http://www.moderntechno.de/index.php/meit/article/view/meit13-02-047
DOI: 10.30890/2567-5273.2020-13-02-047

УДК [004.7-047.72]:656.2

FORMATION OF ICT-COMPETENCE OF CYBERSECURITY SPECIALISTS USING THE RESEARCH APPROACH

ФОРМУВАННЯ ІКТ-КОМПЕТЕНТНОСТІ ФАХІВЦІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» З ВИКОРИСТАННЯМ ДОСЛІДНИЦЬКОГО ПІДХОДУ

Pakhomova V.M. / Пахомова В.М.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Dnipro National University of Railway Transport named after Academician V. Lazaryan, Ukraine, Dnipro, Lazaryan St., 2, 49010
Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, Україна, Дніпро, вул. Лазаряна, 2, 49010
Domanskay H.A. / Доманська Г.А.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-5746-299X
Dnipro National University of Railway Transport named after Academician V. Lazaryan, Dnipro, Lazaryan, 2, 49010
Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, Дніпро, Лазаряна, 2, 49010

Анотація. *Розглядається питання формування ІКТ-компетентності фахівців спеціальності «Кібербезпека» з використанням дослідницького підходу на основі дисципліни «Теорія проектування захищених комп'ютерних мереж». Формування ІКТ-компетентності передбачає три компоненти: когнітивний; практико-орієнтований і аксіологічний, уточнення змісту яких подано в роботі. До основних напрямів набуття дослідницької компетентності здобувачів віднесено: аналіз наукових джерел; математичну постановку задачі; створення програмної моделі; визначення оптимальної структури нейронної (нейронечіткої) мережі; дослідження отриманих результатів на створених моделях; побудову графічних залежностей та їх аналіз. Сформована ІКТ-компетентність фахівців залізничного транспорту спеціальності «Кібербезпека» надає можливість щодо здатності дослідження засобів захисту комп'ютерних мереж при їх проектуванні на відповідних моделях з використанням методів штучного інтелекту.*

Ключові слова: *залізничний транспорт, комп'ютерна мережа, MPLS, кібербезпека, атака, ІКТ-компетентність, дослідницький підхід.*

Вступ

Постановка проблеми. Міжнародна освітня спільнота прагне забезпечити якісну відкриту освіту, впроваджуючи компетентнісний підхід [1]. Одним із головних напрямів удосконалення сучасної вищої освіти є інтеграція в освітній процес наукових досліджень, що сприяє залученню студентів ВНЗ, зокрема університету залізничного транспорту [2], до дослідницького підходу.

Аналіз останніх досліджень. Оцінювання компетентностей являється предметом дослідження таких вчених як: Биков В. Ю., Гуревич Р. С., Гуржій А. М., Жалдак М. І., Морзе Н. В., Овчарук О. В., Сисоєва С.О., Спірін О. М. та ін.

У роботі [3] Спірін О. М. зазначає, що «*ІКТ-компетентність* – це підтверджена здатність особистості автономно і відповідально використовувати на практиці ІКТ для задоволення власних індивідуальних потреб і розв'язання суспільно значущих, зокрема професійних, задач у певній предметній галузі або виді діяльності». У дисертаційній роботі [4] Раков С. А. затверджує, що

дослідницька компетентність – це володіння методами дослідження соціально та індивідуально значущих задач за допомогою ІКТ та математичних методів.

Проведений аналіз останніх досліджень і публікацій виявив наступне: 1) відсутність загальної методики на основі апарату штучного інтелекту проектування нових комп'ютерних мереж, що на сучасному етапі не використовуються в інформаційно-телекомунікаційній системі (ІТС) залізничного транспорту; 2) відсутність універсальності застосування методики дослідження засобів захисту комп'ютерних мереж з використанням комбінованого підходу на основі нейронних мереж (НМ), імунних систем та нейронечітких класифікаторів; 3) існування широкого спектру систем моделювання комп'ютерних мереж, нейропакетів, мов програмування та різних типів НМ**,** і став підставою для уточнення компонентів ІКТ-компетентності.

Метою статті є формування ІКТ-компетентності майбутніх фахівців залізничного транспорту спеціальності «Кібербезпека» з використанням дослідницького підходу на основі дисципліни «Теорія проектування захищених комп'ютерних мереж» (ТПЗКМ).

