ВИКОРИСТАННЯ СУЧАСНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ ФАХІВЦІВ РАДІОТЕЛЕКОМУНІКАЦІЙ

USE OF MODERN INFORMATION SECURITY STANDARDS IN THE PROFESSIONAL TRAINING OF RADIOTELECOMMUNICATIONS SPECIALISTS

УДК 004.056:621.396.67
DOI https://doi.org/10.32782/2663-6085/2025/83.2.22

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

Актуальність дослідження зумовлена необхідністю адаптації освітніх програм спеціальності «Радіотелекомунікації» до сучасних стандартів інформаційної безпеки ISO/IEC 27001 і NIST SP 800-53, що є критично важливим у контексті цифровізації телекомунікаційних систем і відповідного зростання кіберзагроз. Метою дослідження є обґрунтування необхідності впровадження сучасних стандартів інформаційної безпеки у професійну підготовку фахівців радіотелекомунікацій і розроблення рекомендацій щодо вдосконалення освітніх програм з огляду на інтеграцію практичних завдань і реальних кейсів із кібербезпеки. Методологія дослідження охоплює аналіз наукових джерел, системний аналіз вимог міжнародних стандартів і компаративний аналіз освітніх програм трьох українських університетів.

Встановлено, що освітні програми є фрагментарними щодо викладання дисциплін з інформаційної безпеки, а тому не відбувається повноцінного формування у здобувачів освіти комплексних компетентностей. Виявлено обмежене використання симуляційних платформ для моделювання атак і реагування на інциденти, як і недостатню підготовку викладачів до реалізації навчальних курсів відповідно до міжнародних стандартів. Доведено, що інтеграція модульних курсів, орієнтованих на практичну підготовку здобувачів освіти, сприятиме послідовному формуванню навичок з управління інформаційними ризиками, захисту даних та аналізу кіберзагроз.

Наукова новизна дослідження полягає у розробленні рекомендацій щодо комплексного оновлення освітніх програм, які передбачають створення міждисциплінарних курсів з кібербезпеки, упровадження симуляційних платформ та організацію підвищення кваліфікації викладачів. Упровадження оновлених програм, які поєднуватимуть теоретичну й практичну підготовки з відпрацюванням реальних сценаріїв атак, сприятиме формуванню у здобувачів освіти комплексних навичок протидії кіберзагрозам.

Перспективи подальших досліджень полягають у розробленні адаптивних моделей підготовки фахівців радіотелекомунікацій з урахуванням міжнародних стандартів інформаційної безпеки й актуальних викликів цифровізації.

Ключові слова: *кіберзагрози, освітні програми, симуляційні платформи, міждисциплінарна підготовка, управління ризиками, криптографія.*

The relevance of the study is determined by the need to adapt educational programmes in the field of radio telecommunications to modern information security standards ISO/IEC 27001 and NIST SP 800-53, which is critical in the context of the digitalisation of telecommunications systems and the corresponding growth of cyber threats. The aim of the study is to justify the need to introduce modern information security standards into the professional training of radio telecommunications specialists and to develop recommendations for improving educational programmes with a view to integrating practical tasks and real-life cyber security cases. The research methodology includes analysis of scientific sources, systematic analysis of international standards requirements, and comparative analysis of educational programmes at three Ukrainian universities.

It has been established that educational programmes are fragmented in terms of teaching information security disciplines, and therefore, students do not fully develop comprehensive competencies. Limited use of simulation platforms for modelling attacks and responding to incidents has been identified, as well as insufficient training of teachers to deliver courses in accordance with international standards. It has been proven that the integration of modular courses focused on practical training of students will contribute to the consistent development of skills in information risk management, data protection and cyber threat analysis.

The scientific novelty of the research lies in the development of recommendations for a comprehensive update of educational programmes, which include the creation of interdisciplinary courses on cybersecurity, the introduction of simulation platforms and the organisation of advanced training for teachers. The implementation of updated programmes that combine theoretical and practical training with the practice of real attack scenarios will contribute to the formation of comprehensive cyber threat response skills among students.

Prospects for further research lie in the development of adaptive models for training radio and telecommunications specialists, taking into account international information security standards and the current challenges of digitalisation.

