Відокремлений структурний підрозділ
«Чернігівський фаховий коледж інженерії та дизайну
Київського національного університету технологій та дизайну»

Творчо-пошукова робота

Кібербезпека в облікових інформаційних системах

Студентка гр. ОМД-124 Сичова Анастасія

Викладач Наталія МАЛИНОВСЬКА

2026

Зміст

ВСТУП

Сьогодні кібербезпека є однією з ключових тем у сучасному цифровому світі. З кожним роком усе більше процесів переходить в онлайн-середовище: ми зберігаємо інформацію в електронному вигляді, здійснюємо фінансові операції, користуємось цифровими сервісами та працюємо з різними інформаційними системами. Разом із цим зростає і кількість кіберзагроз. Це можуть бути зломи систем, витоки даних, вірусні атаки або шахрайські дії, які можуть призвести до серйозних наслідків — як для окремих користувачів, так і для цілих організацій. Особливо важливою ця тема є у сфері облікових систем. Саме в них зберігається велика кількість фінансової, персональної та організаційної інформації, яка має високу цінність і потребує надійного захисту. Будь-яке порушення безпеки таких систем може вплинути на стабільність роботи підприємства та призвести до значних втрат.

Саме тому кібербезпека сьогодні розглядається не як додатковий елемент, а як необхідна умова ефективного функціонування цифрового середовища. У своїй роботі я розгляну основні поняття кібербезпеки, її аспекти та напрями, а також особливості захисту облікових систем, сучасні кіберзагрози та способи протидії їм.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ

1.1. Поняття кібербезпеки

У сучасному світі, який характеризується стрімким розвитком інформаційних технологій та активною цифровізацією всіх сфер суспільного життя, кібербезпека набуває особливо важливого значення. Практично всі процеси — від особистого спілкування до функціонування великих підприємств і державних інституцій — здійснюються із застосуванням цифрових технологій, що передбачає її обробку, зберігання та передачу інформації в електронному вигляді. У найпростішому розумінні кібербезпека може розглядатися як безпека в мережі Інтернет або безпека користувача під час роботи в цифровому середовищі. Проте таке визначення є лише базовим і не відображає повною мірою сутності цього поняття. З наукової та академічної точки зору кібербезпека визначається як комплекс заходів, технологій, методів і організаційних процесів, спрямованих на захист інформації, інформаційних систем, комп'ютерних мереж і цифрових ресурсів від несанкціонованого доступу, використання, модифікації, пошкодження або знищення. Особливістю кібербезпеки є її системний характер. Вона охоплює не лише технічні засоби захисту, такі як антивірусні програми або засоби шифрування, але й організаційні заходи, політики безпеки, а також поведінкові аспекти діяльності користувачів.

Об'єктами кібербезпеки є широкий спектр цифрових ресурсів, серед яких:

-фінансові системи та банківські сервіси;

-облікові та бухгалтерські програми;

-корпоративні бази даних;

-інформаційні системи підприємств;

-державні електронні ресурси.

Таким чином, будь-яка інформація, що існує в цифровому вигляді, потребує захисту.

Отже, кібербезпека є не просто технічною необхідністю, а стратегічно важливим елементом функціонування сучасного суспільства.

1.2. Структура та складові кібербезпеки

Кібербезпека є складною багаторівневою системою, яка не обмежується використанням окремих технічних засобів або програмного забезпечення. Вона являє собою комплекс взаємопов'язаних елементів, кожен з яких виконує важливу функцію у забезпеченні загального рівня захисту інформації, інформаційних систем і користувачів. Ефективність кібербезпеки досягається лише за умови узгодженої роботи всіх її складових, оскільки слабкість хоча б одного елементу може призвести до порушення безпеки всієї системи.

Саме тому доцільно розглядати структуру кібербезпеки як сукупність кількох основних компонентів.