1. Формування ІКТ-компетентності

На формування ІКТ-компетентності (інформаційно-комунікаційних технологій) впливає: знання сучасних технологій, що використовуються в ІТС залізничного транспорту; навики самостійного пошуку та відповідного аналізу; вміння використовувати спеціальні засоби для створення імітаційних, нейронних та нейронечітких моделей; навики організації досліджень з використанням нейромережної технології. Формування ІКТ-компетентності передбачає три компоненти: знаннєвий (когнітивний); діяльнісний (практико-орієнтований) і ціннісний (аксіологічний), що між собою тісно взємопов'язані [5]. *Когнітивний компонент* передбачає активізацію процесу теоретичної підготовки: основні/додаткові методи проектування нових та дослідження існуючих комп'ютерних мереж; проходження тестів самоконтролю в системі дистанційного навчання. *Практико-орієнтований компонент* передбачає надбання практичних умінь та навичок у сфері використання ІКТ (систем імітаційного моделювання комп'ютерних мереж, нейропакетів та мов програмування): обговорення в робочій групі соціальної мережі питань по створенню в моделюючій системі Opnet Modeler імітаційних моделей мереж фрагментів ІТС залізничного транспорту; пошук інформації в Інтернет; виконання індивідуального завдання за обраним рівнем відповідно до методичних рекомендацій щодо практичних занятій, лабораторних робіт та курсового проектування. *Аксіологічний компонент* передбачає засвоєння переваг використання ІКТ, саморозвитку у відповідності з сучасними світовими тенденціями, стимулювання творчого підходу: результатів проведених досліджень щодо використання в НДР та їх обговорення; особистих розробок електронних ресурсів навчальної діяльності; рекомендацій щодо підготовки матеріалів для обміну досвідом між здобувачами.

2. Використання дослідницького підходу

Гриневич Л. М., Морзе Н. В. та Бойко М. А. наголошують, що «*дослідницько-пізнавальний метод* (метод, заснований на запиті) має стати

найважливішим компонентом наукової програми на всіх рівнях і в усіх галузях науки» [6]. Так, наприклад, з одного боку для підвищення якості роботи мережі в ІТС залізничного транспорту рекомендовано дослідити можливість використання технології MPLS та організації вибору тунелю засобами НМ на основі даних про потоки трафіку та канали зв'язку, що складають відповідні тунелі. Один із можливих варіантів реалізації запропонований здобувачами під час курсового проектування з ТПЗКМ на основі ансамблю НМ (рис. 1, *k* – кількість каналів зв'язку, на основі яких формуються тунелі в MPLS): НМ №1 формує складову метрики з урахуванням завантаженості каналів зв'язку; НМ №2 формує складову метрики на основі часу передачі пакета; НМ №3 формує складову метрики на основі варіацій затримки; НМ №4 розраховує складену метрику каналів для прокладання тунелів. Для НМ підготовлені вибірки на основі даних, які отримані на імітаційній моделі мережі MPLS в системі Opnet Modeler. Проведені відповідні дослідження оптимальних параметрів НМ.

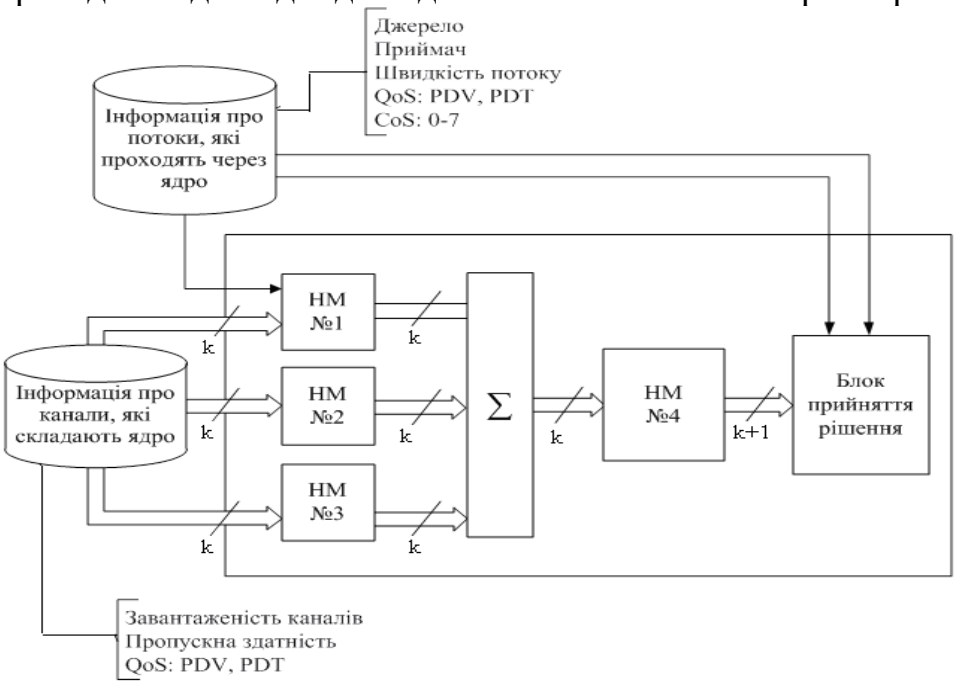

Рис. 1. Структура запропонованої системи розподілу потоків в MPLS:
CoS (Class of sersvice); QoS (Quality of Service); PDV (Packet Delay Variation); PDT (Packet Delay Time)

