ПІДГОТОВКА МАЙБУТНІХ ФАХІВЦІВ ДО ІНТЕГРАЦІЇ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ У СФЕРІ ЕЛЕКТРОНІКИ ТА МЕТРОЛОГІЇ

TRAINING OF FUTURE SPECIALISTS TO INTEGRATE MODERN METHODS OF DATA PROTECTION IN THE FIELD OF ELECTRONICS AND METROLOGY

УДК 378.147:004.056.5:621.3
DOI https://doi.org/10.32782/2663-6085/2025/82.2.18

Магілевський В.В.,
аспірант кафедри менеджменту та інноваційних технологій соціокультурної діяльності, економіки та маркетингу
Українського державного університету імені Михайла Драгоманова

Актуальність дослідження полягає в необхідності удосконалення методів захисту даних у сферах електроніки та метрології, де точність і безпека обробки інформації є критичними для забезпечення ефективності роботи сучасних технологічних систем. З огляду на постійне зростання загроз у кіберпросторі, актуальним є питання підготовки фахівців, які здатні не лише теоретично розуміти основи захисту інформації, але й ефективно застосовувати ці методи в реальних умовах.

Метою статті є дослідження проблем інтеграції сучасних методів захисту даних у сфері електроніки та метрології, а також визначення шляхів підготовки фахівців для їх ефективного застосування в умовах реальних технологічних і безпекових викликів.

Для досягнення поставленої мети було використано методи аналізу навчальних програм, порівняльний метод для визначення рівня інтеграції сучасних технологій захисту даних до навчальних планів, а також метод моделювання реальних загроз для оцінки практичної підготовки студентів у сфері захисту інформації.

Результати дослідження показали, що основними проблемами є недостатнє інтегрування практичних аспектів захисту даних до навчального процесу, а також відсутність достатньої кількості практичних занять із використанням сучасних інструментів для моніторингу та аналізу загроз. У роботі виявлено, що навчальні програми часто не відповідають вимогам ринку праці та технологій, а також існують обмеження у фінансуванні на впровадження сучасних методів навчання.

Висновки дослідження засвідчили необхідність удосконалювати навчальні програми через інтеграцію сучасних методів навчання: використання реальних сценаріїв загроз, а також практичних занять із налаштування безпеки і моніторингу інформаційних систем. У роботі встановлено, що важливою умовою підготовки фахівців є співпраця між навчальними закладами та ІТ-компаніями для створення реальних сценаріїв для студентів, що дозволить формувати практичні навички.

Практична цінність роботи полягає в розроблених рекомендаціях для удосконалення навчальних програм, які можуть бути використані для підвищення ефективності підготовки фахівців у галузі інформаційної безпеки, що покращить рівень захисту даних у різних галузях економіки.

Перспективи подальших досліджень полягають у вивченні ефективності застосування новітніх методів захисту інформації та інтеграції інструментів штучного інтелекту до процесів моніторингу кіберзагроз і управління інформаційною безпекою.

Ключові слова: *інформаційна безпека, захист даних, електронні системи, метрологія, криптографія, безпечна передача даних, контролювання доступу, інформаційні технології.*

The relevance of the study lies in the need to improve data protection methods in the fields of electronics and metrology, where the accuracy and security of information processing are critical to ensure the efficiency of modern technological systems. Given the constant growth of threats in cyberspace, the issue of training specialists who are able not only to understand the basics of information protection theoretically, but also to apply these methods effectively in real life is relevant.

The purpose of the article is to study the problems of integrating modern data protection methods in the field of electronics and metrology, and to identify ways to train specialists for their effective application in the context of real technological and security challenges.

To achieve this goal, the article uses curriculum analysis methods, a comparative method to determine the level of integration of modern data protection technologies into curricula, and a method of modelling real threats to assess students' practical training in the field of information protection.

The results of the study showed that the main problems are insufficient integration of practical aspects of data protection into the educational process, as well as the lack of sufficient practical training using modern tools for monitoring and analysing threats. The study found that curricula often do not meet the requirements of the labour market and technology, and that there are funding limitations for the implementation of modern teaching methods.

The findings of the study demonstrate the need to improve curricula through the integration of modern teaching methods: the use of real-life threat scenarios, as well as practical training on setting up security and monitoring information systems. The paper establishes that an important condition for training specialists is cooperation between educational institutions and IT companies to create real-life scenarios for students, which will allow them to develop practical skills.

The practical value of the work lies in the developed recommendations for improving curricula, which can be used to increase the effectiveness of training information security specialists, which will improve the level of data protection in various sectors of the economy.

Prospects for further research are to study the effectiveness of the latest methods of information protection and the integration of artificial intelligence tools into the processes of monitoring cyber threats and information security management.

Key words: *information security, data protection, electronic systems, metrology, cryptography, secure data transmission, access control, information technology.*

Постановка проблеми. Розвиток електроніки та метрології супроводжується зростанням обсягів даних, що підлягають обробці, передачі та зберіганню. У зв'язку з цим питання їхнього захисту стає одним із ключових аспектів у підготовці майбутніх фахівців, оскільки електронні системи та метрологічні комплекси використовуються у критично важливих сферах, де порушення цілісності, достовірності або конфіденційності інформації може мати серйозні наслідки.

