пропускної здатності, аналізу затримок, оцінено роботу каналів і виявлено особливості проходження пакетів у багатоканальній мережі.

1. O. Mishko, D. Matiuk, M. Derkach, Security of Remote IoT System Management by Integrating Firewall Configuration into Tunneled Traffic, Sci. J. TNTU, 115(3) (2024) 122–129.
2. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T. (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, 1-11.

Підготовка фахівців з кібербезпеки в умовах розвитку штучного інтелекту: необхідність посилення фізичного та радіотехнічного компонентів освіти

УДК 004.056:37.091.3

Сергій Семендяй

Національний університет "Чернігівська політехніка", serhii_semendiai@icloud.com

Сучасний розвиток технологій штучного інтелекту суттєво трансформує підходи до підготовки фахівців у сфері інформаційних технологій та кібербезпеки [1]. Значна частина завдань, пов'язаних із програмуванням, автоматизацією аналізу коду, генерацією конфігурацій та навіть пошуком вразливостей, дедалі активніше виконується із використанням інтелектуальних систем. Це призводить до зміни вимог до професійних компетентностей майбутніх фахівців. Водночас існує категорія знань та практичних навичок, які не можуть бути повністю замінені засобами штучного інтелекту, оскільки вони безпосередньо пов'язані з фізичними процесами поширення сигналів, особливостями роботи апаратури та реальними характеристиками середовищ передавання інформації.

Освітні програми спеціальності «Кібербезпека та захист інформації» традиційно містять дисципліни, пов'язані з технічним захистом інформації, безпекою бездротових і мобільних систем, виявленням технічних каналів витоку інформації та фізичними основами технічних засобів розвідки. Саме ці дисципліни формують у студентів розуміння того, що будь-яка інформаційна система функціонує не лише на програмному чи мережевому рівні, а й у реальному фізичному середовищі, де існують електромагнітні поля, паразитні випромінювання, наведення, побічні електромагнітні випромінювання та інші фактори, здатні створювати додаткові загрози безпеці інформації.

У сучасних умовах особливого значення набуває підготовка фахівців, які здатні працювати із вимірювальним обладнанням та спеціалізованими комплексами технічного контролю. Йдеться про використання аналізаторів спектру, SDR-платформ «HackRF» та Ettus Research USRP, нелінійних локаторів, детекторів поля, детекторів бездротових протоколів, а також спеціалізованих пошукових комплексів, зокрема типу «ANDRE» та «Delta». Ефективне використання таких засобів вимагає не лише теоретичних знань, а й

практичного досвіду роботи з реальними сигналами та розуміння фізичних принципів функціонування апаратури.

Крім того, важливим напрямом розвитку сучасного освітнього процесу є створення можливостей для віддаленої роботи студентів із зазначеним обладнанням під час онлайн-навчання. Організація дистанційного доступу до SDR-платформ, засобів аналізу спектру та спеціалізованих вимірювальних комплексів дозволяє забезпечити безперервність практичної підготовки, розширити доступ студентів до лабораторної бази та сформувати навички роботи з реальними системами навіть в умовах змішаного або дистанційного формату навчання (рис. 1).

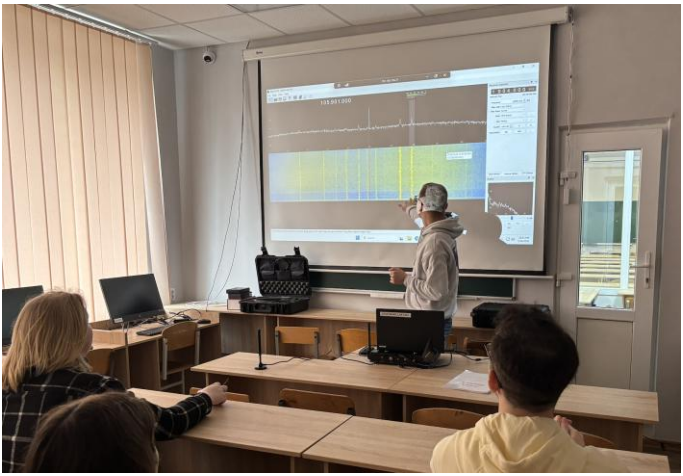

Рис. 1. Практична демонстрація можливостей дистанційного доступу до обладнання лабораторії кібербезпеки для аналізу спектра та дослідження сигналів

Важливим напрямом удосконалення сучасної освіти у сфері кібербезпеки є розширення практичного використання засобів моделювання процесів передавання та аналізу сигналів. Попри достатній рівень підготовки студентів у сфері програмного забезпечення, актуальним залишається формування глибокого розуміння фізичних процесів передавання інформації у дротових та бездротових середовищах, принципів формування спектру сигналів та впливу завад на функціонування систем зв'язку [2]. У цьому контексті перспективним є активніше використання середовищ MATLAB та «GNU Radio» у навчальному процесі.

Використання MATLAB дозволяє реалізовувати імітаційне моделювання каналів передачі інформації (в тому числі й технічних каналів витоку інформації), досліджувати вплив шумів та навмисних завад, аналізувати характеристики модуляції, демодуляції та кодування сигналів. Студенти можуть досліджувати залежність ймовірності бітової помилки від рівня сигнал/шум, моделювати роботу систем із частотним перестроюванням, оцінювати вплив широкосмугових та вузькосмугових завад. Такі підходи

формують фундаментальне розуміння процесів забезпечення стійкості систем передавання інформації, особливо в умовах навмисного завадового впливу (рис.2).

