DOI: https://doi.org/10.36059/978-966-397-332-6-59

ПРИНЦИПИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ДАНИХ В КОНТЕКСТІ ВИКЛАДАННЯ ОБЛІКОВИХ ДИСЦИПЛІН

Сімаков К.І.
кандидат економічних наук, доцент,
доцент кафедри обліку, оподаткування та економічної безпеки
Донбаської державної машинобудівної академії
м. Краматорськ, Україна

Інформаційна діяльність відіграє важливу роль у прогресі та розвитку сучасного суспільства. Вона виступає каталізатором для поширення знань, покращення освіти та науки, а також прискорює розвиток інновацій та технологій, є потужним інструментом для розбудови суспільства, основаного на знаннях, розумінні та відкритому діалозі [1].

Викладання облікових дисциплін може включати різні аспекти. Основні етапи викладання облікових дисциплін у розрізі автоматизації обліку та інформаційної безпеки повинні включати такі елементи як: розвиток практичних навичок та використання додаткових навчальних ресурсів – проведення практичних занять з використанням реальних облікових програм або електронних таблиць; вирішення практичних завдань, ситуаційних задач або кейсів; залучення до виконання проектів або досліджень з обліку; використання відеолекцій, онлайн-курсів та вебінарів; запрошення гостей з практичного бізнесу для проведення лекцій або майстер-класів.

Ці етапи можуть варіюватися залежно від конкретних вимог навчального закладу та програми курсу. Викладання облікових дисциплін має на меті формування у студентів знань та навичок з обліку, що допоможуть їм у майбутній професійній діяльності.

Планування та організація навчального процесу обов’язково повинні включати форми та методи навчання (лекції, практичні заняття, семінари, лабораторні роботи тощо) пов’язані з загальними принципами безпеки інформації. Кожна з цих секцій може бути доповнена конкретними прикладами та ілюстраціями для забезпечення повнішого розуміння принципів безпеки інформаційних даних у контексті викладання облікових дисциплін.

Здобувач повинен розуміти систему впровадження політик та процедур безпеки, які визначають правила для взаємодії з бухгалтерською інформацією.

Виникає необхідність обмеження інформації про діяльність підприємства з комерційної таємниці та питання збереження, обмеження доступу, належного використання. Для забезпечення безпеки інформаційних даних у контексті облікових дисциплін, важливо використовувати ефективні технічні та організаційні заходи [2].

Захист конфіденційності: У контексті облікових дисциплін, інформаційні дані можуть включати фінансову інформацію, персональні дані клієнтів, бухгалтерську звітність та інші конфіденційні дані. Збереження конфіденційності цих даних є критично важливим для запобігання несанкціонованому доступу, крадіжці ідентифікаційних даних та фінансовим зловживанням. Порушення конфіденційності може призвести до серйозних наслідків, включаючи фінансові втрати та втрату довіри з боку клієнтів [3].

Контроль доступу до інформації та захист облікових записів. Мета контролю доступу – забезпечення конфіденційності, цілісності і доступності інформації, а також захист від несанкціонованого доступу чи атак, відповідно законодавчим вимогам і стандартам безпеки, таким як GDPR, HIPAA, або ISO/IEC 27001.

Основні аспекти контролю доступу до облікової інформації включають:

Ідентифікація користувачів: Цей етап передбачає ідентифікацію особи, яка намагається отримати доступ до облікових даних. Ідентифікація зазвичай відбувається за допомогою унікального ідентифікатора, такого як логін або ім’я користувача.

Аутентифікація користувачів: Після ідентифікації особи, процес аутентифікації перевіряє, чи є вона дійсною користувачем, якому дозволяється отримати доступ до облікових даних. Зазвичай цей процес включає введення пароля або використання інших факторів аутентифікації, таких як біометричні дані або токени безпеки.

Авторизація доступу: Після успішної аутентифікації користувача система перевіряє, до яких облікових даних цей користувач має доступ і які дії він може здійснювати з цими даними. Авторизація визначає права та привілеї, які надаються користувачу відповідно до його ролі або функціональних обов’язків.

Моніторинг та аудит доступу: Для забезпечення контролю над доступом до облікової інформації важливо вести моніторинг та аудит всіх дій, здійснених користувачами. Це допомагає виявити незвичайну або підозрілу активність, виявити можливі порушення безпеки та встановити відповідальних осіб.

Фізична безпека: Крім електронних заходів безпеки, також важливо забезпечити фізичну безпеку облікової інформації. Це може включати захист серверних приміщень, обмеження фізичного доступу до

комп'ютерів та інших пристроїв з обліковими даними, а також використання захисних засобів, таких як замки, картки доступу тощо.

Ефективний контроль доступу до облікової інформації забезпечує захист від несанкціонованого доступу, зловживань та витоку даних.

Забезпечення цілісності облікових даних: на підприємствах та в установах цілісність інформаційних даних є важливою для забезпечення точності та достовірності фінансової звітності та інших облікових записів. Порушення цілісності може призвести до спотворення даних, помилок в обліку та неправильних фінансових рішень. Захист цілісності даних передбачає застосування механізмів контролю та захисту, таких як використання цифрових підписів, контроль доступу та резервне копіювання, захист мережевих ресурсів та серверів, фільтрування мережного трафіку та виявлення вторгнень у систему, регулярне створення резервних копій, план відновлення даних.

Захист облікових записів – контроль доступу до облікової інформації – це процес обмеження та регулювання, які особи мають право отримати доступ до облікових даних і які дії вони можуть здійснювати з цими даними. Контроль доступу є важливою складовою безпеки інформації і має на меті забезпечення конфіденційності, цілісності та доступності облікових інформації.

Проведення навчань для співробітників з питань безпеки інформації, а також надання рекомендацій щодо збереження конфіденційності.

Загальна мета безпеки інформаційних даних у контексті облікових дисциплін полягає в тому, щоб забезпечити конфіденційність, цілісність та доступність цих даних. Ці умови допомагають забезпечити правильне функціонування облікової системи, захистити інтереси клієнтів та забезпечити довіру до фінансової звітності та обліку в цілому.

Список використаних джерел:

1. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.

2. Нонік В.В., Дикий А.П., Дика О.С. Інформаційна модель управління економічною безпекою суб'єктів господарювання : монографія. Житомир : Вид. О.О. Євенок, 2017. 248 с.

3. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.