Використання сучасних методів захисту даних передбачає не лише володіння технологічними аспектами криптографії, шифрування, протоколів безпечного зв'язку та механізмів аутентифікації, а й розуміння нормативно-правових вимог, які регулюють захист інформації.

Упровадження відповідних підходів до підготовки спеціалістів вимагає інтеграції новітніх методів навчання, що включають моделювання загроз, роботу з реальними сценаріями кібератак, аналіз уразливостей метрологічних систем та оптимізацію алгоритмів обробки та передачі даних.

У сучасних умовах цифровізації виникає необхідність посилення міждисциплінарного підходу, який поєднує технічну підготовку з розумінням безпекових аспектів, що особливо актуально для спеціалістів у галузі електроніки та метрології. Підвищення рівня знань у цій сфері сприятиме зменшенню ризиків втрати даних, маніпуляцій із результатами вимірювань та несанкціонованого доступу до критично важливої інформації, що є важливим завданням для гарантування безпеки інформаційних і метрологічних систем.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у галузі захисту даних у сферах електроніки та метрології охоплюють кілька важливих напрямків.

Перший напрям досліджень стосується основних методів захисту даних у інформаційно-комунікаційних системах та їх застосування в електроніці та метрології. Дослідники О. Потій, Ю. Горбенко, О. Замула аналізують основні методи захисту даних, зокрема криптографію та протоколи безпеки, підкреслюючи важливість інтеграції сучасних технологій в освітній процес для підготовки фахівців [1]. Зарубіжні вчені A. Hogail, R. Abdellatif наголошують на ролі метрології для покращення захисту інформації у промислових системах, що має вирішальне значення для підготовки фахівців [2]. Автор F. Thiel розглядає цифрову трансформацію в метрології, зокрема впровадження метрологічної хмари для гарантування безпеки даних у правових системах [3]. N. Durakbasa et.al. акцентують на важливості інтеграції інтелектуальних систем для покращення якості продукції і безпеки даних у промисловому виробництві [4].

Для доповнення дослідження в цьому напрямі важливо зосередитися на удосконаленні практичних підходів до інтеграції методів захисту даних у навчальні програми, зокрема через використання реальних сценаріїв загроз і практичних кейсів.

Другий напрям досліджень зосереджується на розвитку інфраструктури для підготовки фахівців у галузі інформаційних і вимірювальних технологій. Група дослідників T. Gordiyenko, O. Velychko, I. Pototskyi, Y. Kuzmenko підкреслюють важливість створення національної інфраструктури для навчання спеціалістів з інтеграцією метрології та інформаційних технологій у навчальні програми [5]. Вчені A. Varshney, N. Garg, K. Nagla, T. Nair, S. Jaiswal, S. Yadav та D. Aswal et.al. досліджують інтеграцію сенсорних технологій до виробничих процесів, що вимагає оновлення методів захисту даних у контексті Industry 4.0 [6]. Значну увагу слід приділяти розробці стандартів та навчальних програм для підготовки фахівців, здатних працювати з новітніми сенсорами та технологіями промислового Інтернету речей, що допоможе забезпечити ефективний захист інформації у сучасному виробництві.

Третій напрям зосереджений на виявленні основних проблем, з якими стикаються спеціалісти під час упровадження методів захисту даних. Розробники A. Somkuwar, S. Satish, P. Siwach et.al. досліджують застосування метрології для гарантії безпеки даних у стратегічних секторах (енергетика), що потребує висококваліфікованих фахівців [7]. Учені T. Mustapää, J. Nummiluikki та R. Viitala розглядає цифровізацію метрології для підвищення надійності та управління вимірювальними даними в умовах промислового Інтернету речей (IoT) [8]. Дослідники V. Makarov, T. Blatova, A. Fedorov та інші підкреслюють важливість метрології для забезпечення якості продукції та послуг у цифровій економіці, що є основою для підготовки фахівців [9]. У цьому напрямі необхідно зосередитися на вирішенні практичних проблем впровадження методів захисту даних до виробничих систем та забезпеченні їх ефективного використання в реальних умовах.

Четвертий напрям базується на перспективних технологіях, які можуть бути інтегровані до навчальних програм для покращення підготовки фахівців. Дослідники K. Gogolinskiy, V. Syasko зазначають важливість інструментів неруйнівного тестування (NDT 4.0) для покращення процесу захисту даних у високих технологіях [10]. Учений S. Mekid вивчає застосування метрології в інженерії для підвищення ефективності вимірювань та захисту даних [11]. Автор W. Osten аналізує роль оптичної метрології у вимірюваннях, що має важливе значення для сучасних технологічних процесів [12]. Група вчених T.-F. Yao, L. Connolly, M. Cullinan підкреслюють важливість метрології для інспекції у нанофабрикації електронних

пристроїв, що важливо для захисту інформації на рівні високих технологій [13]. Для розвитку цього напрямку важливо фокусуватися на дослідженні новітніх інструментів для вимірювань та моніторингу стану, зокрема для безпеки даних у критичних інфраструктурах, а також інтеграції цих технологій до навчальних програм для формування практичних навичок у студентів.

