) мережами, призначений для розміщення загальнодоступних сервісів і захищений міжмережевими екранами з обмеженим доступом до внутрішніх ресурсів із метою ізоляції публічних служб від приватної мережі.

2.4.22 доступність кіберпростору

Принцип, що передбачає можливість доступу до цифрових ресурсів і сервісів у межах установлених процедур, правил і протоколів.

2.4.23 експлойт
Комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості програмного забезпечення для несанкціонованого доступу, виконання шкідливих дій або здійснення кібератак на інформаційну систему.

2.4.24 етичний хакінг
Легальний процес виявлення вразливостей у комп'ютерних системах, мережах та застосунках із дозволу їх власника з метою підвищення рівня кібербезпеки.
Примітка. Етичні хакери використовують ті самі навички, що й кіберзловмисники, щоб виявити слабкі місця в системі та усунути вразливості.
Етичне зламування. Білий хакінг.

2.4.25 журнал
Спеціальний файл, у якому накопичується автоматично зібрана службова та статистична інформація про події в інформаційній системі або мережі.
Лог-файл.

2.4.26 журналювання
Автоматизована фіксація та збереження записів про події в інформаційній системі або мережі для подальшого аналізу, моніторингу або розслідування кіберінцидентів.
Примітка. Журналювання є критично важливим для виявлення атак, реагування на інциденти, аудиту, відновлення систем та аналізу загроз, дає змогу відстежувати підозрілу активність та поведінку кіберзловмисників.
Логування.

2.4.27 зловживання в кіберпросторі
Неправомірне або неналежне використання комп'ютерних систем, мереж або цифрових ресурсів.
Примітка. До зловживань належать: несанкціонований доступ до інформаційних ресурсів, крадіжка або зміна даних, поширення шкідливого програмного забезпечення, розсилання спаму, атаки типу «відмова в обслуговуванні» та інші зловмисні чи деструктивні дії, що можуть завдати шкоди цифровим ресурсам або користувачам.

2.4.28 ідентифікація кіберзагрози
Виявлення потенційної кіберзагрози, що може впливати на інформаційні системи чи ресурси.
Примітка. Ідентифікація кіберзагрози може містити встановлення її типу, джерела, можливого вектора кібератаки та умов, за яких ця кіберзагроза може реалізуватися.

2.4.29 індикатор кіберзагрози
Технічний показник або цифровий артефакт, що свідчить про можливу наявність кіберзагрози та використовується для її виявлення й реагування.

Примітка. До індикаторів кіберзагроз можуть належати IP-адреси, доменні імена, хеші файлів, ознаки поведінкової активності, характеристики мережевого трафіку та інші дані, що використовують для виявлення шкідливих дій.

2.4.30 індикатор компрометації

Цифровий артефакт або ознака, що свідчить про можливу або фактичну компрометацію інформаційної системи чи мережі.

Примітка. До індикаторів компрометації можуть належати IP-адреси, доменні імена, хеші файлів, характеристики мережевого трафіку та інші дані, що вказують на компрометацію.

2.4.31 індикатор стану кібербезпеки

Кількісний або якісний показник рівня захищеності інформаційної системи або її компонентів, який використовують для інтегральної оцінки поточного стану кібербезпеки та ухвалення управлінських рішень.

2.4.32 ін’єкція програмного коду

Техніка кібератаки, під час якої шкідливий код впроваджують у вразливу програму для виконання зловмисних команд або отримання несанкціонованого доступу до системи.

Примітка. Найбільш поширеними видами ін’єкцій є: SQL-ін’єкція, HTML-ін’єкція, DLL-ін’єкція, XML-ін’єкція, ін’єкція команд.

2.4.33 інструмент реагування на кіберінциденти

Програмний або програмно-апаратний засіб, призначений для здійснення реагування на кіберінциденти.

Примітка. До реагування належать аналіз кіберінциденту, локалізація, усунення наслідків та розслідування його причин.

2.4.34 інфраструктура кіберзахисту

Сукупність об’єктів кіберзахисту операторів критичної інфраструктури, а також суб’єктів господарювання, громадян та їх об’єднань, інших осіб, які провадять діяльність та/або надають послуги у сферах електронних комунікацій, електронної комерції, розвитку національних електронних інформаційних ресурсів, захисту інформації та кібербезпеки.

2.4.35 кейлогер

Програмний засіб або апаратний пристрій, призначений для фіксації натискань клавіш на клавіатурі.

Примітка. Кейлогери використовують для викрадення конфіденційної інформації або в легітимних цілях, зокрема в цифровій криміналістиці та тестуванні безпеки.

2.4.36 кіберагресія

Умисна цілеспрямована діяльність у кіберпросторі, що полягає в здійсненні кібератак або інших деструктивних дій, спрямованих на завдання шкоди інформаційним системам, цифровим ресурсам чи критичній інформаційній інфраструктурі.

Примітка. Кіберагресія проявляється у формі тривалих або повторюваних кібератак, шкідливого втручання, знищення чи блокування інформаційних ресурсів, маніпуляції даними або інших деструктивних впливів у кіберпросторі.

2.4.37 кібератака

Навмисні дії в кіберпросторі, здійснювані за допомогою засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, технічних і технологічних засобів і обладнання, спрямовані на порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів, порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем, використання інформаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

2.4.38 кібератака «відмова в обслуговуванні»

Вид кібератаки, під час якої здійснюють несанкціоноване втручання в роботу інформаційної, електронної комунікаційної або інформаційно-комунікаційної системи через штучне створення надмірного навантаження на її ресурси, унаслідок чого відбувається блокування доступу до інформації або порушення штатного режиму функціонування системи, що внеможливлює або суттєво ускладнює надання послуг (сервісів) законним користувачам.

Примітка. DoS-атаки (Denial of Service) здійснюють з одного джерела, тоді як потужніші DDoS-атаки (Distributed Denial of Service) використовують мережу скомпрометованих пристроїв (ботнет) з багатьох IP-адрес для одночасного перевантаження цілі.

2.4.39 кібератака «людина посередині»

Вид кібератаки, коли кіберзловмисник перехоплює інформацію, яку передають під час обміну даними, та може її змінювати.

Активне перехоплення.

2.4.40 кібератака методом повного перебору

Вид кібератаки, під час якої відбувається зламування облікового запису та/або системи захисту методом послідовного перебирання всіх можливих комбінацій логінів і паролів з метою знайти відповідну.

Примітка. Зламування здійснюють автоматизовано за допомогою спеціальних програм і використовують для отримання несанкціонованого доступу до систем і облікових записів, а також для перевірки криптографічної стійкості паролів.

Кібератака перебором. Метод грубої сили. Брутфорс.

2.4.41 кібератака «нульового дня»

Вид кібератаки, під час якої використовують невідому вразливість програмного забезпечення з нульового моменту часу до моменту її виявлення розробниками.

2.4.42 кібербезпека

Захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечують сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, вчасне виявлення, запобігання й нейтралізацію реальних і потенційних кіберзагроз.

2.4.43 кіберборотьба

Сукупність взаємоузгоджених за метою, завданнями, місцем і часом наступальних та оборонних дій військових формувань у кіберпросторі, спрямованих на здобуття інформації про кіберінфраструктуру противника, її знищення або захоплення (виведення з ладу, отримання контролю), заподіяння їй шкоди через кібердії, кібероперації та радіоелектронное подавлення, захист власної кіберінфраструктури від кіберрозвідки та кібердій противника.