2.1. Захист інформації

Однією з ключових складових кібербезпеки є захист інформації. Даний компонент спрямований на забезпечення безпеки даних незалежно від форми їх зберігання або способу передачі. Захист інформації охоплює весь життєвий цикл даних — від моменту їх створення та обробки до зберігання, передачі та, за необхідності, знищення або архівування. Основною метою є недопущення витоку інформації, її несанкціонованого використання або зміни.

Особливо важливим цей аспект є у випадках, коли йдеться про:

-фінансову інформацію підприємств;

-персональні дані клієнтів і працівників;

-внутрішню документацію організацій;

-комерційну або службову таємницю.

Для забезпечення захисту інформації застосовуються різні методи та технології. Серед них:

-шифрування даних, яке дозволяє зробити інформацію недоступною для сторонніх осіб;

-резервне копіювання, що забезпечує можливість відновлення даних у разі їх втрати;

-системи контролю доступу, які обмежують можливість роботи інформацією лише для уповноважених користувачів;

-моніторинг та аудит, які дозволяють відстежувати дії користувачів і виявляти підозрілу активність.

Таким чином, захист інформації є базовим рівнем кібербезпеки, без якого неможливо забезпечити надійне функціонування будь-якої інформаційної системи.

2.2. Захист інформаційних систем

Наступною важливою складовою кібербезпеки є захист інформаційних систем. Він спрямований на забезпечення стабільної, безперервної та безпечної роботи програмного забезпечення, серверів, баз даних і технічної інфраструктури. Інформаційні системи є основою функціонування сучасних організацій, оскільки саме в них здійснюється обробка та зберігання даних. Будь-яке порушення їх роботи може призвести до серйозних наслідків, включаючи зупинку бізнес-процесів, втрату даних або фінансові збитки.

Захист інформаційних систем включає:

-запобігання несанкціонованому доступу до систем;

-захист від шкідливого програмного забезпечення;

-забезпечення стабільності та відмовостійкості роботи;

-своєчасне оновлення програмного забезпечення для усунення вразливостей.

Особливу роль відіграє регулярне оновлення систем, оскільки більшість сучасних кібератак використовують відомі вразливості програмного забезпечення. Якщо такі вразливості не усуваються вчасно, система стає легкою ціллю для зловмисників.

Отже, захист інформаційних систем є критично важливим для забезпечення безперервності діяльності організацій.

2.3. Захист користувачів

Окрему і надзвичайно важливу складову кібербезпеки становить захист користувачів. Це пов’язано з тим, що людський фактор є одним із найбільш уразливих елементів будь-якої системи.

Навіть за наявності сучасних технічних засобів захисту, помилки користувачів можуть призвести до серйозних порушень безпеки.

Наприклад, користувач може:

-відкрити фішинговий лист;

-перейти за підозрілим посиланням

-використовувати слабкий пароль;

-передати свої облікові дані стороннім особам.

Саме тому важливим напрямом кібербезпеки є підвищення рівня обізнаності користувачів і формування у них навичок безпечної поведінки.

Захист користувачів включає:

-навчання основам кібербезпеки;

-пояснення типових загроз і способів їх розпізнавання;

-використання складних і унікальних паролів;

-впровадження багатофакторної автентифікації, яка додає додатковий рівень захисту.

Таким чином, користувачі не лише можуть бути джерелом ризику, але й, за умови належної підготовки, стають важливим елементом системи кіберзахисту.

2.4. Постійність та комплексність кібербезпеки

Важливо підкреслити, що кібербезпека не є одноразовим заходом або встановленням певного програмного забезпечення. Вона являє собою безперервний процес, який потребує постійної уваги, контролю та вдосконалення.

Цей процес включає:

-регулярне оновлення програм і систем;

-контроль доступу до інформаційних ресурсів;

-навчання користувачів;

-моніторинг стану систем;

-оперативне реагування на загрози та інциденти.

Кіберзагрози постійно розвиваються, тому методи захисту також повинні адаптуватися до нових умов. Це означає, що кібербезпека повинна бути динамічною системою, яка постійно вдосконалюється.