Key words: *cyber threats, educational programmes, simulation platforms, interdisciplinary training, risk management, cryptography.*

Постановка проблеми. Сучасні стандарти інформаційної безпеки є неодмінною складовою професійної підготовки фахівців із радіотелекомунікацій, оскільки кібербезпека є передумовою інтеграції новітніх технологій у телекомунікаційні системи. З огляду на це, адаптація освітніх програм до вимог інформаційної безпеки з урахуванням міжнародних стандартів, зокрема ISO/IEC 27001 [1] і NIST SP 800-53 [2], є актуальним освітнім завданням. Формування професійних компетентностей у сфері інформаційної безпеки передбачає методичну підготовку здобувачів освіти до практичної реалізації стандартів безпеки з акцентом на інтеграцію захисних

алгоритмів, шифрувальних протоколів і систем моніторингу мережевих загроз. Необхідно розробити такі навчальні програми, які б акцентували на технічних аспектах захисту даних, і водночас забезпечували розвиток аналітичного мислення здобувачів освіти, формували здатність до оцінювання ризиків і прийняття обґрунтованих рішень у контексті інформаційної безпеки. Тому особливу увагу варто приділити питанням розробки методологічних підходів до інтеграції знань про кібербезпеку у радіотелекомунікаційні курси, зокрема методично обгрунтувати й реалізувати кейс-методи, симуляційні вправи й практичні завдання для формування навичок реагування на кіберзагрози. Аналіз ефективності впровадження таких програм може стати підґрунтям для розроблення рекомендацій щодо удосконалення професійної підготовки з урахуванням новітніх стандартів інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць із проблеми використання сучасних стандартів інформаційної безпеки у професійній підготовці фахівців з радіотелекомунікацій дозволяє виокремити чотири фундаментальні напрями.

У межах першого увагу зосереджено на визначенні теоретичних засад і моделей професійної підготовки з урахуванням інформаційної безпеки. Наприклад, В. Магілевський [3] удокладнює компетентнісний підхід до формування професійних навичок фахівців у радіотелекомунікаційних системах та акцентує на стандартах ISO/IEC [1]. У дослідженні доведено важливість інтеграції міжнародних стандартів у навчальні програми для забезпечення високого рівня інформаційної безпеки. М. Мюкгердже та ін. [4] описують освітні моделі, які застосовують у навчанні кібербезпеки, приділяють увагу стратегічним підходам до формування необхідних компетенцій. Автори деталізують освітні програми, орієнтовані на розвиток критичного мислення й навичок оцінки ризиків. Дж. Гатзівасіліста ін. [5] звертають увагу на адаптацію програм підготовки до сучасних викликів кібербезпеки, а це передбачає постійне оновлення навчального контенту відповідно до еволюції стандартів і загроз. Подальші дослідження в цьому напрямі прогнозовано будуть зосереджені на формуванні комплексних моделей підготовки фахівців, які інтегрують сучасні стандарти інформаційної безпеки й практичні кейси для розвитку навичок реагування на кіберзагрози.

Другий напрям стосується використання стандартів інформаційної безпеки в освітніх процесах і виявлення їх впливу на професійну підготовку. Дж. Дж. Р. Урібе та ін. [6] розглядають перспективи застосування програмних платформ із відкритим кодом у підготовці фахівців з інформаційної безпеки. Особливу увагу автори приділили стандартизації протоколів безпеки в радіотелекомунікаційних системах. Д. Бендлер і М. Фелдерер [7] пропонують нову модель компетентностей для спеціалістів із кібербезпеки, яка враховує вимоги сучасних стандартів та акцентує на формуванні навичок оцінки ризиків і безперервного моніторингу інформаційних систем. М. Алшаіґ [8] переконує у необхідності формування кіберкультури с працівників, що є основою ефективного практичного застосування стандартів безпеки. Подальші дослідження , передбачаємо, будуть зосереджені на адаптації освітніх програм до вимог стандартів ISO/IEC, що дозволить інтегрувати практичні кейси для підготовки спеціалістів до динамічних умов роботи з інформаційними системами.

