МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чернівецький національний університет імені Юрія Федьковича

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Першого рівня вищої освіти

за спеціальністю №125 – Кібербезпека та захист інформації

галузі знань 12 - Інформаційні технології

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ /_____/

(протокол № __ від "__" _____ р.)

Введено в дію наказом

від "__" _____ за № ___

Чернівці
2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

" РОЗРОБЛЕНО "
Робочою групою _____

_____

Керівник робочої групи
_____ _____

«___» _____20__ р.
_____ Г.І. Ластівка

" УХВАЛЕНО "
на засіданні кафедри радіотехніки та інформаційної безпеки
ЧНУ ім. Юрія Федьковича

Протокол № __
від «_____» _____ 20__ р.

Зав. кафедрою
_____ А.П. Саміла

" СХВАЛЕНО "
Вченою радою факультету /інституту
_____
Протокол № _____
від «_____» _____ 20__ р.
Голова Вченої ради факультету /інституту
_____ _____

" ПОГОДЖЕНО "
Начальник навчального відділу
ЧНУ ім. Юрія Федьковича
_____ Я.Д. Гарабажів
«_____» _____ 20__ р.

" РЕКОМЕНДОВАНО "
Комісією з навчально-методичної роботи Вченої ради
ЧНУ ім. Юрія Федьковича
Протокол № ____ від «___» _____ 20__ р.
Голова комісії університету ___ О.В. Мартинюк

ПЕРЕДМОВА

Розроблено робочою групою спеціальності 125 – Кібербезпека та захист інформації у складі:

1. Шпатар Петро Михайлович – к.т.н., доцент, завідувач кафедри радіотехніки та інформаційної безпеки;

2. Вовчук Дмитро Анатолійович – к.т.н., асистент кафедри радіотехніки та інформаційної безпеки;

3. Косован Григорій Васильович – к.т.н., асистент кафедри радіотехніки та інформаційної безпеки.

4. Гресь Олександр Володимирович – к.т.н., доцент, асистент кафедри радіотехніки та інформаційної безпеки.

Гарант освітньої програми:

Ластівка Галина Іванівна – к.т.н., доцент кафедри радіотехніки та інформаційної безпеки

Стейкхолдери:

1. Авасилоає О.Г., здобувачка освіти першого (бакалаврського) рівня вищої освіти ОПП «Кібербезпека» за спеціальністю 125 – Кібербезпека галузі знань 12 – Інформаційні технології

2. Зайцева В.В., випускниця першого (бакалаврського) рівня вищої освіти ОПП «Кібербезпека» за спеціальністю 125 – Кібербезпека галузі знань 12 – Інформаційні технології;

3. Савчук Р., інженер з кібербезпеки компанії «Datami» (м. Чернівці).

Прізвище, ім'я, по батькові керівника та членів проектної групи	Найменування посади, місце роботи	Найменування закладу, який закінчив викладач, рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту*	Науковий ступінь, шифр і найменування наукової спеціальності, тема дисертації, вчене звання, за якою кафедрою (спеціальністю) присвоєно	Стаж науково - педагогічної та/або наукової роботи	Інформація про наукову діяльність (основні публікації за напрямом, науково-дослідній роботі, участь у конференціях і семінарах, робота з аспірантами та докторантами, керівництво науковою роботою студентів)	Відомості про підвищення кваліфікації викладача (найменування закладу, вид документа, тема, дата видачі)
Керівник проектної групи						
Ластівка Галина Іванівна	к.т.н., доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича	Чернівецький державний університет, 1999 р., спеціальність „Радіотехніка", магістр радіотехніки. Диплом ДМ № 003694 від 19.06.1999 р.	Канд. технічних наук, диплом ДК №064434 від 22.12.2010 05.27.01- твердотільна електроніка ; «Оптимізація фотоел. характеристик гетероструктур на основі моноселенідів індію та галію методом ЯКР» Доцент кафедри радіотехніки та інформаційної безпеки (12ДЦ № 035476 протокол № 5/02-Д від 31 травня 2013 р.)	21 р.	1. Методи і засоби ТЗІ: методичні вказівки до курс. проектування/ укл.: Ластівка Г. І., Гресь О. В. [Навч. ел. видання] – Чернівці: Чернівецький нац. університет, 2022. – 90 с. https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view 2. Oleksandr Dubyniak, Halyna Lastivka, Oleksandr Lastivka Study of methods of artificially generated voice information detection // IX International Scientific-Practical Conference Physical and Technological Problems of Transmission, Processing and Storage of Information in Infocommunication Systems 21-23 October 2021, Chernivtsi-Suceava (Ukraine-Romania). 3. Samila, A., Khandozhko, A., Lastivka, G., Khandozhko, V. Evaluation of the contribution of higher-order electron-nuclear interactions to the NQR frequencies using 115In spectra in InSe. Proceedings of SPIE - The International Society for Optical Engineering, 2021, Vol. 12126, 121260H-129–134 https://www.spiedigitallibrary.org/co	Lublin University of Technology, "Lubelska Politechnica", Poland. Traineeship: "New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring", during 15.05.2023-15.07.2023, 180 hours / 6 credits ECTS, Sertificate