Таким чином, сучасні дослідження підтверджують важливість інтеграції методів захисту даних до навчальних програм для підготовки фахівців у галузі метрології та електроніки. Однак, є потреба в додаткових дослідженнях для удосконалення освітніх підходів, упровадження новітніх технологій і практичних кейсів до навчання студентів, що дозволить забезпечити ефективну підготовку фахівців до роботи з сучасними технологіями і викликами безпеки даних.

Незважаючи на значні досягнення в дослідженні захисту інформації у сферах електроніки та метрології, існують певні прогалини, зокрема у впровадженні сучасних методів захисту даних до навчальних програм. У роботі виявлено, що навчальні заклади недостатньо інтегрують практичні аспекти захисту даних, зокрема використання реальних інструментів безпеки та моделювання реальних загроз. Більшість програм зосереджена на теоретичних засадах, що обмежує здатність студентів ефективно застосовувати ці методи в реальних умовах. Це створює потребу в удосконаленні наявних навчальних програм, щоб краще відповідати вимогам ринку праці та сучасним загрозам.

Запропоноване дослідження спрямоване на вирішення цих проблем через аналіз дійсних навчальних програм та окреслення шляхів їх удосконалення. Проведене дослідження дозволяє сформулювати конкретні рекомендації щодо інтеграції сучасних методів захисту даних до навчального процесу, зокрема через використання реальних сценаріїв загроз, інтерактивних методів навчання та сучасних інструментів для моніторингу безпеки. Це сприятиме підготовці фахівців, готових до практичних викликів, які зможуть ефективно застосовувати набуті знання у реальних ситуаціях.

Мета і завдання статті. Метою статті є дослідження проблем інтеграції сучасних методів захисту даних у сфері електроніки та метрології, а також визначення шляхів підготовки фахівців для ефективного використання цих методів у реальних умовах.

Завдання статті:

1. Проаналізувати основні методи захисту даних та оцінити потребу в їх інтеграції до навчального процесу.

2. Дослідити наявні навчальні програми, що включають сучасні методи захисту даних, та оцінити виклики у сфері підготовці фахівців.

3. Розробити рекомендації щодо удосконалення навчальних програм через інтеграцію сучасних методів навчання та моделювання реальних загроз.

Виклад основного матеріалу. У сучасному світі зростання кількості технологічних систем, які працюють з великими обсягами даних, вимагає розробки ефективних методів їх захисту.

Особливо важливим є захист даних у таких галузях як електроніка та метрологія, де точність і достовірність вимірювань та інших критичних даних є необхідними для забезпечення нормальної роботи систем і безпеки користувачів. Використання методів захисту даних у цих сферах передбачає застосування різноманітних технологій і протоколів, що забезпечують цілісність, конфіденційність і доступність інформації.

Основними методами захисту даних є криптографічні технології, які включають шифрування, підписування даних та інші методи для забезпечення конфіденційності та захисту від несанкціонованого доступу. Також використовуються протоколи безпечної передачі даних, які гарантують, що інформація, що передається між системами, не буде змінена або перехоплена третіми особами. Крім того, важливою складовою захисту є контроль доступу, що дозволяє обмежити можливості для користувачів в отриманні даних або їх заміні (табл. 1).

Використання сучасних методів захисту даних є необхідною умовою для гарантії надійності й безпеки вимірювальних та електронних систем. Шифрування даних є основним способом захисту конфіденційної інформації, що передається або зберігається, гарантуючи, що навіть у разі перехоплення переданої інформації вона залишатиметься незрозумілою без відповідного ключа доступу.

У метрології шифрування забезпечує захист результатів вимірювань та гарантує їх цілісність, що є критичним для точних вимірювань у наукових і промислових системах [13]. Підписування даних дає можливість перевірити автентичність виміряних значень, що є надзвичайно важливим у ситуаціях, коли результат вимірювання використовується для прийняття рішень, особливо у фармацевтичних чи медичних пристроях, де навіть найменша похибка може мати серйозні наслідки.

Хеш-функції створюють унікальний цифровий відбиток для конкретного обсягу даних. Це дозволяє швидко перевірити, чи було змінено вміст інформації під час зберігання або передачі. У сфері метрології хешування активно використовується для перевірки цілісності файлів калібрування, результатів вимірювань, а також для захисту програмного забезпечення від несанкціонованих змін. Завдяки своїй ефективності й невисоким обчислювальним витратам, хеш-функції

Таблиця 1

Методи захисту даних у сфері електроніки та метрології: опис і практичне застосування