Своєю чергою, «GNU Radio» є ефективним інструментом для практичного опрацювання як аналогової, так і цифрової обробки сигналів та роботи із SDR-платформами [3]. Використання «GNU Radio» дозволяє студентам реалізовувати системи сканування спектру, виявлення та класифікації сигналів, досліджувати особливості різних протоколів бездротового зв'язку та аналізувати характеристики електромагнітного середовища. Особливу цінність має можливість інтеграції «GNU Radio» із SDR-пристроями, що дає змогу поєднати програмне моделювання з роботою у реальному радіоефірі.

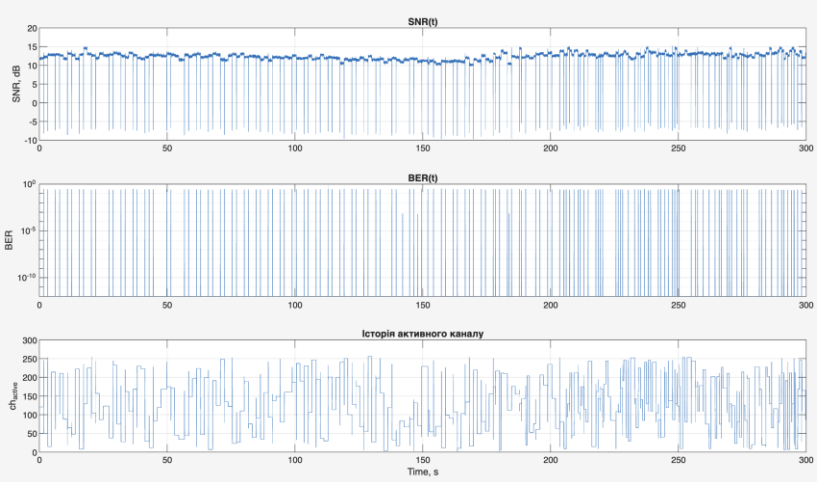

Рис. 2. Моделювання в середовищі MATLAB роботи захищеної системи передавання інформації

Важливим аспектом підготовки сучасного фахівця з кібербезпеки є розуміння принципів роботи засобів технічного контролю та їхніх обмежень. Студенти повинні не лише знати принципи функціонування детекторів поля чи нелінійних локаторів, а й розуміти їхні слабкі місця, можливі способи обходу та методики перевірки ефективності їх роботи. Наприклад, використання прихованих каналів передачі інформації, нестандартних схем модуляції або короткочасних імпульсних передач може суттєво ускладнювати процес виявлення сигналів. Аналогічно, сучасні бездротові пристрої можуть використовувати адаптивні алгоритми зміни частоти та потужності передачі, що також створює додаткові складності для систем моніторингу.

Не менш важливим є формування у студентів навичок аналізу електромагнітної обстановки та практичного виявлення технічних каналів витоку інформації. Фахівець з кібербезпеки повинен розуміти, яким чином можуть виникати побічні випромінювання, як вони поширюються у просторі,

які фактори впливають на дальність їх виявлення та якими методами може бути забезпечений їх контроль. У сучасних умовах ці питання набувають особливого значення у зв'язку із широким використанням бездротових технологій, IoT-пристроїв та програмно-визначених радіосистем.

Таким чином, розвиток технологій штучного інтелекту не зменшує актуальності фізичного та радіотехнічного компонентів підготовки фахівців з кібербезпеки, а навпаки – підвищує їх значення. Автоматизація окремих програмних задач призводить до того, що конкурентною перевагою майбутніх спеціалістів стають саме глибокі фундаментальні знання у сфері фізичних процесів передавання інформації, технічного захисту інформації та роботи зі спеціалізованими вимірювальними комплексами.

У сучасних умовах ефективна підготовка фахівців з кібербезпеки потребує поєднання програмно-аналітичних компетентностей із глибоким розумінням фізичних процесів передавання інформації, практичними навичками аналізу сигналів та роботи зі спеціалізованою вимірювальною апаратурою.

1. Горлинський, В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі / Віктор Горлинський, Борис Горлинський // Information Technology and Security. – 2024. – Vol. 12, Iss. 2 (23). – Pp. 268-282. – Bibliogr.: 36 ref.
2. Лаптєв О. А., Марченко В. В. Застосування завад для захисту інформації від витоку радіоканалом // Сучасний захист інформації. 2025. № 1 (61). С. 89–97.
3. ПІДХІД ДО ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ РАДІОКЕРОВАНИХ МОДЕЛЕЙ ЗА ЇХ РАДІОСИГНАЛОМ / В. О. МАРТОВИЦЬКИЙ та ін. Вісник Херсонського національного технічного університету. 2025. Т. 2, № 2(93). С. 228–237. URL: https://doi.org/10.35546/kntu2078-4481.2025.2.2.27 (дата звернення: 16.04.2026).

Забезпечення стійкості бездротового каналу зв'язку для дистанційного керування мобільною платформою

УДК 004.056.5

Софія Яворівська[1], Марина Деркач[2], Тарас Лобур[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]avorivskasofia@gmail.com, [2]m_derkach@tntu.edu.ua, [3]lobur_t@tntu.edu.ua

У сучасних умовах стрімкого розвитку Інтернету речей (IoT) питання безпечного дистанційного керування пристроями набуває критичного значення [1]. Бездротові канали зв'язку, що використовуються для передачі команд, часто стають об'єктами кіберзагроз, таких як перехоплення сигналу або зловмисна модифікація даних. Для забезпечення надійної роботи подібних систем необхідно поєднувати апаратну стійкість із комплексним управлінням ризиками інформаційної безпеки.

Для реалізації такого підходу було розроблено систему дистанційного керування мобільною платформою. Головним вузлом системи виступає мікроконтролер ESP32-S2-WROVER, який забезпечує отримання, обробку