Отже, структура кібербезпеки включає кілька ключових складових: захист інформації, захист інформаційних систем і захист користувачів.

Усі ці елементи взаємопов’язані та доповнюють один одного. Ефективний захист можливий лише за умови їх комплексного застосування, оскільки порушення в одному з компонентів може призвести до загальної вразливості системи.

Таким чином, кібербезпека виступає як цілісна система, що поєднує технічні, організаційні та людські фактори з метою забезпечення надійного функціонування інформаційного середовища.

1.3. Основні напрями кібербезпеки

Кібербезпека як складна система не може обмежуватися лише загальними принципами або окремими заходами захисту. Для її ефективної реалізації вона поділяється на кілька основних напрямів, кожен з яких відповідає за певний аспект забезпечення безпеки інформаційного середовища. Ці напрями є взаємопов'язаними та доповнюють один одного, формуючи цілісну систему захисту. Важливо розуміти, що ослаблення будь-якого з напрямів може призвести до виникнення вразливостей і, як наслідок, до порушення загальної безпеки системи. У сучасній інформаційній безпеці зазвичай виділяють три основні напрями кібербезпеки: мережевий захист, захист інформації та захист користувачів.

3.1. Захист мереж і комп'ютерних систем

Першим і одним із найважливіших напрямів є захист мережевої інфраструктури та комп'ютерних систем. Цей напрям охоплює комплекс заходів, спрямованих на забезпечення безпечної роботи комп'ютерних мереж, серверів, баз даних і програмного забезпечення. Сучасні інформаційні системи функціонують у мережевому середовищі, що означає постійний обмін даними між різними пристроями. Це створює потенційні ризики, пов'язані з можливістю несанкціонованого доступу або перехоплення інформації під час передачі.

Основними завданнями мережевого захисту є:

-запобігання несанкціонованому доступу до мережі;

-захист від зовнішніх атак, зокрема хакерських вторгнень;

-забезпечення стабільної роботи серверів і мережевих сервісів;

-контроль мережевого трафіку та виявлення підозрілої активності.

Для реалізації цього напряму використовуються такі технології, як міжмережеві екрани (firewalls), системи виявлення та запобігання вторгненням (IDS/IPS), а також засоби моніторингу мережевого трафіку.

Таким чином, мережевий захист є першою лінією оборони інформаційної системи, оскільки саме через мережу найчастіше здійснюються кіберзагрози.

3.2. Захист інформації

Другим важливим напрямом є захист інформації, який спрямований безпосередньо на забезпечення безпеки даних незалежно від середовища їх зберігання або передачі.Інформація є одним із найцінніших ресурсів у сучасному світі, особливо якщо йдеться про фінансові, комерційні або персональні дані. Саме тому її захист є ключовим завданням кібербезпеки.

Основними цілями цього напряму є:

-забезпечення конфіденційності даних;

-збереження їх цілісності;

-гарантування доступності для уповноважених користувачів;

-запобігання несанкціонованій зміні або знищенню інформації.

Для досягнення цих цілей застосовуються різноманітні методи та технології, серед яких:

-криптографічний захист (шифрування даних);

-цифрові підписи для підтвердження автентичності інформації;

-системи резервного копіювання для відновлення даних;

-контроль доступу до інформаційних ресурсів.

Особливо важливою є роль криптографії, оскільки вона дозволяє забезпечити захист інформації навіть у випадку її перехоплення. У зашифрованому вигляді дані залишаються недоступними для сторонніх осіб без відповідного ключа дешифрування.

Отже, захист інформації є фундаментальним елементом кібербезпеки, оскільки саме дані є основним об’єктом потенційних атак.