Метод захисту	Опис	Застосування на практиці
Шифрування даних	Процес перетворення даних у нечитабельну форму, що робить їх зміст недоступним для сторонніх осіб навіть у разі перехоплення	Використовується для захисту вимірювальних даних у системах автоматизації та збереження даних у базах даних
Підписування даних	Технологія, що дозволяє гарантувати цілісність і автентичність даних за допомогою цифрового підпису	Використовується для підтвердження достовірності вимірів в метрології та для захисту інформації в електронних системах управління
Хешування даних	Метод створення унікального цифрового відбитка (хешу) для набору даних з метою виявлення змін або спотворень	Використовується для перевірки цілісності файлів вимірювань, даних калібрування або програмного забезпечення в електронних пристроях
Протоколи захисту передачі даних (SSL/TLS)	Протоколи для захисту даних, що передаються через мережу, забезпечуючи їх конфіденційність і цілісність	Широко застосовуються в системах віддаленого моніторингу та для передачі вимірювальних даних у реальному часі
Контроль доступу	Технологія, що визначає, які користувачі можуть отримувати доступ до певних ресурсів або змінювати дані	Використовується для обмеження доступу до критичних даних у системах автоматизованого управління та в метрологічних лабораторіях
Аудит і моніторинг	Процес спостереження за діями користувачів і систем для виявлення несанкціонованих змін або доступу	Гарантує безпеку даних в електронних системах вимірювань, дозволяючи відстежувати порушення та проводити необхідні заходи для захисту

Джерело: сформовано автором на підставі [1; 6; 7; 8; 9; 13]

стали стандартним елементом систем безпеки, які гарантують достовірність цифрової інформації.

Протоколи захисту передачі даних (наприклад, SSL/TLS) активно застосовуються у віддалених системах вимірювань, зокрема в мережах моніторингу навколишнього середовища або у виробничих процесах, де дані мають високу цінність [3]. Ці протоколи забезпечують шифрування переданої інформації, що унеможливлює її прочитання у разі перехоплення третіми особами, зберігаючи конфіденційність і цілісність даних.

Контроль доступу є ще одним важливим методом для гарантування безпеки системи, що регулює, хто може переглядати чи змінювати дані. Наприклад, у метрологічних лабораторіях часто використовуються системи контролю доступу, щоб виключно авторизовані користувачі могли змінювати параметри калібрування приладів, що знижує ймовірність помилок і маніпуляцій.

Аудит і моніторинг є важливими компонентами гарантії безпеки, оскільки дозволяють виявити будь-які спроби несанкціонованого доступу або маніпуляцій з даними. Відстеження подій у системах дозволяє оперативно виявити порушення та вжити необхідних заходів для їх усунення, що має особливе значення в умовах постійного зростання загроз кібербезпеки.

У сучасному світі інтенсивний розвиток технологій у сфері електроніки та метрології вимагає значної уваги до безпеки даних. Отже, підготовка майбутніх фахівців повинна включати знання і навички в галузі захисту даних, оскільки цей аспект стає критично важливим для забезпечення стабільної роботи систем, що використовуються в наукових, промислових та комерційних сферах.

Інтеграція методів захисту даних до навчального процесу дозволяє майбутнім фахівцям не лише здобути теоретичні знання, а й набувати практичних навичок у використанні передових технологій для забезпечення цілісності, конфіденційності та доступності інформації.

Особливу увагу потрібно приділяти впровадженню сучасних методів захисту даних: криптографія, протоколи безпечної передачі даних, контроль доступу та аудит, які слід упроваджувати до навчальних програм з підготовки фахівців у галузі електроніки та метрології. Це дозволить створити нові освітні моделі, які відповідають вимогам сучасного ринку праці та технологічним стандартам.

Однак для ефективної інтеграції цих методів необхідно врахувати специфіку галузей, де будуть працювати випускники, а також забезпечити використання реальних сценаріїв і задач у навчальних курсах. У таблиці 2 відображено основні аспекти інтеграції методів захисту даних до навчального процесу для підготовки фахівців. Інтеграція методів захисту даних до навчального процесу є надзвичайно важливою для підготовки висококваліфікованих фахівців у галузях електроніки та метрології. Викладання криптографії дає студентам розуміння основних принципів захисту

Таблиця 2

Інтеграція методів захисту даних до навчального процесу для підготовки фахівців у сфері електроніки та метрології

Метод інтеграції	Опис застосування в навчальному процесі	Практичне застосування в навчальних курсах
Викладання криптографії	Викладання основ криптографії для гарантування безпеки інформації в електронних та метрологічних системах	Лабораторні роботи, де студенти виконують шифрування даних та аналізують рівень безпеки
Інтеграція протоколів безпеки	Вивчення протоколів безпеки передачі даних, таких як SSL/TLS, для використання в реальних системах	Створення і тестування захищених каналів зв'язку для передачі вимірювальних даних
Контроль доступу	Викладання принципів контролю доступу для обмеження доступу до важливих даних	Практичні заняття з налаштування систем контролю доступу в автоматизованих системах управління
Використання технологій аудиту	Ознайомлення студентів з методами аудиту для моніторингу безпеки та виявлення порушень	Аналіз логів систем та проведення аудиту для виявлення несанкціонованих змін у даних

Джерело: сформовано автором на підставі [1; 3; 7; 8; 12]

інформації, що є важливим у будь-якій сфері, де працюють з чутливою інформацією. Лабораторні роботи з шифрування даних дозволяють студентам на практиці оволодіти методами криптографії, що гарантують безпеку в реальних умовах. Інтеграція протоколів безпеки (SSL/TLS) допомагає студентам зрозуміти, як забезпечується захищена передача даних між системами, що особливо важливо для автоматизованих систем моніторингу та вимірювань.

