Купчик Н.С., здобувач
Кльоц Ю.П., к.т.н., доцент
Хмельницький національний університет

ПРОБЛЕМИ СТВОРЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Захист інформації на сьогоднішній день є одним з найважливіших заходів при провадженні діяльності з різного роду відомостями. В залежності від ступеня важливості даних застосовуються різні методи, засоби та заходи захисту. На законодавчому рівні в Україні визначено ряд заходів, які регламентують захист інформації. Одним з таких заходів є впровадження комплексних систем захисту інформації. Впровадження комплексних систем захисту інформації запобігає неконтрольованому витоку даних через технічні канали та несанкціонованому доступу. Відповідно до потреб установи та вимог законодавства застосовуються необхідні заходи безпеки [1]. Так до прикладу, захист інформації від витоку технічними канали необхідно забезпечити тільки в тих випадках, коли там циркулює інформація, що становить державну таємницю або коли є відповідне рішення розпорядника інформації [2].

Заклади вищої освіти обробляють значний обсяг інформації з обмеженим доступом, зокрема персональні дані учасників освітнього процесу, наукові розробки, дослідження, фінансова документація тощо. У зв'язку зі зростанням кількості кібератак, витоків технічними каналами, несанкціонованому доступу, а також дотриманням вимог законодавства України, створення комплексних систем захисту інформації у закладах вищої освіти є важливою умовою при роботі з такою інформацією.

Створення комплексних систем захисту інформації несе за собою низку проблем з якими стикаються заклади вищої освіти при спробі реалізації такого комплексного підходу захисту. Однією з найважливіших проблем є людський фактор: низька обізнаність працівників у сфері інформаційної безпеки та недостатній кадровий потенціал, який міг би провадити відповідну діяльність, адже відповідно до нормативних документів, такі працівники повинні мати необхідний рівень знань та навичок.

Наступною проблемою з якою найчастіше стикаються заклади вищої освіти є недостатнє фінансування, адже бюджети університетів не завжди передбачають значні витрати на забезпечення безпеки інформації. Проєктування, впровадження та супровід комплексних систем захисту вимагає використання ліцензійних комплексів засобів захисту, як приклад: програмне забезпечення від несанкціонованого доступу (Гриф, Лоза тощо), антивірусного програмного забезпечення, операційних систем і т.д., для яких необхідно попередньо закупити ліцензії. А за потребою, закупівля обладнання, яке забезпечуватиме ефективний захист від витоку технічними каналами, як приклад: генератори шуму, засоби мережевого захисту, засоби відеонагляду тощо. Необхідно враховувати і те, що навіть після впровадження комплексних систем захисту інформації потрібні кошти на її оновлення, аудит та адміністрування. Ще однією важливою умовою, що має зв'язок з вище наведеною проблемою, є забезпечення належної оплати праці працівникам, які виконують усі необхідні заходи.

Також однією з поширених проблем є застаріла нормативна документація у сфері технічного захисту інформації та відсутність необхідних вимог до розробки окремих документів, як приклад відповідно до нормативного документу «Програми й методики випробувань» необхідно розробляти та оформляти відповідно до РД 50-34.698 [3], який на даний момент часу має невизначений статут та є наявний тільки російською мовою, що в свою чергу потребує залучення профільних фахівців та розроблення власної структури документа.

Основними шляхами вирішення вище наведених проблем є підвищення рівня обізнаності працівників шляхом навчання та підготовки кадрів, співпраця з фахівцями у галузі інформаційної безпеки, збільшення фінансування кібербезпеки, що дозволить здійснювати закупівлю необхідного програмного і апаратного забезпечення та належну оплату праці спеціалістів.

Список використаних джерел:

1. Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

2. Постанова Кабінету Міністрів України від 29 березня 2006р. №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 10.03.2025).

3. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 11.03.2025).