					nference-proceedings-of-spie/12126/2615420/Evaluation-of-the-contribution-of-higher-order-electron-nuclear-interactions/10.1117/12.2615420.full 4. Samila, A.P., Lastivka, G.I., Tanasyuk, Y.V. Actual problems of computer parametric identification of the NMR and NQR spectra: A review. J. Nano- Electron. Phys. 2019. Vol. 11, No 5. P. 05036-1–10. https://www.scopus.com/record/display.uri?eid=2-s2.0-85075778494&origin=resultslist https://www.scopus.com/sourceid/21100210917?origin=resultslist 5. A. Veryha, R. Politansky, M. Rozhdestvenska and H. Lastivka. Analysis of Self-Similar Binary Sequences // Security of Infocommunication Systems and Internet of Things. – 2023. Vol 1, №1. P. 01003-1-5. https://doi.org/10.31861/sisiot2023.1.01003 6. Дубиняк О., Ластівка Г., Ластівка О. Вивчення та дослідження методів виявлення штучно згенерованої мовної інформації // VI Всеукр. науково-практична конф. «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем» (MEICS-2021). Дніпро, 24-26 листопада 2021 р. http://meics.dnure.dp.ua/program 7. В. В. Браїловський, Г. І. Ластівка, І. С. Паюк, М. Г. Рождественська, П. М. Шпатар. Використання засобів платформи MOODLE для підготовки здобувачів вищої освіти з кібербезпеки до ЄДКІ. XI Міжнар. науково-практична конференція	№ 5-2023-ChNU, 15-07-2023. Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001740-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії». Програма підвищення каліф. з серії наук.-метод. семінарів-практикумів «Алгоритм підготовки до викладання фахових дисциплін англійською мовою» (ЧНУ). З 29.01.2020 по 25.06.2020. Сертифікат, наказ №190 від