Заняття з контролю доступу дають можливість студентам ознайомитися з методами обмеження доступу до критичних даних, що є важливим для уникнення несанкціонованих змін у системах управління. Практичні заняття з налаштування та тестування систем контролю доступу сприяють формуванню навичок у роботі з реальними інформаційними системами.

Аудит і моніторинг є також важливими для підготовки фахівців, оскільки вони вчать студентів виявляти порушення безпеки та реагувати на них. Це допомагає підготоувати професіоналів, здатних ефективно захищати інформаційні системи в умовах постійних загроз кібербезпеки. Так, інтеграція цих методів у навчальний процес дозволить підготувати фахівців, які будуть готові до реальних викликів у сфері захисту даних.

Аналіз сучасних навчальних програм, що інтегрують новітні методи захисту даних у підготовку фахівців, є важливим кроком для оцінки стану освіти в Україні у контексті гарантії безпеки даних у сферах електроніки та метрології. З огляду на зростання потреби у кваліфікованих фахівцях цієї галузі, навчальні програми повинні бути адаптовані до вимог сучасного ринку праці та містити курси, що охоплюють технології захисту даних.

Враховуючи розвиток цифрових технологій, питання інтеграції криптографії, протоколів безпеки, контролю доступу та аудиту є надзвичайно важливими для підготовки фахівців, здатних ефективно працювати з інформацією у високотехнологічних середовищах.

Аналіз навчальних програм в Україні показує, що декілька закладів вищої освіти активно включають ці аспекти до освітніх програм. Наприклад, курси з інформаційної безпеки, криптографії та захисту даних стають невід'ємною частиною спеціальностей у галузях комп'ютерних наук, електроніки та метрології. Однак варто зазначити, що рівень інтеграції методів захисту даних у різних навчальних закладах може значно варіюватися в залежності від напрямку підготовки та актуальних освітніх стандартів (табл. 3).

Інтеграція методів захисту інформації до навчальних програм в українських закладах вищої освіти є важливим кроком для підготовки майбутніх фахівців, які працюватимуть у сферах, де безпека інформації є критично важливою. Програми таких навчальних закладів, як Національний університет «Львівська політехніка» та Київський політехнічний інститут, включають курси з криптографії, протоколів безпеки та управління доступом, необхідні для забезпечення захисту даних у цифрових системах. Практичні заняття, на яких студенти виконують шифрування даних або налаштовують системи безпеки, дають їм реальні навички, потрібні для роботи в умовах високих вимог до захисту інформації [14; 15].

Викладачі Харківського національного університету радіоелектроніки акцентують увагу на використанні методів захисту даних у метрологічних системах, де точність і достовірність інформації має критичне значення [16].

У свою чергу, навчальні програми Державного університету інтелектуальних технологій і зв'язку містять сучасні протоколи безпеки та технології аудиту для забезпечення захисту в телекомунікаційних і інформаційних системах [17]. Ці навчальні

Таблиця 3

Інтеграція методів захисту даних у навчальні програми для підготовки фахівців у галузях електроніки та метрології в українських закладах вищої освіти

Навчальний заклад	Програма	Ключові методи захисту даних, що вивчаються	Опис інтеграції до навчального процесу
Національний університет «Львівська політехніка» Інформаційна безпека	Криптографія, захист мереж, контролю доступу	Програма містить курси з криптографії, управління доступом, захисту інформації в автоматизованих системах	Лабораторні заняття з шифрування даних та використання сучасних протоколів безпеки
Київський політехнічний інститут ім. Ігоря Сікорського	Комп'ютерні науки	Протоколи безпеки, криптографія, аудит даних	Програма включає вивчення протоколів SSL/TLS, методів криптографічного захисту даних та використання інструментів для моніторингу безпеки в мережах. Студенти виконують лабораторні роботи з налаштування та аналізу безпеки
Харківський національний університет радіоелектроніки	Метрологія та інформаційно-вимірювальна техніка	Захист даних, безпечне зберігання даних, аутентифікація	Програма охоплює курси із захисту даних у метрологічних системах, аналізу уразливостей інформаційних систем, безпечне зберігання даних. Практичні заняття з налаштування систем аутентифікації та шифрування даних
Державний університет інтелектуальних технологій і зв'язку	Магістратура Телекомунікації та радіотехніка	Протоколи Протоколи безпеки, аудит, шифрування	Курс з інформаційної безпеки, що включає вивчення стандартів безпеки даних, методів шифрування та захисту від атак. Використання реальних сценаріїв для моніторингу систем безпеки та аналізу логів

Джерело: сформовано автором на підставі [14-17]

програми дозволяють студентам не лише вивчати теоретичні аспекти, але й активно застосовувати отримані знання в практичних ситуаціях, що є важливим для підготовки кваліфікованих фахівців у галузі безпеки даних.