Третій напрям охоплює проблеми впровадження сучасних стандартів інформаційної безпеки у навчальні програми. Н. Ріді та ін. [9] описують труднощі інтеграції стандартів у програми підготовки зв'язківців та вказують на недоліки уніфікації навчальних матеріалів з міжнародними вимогами. Н.Чітадзе [10] аналізує основні принципи інформаційної та кібербезпеки і вказує на недостатнє охоплення стандартами навчальних планів закладів вищої освіти. А. Іманбаева та ін. [11] інтерпретують досвід використання проблемного навчання для формування базових знань з інформаційної безпеки й акцентують на застосуванні практичних кейсів. Подальші дослідження будуть зосереджені на розробці методик інтеграції стандартів інформаційної безпеки у навчальні плани спеціальностей радіотелекомунікацій, зокрема з урахуванням специфіки захисту даних у IoT-системах.

Четвертий напрям пов'язаний із розробленням рекомендацій і перспективами вдосконалення навчальних програм з урахуванням інформаційної безпеки. Дж. Бреда й М. Кісс [12] розглядають стандарти інформаційної безпеки в промисловості 4.0 і наголошують на необхідності формування фахівців, здатних працювати з захищеними системами в умовах підвищеної технологічної складності. Т. Сенанаяке і С. Фернандо [13] пропонують інноваційні підходи до формування інформаційної обізнаності студентів, що сприяє підвищенню кібербезпеки у професійному середовищі. Р. Прасад і В. Рохокал [14] переконують у важливості кібербезпеки як складової інформаційних і комунікаційних технологій і пропонують унікальні методи навчання на основі стандартів ISO/IEC [1]. Подальші дослідження у цьому напрямі мають бути спрямовані на розроблення рекомендацій щодо впровадження інноваційних методів навчання, які враховують динамічні зміни у стандартах інформаційної безпеки й забезпечують практичну підготовку фахівців до роботи у цифровому середовищі.

Отже, аналіз наукових праць демонструє важливість інтеграції сучасних стандартів

інформаційної безпеки у професійну підготовку фахівців радіотелекомунікацій. Здебільшого увагу приділено розробленню адаптивних освітніх програм, які відповідають актуальним викликам кібербезпеки й забезпечують високий рівень підготовки майбутніх спеціалістів у цій галузі.

Незважаючи на впровадження окремих курсів з інформаційної безпеки, освітні програми за спеціальністю «Радіотелекомунікації» є фрагментарними, що ускладнює формування цілісного переліку компетентностей у сфері кіберзахисту. Недостатньо вивченими є питання адаптації стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2] до специфіки телекомунікаційних систем, а також ефективність практичних завдань на симуляційних платформах у контексті реагування на реальні кіберзагрози. Відсутність інтегрованих модульних курсів і недостатнє використання сучасних платформ обмежують практичну підготовку студентів до реальних викликів кібербезпеки.

Запропоноване дослідження спрямоване на розроблення рекомендацій щодо структурування освітніх програм з урахуванням вимог міжнародних стандартів і специфіки радіотелекомунікаційних систем. Встановлено необхідність створення модульних курсів з інформаційної безпеки, інтеграції симуляційних платформ для відпрацювання сценаріїв атак та розробки методичних підходів до формування практичних навичок протидії кіберзагрозам. Таке методичне обґрунтування й забезпечення дозволить усунути фрагментарність програм, удокладнить професійні компетентності й підвищить ефективність практичної підготовки здобувачів освіти.

Мета статті – аналіз шляхів інтеграції сучасних стандартів інформаційної безпеки у професійній підготовці фахівців радіотелекомунікацій і розроблення рекомендації щодо вдосконалення освітніх програм з урахуванням актуальних викликів кібербезпеки.

Завдання статті:

1. Визначити вимоги до професійної підготовки фахівців радіотелекомунікацій у межах інформаційної безпеки відповідно до стандартів ISO/IEC 27001 і NIST SP 800-53 на основі аналізу освітніх програм у трьох вітчизняних університетах (Національний університет «Львівська політехніка», Київський національний університет будівництва і архітектури, Ужгородський національний університет).

2. Оцінити технічні й методичні перешкоди процесу інтеграції стандартів інформаційної безпеки у структуру навчальних програм спеціальності «Радіотелекомунікації».