2.4.44 кібервійна

Організована, цілеспрямована та тривала форма збройної агресії в кіберпросторі, яку здійснює держава або підконтрольні їй структури, зокрема із застосуванням кіберзброї, з політичною, воєнною або економічною метою.

Примітка. Кібервійна передбачає навмисне втручання в інформаційний простір іншої держави з метою порушення її суверенітету, завдання шкоди воєнній інфраструктурі, об’єктам критичної інфраструктури, органам державної влади та критичній інформаційній інфраструктурі.

2.4.45 кібервплив

Цілеспрямоване використання кіберпростору та цифрових технологій державами, недержавними суб’єктами або організованими групами для досягнення стратегічних, політичних, економічних, соціальних або військових цілей через вплив на інформаційні системи, критичну інформаційну інфраструктуру, суспільну свідомість або процеси ухвалення рішень, що може супроводжуватися деструктивними діями, аналогічними до традиційних воєнних операцій.

2.4.46 кібергігієна

Комплекс технічних та організаційних заходів безпеки для персональних цифрових пристроїв, облікових записів і онлайн-сервісів, що передбачає вчасне оновлення програмного забезпечення, впровадження рекомендованих практик для користувачів, керування доступом, регулярне резервне копіювання та моніторинг активності, дотримання політик і процедур безпеки з боку персоналу з метою запобігання проникненню шкідливого програмного забезпечення, несанкціонованому доступу та витоку чутливої інформації.

2.4.47 кібердоктрина

Стратегічний документ держави, що визначає принципи, цілі, підходи та межі застосування кіберспроможностей, а також порядок організації кібероборони, взаємодії суб'єктів кібербезпеки та забезпечення стійкості держави в кіберпросторі.

2.4.48 кіберзагроза

Наявні та потенційно можливі явища, чинники або дії в кіберпросторі, що створюють небезпеку життєво важливим інтересам особи, суспільства та держави в кіберпросторі і можуть призвести до порушення конфіденційності, цілісності або доступності інформаційних систем, електронних інформаційних ресурсів чи цифрових сервісів.

2.4.49 кіберзагроза воєнного характеру

Потенційні або реальні цілеспрямовані дії військових формувань чи інших підтримуваних державою суб'єктів у кіберпросторі, спрямовані на порушення, руйнування або блокування функціонування інформаційних систем, критичної інформаційної інфраструктури чи систем управління противника з метою досягнення військово-стратегічних або тактичних переваг.

2.4.50 кіберзагроза терористичного характеру

Потенційні або реальні цілеспрямовані дії терористичних організацій чи пов'язаних із ними осіб у кіберпросторі, спрямовані на порушення, руйнування або блокування функціонування критичної інформаційної інфраструктури, цифрових сервісів чи суспільно важливих систем із метою залякування населення, дестабілізації державних або суспільних процесів та досягнення політичних, ідеологічних чи релігійних цілей.

2.4.51 кіберзахист

Сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, здатності інформаційної інфраструктури до їх обробки.

2.4.52 кіберзброя

Сукупність технічних, технологічних, програмних, програмно-апаратних та інших засобів, призначених для деструктивних впливів на об'єкти кіберпростору противника або на його системи керування з метою порушення їх функціонування чи процесів керування.

2.4.53 кіберзловмисник

Особа, яка діє індивідуально або в складі групи осіб та здійснює умисні шкідливі дії в кіберпросторі, спрямовані на несанкціоноване втручання,

порушення роботи інформаційних систем, зміну або знищення даних чи інші форми шкідливого кібервпливу.

2.4.54 кіберзлочин
Суспільно небезпечне діяння, вчинене в кіберпросторі та/або з використанням комп'ютерних систем, електронних пристроїв чи інформаційно-комунікаційних технологій, за яке передбачена кримінальна відповідальність законодавством України та/або міжнародними договорами України.
Примітка. Злочинні дії в кіберпросторі полягають у протиправному та несанкціонованому створенні, відтворенні, зберіганні, обробці, підробці, блокуванні та/або знищенні об'єктів інформаційної інфраструктури.
Комп'ютерний злочин.

2.4.55 кіберзлочинність
Сукупність кіберзлочинів та пов'язаних із ними форм злочинної діяльності, що вчиняють у кіберпросторі з використанням електронних пристроїв та інформаційно-комунікаційних технологій.
Комп'ютерна злочинність.

2.4.56 кіберінцидент
Подія або низка подій у кіберпросторі ненавмисного характеру (технічного, технологічного, природного, помилкового, зокрема внаслідок дії людського чинника) та/або таких, що мають ознаки можливої кібератаки, які фактично або потенційно порушують конфіденційність, цілісність або доступність інформаційних систем, електронних інформаційних ресурсів чи цифрових сервісів.
Інцидент кібербезпеки.

2.4.57 кіберконтррозвідка
Сукупність заходів та операцій у кіберпросторі, спрямованих на виявлення, попередження, нейтралізацію та протидію розвідувально-підривній діяльності іноземних спеціальних служб, кіберугруповань та окремих кіберзловмисників, зокрема виявлення агентів впливу, каналів витоку інформації, методів кіберрозвідки противника та запобігання компрометації критичних інформаційних ресурсів організації або держави.

2.4.58 кібернавчання
Організована підготовка штатних посадових осіб, відповідальних за кібербезпеку, спрямована на формування й відпрацювання професійних знань і навичок виявлення, запобігання та реагування на кіберзагрози й кіберінциденти, а також набуття користувачами цифрових послуг знань і навичок із кібергігієни.
Примітка. Кібернавчання допомагає фахівцям і користувачам мінімізувати ризики в цифровому просторі, захистити дані та пристрої.

2.4.59 кібероборона
Сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюють у кіберпросторі та спрямовують на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

2.4.60 кібероперація
Сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом кібердій, атак, ударів, а також заходів кіберрозвідки та кіберзахисту, які проводять за єдиним замислом і планом центри захисту інформації та кібербезпеки самостійно або у взаємодії з визначеними військовими частинами об'єднаних сил із метою руйнівного впливу на автоматизовані системи управління, системи зв'язку й управління зброєю, інформаційно-телекомунікаційні мережі й системи противника з одночасним захистом власного кіберпростору.

2.4.61 кіберпростір
Глобальне віртуальне середовище, утворене в результаті функціонування взаємопов'язаних інформаційних систем, комунікаційних мереж та їх фізичної інфраструктури, що забезпечує електронні комунікації, обмін даними та реалізацію суспільних відносин між користувачами незалежно від географічних кордонів.
Віртуальний простір.

2.4.62 кіберризик
Імовірність виникнення фінансових збитків, операційних порушень або репутаційної шкоди внаслідок реалізації кіберзагроз, що впливають на конфіденційність, цілісність або доступність інформаційних ресурсів, комунікаційних та технологічних систем організації в кіберпросторі.

2.4.63 кіберрозвідка
Діяльність, яку здійснюють у кіберпросторі або з його використанням із метою отримання даних про потенційні загрози, цілі та вразливості для досягнення особистої, економічної, політичної чи військової переваги.