3.3. Захист користувачів та людський фактор

Третім ключовим напрямом кібербезпеки є захист користувачів. цей аспект має особливе значення, оскільки більшість кіберінцидентів у сучасних умовах пов’язана саме з людським фактором. Навіть найсучасніші технічні системи не можуть повністю гарантувати безпеку, якщо користувачі не дотримуються базових правил кібергігієни. Помилки, необережні дії або недостатній рівень обізнаності можуть стати причиною витоку інформації або компрометації системи.

До найпоширеніших ризиків, пов’язаних із користувачами, належать:

-використання слабких або повторюваних паролів;

-відкриття фішингових електронних листів;

-перехід за підозрілими посиланнями;

-встановлення неперевіреного програмного забезпечення;

-передача облікових даних стороннім особам.

Для мінімізації цих ризиків застосовуються такі заходи:

-навчання користувачів основам кібербезпеки;

-формування навичок розпізнавання кіберзагроз;

-використання багатофакторної автентифікації;

-впровадження політик безпечного використання систем.

Таким чином, користувачі є не лише потенційним джерелом ризику, але й важливою складовою системи захисту, якщо вони належним чином підготовлені.

РОЗДІЛ 2. ОБЛІКОВІ СИСТЕМИ ЯК ОБ'ЄКТ КІБЕРЗАХИСТУ

2.1. Сутність і роль облікових систем

Облікові системи — це спеціалізовані програмні комплекси, які використовуються для автоматизації процесів обліку в організаціях і на підприємствах. Якщо говорити простіше, це цифрові системи, в яких зберігається та обробляється вся основна інформація про діяльність компанії, але в академічному розумінні вони являють собою комплексні інформаційні середовища, що забезпечують систематизовану роботу з даними та підтримують управлінські процеси. У таких системах фіксуються всі основні дані, які необхідні для функціонування організації. Зокрема, це фінансові операції, тобто доходи і витрати, бухгалтерський облік, нарахування заробітної плати працівникам, формування податкової та фінансової звітності. Окрім цього, облікові системи можуть містити інформацію про клієнтів, постачальників, контрагентів, товари, складські запаси та інші ресурси підприємства.

Таким чином, облікова система виступає як централізоване середовище зберігання та обробки даних, яке об'єднує різні напрями є діяльності організації в єдину інформаційну структуру.

Головна перевага облікових систем полягає в автоматизації великої кількості рутинних процесів. Завдяки цьому значно зменшується кількість помилок, які можуть виникати при ручному введенні даних, а також суттєво прискорюється обробка інформації. Це особливо постійно зростає. Крім того, використання облікових систем дозволяє забезпечити більш точний контроль за фінансовими та матеріальними ресурсами підприємства. Інформація в таких системах оновлюється в режимі реального часу, що дає можливість оперативно приймати управлінські рішення. Як приклади облікових систем можна назвати 1С:Підприємство, яка широко використовується в бухгалтерському обліку, особливо в країнах Східної Європи. Також існують міжнародні системи, наприклад SAP або Microsoft Dynamics 365, які застосовуються у великих корпораціях для комплексного управління бізнес-процесами. Для малого та середнього бізнесу часто використовуються простіші рішення, такі як QuickBooks, які дозволяють вести фінансовий облік і звітність без складної інфраструктури. Водночас важливо розуміти, що облікові системи містять дуже чутливу та конфіденційну інформацію. Це

означає, що будь-які порушення їх роботи або несанкціонований доступ можуть призвести до серйозних наслідків. Серед таких наслідків можна виділити фінансові втрати, витік даних, порушення внутрішніх процесів організації або навіть повну зупинку діяльності підприємства.

Саме тому облікові системи є критично важливою складовою сучасного бізнесу. Вони не лише спрощують управління організацією та автоматизують обробку даних, але й потребують високого рівня захисту, оскільки є одним із основних об’єктів кіберзагроз у сучасному цифровому середовищі.

Отже, облікові системи можна розглядати як ключовий інструмент управління підприємством, який поєднує в собі функції обліку, аналізу та підтримки прийняття рішень, забезпечуючи ефективну роботу організації в умовах цифрової економіки.