3. Розробити рекомендації щодо вдосконалення освітніх програм з інформаційної безпеки з огляду на практичну підготовку здобувачів до протидії кіберзагрозам.

Виклад основного матеріалу. Сучасні вимоги до професійної підготовки фахівців радіотелекомунікацій у сфері інформаційної безпеки зумовлені необхідністю адаптації освітніх програм до стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2], які визначають ключові напрями формування компетентностей у галузі кібербезпеки. Враховуючи високий рівень загроз у телекомунікаційному секторі, актуальним завданням є створення таких навчальних курсів, які забезпечать здобувачів освіти знаннями й сприятимуть виробленню навичок у сфері захисту даних, управління інформаційними ризиками й реагування на інциденти кібербезпеки. Міжнародні стандарти акцентують на необхідності інтеграції модулів з виявлення вразливостей, шифрування даних, управління доступом та аналізу ризиків у навчальні програми, що дозволить майбутнім фахівцям з радіотелекомунікацій ефективно виконувати професійні завдання в контексті підтримання безпеки інформаційних систем (табл. 1).

Практична реалізація цих вимог передбачає застосування кейс-методів, симуляційних завдань

Таблиця 1

Вимоги до професійної підготовки фахівців радіотелекомунікацій з інформаційної безпеки за стандартами ISO/IEC 27001 та NIST SP 800-53

Напрям підготовки	Вимоги ISO/IEC27001	Вимоги NIST SP 800-53
Управління інформаційними ризиками	Визначення активів, оцінка загроз та вразливостей, розробка планів реагування	Категоризація систем, оцінка ризиків, упровадження заходів контролю
Захист даних	Впровадження шифрувальних алгоритмів, захист даних при передачі й зберіганні	Захист конфіденційних даних, криптографічний захист інформації
Управління доступом	Розмежування прав доступу, автентифікація та авторизація користувачів	Контроль доступу до систем, управління обліковими записами
Реагування на інциденти	Розробка планів реагування, відновлення після інцидентів	Виявлення, аналіз та реагування на кіберінциденти
Оцінка ефективності заходів	Періодичний аудит систем, аналіз результатів упроваджених заходів	Моніторинг систем безпеки, оцінка ефективності заходів контролю

Джерело: сформовано автором на підставі [4; 6; 7].

і тестових середовищ для моделювання реальних кіберзагроз. Наприклад, під час навчання управлінню інформаційними ризиками здобувачі освіти розробляють сценарії можливих атак на телекомунікаційні мережі й формують плани реагування з урахуванням стандартів ISO/IEC 27001 [1]. Практичні заняття із захисту даних передбачають побудову криптографічних систем та оцінку їх стійкості до атак методом перебору [9]. Упровадження реальних кейсів із управління доступом дозволяє майбутнім фахівцям не лише аналізувати потенційні вразливості у системах автентифікації, але й розробляти алгоритми моніторингу несанкціонованих дій користувачів відповідно до вимог NIST SP 800-53 [2]. Водночас практичні заняття з реагування на інциденти формують компетенції з аналізу журналів подій і моделювання атак з метою ідентифікації векторів проникнення й оцінки ефективності застосованих контрзаходів [6]. Такий підхід забезпечує не лише опанування теоретичної бази стандартів безпеки, але й дозволяє розвинути навички практичної імплементації вимог кібербезпеки у контексті реальних професійних завдань.

В умовах стрімкого розвитку інформаційних технологій і відповідного зростання кіберзагроз, формування компетентностей з інформаційної безпеки у навчальних програмах за спеціальністю «Радіотелекомунікації» набуває особливої актуальності. А тому важливо готувати фахівців, здатних ефективно забезпечувати захист інформаційних і телекомунікаційних систем від потенційних загроз. Методичні підходи до формування таких компетентностей повинні враховувати як теоретичні аспекти, так і практичні навички, що відповідають сучасним вимогам галузі (табл. 2).