2.4.64 кіберстійкість
Здатність організацій, інформаційно-комунікаційних технологій передбачати кіберзагрози, протистояти кібератакам, обмежувати їхні наслідки, швидко відновлювати функціонування після кіберінцидентів й адаптуватися до мінливого середовища загроз, забезпечуючи безперервність критичних операцій та послуг.
Стійкість кіберпростору.

2.4.65 кібертеракт
Процес використання комп'ютерних мереж для здійснення терористичних актів із метою залякування населення, дестабілізації уряду або нанесення шкоди критично важливим об'єктам інфраструктури.

2.4.66 кібертероризм
Навмисні, політично вмотивовані дії, які здійснюють у кіберпросторі або з його використанням із метою порушити державну чи громадську безпеку, викликати страх і паніку, залякати населення, завдати значної фізичної, фінансової чи психологічної шкоди суспільству, зруйнувати критичну інфраструктуру, спровокувати військовий конфлікт.

2.4.67 кіберудар
Воєнні дії підрозділів кібероборони, спрямовані на руйнування визначених елементів у кіберпросторі противника з метою їх блокування, знищення об'єктів інфраструктури, інформації, техніки та озброєння.

2.4.68 кібершпигунство
Несанкціоноване отримання конфіденційної інформації (державної, військової чи комерційної таємниці), яке здійснюють у кіберпросторі або з його використанням із метою здобуття особистої, економічної, політичної чи військової переваги.

2.4.69 кібершахрайство
Умисне введення в оману та/або маніпулювання в кіберпросторі або з його використанням із метою незаконного заволодіння майном, інформацією чи іншою вигодою.

2.4.70 ключ керування доступом
Унікальний криптографічний або програмний ідентифікатор, що використовують для автентифікації та надання доступу до цифрових ресурсів, інформації або сервісів.

2.4.71 компрометація засобу електронної ідентифікації
Подія або стан, унаслідок яких засіб електронної ідентифікації може бути несанкціоновано використаний, підроблений, скопійований або втрачений, що створює ризик неправомірного доступу або несанкціонованого підтвердження особи.

2.4.72 компрометація інформаційної системи
Порушення безпеки та/або нормального функціонування інформаційної системи, що призводить або може призвести до втрати конфіденційності, цілісності, доступності інформації чи контролю над нею або її окремими процесами.

2.4.73 комп’ютерний вірус
Шкідливе програмне забезпечення, що може самостійно створювати свої копії завдяки модифікації коду у файлах, програмах або завантажувальних секторах, що призводить до їх зараження та можливого подальшого поширення.

2.4.74 контрфорензика
Сукупність методів, інструментів та технік, що використовують кіберзловмисники для приховування, знищення або підроблення цифрових слідів, із метою завадити проведенню цифрової криміналістичної експертизи.

2.4.75 кризова ситуація у сфері кібербезпеки
Порушення або загроза порушення режиму функціонування інформаційних, електронних комунікаційних та/або інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури у зв’язку з кіберінцидентом, кібератакою або кіберзагрозою, порушення функціонування яких може призвести до значних негативних наслідків для національної безпеки.

2.4.76 критична інформаційна інфраструктура
Сукупність інформаційних систем, мереж електронних комунікацій, цифрових платформ, сервісів та інформаційних ресурсів, які забезпечують виконання життєво важливих функцій держави, суспільства та економіки, порушення чи припинення роботи яких може завдати значної шкоди національній безпеці, обороноздатності, громадському порядку або сталому розвитку.

2.4.77 ланцюг кібератаки
Структурована послідовність фаз, через які проходить кібератака від початкової підготовки до досягнення зловмисником цільового впливу на інформаційну систему.

2.4.78 логічна бомба
Шкідливе програмне забезпечення, яке активується за визначених часових або інформаційних умов для здійснення несанкціонованого доступу до інформації, спотворення або знищення даних.

2.4.79 мережеве виявлення та реагування
Технологія кіберзахисту, призначена для безперервного моніторингу та глибокого аналізу мережевого трафіку (з використанням поведінкового аналізу, машинного навчання та сигнатур) із метою вчасного виявлення кібератак та аномальної активності, а також для надання інструментів автоматизованого реагування на виявлені кіберінциденти через їх блокування, ізоляцію уражених систем чи збір даних для подальшого розслідування.

2.4.80 міжмережевий екран
Програмний або апаратно-програмний комплекс, що контролює та фільтрує мережевий трафік відповідно до встановлених правил доступу.
Файєрвол.

2.4.81 міжнародна кіберзлочинність
Учинення правопорушень із використанням комп'ютерних систем, інформаційно-комунікаційних технологій та мереж унаслідок спільних дій представників різних країн або представником/-ами однієї країни щодо конфіденційності, цілісності та доступності комп'ютерних систем, інформаційно-комунікаційних технологій, мереж, даних, користувачів іншої країни (країн), що становлять загрозу для міжнародної інформаційної та кібербезпеки і за які законодавством передбачена відповідальність.
Примітка. Правопорушення визначені у статтях 2 – 12 Конвенції про кіберзлочинність.

2.4.82 модель нульової довіри
Концепція кібербезпеки, за якої жоден користувач, пристрій, служба та/або компонент мережі не є довіреними за замовчуванням, а доступ до ресурсів можливий лише після перевірки автентичності, авторизації та відповідності умовам безпеки під час кожної взаємодії.

2.4.83 національна система кібербезпеки
Сукупність суб'єктів кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів створення, використання та захисту національних електронних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, що формують кіберпростір держави.

2.4.84 несанкціонована точка доступу
Мережевий пристрій або програмне забезпечення, підключене до інформаційної системи без офіційного дозволу власника та/або поза встановленими процедурами.

2.4.85 об'єкт кібербезпеки
Цінність, інтерес та/або життєво важлива функція особи, суспільства, держави, що підлягають захисту від кіберзагроз.
Примітка. Об'єктами кібербезпеки є: конституційні права і свободи людини і громадянина; суспільство, його сталий розвиток як інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цільність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури.

2.4.86 об'єкт кіберзахисту

Інформаційна, електронна комунікаційна та/або інформаційно-комунікаційна система, що потребує технічного захисту від кіберзагроз.

2.4.87 об’єкт критичної інформаційної інфраструктури

Інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, що забезпечує стійке та безперервне функціонування об’єкта критичної інфраструктури, істотно впливає на безперервність та стійкість процесу надання життєво важливих функцій та/або послуг об’єктом критичної інфраструктури, на якому відсутній альтернативний об’єкт (спосіб) їх надання.

2.4.88 обфускація

Навмисна зміна вихідного коду, алгоритмів або даних для ускладнення їх аналізу, розуміння чи відтворення разом зі збереженням їх функціональної цілісності.

Заплутування.

2.4.89 патч безпеки

Модуль програмного коду, призначений для автоматизованого внесення змін до встановленої програми з метою виправлення помилок, усунення вразливостей безпеки, покращення функціональності або забезпечення сумісності інформаційної системи.

Виправлення безпеки.

2.4.90 пісочниця

Програмний або програмно-апаратний засіб, який містить технології, механізми та/або засоби для безпечного виконання програмного коду в ізольованому контрольованому середовищі та призначений для виявлення й аналізу підозрілої або шкідливої поведінки програмного елемента без ризику для цілісності основної системи.

