УДК 657.1.011.56:378

О.М. Бунда

bundaolga@yahoo.com

*Київський національний університет технологій та дизайну, Київ*

# ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМИ БУХГАЛТЕРСЬКОГО ОБЛІКУ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Глобалізація та діджиталізація економіки сприяють швидкому розвитку новітніх інтегрованих систем обробки та зберігання облікової інформації та вимагають не тільки організації належної інформаційної безпеки діяльності підприємств, але передусім інформаційної безпеки діяльності закладів вищої освіти як в Україні, так і у світі.

Вплив інтегрованих систем обробки та зберігання інформації на обліково-аналітичне забезпечення та інформаційну безпеку підприємств і організацій досліджено вітчизняними та зарубіжними науковцями: Дж. Андресс, М. Бішоп, Т. Бочуля, С. Василишин, В. Гребенніков, В. Дерій, Г. Кононенко, А. Крутова, В. Муравський, Д. Тепскот та ін. Однак виникає необхідність дослідження питань побудови і функціонування систем захисту бухгалтерських даних в умовах застосування інтегрованих систем обробки та зберігання облікової інформації у закладах вищої освіти.

Для цього насамперед необхідно забезпечити високий рівень інформаційної безпеки інтегрованих систем обробки та зберігання облікової інформації у закладах вищої освіти.

Інформаційна безпека – це оптимальний стан стабільності і захищеності інформаційної оболонки підприємства, який унеможливлює її втрату, несанкціоноване розповсюдження та забезпечує її захист в інтересах власників підприємства чи держави [1, с. 102].

Інформаційна безпека – це одне з найважливіших завдань, що стоять перед підприємствами, що здійснюють міжнародне співробітництво [2, с. 115].

Міжнародне співробітництво є одним із вагомих аспектів функціонування і стратегічного розвитку діяльності закладів вищої освіти в умовах глобалізації.

При побудові системи інформаційної безпеки закладам вищої освіти необхідно враховувати ряд особливостей. У сучасному вузі зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням навчального процесу, а й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація [3, с. 125].

Інформаційна безпека системи бухгалтерського обліку у закладах вищої освіти передбачає впровадження та управління необхідними заходами безпеки, які включають в себе виявлення широкого діапазону загроз, з метою забезпечення досягнення стратегічних завдань і безперервності діяльності закладів вищої освіти.

Інформаційна безпека системи бухгалтерського обліку у закладах вищої освіти досягається застосуванням відповідних критеріїв захисту облікової інформації, визначених за допомогою процесу управління ризиками і керованого з використанням системи управління інформаційної безпеки, включаючи політики, процеси, процедури, організаційні структури, програмні та апаратні засоби, щоб захистити облікові інформаційні масиви даних.

Ці заходи захисту повинні бути визначені, реалізовані, проконтрольовані, перевірені і при необхідності поліпшені, щоб гарантувати, що рівень інформаційної безпеки системи бухгалтерського обліку у закладах вищої освіти відповідає стратегічним цілям. Відповідні заходи і засоби інформаційної безпеки системи бухгалтерського обліку слід органічно інтегрувати у загальну систему інформаційної безпеки у закладах вищої освіти [4, с. 115].

Система інформаційної безпеки закладів вищої освіти базується на таких принципах:

1. Цілісність даних – захист від збоїв, що призводять до втрати інформації, а також захист від неавторизованого створення або знищення даних.
2. Конфіденційність даних.
3. Доступність даних для всіх авторизованих користувачів [5, с. 4–5; 6, с. 4–6].

Дані принципи інформаційної безпеки необхідно враховувати при застосуванні бухгалтерських інформаційних систем в закладах вищої освіти.

Бухгалтерські інформаційні системи – це інформаційні системи, які здійснюють збір даних про бізнес-процеси підприємства та необхідні зовнішні дані, виконання процедур їх обробки, забезпечуючи створення необхідної інформації для різних груп внутрішніх і зовнішніх користувачів та її представлення в необхідному вигляді.

Наприклад, для збору внутрішніх даних використовуються системи документообігу, для збору зовнішніх даних – бази даних, вебсторінки клієнтів, інших видів зовнішніх контрагентів. Для

перетворення даних на облікову інформацію на основі використання бухгалтерської методології, що базується на системі подвійного запису, застосовується прикладне бухгалтерське програмне забезпечення, яке дозволяє забезпечити представлення кінцевої облікової інформації у вигляді фінансової, управлінської та податкової звітності. Як додаткові засоби представлення облікової інформації, її консолідації, передачі та обміну можуть використовуватися спеціалізовані вебресурси, сервіси та платформи, стандарти обміну діловою інформацією (XBRL) та електронні формати її представлення (ESEF) [7, с. 67].