Практична реалізація наведених методичних підходів до формування компетентностей з інформаційної безпеки у сфері радіотелекомунікацій дозволяє говорити про достатню професійну підготовку здобувачів освіти. У Національному університеті «Львівська політехніка» акцентовано на проєктно-орієнтованому навчанні, що уможливлює засвоєння теоретичного матеріалу й дозволяє практично застосувати знання під час створення проєктів під керівництвом досвідчених менторів з ІТ-сфери [15]. Такий підхід сприяє розвитку системного мислення, критичного аналізу й формує компетентності з управління ризиками інформаційної безпеки. Залучення студентів до проєктів на ранніх етапах підготовки сприяє поглибленню знань у сфері кіберзахисту і знайомить майбутніх фахівців з інструментами моніторингу загроз, що відповідає вимогам ISO/IEC 27001 [1].

У Київському національному університеті будівництва і архітектури акцентовано на вивченні нормативно-правових аспектів і стандартів інформаційної безпеки, що сприяє комплексному підходу до підготовки фахівців з урахуванням міжнародних вимог [16]. Вивчення законодавчих основ відбувається з огляду на взаємозв'язок національних регуляторних актів і вимог NIST SP 800-53 [2], а це формує цілісне уявлення про юридичні аспекти захисту інформації. У цьому контексті доцільним є застосування кейс-методів для моделювання сценаріїв порушення безпеки інформаційних систем, що дозволяє студентам розробляти стратегії протидії кіберзагрозам на підставі актуальних нормативних документів.

Навчання в Ужгородському національному університеті орієнтоване на формування інтегрованих компетентностей через упровадження практичних занять з аналізу й реагування на кіберзагрози [17]. Під час навчання використано сучасні симуляційних платформи, на яких студенти моделюють можливі вектори атак на інформаційні системи й розробляють алгоритми реагування відповідно до стандартів ISO/IEC 27001 [1]. Такий підхід забезпечує поглиблене розуміння технологічних аспектів захисту даних, зокрема упровадження криптографічних протоколів та оцінки ефективності шифрувальних алгоритмів. Практичні

Таблиця 2

Методичні підходи до формування компетентностей з інформаційної безпеки у навчальних програмах за спеціальністю «Радіотелекомунікації»

Університет	Методичні підходи	Особливості реалізації
Національний університет «Львівська політехніка»	Інтеграція практико-орієнтованого навчання через проєктну діяльність та співпрацю з ІТ-компаніями	Студенти з другого курсу створюють власні проєкти, де менторами є ІТ-спеціалісти; розвиток м'яких навичок та основ проєктного менеджменту
Київський національний університет будівництва і архітектури	Вивчення законодавчої та нормативно-правової бази України, міжнародних стандартів і практик	Грунтовне вивчення вимог міжнародних стандартів щодо здійснення професійної діяльності у галузі кібербезпеки й захисту інформації
Ужгородський національний університет	Комплексне вивчення теоретичних основ кібербезпеки й практичних аспектів захисту інформації	Формування навичок аналізу й реагування на кіберзагрози, упровадження практичних занять з використанням сучасних технологій

Джерело: сформовано автором на підставі [15-17].

заняття сприяють формуванню навичок аналізу даних, управління інцидентами й адаптації захисних механізмів до реальних умов інформаційної інфраструктури.

Інтеграція навчальних модулів з інформаційної безпеки у структуру освітніх програм спеціальності «Радіотелекомунікації» здійснена на основі адаптації навчального плану до сучасних вимог кібербезпеки і передбачає не лише розроблення нових дисциплін, але й зміну логіки організації навчального процесу, що сприяє формуванню комплексу компетентностей з урахуванням специфіки професійної діяльності. Водночас методичним викликом є забезпечення цілісності підготовки й збереження балансу між фундаментальними й прикладними знаннями, враховуючи постійне оновлення стандартів інформаційної безпеки. Логіка інтеграції передбачає введення базових дисциплін на молодших курсах, що створює підґрунтя для розуміння принципів безпеки, із подальшою спеціалізацією на старших курсах через прикладні модулі (табл. 3).

Отже, інтеграція модулів з інформаційної безпеки у структуру освітніх програм сприяє формуванню комплексного підходу до підготовки фахівців радіотелекомунікацій. Зокрема в Національному університеті «Львівська політехніка» під час опанування дисциплін студентами 1-2 курсів формуються базові знання з кібербезпеки, що забезпечує поступове ускладнення навчального матеріалу студентам старших курсів [15]. Такий підхід дозволяє удокладнити матеріали з основ інформаційної безпеки ще до початку спеціалізованої підготовки й створює передумови для опанування складних концепцій на пізніших етапах навчання.