2.4.91 поточний профіль безпеки системи

Задокументований результат оцінки фактично реалізованих та чинних заходів кіберзахисту в організації визначених міжнародним, національними стандартами та/або чинними нормативно-правовими актами, що відображає реальну картину захищеності на конкретний момент часу та слугує відправною точкою для планування покращень.

2.4.92 прихований контент

Сукупність зашифрованих вебресурсів, контенту та сервісів, доступ до яких можливий через спеціалізоване програмне забезпечення, конфігурації або авторизацію, що забезпечує високий рівень анонімності користувачів та власників ресурсів.

Дарквеб.

2.4.93 прихована мережа
Накладна анонімна мережа, побудована поверх мережі «Інтернет» із використанням спеціальних протоколів та технологій шифрування, що забезпечує приховування ідентифікаційної інформації учасників та вимагає спеціалізованого програмного забезпечення для доступу.
Даркнет.

2.4.94 програмний засіб захисту
Програмне забезпечення, призначене для виявлення, запобігання та нейтралізації кіберзагроз в інформаційних системах.

2.4.95 проксі-сервер
Сервер, який використовують для опосередкування взаємодії між користувачем і цільовим ресурсом, фільтрування трафіку, кешування, контролю доступу або анонімізації.

2.4.96 протидія агресії в кіберпросторі
Сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави через вплив на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак із метою захисту національної безпеки.

2.4.97 протидія комп'ютерній злочинності
Комплекс правових, організаційних та інженерно-технічних заходів для запобігання, виявлення та нейтралізації дій, що пов'язані з неправомірним використанням інформаційних систем або цифрового середовища.

2.4.98 профіль безпеки системи
Визначений набір вимог і заходів кібербезпеки, сформований для інформаційної системи на підставі результатів оцінки ризиків та нормативно-правових вимог.

2.4.99 реагування на кіберінцидент
Сукупність дій, спрямованих на аналіз кіберінциденту, обмеження його впливу, усунення наслідків та відновлення нормального функціонування інформаційної системи.

2.4.100 ретроспективний аналіз кіберінциденту
Вивчення причин та наслідків кіберінциденту для вдосконалення відповідного реагування та запобігання подібним подіям у майбутньому.

2.4.101 розширене виявлення та реагування

Технологія кіберзахисту, яка автоматично збирає й порівнює дані з різних інформаційних систем і засобів безпеки для виявлення кіберзагроз, кореляції подій та автоматизованого реагування на кіберінциденти.

2.4.102 розвідка кіберзагроз

Систематичний збір, обробка, аналіз і поширення інформації про наявні та потенційні кіберзагрози, суб'єкти кіберзагроз, їхні тактики, техніки та процедури з метою проактивного виявлення, прогнозування кібератак та ухвалення обґрунтованих рішень щодо управління кіберризиками.

2.4.103 руткіт

Програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі.

2.4.104 система автоматизованого реагування на кіберінциденти

Програмно-апаратний засіб для автоматичного виявлення, класифікації, аналізу та усунення кіберінцидентів на основі заздалегідь визначених сценаріїв реагування, алгоритмів машинного навчання та інтеграції із системами моніторингу безпеки, що забезпечує швидке реагування на загрози без участі оператора.

Примітка. Реагування охоплює, зокрема, ізоляцію скомпрометованих пристроїв, блокування шкідливого трафіку, припинення підозрілих процесів та автоматичне збирання цифрових доказів для подальшого розслідування.

AIR-система.

2.4.105 система виявлення вторгнень

Програмний або програмно-апаратний засіб для моніторингу комп'ютерних мереж і систем із метою виявлення несанкціонованої активності або зловмисних кібератак, що сповіщає оператора про інциденти.

IDS-система.

2.4.106 система виявлення та реагування на загрози на кінцевих точках

Програмний засіб для постійного моніторингу роботи комп'ютерів, серверів та інших пристроїв, що здатен виявляти шкідливу активність і дає змогу автоматично або вручну нейтралізувати їх, запобігаючи поширенню загроз у мережі.

EDR-система.

2.4.107 система дистанційної біометричної ідентифікації

Система штучного інтелекту, призначена для дистанційної цифрової ідентифікації фізичних осіб без їхньої активної участі, через порівняння біометричних даних особи з біометричними даними, що містяться в довідковій базі даних, незалежно від конкретної технології, процесів чи типів біометричних даних, що використовуються.

2.4.108 система запобігання вторгненням
Програмні або апаратні засоби кібербезпеки, які виявляють й автоматично блокують несанкціонований доступ та шкідливу активність у мережі, аналізуючи трафік на основі сигнатур, аномалій чи стану протоколів, захищаючи від атак у реальному часі.
IPS-система.

2.4.109 система керування оновленнями
Автоматизований комплекс програмних і технічних засобів для централізованого виявлення, тестування, розгортання та моніторингу оновлень безпеки операційних систем, прикладних програм та мікропрограмного забезпечення на всіх пристроях організації з метою вчасного усунення відомих вразливостей, зменшення поверхні кібератаки, забезпечення відповідності нормативним вимогам та запобігання використанню вразливостей кіберзловмисниками.

2.4.110 система керування подіями інформаційної безпеки
Програмне забезпечення, яке дає змогу організації збирати, аналізувати та реагувати на події безпеки, що відбуваються в її інформаційно-технологічній інфраструктурі, і застосовується для виявлення інцидентів, генерації сповіщень, розслідувань.
SIEM-система.

2.4.111 система контролю доступу до мережі
Сукупність технічних і програмних засобів для автентифікації користувачів, авторизації пристроїв, оцінки їх відповідності політикам безпеки та безперервного моніторингу мережевої активності з метою запобігання несанкціонованому доступу до корпоративної мережі та захисту від внутрішніх загроз.
NAC-система.

2.4.112 система оркестрації, автоматизації та реагування на безпеку
Інтегрована платформа кібербезпеки, що об’єднує технології оркестрації (координації взаємодії різних систем безпеки), автоматизації (виконання рутинних операцій без участі людини) та реагування на інциденти (швидкого усунення загроз) завдяки використанню програмованих сценаріїв, машинного навчання та інтеграції з іншими системами безпеки для скорочення часу виявлення та нейтралізації кіберзагроз, зменшення навантаження на аналітиків із кіберзахисту та забезпечення централізованого управління інцидентами безпеки.
SOAR-система.

2.4.113 сканер вразливостей

Програмний або апаратний засіб, який автоматично сканує комп'ютери, мережі та програмне забезпечення на наявність вразливостей у кіберзахисті, щоб виявити та оцінити кіберзагрози.

2.4.114 спам

Автоматизоване розповсюдження небажаних електронних повідомлень без згоди отримувачів.

2.4.115 спуфінг

Вид кібератаки, під час якої зловмисник маскується під надійне джерело (особу, програму, пристрій) для несанкціонованого доступу до конфіденційної інформації, коштів та/або поширення шкідливого програмного забезпечення.

Примітка. Найпоширенішими видами спуфінгу є: спуфінг ARP (підміна ARP-таблиці з метою перехоплення трафіку), спуфінг DNS (підміна DNS-відповіді для спрямування користувача на фальшивий сайт), спуфінг IP (підміна вихідної IP-адреси для приховування справжнього відправника).

2.4.116 суб'єкт кібербезпеки

Юридична чи фізична особа, що здійснює діяльність із забезпечення кібербезпеки та відповідає за стан кіберзахисту інформаційних систем чи цифрових сервісів.