					"Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій", 12–14 грудня 2022 р., м. Запоріжжя.- С. 89-91. URL: https://scholar.google.com/scholar?oi=bibs&cluster=18208501513419092697&btnI=1&hl=uk Відповідальний секретар редакційної колегії журналу «Безпека інфокомунікаційних систем та Інтернету речей», сформованого відповідно до наказу № 239 від 1.09.2022 р. Мережна Академія Cisco (Cisco Networking Academy in Ukraine), інструктор Участь в роботі міжнародного освітнього гранту G-202206-68835 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University» під егідою CRDF Global в Україні (Меморандум про взаєморозуміння між Чернівецьким нац. ун-том ім. Юрія Федьковича та Представництвом Фонду цивільних досліджень та розвитку США від 17.06.2022 р.).	17.07.2020. Підвищення кваліфікації у Центрі підтримки академій Cisco Нац. технічного університету «Харківський політехнічний інститут» в рамках Програми Академій Cisco (курс «Основи апаратного та програмного забезпечення ПК» та СТЕМ-практика з Інтернету речей та кібербезпеки). З 1.09.2020 по 25.10.2020. Сертифікат від 25.10.2020 р.
Члени проектної групи						
Шпатар Петро Михайлович	к.т.н., завідувач кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича	Чернівецький державний університет, 1999 р., спеціальність „Радіотехніка”, магістр радіотехніки. Диплом ДМ № 003695	Канд. технічних наук, диплом ДК № 042595 від 11 жовтня 2007 р. (прот. № 19-08/8) 05.27.01-твердотільна електроніка ; «Розробка електронних схем	20 р.	1. Ластівка Г. І., Шпатар П. М. Технічний захист інформації в інформаційних та телекомуніка-ційних системах: навч. посіб. Чернівці: ЧНУ, 2018. – 252 с. 2. Криптографія. Методичні вказівки до вивчення дисципліни. Укл.: Шпатар П.М. Електронний навчальний посібник.	Lublin University of Technology, “Lubelska Politechnica”, Poland. Traineeship: “New knowledge in the development of information

		від 03.07.1999 р.	сенсорів теплових величин» Доцент кафедри радіотехніки та інформаційної безпеки (12 ДЦ № 032416 26 вересня 2012 р.)		http://radiotech.cv.ua/?view=methodical-work 3. Rozorinov H., Hres O., Rusyn V., Shpatar P. Environment of electromagnetic compatibility of radio-electronic communication means. IAPGOŚ. 2020. №1. Pp. 16-19. ISSN: 2391-6761 (on-line), 2083-0157 (print) (https://ph.pollub.pl/index.php/iapgos/article/view/917/1281) 4. Шпатар П.М., Гресь О.В., Качур В.В., Томулець А.Я. Детектування поодиноких фотонів в квантових криптографічних системах. Вісник ХНУ, Серія: технічні науки. 2020. №6. С. 28-32. ISSN 2307-5732 http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291-1.pdf. 5. P.M. Shpatar, O.V. Hres, H.M. Rozorinov. Single photons receiver based on avalanche photodiodes. 15th International Conference on Correlation Optics. Ukraine, September 13-16, 2021 http://icco.chnu.edu.ua/2021/09/13/single-photons-receiver-based-on-avalanche-photodiodes/ 6. R. Politanskyi, P. Shpatar, M. Vistak, O. Malanchuk, I. Kremer, I. Diskovskyi. Nanostructured Detector of Electromagnetic Radiation Based on Spintronics Devices. 2021 IEEE 11 th International Conference “Nanomaterials: Applications & Properties” (NAP-2021) Odessa, Ukraine, September 05–11, 2021, NMM-A-05 https://drive.google.com/file/d/11RWKVgZot1Bv1OYIoSFdPqjiqhqrGpAI/view?usp=sharing	technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, during 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 4-2023-ChNU, 06-05-2023. Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001751-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного

					7. Rozorinov H. Generalized model of the process of information protection in audiovisual content networks / Rozorinov H., Sirchenko I., Shpatar P., Hres O., Nichyy B. // Proccedings of IX International Scientific and Practical Conference “Physical and technical problems of information transmission, processing and storage of information communication systems”. – 21-23 October, 2021, Chernivtsi Suceava (Ukraine-Romania). – Pp. 78-80.	навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії».
Вовчук Дмитро Анатолійович	к.т.н., асистент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича	Чернівецький національний університет імені Юрія Федьковича, 2013 р., „Системи технічного захисту інформації, автоматизація її обробки”, магістр з інформаційної безпеки. Диплом РН № 45653525 від 30.06.2013 р.	Канд. технічних наук, диплом ДК № 039891, 13.12.2016 р; 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій; «Елементи широкосмугових засобів зв’язку на основі детермінованого хаосу та провідникових метаструктур»	7 р.	1. Serhii Haliuk, Oleh Krulikovskyi, Dmytro Vovchuk, and Fernando Corinto Memristive Structure-Based Chaotic System for PRNG. Symmetry (MPDI). 2022. Vol. 14(1), No. 68. https://www.mdpi.com/2073-8994/14/1/68/html 2. Mykola Kushnir, Dmytro Vovchuk, Serhii Haliuk, Petro Ivaniuk and Ruslan Politanskyi “Approaches to Building a Chaotic Communication System”, Data-Centric Business and Applications (Book Chapter), Springer, Vol. 48, pp. 207-227, 2020. DOI: 10.1007/978-3-030-43070-2_11 3. Д. А. Вовчук, С.Д. Галюк, Л.Ф. Політанський, П.Ф. Робулець Спектральні характеристики сигналів, що передаються через провідникову метаструктуру. Вісник Хмельницького національного університету. 2019, – №4(275), с. 141-146. http://journals.khnu.km.ua/vestnik/pdf/tech/pdfbase/2019/2019_4/(275)%202019-4-t.pdf Підготовлено студентів до участі у	Наукове стажування в Університеті Тель-Авіва (м. Тель-Авів, Ізраїль). З 01.07.2021 до 1.06.2023. Наказ №204-від (01.07.2021) та №160-від (24.06.2022).