РОЗДІЛ 3. КІБЕРБЕЗПЕКА ОБЛІКОВИХ СИСТЕМ:ЗАГРОЗИ ТА ЗАХИСТ

3.1. Кіберзагрози в облікових системах

У сучасних умовах облікові системи займають центральне місце в інформаційній інфраструктурі підприємств, оскільки саме в них накопичується, обробляється та зберігається великий обсяг важливої інформації. До такої інформації належать фінансові дані, бухгалтерська звітність, відомості про клієнтів і працівників, а також внутрішні документи організації. Саме тому такі системи є постійною ціллю для різноманітних кіберзагроз, які можуть мати як технічний, так і організаційний характер.

Одним із найпоширеніших видів загроз є фішингові атаки. Вони полягають у спробах обману користувачів із метою отримання конфіденційної інформації, наприклад логінів і паролів. Найчастіше це відбувається через підроблені електронні листи, повідомлення або сайти, які візуально майже не відрізняються від справжніх. Користувач, не підозрюючи небезпеки, може самостійно передати зловмисникам доступ до системи. Ще однією серйозною загрозою є шкідливе програмне забезпечення. До нього належать віруси, трояни, шпигунські програми та інші типи шкідливих кодів. Таке програмне забезпечення може проникати в систему через завантаження файлів, електронну пошту або вразливості в програмному забезпеченні. Його наслідками можуть бути викрадення даних, пошкодження файлів, порушення роботи системи або повна її недоступність. Особливо небезпечними є ransomware-атаки, коли дані шифруються, а за їх відновлення вимагається викуп.

Також важливою загрозою є несанкціонований доступ до облікових систем. Він може виникати через використання слабких паролів, повторне використання однакових паролів, помилки користувачів або недостатній рівень захисту системи. У таких випадках сторонні особи можуть отримати повний або частковий доступ до конфіденційної інформації, змінювати її або використовувати у власних цілях.

Окремо слід виділити витоки інформації, які можуть бути як навмисними, так і випадковими. Наприклад, дані можуть бути викрадені внаслідок кібератаки або оприлюднені через технічні помилки, неправильні налаштування системи чи людський фактор. Наслідки таких витоків можуть

бути дуже серйозними, особливо як що йдеться про фінансові або персональні дані.

Крім того, існують атаки типу DDoS, які спрямовані на перевантаження системи великою кількістю запитів. У результаті система може працювати повільно або взагалі стати недоступною для користувачів, що призводить до зупинки бізнес-процесів.

Таким чином, кіберзагрози для облікових систем є різноманітними, постійно розвиваються та стають більш складними, що потребує постійного вдосконалення систем захисту.

3.2. Захист облікових систем від кіберзагроз

Отже, ми розглянули основні види кіберзагроз, які можуть впливати на роботу облікових систем, а також можливі наслідки їх виникнення. Виходячи з цього, логічно постає наступне питання: яким чином забезпечити захист таких систем і зменшити ризики їхнього порушення?

Для відповіді на це необхідно розуміти, що захист облікових систем — це не один конкретний інструмент, а комплекс взаємопов'язаних заходів, які працюють одночасно і доповнюють один одного. Саме такий підхід дозволяє створити багаторівневу систему безпеки, яка ускладнює або повністю унеможливлює реалізацію кіберзагроз.

Одним із базових і водночас найважливіших методів захисту є використання складних паролів. Вони повинні містити комбінацію літер різного регістру, цифр і спеціальних символів, що значно ускладнює їх підбір сторонніми особами. Проте одного пароля не достатньо, тому додатково використовується багатофакторна автентифікація, яка передбачає підтвердження входу через кілька рівнів перевірки, наприклад за допомогою одноразового коду або мобільного пристрою.

Ще одним важливим елементом є шифрування даних. Його суть полягає в тому, що інформація перетворюється у спеціальний формат, який неможливо прочитати без відповідного ключа. Це дозволяє захистити дані навіть у випадку їх перехоплення або несанкціонованого доступу.