2.4.117 сфера кібербезпеки

Комплекс правових, організаційних, технічних, оперативних та освітніх відносин, процесів і ресурсів державних і приватних суб'єктів, інтегрований з інформаційною, технологічною, економічною й правовою сферами та спрямований на запобігання, виявлення, стримування кіберзагроз, реагування на них і відновлення після кібератак із метою забезпечення конфіденційності, цілісності, доступності та стійкості інформаційних активів, цифрових сервісів і критичної інфраструктури в кіберпросторі та підтримання сталого розвитку цифрового суспільства.

Сфера кібербезпеки та кіберзахисту.

2.4.118 таксономія кіберінцидентів

Схема понять та класифікації кіберінцидентів, призначена для застосування під час обміну, повідомлення, зберігання інформації та підготовки звітів про кіберінциденти.

2.4.119 тестування на проникнення

Контрольована імітація реальної кібератаки на інформаційну систему з метою виявлення її вразливостей та запобігання можливого їх використання кіберзловмисниками.

Пентестинг.

2.4.120 технологія кіберзахисту

Апаратний, програмний або програмно-апаратний засіб захисту для забезпечення конфіденційності, цілісності та доступності інформації під час її обробки в інформаційно-комунікаційній системі.

2.4.121 хакер

Особа, яка використовує свої глибокі знання та навички у сфері комп'ютерних систем і програмування для отримання несанкціонованого доступу до комп'ютерів, мереж та інформації.

2.4.122 цифрова ідентифікація

Процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи.

Електронна ідентифікація.

2.4.123 цифрова криміналістика

Галузь судової науки, що займається виявленням, збереженням, аналізом та представленням цифрових доказів для розслідування кіберзлочинів та інцидентів інформаційної безпеки, охоплюючи дослідження жорстких дисків, мережевого трафіку, мобільних пристроїв тощо, щоб відновити дані та встановити обставини інцидентів.

Комп'ютерна криміналістика. Цифрова форензика.

2.4.124 цифровий артефакт

Цифрові дані, створені чи змінені під час функціонування інформаційної системи, які можуть бути використані для аналізу чи розслідування кіберінцидентів.

2.4.125 цифровий доказ

Інформація в електронному форматі, яка містить дані про обставини справи та може бути використана як доказ у суді.

Примітка. Цифровими доказами можуть бути електронні документи, зокрема текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи, вебсайти, текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі

Електронний доказ.

2.4.126 цифровий ідентифікатор

Унікальний набір символів або числовий код, який присвоюється певному об'єкту, сутності чи елементу даних у цифровій системі.

Примітка. Ідентифікатор використовують для однозначного розпізнавання об'єкта, проведення автентифікації (підтвердження особи), авторизації (надання доступу до ресурсів), аудиту (обліку та контролю дій у системі).

Електронний ідентифікатор.

2.4.127 цифровий слід
Інформація про дії користувача під час його перебування в мережі.

2.4.128 цільовий профіль безпеки системи
Задокументований опис бажаного рівня захищеності та зрілості заходів кіберзахисту, визначених міжнародними, національними стандартами та/або чинними нормативно-правовими актами, якого організація прагне досягти та який визначають на основі цілей організації, аналізу ризиків та застосованих стандартів безпеки.

2.4.129 чорний хід
Механізм доступу, що дає змогу обійти стандартні засоби автентифікації та контролю доступу в інформаційній та інформаційно-комунікаційній системі.
Примітка. Чорний хід використовують кіберзловмисники для дистанційного керування системою, викрадення даних або встановлення шкідливого програмного забезпечення.
Бекдор.

2.4.130 шкідливе програмне забезпечення
Програмне забезпечення, код або скрипт, створені з навмисним наміром порушити функціонування комп’ютерної системи, отримати несанкціонований доступ до інформаційного ресурсу, скомпрометувати конфіденційність, цілісність або доступність даних та/або завдати шкоди користувачеві та/або організації.
Зловмисне програмне забезпечення. Шкідлива програма. Зловмисна програма.

2.5. АБЕТКОВИЙ ПОКАЖЧИК ТЕРМІНІВ

3. ДОВІДКОВІ МАТЕРІАЛИ

Додаток
до стандарту державної мови
«Термінологія у сфері кібербезпеки»

Відповідники до термінів англійською мовою

автентифікація 2.4.1	Authentication *Англо-український військовий словник 64464 гасла. Упорядник Ukrop. Austria, 2026. URL: https://english-military-dictionary.org.ua/A*
автентифікація багатофакторна 2.4.10	Multi-Factor Authentication (MFA) *Multifactor Authentication for E-Commerce. Risk-Based, FIDO Universal Second Factor Implementations for Purchasers. July 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf*
автентифікація біометрична 2.4.13	Biometric Authentication *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/biometric_authentication*
авторизація 2.4.3	Authorization *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
акредитація з безпеки 2.4.4	Accreditation / Security Authorization *Glossary of Key Information Security Terms. NIST IR 7298. April 25, 2006. URL: https://csrc.nist.rip/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf*
аналіз кіберінциденту ретроспективний 2.4.100	Retrospective Incident Analysis *Results of cybersecurity incident investigations in 2021–2023. December 13, 2023. URL: https://global.ptsecurity.com/en/research/analytics/results-of-cybersecurity-incident-investigations-in-2021-2023/*
анонімізація 2.4.6	Anonymization *Simson Garfnkel, Joseph Near, Aref N. Dajani, Phyllis Singer, Barbara Guttman. De-Identifying Government Datasets: Techniques and Governance. NIST Special Publication NIST SP 800-188. September 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.pdf*
антиспам 2.4.8	Anti-Spam *Cambridge Dictionary. URL: https://dictionary.cambridge.org/*

артефакт цифровий 2.4.124	Digital Artifact *Encyclopedia of Forensic Sciences, Third Edition , 2023 pp 19-25. URL: https://www.sciencedirect.com/topics/computer-science/digital-artifact*
атрибуція кібератаки 2.4.9	Cyberattack Attribution *European Repository of Cyber Incidents. Glossary. URL: https://eurepoc.eu/glossary/*
безпека мережевого порту 2.4.12	Network Port Security *Cisco Systems. Port Security (definition). URL: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011111.html*
блокування облікового запису 2.4.14	Account Lockout *Jericho's Cybersecurity Glossary. URL: https://www.jerichosecurity.com/glossary/account-lockout?utm_source*
бомба логічна 2.4.78	Logic Bomb *Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security. NIST Special Publication 800-12. Revision 1. June 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf*
бот 2.4.15	Bot *Collins Dictionaries. URL: https://www.collinsdictionary.com/dictionary/english/bot?utm_source*
ботнет 2.4.16	Botnet *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/botnet*
виявлення та реагування мережеве 2.4.79	Network Detection and Response (NDR) *N2K CyberWire. Glossary. URL: https://thecyberwire.com/glossary/network-detection-and-response?utm_source*
виявлення та реагування розширене 2.4.101	Extended Detection and Response (XDR) *N2K CyberWire. Glossary. URL: https://thecyberwire.com/glossary/extended-detection-and-response?utm_source*
відкритість кіберпростору 2.4.17	Openness of Cyberspace *Internet Governance Glossary. URL: https://www.unesco.org/en/internet-governance/internet-governance-glossary?utm_source*
вірус комп'ютерний	Virus *(Computer Virus)* *Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An*