Авторська розробка

З другого боку, щоб підвищити точність виявлення атак на комп'ютерну мережу, зменшити кількість помилкових спрацьовувань та досягти більш високий рівень їх виявлення доречно розглянути комбінований підхід. Відомо, що на сучасному етапі найчастіше пропонуються системи виявлення мережевих атак, що побудовані на основі наступних НМ: багатошарового персептрону; мережі RBF; мережі Кохонена або самоорганізованої карти. Так, наприклад, під час виконання курсового проекту здобувачами ступеня «магістр» на основі нормалізованих даних відкритої бази NSL-KDD розглянуто питання ефективності двох підходів до виявлення атак: однієї НМ, що визначає клас атаки (перший підхід) та ансамблю із п'яти НМ (другий підхід), який на першому етапі визначає категорію атаки (DoS, Probe, U2R, R2L), а на другому

етапі клас атаки, що належить до певної категорії. У ході проведення експериментів за різними підходами отримані результати, на основі яких розраховані наступні показники оцінки якості рішень: коректність визначення мережевих атак; помилкові спрацьовування; достовірність; точність та повнота, що доказують доцільність використання ансамблю НМ (другого підходу) та в подальшому представлені в науковій роботі [7].

До основних напрямів набуття дослідницької компетентності здобувачів необхідно віднести: аналіз наукових джерел; складання математичної постановки задачі; створення програмної моделі (імітаційної, нейронної та нейронечіткої); виконання перевірки імітаційної моделі на адекватність; визначення оптимальної структури нейронної (нейронечіткої) мережі; дослідження отриманих результатів на моделях; побудову графічних залежностей та їх аналіз; формулювання висновків. Нейропакет (MatLAB, Fann Explorer, Deductor Studio та ін.) при створенні НМ, а також мова програмування (C++, Java, Python та ін.) при написанні програмної моделі обиралася здобувачами за їх особистими побажаннями та здібностями.

Висновки

1. Розглянуто питання формування ІКТ-компетентності фахівців залізничного транспорту спеціальності «Кібербезпека» з використанням дослідницького підходу на основі дисципліни ТПЗКМ. Запропонована методика складається з наступних етапів: використання моделюючій системи Opnet Modeler для створення моделі мережі MPLS в ІТС (на практичних заняттях); використання нейропакетів для створення нейронних (нейронечітких) мереж (на лабораторних роботах); створення програмної моделі (під час виконання курсового проекту) з метою організації досліджень.

2. Фахівцями залізничного транспорту спеціальності «Кібербезпека» було доведено: по-перше, доцільність використання технології MPLS в ІТС залізничного транспорту, запропонована система розподілу потоків з урахуванням параметрів QoS, основу якої складає ансамбль НМ; по-друге, доцільність використання дворівневої системи виявлення мережевих атак, яка на першому етапі визначає категорію атаки (DoS, Probe, U2R, R2L), а на другому етапі клас атаки, що належить до певної категорії.

Література:

1. Commission working document. Consultation on the future «EU2020» strategy. [Електронний ресурс]. URL: http://eur-lex.europa.eu/

2. A Railway Strategy for CAREC, 2017-2030 – Asian Development Bank. [Електронний ресурс]. URL: https://www.adb.org/sites/default/files/-institutionaldocument/227176/carec-railway-strategy-2017-2030.pdf

3. Спірін О. М. Критерії і показники якості інформаційно-комунікаційних технологій навчання. Інформаційні технології і засоби навчання, №1(33), 2013. [Електронний ресурс]. URL: http:// journal.iitta.gov.ua

4. Раков С. А. Формування математичних компетентностей учителя математики на основі дослідницького підходу у навчанні з використанням інформаційних технологій: дис. докт. педаг. наук, Харківський нац. педаг. ун-т

ім. Г. С. Сковороди, Харків, 2005.

5. Самборська О. Д. Понятійний тезаурус інформаційно-цифрової компетентності майбутнього педагогічного працівника початкової освіти. Інформаційні технології в освіті, № 1(38), 85-96, 2019.

6. Гриневич Л. М., Морзе Н. В., Бойко М. А. Наукова освіта як основа формування інноваційної компетентності в умовах цифрової трансформації суспільства. Інформаційні технології і засоби навчання, т. 77, № 3, 1-26, 2020.

7. Пахомова В. М., Коннов М. С. Дослідження двох підходів до виявлення мережевих атак з використанням нейромережної технології. Наука та прогрес транспорту, 2020, № 3(87), 81-93. DOI: 10.15802/stp2020/208233

Abstract. *Considers the formation of ICT-competence of specialists in the specialty «Cybersecurity» using a research approach based on the discipline «Theory of design of secure computer networks». The formation of ICT-competence involves three components: cognitive; practice-oriented and axiological, the content of which is specified in the article. The main areas of acquisition of research competence of applicants include: analysis of scientific sources; mathematical formulation of the problem; creation of a software model; determination of the optimal structure of the neural (fuzzy) network; research of the received results on the created models; construction of graphic dependencies and their analysis. The formed ICT-competence of railway transport specialists in the specialty «Cybersecurity» provides an opportunity for the ability to study the means of protection of computer networks when designing them on appropriate models using artificial intelligence methods.*

Keywords: *railway transport, computer network, MPLS, cybersecurity, attack, ICT-competence, research approach.*