У Київському національному університеті будівництва і архітектури логіка інтеграції модулів відрізняється вивченням нормативно-правової бази на 3-4 курсах, що дозволяє студентам краще орієнтуватися у вимогах міжнародних стандартів [16]. Такий підхід сприяє формуванню системного уявлення щодо кібербезпеки як комплексної діяльності з урахуванням як технічних, так і правових аспектів, що особливо важливо в контексті професійної відповідальності фахівців, які працюють з інформаційними системами.

В Ужгородському національному університеті структура модулів орієнтована на раннє формування базових знань з кібербезпеки з подальшим поглибленням під час практичних тренінгів [17]. Студенти старших курсів під час лабораторних занять набувають практичних навичок моделювання кіберзагроз, що дозволяє здобувачам освіти працювати з реальними даними й аналізувати мережеві атаки у безпечному середовищі. Поєднання програмування й захисту даних дозволяє студентам створювати комунікаційні системи з підвищеною стійкістю до атак.

Отже, аналіз логіки інтеграції навчальних модулів з інформаційної безпеки у структуру освітніх програм демонструє різні підходи до організації підготовки фахівців радіотелекомунікацій. Найбільш ефективним видається поєднання раннього засвоєння базових знань з поступовим переходом до спеціалізованих дисциплін, що дозволяє забезпечити навчальну системність і виробити готовність до реальних викликів у професійній діяльності.

Інтеграція стандартів інформаційної безпеки у навчальний процес спеціальності «Радіотелекомунікації» супроводжується системними проблемами, актуальними для більшості вітчизняних університетів. Однією з ключових є недостатня адаптація освітніх програм до вимог міжнародних стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2], які охоплюють не лише технічні аспекти захисту даних, але й компетентності з управління ризиками й реагування на інциденти. В освітніх програмах враховано переважно теоретичні дисципліни, тим часом практичних занять з моделювання

Таблиця 3

Логіка інтеграції модулів з інформаційної безпеки у структуру освітніх програм спеціальності «Радіотелекомунікації»

Елемент програми	Національний університет «Львівська політехніка»	Київський національний університет будівництва і архітектури	Ужгородський національний університет
Раннє впровадження базових курсів	На 1-2 курсах введено основи кібербезпеки	Базові курси з безпеки інформаційних систем з 2-го курсу	Модуль з основ захисту даних на першому курсі
Логіка спеціалізації на старших курсах	На 3-4 курсах посилено практичну підготовку у межах проєктів з кіберзахисту	Акцент на вивченні нормативної бази та юридичних аспектів на старших курсах	Упровадження лабораторних модулів з аналізу атак на старших курсах
Інтеграція з іншими дисциплінами	Поєднання з курсами радіотехніки та мережевих технологій	Інтеграція з курсами інженерії безпеки й технічного захисту інформації	Синтез з програмуванням для створення захищених комунікаційних систем
Баланс теоретичних і практичних занять	Збільшено кількість лабораторних робіт на старших курсах	Введено семінари з аналізу кіберзагроз на основі нормативних актів	Комбінування лекцій з практичними тренінгами з кібербезпеки

Джерело: сформовано автором на підс таві [15-17].

кіберзагроз і реагування на атаки недостатньо, що знижує готовність студентів до вирішення реальних завдань у сфері захисту інформаційних систем.

З-поміж технічних перешкод вкажемо на брак сучасних симуляційних платформ і програмних комплексів для відпрацювання практичних навичок з аналізу мережевих загроз. Частина університетів не має фінансових можливостей для придбання обладнання й програмного забезпечення, яке відповідає вимогам стандартів, а це обмежує доступ до інтегрованих систем моніторингу загроз і криптографічних протоколів [9] і ускладнює формування комплексних компетентностей з реагування на інциденти, що є критично важливим для фахівців у галузі радіотелекомунікацій.