2.4.73	*Introduction to Information Security. NIST Special Publication 800-12. Revision 1. June 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf*
вразливість 2.4.19	Vulnerability *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/vulnerability*
доказ цифровий 2.4.125	Digital Evidence *Rick Ayers, Sam Brothers, Wayne Jansen. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revision 1. May 2014. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf*
доступність кіберпростору 2.4.22	Availability of Cyberspace *ENISA overview of cybersecurity and related terminology. Version 1. September 2017. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf?utm_source*
екран міжмережевий 2.4.80	Firewall *Glossary of Key Information Security Terms. NISTIR 7298. Revision 2. May 2013. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*
експлойт 2.4.23	Exploit *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
журнал 2.4.25	Log Viewing *Karen Kent, Murugiah Souppaya. Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology. Special Publication 800-92. September 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf*
журналювання 2.4.26	Log Perorting *Karen Kent, Murugiah Souppaya. Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology (NIST). Special Publication 800-92. September 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf*
забезпечення програмне антивірусне 2.4.7	Antivirus Software *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL:*

	https://niccs.cisa.gov/resources/glossary
забезпечення програмне шкідливе 2.4.130	Malware / Malicious Software *Glossary of Key Information Security Terms. NIST IR 7298. April 25, 2006. URL: https://csrc.nist.rip/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf*
засіб захисту програмний 2.4.94	Security Software *NordVPN. Cybersecurity glossary. URL: https://nordvpn.com/uk/cybersecurity/glossary/security-software/?srsltid=AfmBOoqCd53IwUy-GbnZ0bxlrjCQzu1gRSN5aFOQHfp9FAsgoovBLYB2&utm_source*
зловживання в кіберпросторі 2.4.27	Computer Abuse *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/computer_abuse?utm_source*
зона демілітаризована 2.4.21	Demilitarized Zone (DMZ) *Glossary of Key Information Security Terms. NIST IR 7298. April 25, 2006. URL: https://csrc.nist.rip/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf*
ідентифікатор цифровий 2.4.126	Digital Identifier / Digital ID *Information Technology Laboratory. NIST Computer Security Resource Center. Glossary: Identifier. URL: https://csrc.nist.gov/glossary/term/identifier* *Information Technology Laboratory. NIST Computer Security Resource Center. Glossary: Digital identity. URL: https://csrc.nist.gov/glossary/term/digital_identity*
ідентифікація кіберзагрози 2.4.28	Threat Identification *Threat Identification. URL: https://flare.io/glossary/threat-identification/?utm_source*
ідентифікація цифрова 2.4.122	Digital Identification *Digital Convergence Initiative (DCI). Terminology. URL: https://standards.spdci.org/standards/dci/terminology?utm_source*
індикатор кіберзагрози 2.4.29	Cyber Threat Indicator *Legal Information Institute. URL: https://www.law.cornell.edu/search/searchResultsForm.html#5*
індикатор компрометації 2.4.30	Indicator of Compromise (IOCs) *Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, Karen Scarfone. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST SP 800-61r3. April 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf*
індикатор стану	Cybersecurity Status Indicator

кібербезпеки 2.4.31	*Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. October 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf*
ін'єкція програмного коду 2.4.32	Code Injection *Weilin Zhong. Code Injection. URL: https://owasp.org/www-community/attacks/Code_Injection?utm_source*
інструмент реагування на кіберінциденти 2.4.33	Incident Response Tools *Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, Karen Scarfone. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST SP 800-61r3. April 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf?utm_source=chatgpt.com*
інфраструктура інформаційна критична 2.4.76	Critical Information Infrastructure (CII) *https://legalinstruments.oecd.org/public/doc/659/b20136fe-09b6-44bc-b032-c21ec67802b5.pdf*
інфраструктура кіберзахисту 2.4.34	Cybersecurity Infrastructure *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
кейлогер 2.4.35	Keylogger *Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, Michael Thompson. Guide to Operational Technology (OT) Security. NIST SP 800-82r3. September 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf*
кіберагресія 2.4.36	Cyber Aggression *Cyberdiplomacy as an important tool for international cooperation. 28.07.2025. Official website of the National Security and Defense Council of Ukraine. URL: https://www.rnbo.gov.ua/en/Diialnist/7248.html*
кібератака 2.4.37	Cyberattack *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
кібератака «відмова в обслуговуванні» (розподілена) 2.4.38	Denial-of-Service Attack (DoS attack) (Distributed Denial-of-Service (DDoS) Attack) *Glossary of Key Information Security Terms. NISTIR 7298. Revision 2. May 2013. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*

кібератака «людина посередині» 2.4.39	Man-In-The-Middle Attack (MITM attack) *Glossary of Key Information Security Terms. NISTIR 7298.Revision 2. May 2013. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*
кібератака методом повного перебору 2.4.40	Brute-Force Attack *Mary E. Shacklett, Katie Terrell Hanna. What is a brute-force attack? Apr 21, 2025. URL: https://www.techtarget.com/searchsecurity/definition/brute-force-cracking*
кібератака нульового дня 2.4.41	Zero-Day Attack *Kelley Dempsey, Paul Eavy, Nedim Goren, George Moore. Automation Support for Security Control Assessments. NISTIR 8011. Volume 3. December 2018. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8011-3.pdf*
кібербезпека 2.4.42	Cybersecurity *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
кіберборотьба 2.4.43	Cyber Warfare / Cyber Struggle *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
кібервійна 2.4.44	Cyberwar / Cyber War / Cyber Warfare / Cyberwarfare *Encyclopedia Britannica. Cyberwar. URL: https://www.britannica.com/topic/cyberwar?utm_source*
кібервплив 2.4.45	Cyber Influence *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations (2016). URL: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf*
кібергігієна 2.4.46	Cyber Hygiene *Cyber hygiene. ENISA. The European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/topics/cyber-hygiene?utm_source*
кібердоктрина 2.4.47	Cyber Doctrine *UK Ministry of Defence. Allied Joint Doctrine for Cyberspace Operations (AJP-3.20) – publication page. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320*
кіберзагроза 2.4.48	Cybersecurity Threat *Information Technology Laboratory. NIST Computer Security Resource*

	Center (CSRC). Glossary. Cyber Threat. URL: https://csrc.nist.gov/glossary/term/cyber_threat
кіберзагроза воєнного характеру 2.4.49	Military Cyber Threat *NATO. Official website. Topic page. Cyber defence. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence*
кіберзагроза терористичного характеру 2.4.50	Terrorist Cyber Threat / Cyber Threat of a Terrorist Nature *United Nations Office on Drugs and Crime (UNODC). Cybercrime Module 14. Key Issues: Cyberterrorism. URL: https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-14/key-issues/cyberterrorism.html*
кіберзахист 2.4.51	Cyber Defense *ENISA overview of cybersecurity and related terminology. Version 1. September 2017. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf*
кіберзахист автоматизований 2.4.2	Automated Cybersecurity *ENISA overview of cybersecurity and related terminology. Version 1. September 2017. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf* Cyberspace Defense *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyberspace_defense*
кіберзброя 2.4.52	Cyber Weapon *Clay Wilson. Cyber weapons: 4 defining characteristics. June 4, 2015. URL: https://www.route-fifty.com/cybersecurity/2015/06/cyber-weapons-4-defining-characteristics/287193/?utm_source*
кіберзловмисник 2.4.53	Cyber Attacker / Cyber Malicious Actor / Cyber Threat Actor / Attacker *Simson Garfnkel, Joseph Near, Aref N. Dajani, Phyllis Singer, Barbara Guttman. De-Identifying Government Datasets: Techniques and Governance. NIST Special Publication NIST SP 800-188. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.pdf*
кіберзлочин 2.4.54	Cybercrime *Encyclopaedia Britannica. Cybercrime. URL: https://www.britannica.com/topic/cybercrime.*
кіберзлочинність 2.4.55	Cybercrime *Cambridge Dictionary. URL: https://dictionary.cambridge.org/uk/dictionary/english/cybercrime?utm*