Велику роль відіграє також контроль доступу до системи. Він передбачає обмеження прав користувачів відповідно до їхніх посадових обов'язків. Іншими словами, кожен користувач має доступ лише до тієї інформації, яка

необхідна йому для виконання роботи, що зменшує ризик як зовнішніх, так і внутрішніх загроз.

Окрім цього, використовуються антивірусні програми та системи виявлення вторгнень, які дозволяють оперативно виявляти підозрілу активність і блокувати потенційні атаки. Такі засоби постійно оновлюються, щоб ефективно протидіяти новим типам шкідливого програмного забезпечення.

Не менш важливим є регулярне оновлення програмного забезпечення, оскільки саме через застарілі версії систем часто виникають уразливості, які можуть бути використані зловмисниками.

Також варто враховувати людський фактор. Тому важливим елементом захисту є навчання користувачів основам кібербезпеки, щоб вони могли розпізнавати потенційно небезпечні повідомлення, уникати фішингових атак і правильно поводитися з конфіденційною інформацією.

Таким чином, ефективний захист облікових систем можливий лише за умови комплексного підходу, який поєднує технічні засоби, організаційні заходи та обізнаність користувачів. Саме це дозволяє забезпечити стабільну, безпечну та безперебійну роботу систем у сучасному цифровому середовищі.

3.3. Кібербезпека в Україні

Кібербезпека в Україні сьогодні є однією з ключових складових національної безпеки, оскільки все більше сфер життя переходять у цифровий формат. Це означає, що державні послуги, фінансові операції, медичні дані, освітні платформи та інші важливі процеси все частіше зберігаються і обробляються в електронних інформаційних системах. Саме тому захист таких систем набуває критично важливого значення. Йдеться не лише про окремі підприємства чи приватні компанії, а й про державні ресурси, об’єкти критичної інфраструктури, енергетичний сектор, банківську систему та інші стратегічно важливі сфери, від стабільної роботи яких безпосередньо залежить функціонування країни в цілому.

В Україні функціонують спеціалізовані структури, які відповідають за забезпечення кіберзахисту. Наприклад, кіберполіція займається виявленням, попередженням і розслідуванням кіберзлочинів, а також реагуванням на випадки порушення інформаційної безпеки. Окремо діє CERT-UA — команда

реагування на комп'ютерні надзвичайні події, яка здійснює моніторинг кіберінцидентів, аналізує загрози, координує дії під час атак і допомагає відновлювати роботу систем після інцидентів. Водночас варто зазначити, що Україна регулярно стикається з кібератаками різного рівня складності. Це можуть бути як масові атаки на державні вебресурси, так і цілеспрямовані спроби втручання в роботу інформаційних систем або об'єктів критичної інфраструктури. Мета таких атак може бути різною — від викрадення конфіденційної інформації до повного порушення або блокування роботи систем. Через це в Україні постійно посилюється система кіберзахисту. Впроваджуються сучасні технології безпеки, удосконалюються системи моніторингу та реагування на загрози, а також підвищується рівень цифрової грамотності користувачів, оскільки саме людський фактор часто є одним із найслабших елементів у системі безпеки.

Кібербезпека в Україні сьогодні є динамічною та безперервно розвиваючою сферою, яка змінюється разом із розвитком цифрових технологій. Чим більше процесів переходить в онлайн-середовище, тим більшу роль відіграє захист інформації та стабільна робота інформаційних систем.

Таким чином, можна зробити висновок, що кібербезпека вже стала невід'ємною частиною сучасного життя як для держави, так і для бізнесу та кожного користувача. Вона перестала бути додатковим елементом і фактично перетворилася на базову умову стабільного функціонування цифрового суспільства. У зв'язку з цим розвиток кіберзахисту, постійне вдосконалення технологій безпеки та підвищення обізнаності користувачів залишаються одними з ключових і пріоритетних напрямів у сучасній Україні.