Упровадження методів захисту даних у сучасних інформаційних системах є надзвичайно важливим аспектом для гарантування безпеки та цілісності даних, особливо в сферах, де обробляються чутливі чи критично важливі відомості. Однак процес інтеграції таких методів супроводжується низкою викликів і проблем, що можуть значно ускладнити його ефективність.

Однім з викликів є складність гарантування безпеки даних при одночасному збереженні доступності та оперативності інформації. Кожен метод захисту (криптографія, шифрування чи контроль доступу) потребує ретельнго налаштування і може негативно впливати на швидкість обробки та передачі даних, що є критичним фактором для систем, що працюють у реальному часі.

Ще однією проблемою є постійно змінювані загрози, пов'язані з кібербезпекою [3]. Технології, які ефективно працюють на сьогодні, можуть швидко застаріти через розвиток нових методів атак: шкідливі програми, фішинг або інші види кібератак. Тому спеціалісти повинні постійно оновлювати свої знання, навички та інструменти для боротьби з новими загрозами, що вимагає значних ресурсів для постійного навчання та адаптації до змінюваних умов.

Також важливим викликом є інтеграція різних методів захисту в наявні системи безпеки без порушення їх функціональності. Системи часто мають складну архітектуру і залежать від багатьох компонентів, що ускладнює реалізацію нових механізмів захисту без ризику виникнення сумісності чи функціональних проблем [11]. Цей процес вимагає ретельного налаштування та проведення аудиту безпеки на всіх етапах інтеграції.

Додатковою складністю є забезпечення відповідності міжнародним стандартам і нормативно-правовим вимогам, що стосуються захисту даних. Законодавчі та нормативні акти постійно змінюються, що вимагає від спеціалістів регулярного перегляду та оновлення політик і процедур захисту даних для забезпечення відповідності новим вимогам [6].

Не менш важливою є проблема ресурсного забезпечення впровадження методів захисту даних. Вартість розробки і впровадження ефективних технологій захисту може бути значною,

особливо для малих і середніх підприємств [2]. Крім того, ресурси можуть бути обмежені для проведення регулярних перевірок, моніторингу та оновлення засобів захисту.

Розробка рекомендацій для удосконалення навчальних програм, що сприяють формуванню необхідних навичок у фахівців, є важливим етапом у підготовці майбутніх спеціалістів в галузі захисту даних. Однією з основних стратегій для досягнення цього є інтеграція сучасних методів навчання, зокрема шляхом застосування інтерактивних технологій та моделювання реальних загроз, що дозволяє студентам не лише ознайомлюватися з теоретичними основами, а й отримувати практичні навички.

Перша рекомендація полягає у впровадженні інтерактивних методів навчання (лабораторні роботи, симуляції та рольові ігри), де студенти можуть практично взаємодіяти з реальними або наближеними до реальних ситуаціями. Це дозволяє майбутнім фахівцям не лише засвоювати теоретичні знання з криптографії, протоколів безпеки та методів контролю доступу, а й набувати навичок оперативного реагування на різноманітні загрози. Наприклад, симуляція кібератак або моделювання процесу шифрування інформації в реальних умовах дасть студентам уявлення про практичні труднощі та можливі загрози.

Другою важливою рекомендацією є використання методів моделювання реальних загроз і атак на інформаційні системи, що дозволяє студентам ознайомитись із сучасними техніками зломів та способами їх запобігання. Це можуть бути як навчальні програми для аналізу уразливостей, так і курси, що дозволяють створювати та тестувати системи захисту від реальних загроз. Такий підхід дозволяє підготувати студентів до роботи в умовах постійно змінюваного кіберпростору, де важливо швидко реагувати на нові види атак.

Наступною рекомендацією є впровадження інструментів для моніторингу та аналізу безпеки, що допоможе студентам на практиці засвоїти основні механізми виявлення вторгнень, захисту від вірусних атак та інших загроз. Практичні заняття з використання таких інструментів як Wireshark [18], Metasploit [19] або Kali Linux [20] дозволяють студентам отримати безпосередній досвід роботи з інструментами для виявлення уразливостей та проведення аудиту безпеки.

Ще однією важливою складовою є забезпечення студентів доступом до реальних баз даних, де вони можуть практично відпрацьовувати методи захисту, шифрування та зберігання даних. Реальні дані дають змогу студентам зрозуміти, як ефективно впроваджувати методи захисту в умовах, коли працюють великі обсяги інформації та виникають складні сценарії безпеки.

Крім того, важливо забезпечити постійну адаптацію навчальних програм до змін у нормативно-правовому середовищі, яке регулює питання захисту даних. Враховуючи швидкий розвиток технологій та зміну стандартів безпеки, навчальні курси повинні бути актуалізовані відповідно до нових вимог законодавства, таких як впровадження стандартів ISO [21], GDPR [22] та інших регламентів.