	_source
кіберзлочинність міжнародна 2.4.81	International Cybercrime *Cambridge Dictionary. URL: https://dictionary.cambridge.org/uk/dictionary/english/cybercrime?utm_source*
кіберінцидент 2.4.56	Cyber Incident *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyber_incident*
кіберконтррозвідка 2.4.57	Cyber Counterintelligence *Shanika Wickramasinghe. Cyber Counterintelligence (CCI): Offensive & Defensive Strategies for Cybersecurity. March 06, 2023. URL: https://www.splunk.com/en_us/blog/learn/cci-cyber-counterintelligence.html?utm_source*
кібернавчання 2.4.58	Cyber Training *What is cybersecurity training? URL: https://phantomslab.io/cybersecurity-awareness/terminology/what-is-cybersecurity-training/*
кібероборона 2.4.59	Cyberspace Defense *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyberspace_defense*
кібероперація 2.4.60	Cyberspace Operation *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyberspace_operations*
кіберпростір 2.4.61	Cyberspace *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cybersecurity_risk*
кіберризик 2.4.62	Cybersecurity Risk *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cybersecurity_risk*
кіберрозвідка 2.4.63	Cyber Intelligence *Cyber Intelligence. Aug 18, 2025. URL: https://www.europol.europa.eu/how-we-work/services-support/intelligence-analysis/cyber-intelligence?utm_source*
кіберстійкість 2.4.64	Cyber Resilience *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL:*

	https://csrc.nist.gov/glossary/term/cyber_resiliency
кібертеракт 2.4.65	Cyberterrorism Attack *Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/cyberterrorism?utm_source*
кібертероризм 2.4.66	Cyberterrorism *Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/cyberterrorism?utm_source*
кіберудар 2.4.67	Cyber Strike *Andrew F. Krepinevich. Cyber Warfare: A "Nuclear Option"? 2012. URL: https://www.files.ethz.ch/isn/154628/CSBA_Cyber_Warfare_For_Web_1.pdf?utm_source*
кібершпигунство 2.4.68	Cyberespionage *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
кібершахрайство 2.4.69	Cyber Fraud *Cyber Fraud. Cyber Security. The Law Society Learning. URL: https://learn.lawsociety.org.uk/product/cyber-fraud/?utm_source*
ключ керування доступом 2.4.70	Access Control Key *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/access_control*
компрометація засобу електронної ідентифікації 2.4.71	Compromise of Electronic Identification / eID Compromise *Jide Edu, Mark Hooper, Carsten Maple, Jon Crowcroft. An Impact and Risk Assessment Framework for National Electronic Identity (eID) Systems. Oct 24, 2023. URL: https://arxiv.org/abs/2310.15784?utm_source=chatgpt.com*
компрометація інформаційної системи 2.4.72	Security Breach / Compromise of an Information System *Security Breach and Cyber Fraud. Industry Definitions. Release 1.0. April 2, 2019. URL: https://www.sparkinstitute.org/wp-content/uploads/2021/06/SPARK-DSOB-Security-Breach-Definition-Best-Practice-Standard-4-2-2019.pdf*
контент прихований 2.4.92	Dark Web *U.S. Department of Justice. Office of the Inspector General. Press Release. Audit of the FBI's Strategy and Efforts to Disrupt Illegal Dark Web Activities. URL: https://oig.justice.gov/news/doj-oig-releases-report-fbis-strategy-and-efforts-disrupt-illegal-dark-web-activities*
контрфорензика 2.4.74	Anti-Computer Forensic / Counter Forensic

	National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary
криміналістика цифрова 2.4.123	Forensics *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
ланцюг кібератаки 2.4.77	Cyber Kill Chain *Chrissy Kidd. Cyber Kill Chains: Strategies & Tactics. August 26, 2024. URL: https://www.splunk.com/en-us/blog/learn/cyber-kill-chains.html*
мережа приватна віртуальна 2.4.18	Virtual Private Network (VPN) *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/vpn*
мережа прихована 2.4.93	Darknet *Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/darknet?utm_source*
модель нульової довіри 2.4.82	Zero Trust Model *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/zero_trust*
об'єкт кібербезпеки 2.4.85	Cybersecurity Object *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/object?utm_source*
об'єкт кіберзахисту 2.4.86	Object of Cyber Protection *National Institute of Standards and Technology (NIST). Computer Security Resource Center (CSRC). Glossary. Information system. URL: https://csrc.nist.gov/glossary/term/information_system*
об'єкт критичної інформаційної інфраструктури 2.4.87	Critical Information Infrastructure Object / Object CII *Cyber Security Agency of Singapore (CSA). Cybersecurity Act – FAQs. Definition of Critical Information Infrastructure (CII) under section 7(1). URL: https://www.csa.gov.sg/faqs/cybersecurity-act/*
обфускація 2.4.88	Obfuscation *Rahul Awati. What is obfuscation and how does it work? Nov 27, 2024. URL: https://www.techtarget.com/searchsecurity/definition/obfuscation*
патч безпеки 2.4.89	Security Patch *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/patch*
пісочниця 2.4.90	Sandbox

	Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/sandbox
проксі-сервер 2.4.95	Proxy Server *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/proxy_server*
протидія агресії в кіберпросторі 2.4.96	Cyberspace Defense *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyberspace_defense?utm_source=chatgpt.com*
протидія комп'ютерній злочинності 2.4.97	Cybercrime Prevention *Cybercrime prevention. URL: https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-prevention.html*
профіль безпеки системи 2.4.98	Security Profile *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/profile?utm_source=chatgpt.com*
профіль безпеки системи базовий 2.4.11	Baseline Security Profile *National Institute of Standards and Technology (NIST). Computer Security Resource Center (CSRC). SP 800-53B: Control Baselines for Information Systems and Organizations (Final). URL: https://csrc.nist.gov/pubs/sp/800/53/b/final*
профіль безпеки системи галузевий 2.4.20	Sectoral Security Profile *National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0 (defines CSF Organizational Profile: current/target posture in terms of CSF outcomes). URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*
профіль безпеки системи поточний 2.4.91	Current Security Profile *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/profile?utm_source=chatgpt.com*
профіль безпеки системи цільовий 2.4.128	Target Security Profile *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/profile?utm_source=chatgpt.com*
реагування на кіберінцидент 2.4.99	Cyber Incident Response *Sybersecurity and Infrastructure Security Agency. An official website of the U.S. Department of Homeland Security. URL: https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response*