Суттєві методичні перешкоди зумовлені здебільшого фрагментарністю навчальних програм, у яких курси з інформаційної безпеки подано окремо від інших дисциплін, що призводить до порушення логіки викладання й послідовного формування компетентностей [12]. Відсутність інтегрованих курсів, які б інтегрували захист даних, програмування й аналіз загроз, не дозволяє створити цілісну систему підготовки.Тим часом і викладачі часто не мають необхідної підготовки для впровадження стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2] у навчальний процес, що обмежує можливість адаптації освітніх програм до актуальних вимог ринку праці [4]. Тому розроблення рекомендацій щодо вдосконалення освітніх програм з інформаційної безпеки для спеціальності «Радіотелекомунікації» мусить враховувати як технічні, так і методичні аспекти з огляду на вимоги міжнародних стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2]. Необхідний комплексний підхід, який поєднує теоретичну підготовку з практичними завданнями, спрямованими на формування системних компетентностей у сфері кібербезпеки.

Вихід може бути знайдено в розробленні модульних курсів, орієнтованих на послідовне вивчення тем, пов'язаних із захистом інформаційних систем у радіотелекомунікаційних мережах: на 1-2 курсах доцільно запровадити модулі з основ інформаційної безпеки, які охоплюють базові принципи кібербезпеки, типи загроз і методи їх виявлення. Такі практикоорієнтовані модулі передбачають аналіз мережевих атак, використання криптографічних алгоритмів та управління ризиками. На старших курсах доцільно впровадити спеціалізовані модулі, які охоплюють стандарти ISO/IEC 27001 і NIST SP 800-53 й удокладнюють практичну реалізацію вимог цих стандартів у радіотелекомунікаційних системах. Це можуть бути лабораторні заняття зі створення й налаштування захищених комунікаційних каналів, моніторингу інцидентів та аналізу вразливостей.

Необхідно розробити інтегровані міждисциплінарні курси, які б поєднували знання з програмування, телекомунікацій та інформаційної безпеки й дозволили здобувачам освіти не лише опанувати основи аналізу даних і створення захищених систем, але й розуміти, як їх застосовувати у контексті протидії реальним кіберзагрозам. Такий підхід дозволить уникнути фрагментарності навчальних програм і сприятиме формуванню комплексних навичок.

Таким же важливим є оновлення матеріально-технічної бази й забезпечення доступу до симуляційних платформ, які імітують реальні сценарії атак на інформаційні системи. Залучення сучасних технологій дозволить не лише підвищити ефективність навчання, але й забезпечить відповідність освітніх програм вимогам міжнародних стандартів.

У межах удосконалення освітніх програм для студентів допускаємо організацію модулів у межах підвищення кваліфікації викладачів з інформаційної безпеки, орієнтованих на впровадження вимог ISO/IEC 27001 і NIST SP 800-53.

Висновки. Інтеграція стандартів ISO/IEC 27001 [1] і NIST SP 800-53 [2] у професійну підготовку фахівців радіотелекомунікацій забезпечить комплексне формування у здобувачів освіти компетентностей з управління інформаційними ризиками, захист даних і реагування на інциденти. Виявлено, що основними проблемами такої інтеграції є відсутність системного підходу у формуванні курсів з інформаційної безпеки й фрагментарність освітніх програм, у яких порушена логіка формування компетентностей. Обмежені можливості використання симуляційних платформ і недостатня підготовка викладачів до реалізації стандартів навчального процесу також є перешкодами в питанні інтеграції нових стандартів захисту інформації.

Рекомендовано створити модульні курси з інформаційної безпеки; інтегрувати в освітні програми практичні завдання на симуляційних платформах; розробити міждисциплінарні модулі, які б удокладнювали знання з програмування, аналізу загроз і криптографії; оновити матеріально-технічну базу й організувати підвищення кваліфікації викладачів для актуалізації новітніх методик навчання.