Отже, варто розвивати співпрацю між навчальними закладами та промисловими компаніями, що займаються кібербезпекою. Спільні проєкти, стажування та практики можуть допомогти студентам отримати практичний досвід і зрозуміти, як теоретичні знання застосовуються в реальних умовах. Така співпраця також сприятиме адаптації навчальних програм до реальних потреб ринку праці та технологічних змін.

Таким чином, для удосконалення навчальних програм необхідно активно інтегрувати сучасні методи навчання, зокрема через симуляції, моделювання загроз і використання реальних інструментів безпеки, що дозволяють студентам набути практичних навичок для роботи з реальними проблемами у сфері захисту даних.

Висновки. Дослідження підтвердило, що інтеграція сучасних методів захисту даних у сфері електроніки та метрології є критично важливою для гарантування безпеки інформації та достовірності вимірювань. Аналіз навчальних програм закладів вищихої освіти України показав, що певні освітні напрями вже включають основи криптографії, контролю доступу та протоколів безпеки, однак рівень інтеграції таких методів залишається нерівномірним. Практична підготовка студентів переважно зосереджена на теоретичних аспектах безпеки, тоді як моделювання реальних загроз та відпрацювання практичних навичок у більшості навчальних закладів є обмеженим.

Серед основних викликів упровадження методів захисту даних виділено низький рівень практичної підготовки студентів, що ускладнює їхню адаптацію до реальних умов роботи. Відзначено складність інтеграції технологій безпеки у вже наявні системи через відмінності їхніх архітектур, що вимагає значних ресурсів на оновлення інфраструктури. Постійна еволюція загроз у сфері кібербезпеки створює додатковий тиск на необхідність регулярного оновлення знань та інструментів, що використовуються спеціалістами. Додатково виявлено проблему обмежених фінансових ресурсів, що ускладнює модернізацію освітнього процесу та проведення практичних тренінгів з реальними сценаріями атак.

Для усунення зазначених проблем необхідно впроваджувати інтерактивні методи навчання, що включають моделювання реальних кіберзагроз, використання сучасних інструментів аудиту та аналізу безпеки, а також розширення курсів

з криптографії та кібербезпеки. Розвиток співпраці між навчальними закладами та IT-компаніями дозволить студентам проходити практичні стажування у сфері інформаційної безпеки та отримувати реальний досвід роботи з актуальними загрозами. Важливим напрямом удосконалення є адаптація навчальних програм відповідно до міжнародних стандартів кібербезпеки, таких як ISO 27001 та GDPR, що дозволить підготувати фахівців, які відповідатимуть глобальним вимогам безпеки даних.

Подальші дослідження можуть бути спрямовані на розробку методологій адаптивного навчання, що поєднуватимуть використання штучного інтелекту для автоматичного аналізу загроз та оцінки рівня підготовки студентів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Потій О.В., Горбенко Ю.І., Замула О.А. Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах. *Радіотехніка*. 2021. Вип. 206. С. 5-24. DOI: https://doi.org/10.30837/rt.2021.3.206.01 (дата звернення: 15.03.2025).

2. Hogail A., Abdellatif R. The New Era of Metrology and Its Role in Information Technology: A Survey. *Journal of Measurement Science and Applications* (JMSA). 2024. Vol. 4, № 1. P. 32-65. URL: https://jmsa.journals.ekb.eg/article_360347.html (date of access: 15.03.2025).

3. Thiel F. Digital transformation of legal metrology–the European metrology cloud. *OIML Bulletin*. 2018. Vol. 59, 1. P. 10-21. URL: https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_8/8.5_metrologische_informationstechnik/Thiel_OIML_Bulletin_2018_Metrology_Cloud.pdf (date of access: 15.03.2025).

4. Durakbasa N.M., Bauer J., Kräuter L., Bas G., Poszvek G. Intelligent Integrated Management and Advanced Metrology for Quality Toward the Factory of the Future. In: Ni J., Majstorovic V., Djurdjanovic D. (eds) *Proceedings of 3rd International Conference on the Industry 4.0 Model for Advanced Manufacturing*. AMP 2018. Lecture Notes in Mechanical Engineering. 2018. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-89563-7 (date of access: 15.03.2025).

5. Gordiyenko T., Velychko O., Pototskyi I., Kuzmenko Y. Development of national infrastructure for training specialists in the specialty «Information and Measurement Technologies». *Measurements Infrastructure*. 2024. Vol. 8. DOI: https://doi.org/10.33955/v8(2024)-072 (date of access: 15.03.2025).

6. Varshney A., Garg N., Nagla K.S., Nair T.S., Jaiswal S.K., Yadav S., Aswal D.K. Challenges in Sensors Technology for Industry 4.0 for Futuristic Metrological Applications. MAPAN. 2021, Vol. 36: 215–226. https://doi.org/10.1007/s12647-021-00453-1 (date of access: 15.03.2025).