Висновок

Сьогодні кібербезпека є однією з найважливіших складових сучасного цифрового суспільства, оскільки майже всі сфери життя поступово переходять в електронний формат. З кожним роком зростає залежність людей, організацій та держави від інформаційних технологій. Електронні сервіси використовуються для зберігання та обробки даних, здійснення фінансових операцій, надання державних послуг, ведення бізнесу, навчання та комунікації. Усе це формує єдиний цифровий простір, у якому інформація стає одним із найцінніших ресурсів.

Разом із розвитком цифрових технологій зростає і кількість кіберзагроз. Це пов’язано з тим, що будь-яка система, яка працює з інформацією, потенційно може стати об’єктом атак.

Серед основних загроз можна виділити злами інформаційних систем, несанкціонований доступ до даних, вірусні та шкідливі програми, фішингові атаки, витоки конфіденційної інформації, а також цілеспрямовані кібератаки на сервери та мережеву інфраструктуру. Подібні загрози можуть призводити до серйозних наслідків, включаючи втрату даних, фінансові збитки, порушення роботи організацій та зниження рівня довіри користувачів до цифрових систем.

Особливо важливу роль у цьому контексті відіграють облікові системи, оскільки саме в них зберігається та обробляється велика кількість критично важливої інформації. До такої інформації належать фінансові дані підприємств, бухгалтерська звітність, відомості про клієнтів і працівників, а також внутрішні управлінські документи. Через це облікові системи є одними з найвразливіших елементів інформаційної інфраструктури організацій і водночас однією з основних цілей для кіберзлочинців. Будь-яке порушення цілісності або доступності таких систем може мати серйозні наслідки. Наприклад, несанкціоноване втручання може призвести до викрадення фінансової інформації, зміни або видалення даних, блокування доступу до системи або повного зупинення роботи підприємства. У результаті це може викликати не лише прямі фінансові втрати, але й втрату ділової репутації,

зниження довіри з боку клієнтів та партнерів, а також довготривалі проблеми в роботі організації.

У зв'язку з цим питання кібербезпеки набуває особливої актуальності. Сьогодні вона розглядається не як допоміжний елемент, а як необхідна умова стабільного функціонування будь-яких інформаційних систем. Кібербезпека включає комплекс технічних, програмних та організаційних заходів, спрямованих на захист даних, систем і користувачів від потенційних загроз. Вона забезпечує не лише захист інформації, але й стабільність, безперервність та надійність роботи цифрових систем.

Крім того, важливо розуміти, що кіберзагрози постійно розвиваються та стають більш складними. Зловмисники використовують нові технології, автоматизовані методиатак і соціальну інженерію, що робить традиційні методизахисту недостатніми. Саме тому системи кібербезпеки повинні постійно вдосконалюватися, оновлюватися та адаптуватися до нових умов цифрового середовища.

Отже, можна зробити загальний висновок, що кібербезпека є невід'ємною частиною сучасного інформаційного суспільства. Вона забезпечує захист даних, стабільну роботу цифрових систем і безпеку користувачів. Особливо важливою вона є для облікових систем, які містять критично важливу інформацію та потребують підвищеного рівня захисту.

Таким чином, у сучасних умовах розвиток кібербезпеки, впровадження сучасних технологій захисту та підвищення цифрової грамотності користувачів є одними з ключових напрямів, від яких залежить безпечне функціонування як окремих організацій, так і суспільства в цілому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 1С:Підприємство. URL: https://1c.livesta.com.ua/unf/uk_UA/ (дата звернення: 30.04.2026)
2. SAP. URL: https://www.sap.com/centralasiacaucasus/products/trysap.html?sort=latesdesc (дата звернення: 30.04.2026)
3. QuickBooks. URL: https://quickbooks.intuit.com/global/login/ (дата звернення: 1.05.2026)
4. CERT-UA. URL: https://cert.gov.ua/ (дата звернення: 1.05.2026)