Перспективи подальших досліджень пов'язані з розробленням адаптивних моделей професійної підготовки, які поєднують стандарти ISO/IEC 27001 [1] і NIST SP 800-53 [2] із практичними кейсами для протидії кіберзагрозам у телекомунікаційних системах.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. ISO/IEC 27001:2013. ISO: website. 2025. URL: https://www.iso.org/isoiec-27001-information-security.html (date of access: 05.05.2025)

2. NIST SP 800-53 Rev. 5. National Institute of Standards and Technology: website. 2025. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (date of access: 05.05.2025)

3. Магілевський В. В. Формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах. Педагогічна академія: наукові записки. 2025. Вип. 14. DOI: https://doi.org/10.5281/zenodo.14723771

4. Mukherjee M., Le N. T., Chow Y.-W., Susilo W. Strategic approaches to cybersecurity learning: a study of educational models and outcomes. Information. 2024. Vol. 15, № 2. DOI: https://doi.org/10.3390/info15020117

5. Hatzivasilis G., Ioannidis S., Smyrlis M., Spanoudakis G., Frati F., Goeke L., Hildebrandt T., Tsakirakis G., Oikonomou F., Leftheriotis G., Koshutanski H. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied sciences. 2020. Vol. 10, № 16. Article 5702. URL: https://www.academia.edu/73709685/Modern_Aspects_of_Cyber_Security_Training_and_Continuous_Adaptation_of_Programmes_to_Trainees (date of access: 14.10.2024).

6. Uribe J. J. R., Guillen E. P., Cardoso L. S. A technical review of wireless security for the Internet of Things: software defined radio perspective. Journal of King Saud University-Computer and Information Sciences. 2022. Vol. 34, № 7. P. 4122–4134. DOI: https://doi.org/10.1016/j.jksuci.2021.04.003

7. Bendler D., Felderer M. Competency models for information security and cybersecurity professionals: analysis of existing work and a new model. ACM transactions on computing education. 2023. Vol. 23, № 2. P. 1-33. DOI: https://doi.org/10.1145/3573205

8. Alshaikh M. Developing cybersecurity culture to influence employee behavior: a practice perspective. Computers & security. 2020. Vol. 98. Article 102003. DOI: https://doi.org/10.1016/j.cose.2020.102003

9. Ridei N., Tymoshenko V., Tytova N., Khodunova V., Biletska A. Organization of professional training of communication management and communications specialists. Journal of Education, Technology and Computer Science. 2022. Vol. 33, № 3. P. 109–117. DOI: https://doi.org/10.15584/jetacomps.2022.3.12

10. Chitadze N. Basic principles of information and cyber security. In: Analyzing new forms of social disorders in modern virtual environments. IGI Global. 2023. P. 193-223. URL: https://www.igi-global.com/chapter/basic-principles-of-information-and-cyber-security/328110 (date of access: 05.05.2025)

11. Imanbayeva A., Temirbayev A., Syzdykova R., Saduev N. Practical experience of using problem training in the formation of a knowledge system for students in the field of information security. In: EDULEARN18 proceedings. IATED. 2018. P. 9919-9924. DOI: 10.21125/edulearn.2018.2387

12. Breda G., Kiss M. Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. Procedia manufacturing. 2020. Vol. 46. P. 580-590. DOI: https://doi.org/10.1016/j.promfg.2020.03.084

13. Senanayake T., Fernando S. Information security education: watching your steps in cyberspace. The online journal of science and technology. 2018. Vol. 8, № 2. URL: https://tojsat.net/journals/tojsat/articles/v08i02/v08i02-16.pdf (date of access: 05.05.2025)

14. Prasad R., Rohokale V. Cyber security: the lifeline of information and communication technology. Cham, Switzerland: Springer International Publishing. 2020. URL: https://link.springer.com/book/10.1007/978-3-030-31703-4 (date of access: 05.05.2025)

15. Освітня програма «Програмно-апаратні пристрої інфокомунікаційних систем». Національний університет «Львівська політехніка»: вебсайт. 2025. URL: https://directory.lpnu.ua/majors/icte/6.172.00.10/8/2024/ua/full (дата звернення: 10.05.2025).

16. Освітня програма «Інформаційні управляючі системи і технології». Київський національний університет будівництва і архітектури: вебсайт. 2025. URL: https://surl.li/zoufso (дата звернення: 10.05.2025).

17. Освітня програма «Телекомунікації та радіотехніка». Ужгородський національний університет: вебсайт. 2025. URL: https://www.uzhnu.edu.ua/uk/program/160/telekomunikatsiji-ta-radiotehnika (дата звернення: 10.05.2025).