У закладах вищої освіти можлива низка як внутрішніх, так і зовнішніх загроз безпеки інформації: спроби несанкціонованого адміністрування баз даних; дослідження мереж, несанкціонований запуск програм з аудиту мереж; видалення інформації, у тому числі бібліотек; запуск на виконання ігрових програм; установка вірусних програм і троянських коней; сканування мереж, у тому числі інших організацій через Інтернет; несанкціоноване використання з Інтернету неліцензійного програмного забезпечення та інсталяція його на робочі станції; спроби несанкціонованого віддаленого адміністрування операційних систем; сканування портів тощо [8].

У загальному вигляді і відповідно до міжнародних стандартів управління ризиками інформаційної безпеки навчального закладу передбачає: визначення основних цілей і завдань захисту інформаційних активів закладів; створення ефективної системи оцінки та управління ризиками інформаційної безпеки; розрахунок сукупності деталізованих якісно, а при можливості і кількісно оцінок ризиків; застосування спеціального інструментарію оцінки та управління ризиками із використанням для моделювання причинних взаємозв'язків, виявлених між концептами деякої області інформаційних і технічних аспектів закладів вищої освіти [3].

У Державному стандарті України „Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 формулювання класифікації загроз відсутнє, проте передбачено можливі шляхи їх реалізації, що дозволяє визначити ймовірні загрози і ввести різні класифікаційні ознаки їх проявів в інформаційній безпеці.

Для мінімізації впливу загроз в інформаційній безпеці системи бухгалтерського обліку закладам вищої освіти необхідно:

1. Визначити внутрішніх та зовнішніх користувачів інтегрованих систем обробки та зберігання облікової інформації і адміністраторів, необхідних для захисту комп'ютерних систем та мереж, усіх облікових даних та додаткової інформації у будь-якій формі представлення і їх передачі;

2. Сформувати алгоритми виконання конкретних посадових обов'язків кожним працівником закладу вищої освіти, який має доступ до роботи з інтегрованими системами обробки та зберігання облікової інформації, визначити рівень його відповідальності при виникненні ризиків втрати безпеки облікових даних та додаткової інформації;

3. Охарактеризувати процедури, які сприятимуть мінімізації та уникненню загроз та ризиків втрати (або зниження рівня) безпеки облікових даних та додаткової інформації, а також способів боротьби з ними при їх виникненні.

4. Забезпечити дотримання принципів системи інформаційної безпеки при застосуванні бухгалтерських інформаційних систем в закладах вищої освіти.

ЛІТЕРАТУРА:

1. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник Економіки*. 2021. No. 1. С. 97–110. URL: http://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1218.

2. Бунда О. М. Аудит інформаційної безпеки міжнародних договорів. *Імперативи економічного зростання в контексті реалізації глобальних цілей сталого розвитку*: тези доповідей Міжнародної науково-практичної Інтернет-конференції, присвяченої 90-річчю Київського національного університету технологій та дизайну (м. Київ, 9 квітня 2020 року). Київ: КНУТД, 2020. С. 115–117.

3. Кононенко Г. І. Проблеми інформаційної безпеки вищої освіти в умовах глобалізації. *Матеріали Міжнародної науково-практичної конференції «Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації»*: тези доповідей (м. Київ, 4 жовтня 2019 р.). Київ: КНУТД, 2019. С. 125–126.

4. Гребенніков В. Політика управління інформаційною безпекою. URL: https://beasthackerz.ru/uk/audio/politika-upravleniya-informacionnoi-bezopasnostyu-sistema-upravleniya.html.

5. Andress J. Foundations of information security. A Straightforward Introduction. San Francisco: No Starch Press, 2019. 222 p.

6. Bishop M. Computer Security. Art and Science. 2nd ed.; with contributions from E. Sullivan and M. Ruppel. Pearson Education, Inc, 2019. 1384 p.

7. Легенчук С. Ф.. Царук І. М., Назаренко Т. П. Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування*. 2021. No. 2 (96). С. 61–69. URL: http://ema.ztu.edu.ua/article/view/236861.

8. Кухарська Н. П. Оцінка інформаційного середовища вищих навчальних закладів та аналіз загроз його безпеці. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/760/1/21.pdf.