розвідка кіберзагроз 2.4.102	Cyber Threat Intelligence *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/cyber_threat_intelligence*
руткіт 2.4.103	Rootkit *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/rootkit*
система автоматизованого реагування на кіберінцидент 2.4.104	Automated Incident Response System *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/incident_response*
система акредитована з безпеки 2.4.5	Security-Accredited System *Edward Roback. Automated Information System Security Accreditation Guidelines. NIST IR 4378. Information Technology Laboratory. Computer Security Resource Center. August 1990. URL: https://csrc.nist.gov/pubs/ir/4378/final?utm_source=chatgpt.com*
система виявлення вторгнень 2.4.105	Intrusion Detection System (IDS) *Glossary of Key Information Security Terms. NIST IR 7298. April 25, 2006. URL: https://csrc.nist.rip/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf*
система виявлення та реагування на загрози на кінцевих точках 2.4.106	Endpoint Detection and Response (EDR) *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/edr*
система дистанційної біометричної ідентифікації 2.4.107	Remote Biometric Identification System *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. Official Journal of the European Union. 12.7.2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689*
система запобігання вторгненням 2.4.108	Intrusion Prevention System (IPS) *Glossary of Key Information Security Terms. NIST IR 7298. April 25, 2006. URL: https://csrc.nist.rip/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf*
система кібербезпеки національна 2.4.83	National Cybersecurity Awareness System *Sybersecurity and Infrastructure Security Agency. An official website of the U.S. Department of Homeland Security. URL: https://www.cisa.gov/resources-tools/services/national-cyber-awareness-system*
система керування оновленнями	Patch Management System *Information Technology Laboratory. Computer Security Resource*

2.4.109	*Center. Glossary. URL: https://csrc.nist.gov/glossary/term/patch_management*
система керування подіями інформаційної безпеки 2.4.110	Security Information and Event Management System (SIEM) *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
система контролю доступу до мережі 2.4.111	Network Access Control System (NAC) *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/network_access_control*
система оркестрації, автоматизації та реагування на безпеку 2.4.112	Security Orchestration, Automation and Response (SOAR) *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/soar*
ситуація кризова у сфері кібербезпеки 2.4.75	Cybersecurity Crisis *European Union Agency for Cybersecurity (ENISA). Best Practices for Cyber Crisis Management. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf*
сканер вразливостей 2.4.113	Vulnerability Scanner *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
слід цифровий 2.4.127	Digital Footprint *Collins Dictionaries. URL: https://www.collinsdictionary.com/dictionary/english/digital-footprint*
спам 2.4.114	Spam *Collins Dictionaries. URL: https://www.collinsdictionary.com/dictionary/english/spam*
спуфінг 2.4.115	Spoofing *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
суб'єкт кібербезпеки 2.4.116	Cybersecurity Actor *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/actor; https://csrc.nist.gov/glossary/term/subject*
сфера кібербезпеки 2.4.117	Cybersecurity Area *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL:*

	https://csrc.nist.gov/glossary/term/cybersecurity
таксономія кіберінцидентів 2.4.118	Cyber Incident Taxonomies *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/taxonomy*
тестування на проникнення 2.4.119	Penetration Testing *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
технологія кіберзахисту 2.4.120	Cybersecurity Technology *Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity?utm_source*
точка доступу несанкціонована 2.4.84	Rogue Device *Information Technology Laboratory. Computer Security Resource Center. Glossary. URL: https://csrc.nist.gov/glossary/term/rogue_device?hl=uk-UA*
хакер 2.4.121	Hacker *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*
хакінг етичний 2.4.24	Ethical Hacking *Encyclopaedia Britannica. Cybercrime: Hacking. URL: https://www.britannica.com/topic/cybercrime/Hacking* *OWASP Foundation. Web Security Testing Guide (WSTG) v4.1. Introduction. URL: https://owasp.org/www-project-web-security-testing-guide/v41/2-Introduction/*
хід чорний 2.4.129	Backdoor *National Initiative for Cybersecurity Careers and Studies. Official website of the Cybersecurity and Infrastructure Security Agency. URL: https://niccs.cisa.gov/resources/glossary*

4. БІБЛІОГРАФІЯ

Національні нормативно-правові акти та державні інформаційні ресурси:

1. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : Постанова Каб. Міністрів України від 18 червня 2025 року № 712. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text

2. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk

3. Перелік категорій кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації.* URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

4. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лютого 2006 року № 3475-IV. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

5. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовтня 2017 року № 2155-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19 червня 2019 року № 518. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

7. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 03 липня 2023 року № 570. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text

8. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Каб. Міністрів України від 29 грудня 2021 року № 1426. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

9. Про затвердження Порядку акредитації з безпеки комунікаційно-інформаційних систем (інформаційно-комунікаційних систем), де обробляється інформація НАТО з обмеженим доступом : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 13 листопада 2024 року № 655. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/z1880-24#Text

10. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 липня 1994 року № 80/94-ВР. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

11. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. *Офіційне інтернет-представництво Президента України.* URL: https://www.president.gov.ua/documents/4472021-40013

12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

Наукова та навчально-методична література:

1. Англо-український словник термінів з інформаційних технологій та кібербезпеки / ІСЗЗІ КПІ ім. Ігоря Сікорського ; уклад. : А. Я. Гладун, О. О. Пучков, І. Ю. Субач, К. О. Хала. Київ : КПІ ім. Ігоря Сікорського, 2018. 380 с.

2. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки : навч. посіб. Київ, 2018. 320 с.

3. Вавіленкова А. І. Методи і моделі протидії кібератакам : навч. посіб. Київ : НА СБУ, 2023. 136 с.

4. Довгань О. Д., Тарасюк А. В., Ткачук Т. Ю. Кібербезпека «суспільства знань» : монографія. Київ ; Одеса : Фенікс, 2021. 176 с.

5. Довгань О. Д., Ткачук Т. Ю. Кібербезпека критичної інфраструктури України: моделювання ризиків counter-forensics та механізми забезпечення цифрової доказовості : наук.-практ. посіб. Київ ; Одеса : Фенікс, 2025. 80 с.

6. Довгань О. Д., Ткачук Т. Ю. Кіберризики критичної інфраструктури: від аналізу загроз до впровадження рішень : наук.-практ. посіб. Київ ; Одеса : Фенікс, 2024. 77 с.

7. Жовтяк В. А. Структурні особливості англомовних термінів кібербезпеки. Закарпатські філологічні студії / редкол. : І. М. Зимомря (голов. ред.), М. М. Палінчак, Ю. М. Бідзіля та ін. Ужгород : Гельветика, 2024. Т. 1, вип. 34. С. 79–84. URL: http://zfs-journal.uzhnu.uz.ua/a

8. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа ; за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

9. Кібер Брама. URL: https://stopfraud.gov.ua/

10. Когут Ю. І. Кібервійна та безпека об’єктів критичної інфраструктури : практ. посіб. Київ, 2021. 332 с.

11. Лісовська Ю. П. Кібербезпека: ризики та заходи. Кондор, 2019. 272 с.

12. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки : підручник. Київ : НА СБ України, 2020. 256 с.

13. Посібник з додаткових ресурсів CRR. Т. 5. Управління кіберінцидентами. Версія 1.1. Університет Карнегі-Меллона, 2016. 54 с.

14. Словник «Кібербезпека та кібергігієна». URL: https://cyber.kbs.kharkiv.ua/словник/

15. Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ : Аванпост-Прим, 2012. 214 с.