7. Somkuwar A.S., Satish, Siwach P.K., Kumar A., Shukla A.K., Kushvaha S.S., Rakshit R.K., Jain P., Meena R.S., Sahoo S., Aloysius R.P., Dogra A., Singh M.A., Ansari M., Khanna S.P., Pulikkotil J., Singh H.K., Awana V.P.S., Biswas J.C. Electrical and Electronics Metrology: From Quantum Standard to Applications in Industry and Strategic Sectors. In: Aswal D.K. (ed) *Metrology for Inclusive Growth of India*. Springer. 2025. Singapore. DOI: https://doi.org/10.1007/978-981-15-8872-3_10 (date of access: 15.03.2025).

8. Mustapää T., Nummiluikki J., Viitala R. Digitalisation of metrology for improving trustworthiness and management of measurement data in industrial IoT systems. *Appl. Sci.* 2022. Vol. 12, № 15. Article 7531; https://doi.org/10.3390/app12157531 (date of access: 15.03.2025).

9. Makarov V.V., Blatova T.A., Fedorov A.V., Shukla A.S. Metrology in ensuring the quality of products and services in digital economy. *Economic and Social Trends for Sustainability of Modern Society (ICEST 2020), European Proceedings of Social and Behavioural Sciences.* European Publisher, 2020. Vol. 90. (pp. 490-498). DOI: https://doi.org/10.15405/epsbs.2020.10.03.55 *(*date of access: 15.03.2025).

10. Gogolinskiy K.V., Syasko V.A. Metrological Assurance and Standardization of Advanced Tools and Technologies for Nondestructive Testing and Condition Monitoring (NDT4.0). *Research in Nondestructive Evaluation*. 2020. Vol. 31, № 5-6. P. 325-339. DOI: https://doi.org/10.1080/09349847.2020.1841863 (date of access: 15.03.2025).

11. Mekid S. Metrology and Instrumentation: Practical Applications for Engineering and Manufacturing. *John Wiley & Sons*. 2021. https://books.google.com.ua/books?hl=uk&lr=&id=1zNPEAAAQBAJ&oi=fnd&pg=PA1&dq=+MODERN+DATA+PROTECTION+METHODS+IN+THE+FIELD+OF+ELECTRONICS+AND+METROLOGY&ots=rqovEiQVCU&sig=07wrMdUqPuaIJKQzSF6cf4PMqJY&redir_esc=y#v=onepage&q&f=false (date of access: 15.03.2025).

12. Osten W. Optical metrology: the long and unstoppable way to become an outstanding measuring tool. In: *Speckle 2018: VII International Conference on Speckle Metrology*. SPIE, 2018. Article 1083402. https://doi.org/10.1117/12.2322533 (date of access: 15.03.2025).

13. Yao T.-F., Connolly L.G., Cullinan M. Expanded area metrology for tip-based wafer inspection in the nanomanufacturing of electronic devices. *Journal of Micro/Nanolithography, MEMS, and MOEMS*. 2019. Vol. 18, № 3. P. 034003-034003. https://doi.org/10.1117/1.JMM.18.3.034003 (date of access: 15.03.2025)

14. Національний університет «Львівська політехніка»: ОСВІТНЬО-ПРОФЕСІЙНА Програма «Інформаційна безпека». Львівська політехніка: офіційний вебсайт, 2024. URL: https://lpnu.ua/informatsiina-bezpeka (дата звернення: 07.03.2025).

15. Київський політехнічний інститут ім. Ігоря Сікорського: ОСВІТНЬО-ПРОФЕСІЙНА Програма «Комп'ютерні науки». КПІ ім. Ігоря Сікорського: офіційний вебсайт, 2024. URL: https://osvita.kpi.ua/122 (дата звернення: 07.03.2025).

16. Харківський національний університет радіоелектроніки: ОСВІТНЬО-ПРОФЕСІЙНА Програма «Метрологія та інформаційно-вимірювальна техніка». Харківський національний університет радіоелектроніки: офіційний вебсайт, 2024. URL: https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/

spetsialnosti-ta-osvitni-prohramy-2018-2024-rokiv-pryjomu/spetsialnist-152-metrologiya-ta-informatsiyno-vimiryuvalna-tehnika-2 (дата звернення: 07.03.2025).

17. Державний університет інтелектуальних технологій і зв'язку: ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Телекомунікації та радіотехніка». Державний університет інтелектуальних технологій і зв'язку: офіційний вебсайт, 2024. URL: https://suitt.edu.ua/wp-content/uploads/2024/08/172-op-mahystr-2024.pdf (дата звернення: 07.03.2025).

18. Wireshark: official website, 2024. URL: https://www.wireshark.org/ (date of access: 15.03.2025).

19. Metasploit: official website, 2024. URL: https://www.metasploit.com/ (date of access: 15.03.2025).

20. Kali Linux: official website, 2024. URL: https://www.kali.org/ (date of access: 15.03.2025).

21. ISO 27001 – Information Security Management System Standard: ISO, official website, 2024. URL: https://www.iso.org/isoiec-27001-information-security.html (date of access: 15.03.2025).

22. GDPR (General Data Protection Regulation): European Union official website, 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (date of access: 15.03.2025).