Змістовий модуль 3
Безпека облікових процесів в умовах їх цифровізації.

Тема 4. Безпека та управління даними в цифровому обліку

Мета вивчення теми

Метою вивчення теми є ознайомлення студентів із сучасними підходами до забезпечення безпеки даних у цифрових системах обліку, а також управління інформацією, яка генерується, зберігається і використовується в процесах бухгалтерського обліку. Студенти повинні зрозуміти основні загрози для безпеки даних, методи захисту інформації та важливість дотримання стандартів безпеки при роботі з обліковими даними.

Питання для самостійного вивчення

1. Які основні загрози безпеці даних у цифрових облікових системах?
2. Які інструменти та технології використовуються для забезпечення безпеки даних в обліку?
3. Як впроваджуються політики захисту даних на підприємствах для захисту фінансової інформації?
4. Що таке криптографія та як вона застосовується для захисту даних в облікових системах?
5. Які стандарти та регуляторні вимоги необхідно дотримуватися для забезпечення безпеки даних у фінансових системах?

Ключові терміни та поняття: *захист даних, цифрова трансформація, кібербезпека, персональні дані, кібератаки, штучний інтелект, блокчейн, управління доступом до даних, інтегрованість даних, кібербезпека, інформаційна безпека, стандарти, регулювання, МСФЗ, GDPR, COSO.*

Методичні рекомендації

При опрацюванні **першого питання** необхідно звернути увагу на те, що В епоху цифрової трансформації облікові системи стали вразливішими до різноманітних кіберзагроз, таких як хакерські атаки, фішинг, зломи систем тощо. Для захисту облікових даних використовуються різні технології, серед яких криптографія, автентифікація користувачів та багаторівневі системи захисту доступу до даних. Кожна облікова система повинна відповідати високим стандартам безпеки, аби гарантувати збереження фінансової інформації та запобігти фінансовим втратам.

Одним із важливих аспектів безпеки є управління даними. Підприємства повинні розробляти політики управління даними, які охоплюють їх збирання, зберігання, використання та знищення. Ці політики повинні бути чітко регламентовані та відповідати міжнародним стандартам, таким як GDPR для захисту персональних даних.

Значну роль у безпеці даних відіграють резервні копії (бекапи), які дозволяють відновити інформацію у разі втрати або пошкодження основних даних. Зважаючи на стрімке збільшення обсягів цифрової інформації, правильне управління та захист даних стають стратегічним завданням для будь-якої організації.

Питання для самоконтролю

1. Які основні методи захисту даних у цифрових облікових системах?
2. Як кіберзагрози можуть вплинути на безпеку облікових даних?
3. Що таке криптографія, і як вона застосовується в бухгалтерському обліку?
4. Які регуляторні стандарти забезпечують захист персональних даних у фінансових системах?
5. Як регулярне резервування даних допомагає зберігати їхню безпеку?

Завдання

1. Проведіть аналіз кіберзагроз, з якими може зіткнутися сучасне підприємство, що використовує цифрові облікові системи. Запропонуйте стратегії захисту від цих загроз.
2. Розробіть політику управління даними для середнього підприємства, враховуючи зберігання, обробку та захист облікових даних відповідно до міжнародних стандартів (наприклад, GDPR).
3. Здійсніть дослідження ефективності використання криптографії для захисту облікових даних. Оцініть, наскільки криптографічні методи зменшують ризики несанкціонованого доступу до фінансової інформації.