					всеукраїнському конкурсі студентських наукових робіт (ХНУРЕ, 2021р.); нагороджено дипломом ІІ ступеня. Студенти: Деревеснікова Євгенія, Андрійчук Ксенія (здобувачі освіти за спец. 125 – Кібербезпека).	
Косован Григорій Васильович	к.т.н., асистент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича	Чернівецький національний університет імені Юрія Федьковича, 2009 р., „Захист інформації з обмеженим доступом та автоматизація її обробки”, магістр з інформаційної безпеки. Диплом РН № 37432254 від 30.06.2009 р.	Канд. технічних наук, диплом ДК №052173 від 23 квітня 2019 р.; 05.13.21 – системи захисту інформації; «Синтез генераторів псевдовипадкових послідовностей із нелінійною динамікою для захисту інформації в телекомунікаційних системах»	9 р.	1. Mykola Kushnir Synthesis of pseudorandom sequences generators based on chaotic systems and study of their statistical characteristics / Mykola Kushnir, Hryhorii Kosovan, Andrii Veryga and Serhii Haliuk // Information Security in Critical Infrastructures. Collective monograph. Edited Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019. 445p. 2. Mykola Kushnir Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic / Mykola Kushnir, Hryhorii Kosovan, Petro Krojalo and Andrii Komarnytskyy // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET - 2020), February 25-29, 2020. Lviv-Slavske, Ukraine. – 4 Pp. 3. Кушнір М. Я. Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ. № 1 (01) 2021. Київ. Україна. С 63-72. 4. Kushnir M. Ya. Properties of	Центр перепідготовки та післядип. освіти, Тернопільський нац. технічний ун-т ім. І.Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102 / 001738-21 від 18.06.2021 Тема: «Наукові основи та прогр.-апаратні засоби запровадження технологій електрон. навчання в освітній процес з метрології, телеком. електр. інженерії та поліграфії» Кафедра безпеки інф. технологій Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020 р. Свідоцтво АА № 02071197 / 000004-20 від 19.02.2020 Тема: «Оцінювання захищеності

					generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems / Kushnir M. Ya., Kosovan Hr. V., Kroyalo P. M. // The scientific journal "Radio Electronics, Computer Science, Control". 2022. № 1. Vol.60. P. 39-47. p-ISSN 2313-688X. 5. Kushnir M. Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic / Kushnir M., Kosovan Hr., Kroyalo P. // The scientific journal "Radioelectronic and Computer Systems". 2022. № 4. Vol. 104. P. 117-128. p-ISSN 1814-4225. 6. Засоби радіопротидії в інформаційно-телекомунікаційних системах/ Браїловський В.В., Рождественська М.Г., Гресь О.В., Косован Г.В./ Електронний навч. посібник, Чернівці: Чернівецький нац. університет, 2021. URL: http://surl.li/jwsdf Підготовлено студентів до участі у всеукраїнському конкурсі студентських наукових робіт з галузі знань "Інформатика та Кібернетика". (22-23 квітня 2021р.). Здобуто 3 місце. Студенти Мочернюк Т. М., Антоняк С. М. Тема роботи: "Метод шифрування зображень на основі хаотичних систем із застосуванням нечіткої логіки"	інформації. Експертні оцінювання у сфері захисту інформації». Кафедра безпеки інф. технологій Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020. Свідоцтво АА № 02071197 / 0000010-20 від 21.02.2020. Тема: «Виявлення закладних пристроїв». Захист кандидатської дисертації, 2019 р.
Гресь Олександр Володимирович	к.т.н., доцент, асистент кафедри радіотехніки та інформаційної безпеки Чернівецького	Чернівецький національний університет імені Юрія Федьковича, 2008 р.,	Канд. технічних наук, диплом ДК №056646 від 14 травня 2020 р.; 05.13.21 – системи захисту інформації;	13 р.	1. Larin V., Rozorinov H., Hres O., Rusyn V., Subbotin S., Chichikalo N., Larina K. (2022) Decision-making Algorithm in Case of Failure of the Electric Motor of a Multi-rotor	Lublin University of Technology, "Lubelska Politechnica", Poland. Traineeship: "New

	національного університету імені Юрія Федьковича	“Захист інформації з обмеженим доступом та автоматизація її обробки”, спеціаліст з інформаційної безпеки. Диплом РН №35176121 від 30 червня 2008 р.	«Методи потокового шифрування інформації на основі генераторів хаосу з дискретними функціями відображення»		Unmanned Aerial Vehicle. CEUR Workshop Proceedings, 3137, 154-163, ISSN 1613-0073. (індексується Scopus) https://ceur-ws.org/Vol-3137/paper13.pdf 2. Rozorinov, H., Hres, O., Rusyn, V. (2022) GENERALIZED MODEL OF INFORMATION PROTECTION PROCESS IN AUDIOVISUAL CONTENT DISTRIBUTION NETWORKS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 12(4), pp. 21–25, ISSN 2083-0157 (індексується Scopus) https://ph.pollub.pl/index.php/iapgos/article/view/3317 3.Rozorinov H., Hres O., Rusyn V., Shpatar P. Environment of electromagnetic compatibility of radio-electronic communication means. IAPGOŚ. 2020. №1. Pp. 16-19. ISSN: 2391-6761 (on-line), 2083-0157 (print) (https://ph.pollub.pl/index.php/iapgos/article/view/917/1281) 4. Гресь О. В., Розорінов Г. М., Пількевич Ю. Г., Костяк М. Ю., Пархуць Л. Т. Програмна реалізація системи потокового шифрування інформації на основі дискретних відображень. Вимірювальна та обчислювальна техніка в технологічних процесах. 2020. №1. С.60-66. ISSN 2219-9365 https://journals.khnu.km.ua/index.php/MeasComp/article/view/2021/2480 , 5. Шпатар П.М., Гресь О.В., Качур В.В., Томулець А.Я. Детектування поодиноких фотонів в квантових криптографічних системах. Вісник	knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, during 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 3-2023-ChNU, 06-05-2023. Підвищення кваліфікації на тему: “Оцінювання захищеності інформації. Експертні оцінювання у сфері технічного захисту інформації”, (“Information protection assessment. Expert evaluation in the technical protection of information”, Харківський нац.

					ХНУ, Серія: технічні науки. 2020. №6. С. 28-32. ISSN 2307-5732 http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291-1.pdf. 6. Rozorinov H. Generalized model of the process of information protection in audiovisual content networks / Rozorinov H., Sirchenko I., Shpatar P., Hres O., Nichyy B. // Proccedings of IX International Scientific and Practical Conference "Physical and technical problems of information transmission, processing and storage of information communication systems". – 21-23 October, 2021, Chernivtsi Suceava (Ukraine-Romania). – Pp. 78-80. 7. Гресь О.В., Косован В.М. Програмні засоби для дослідження властивостей генератора псевдовипадкових послідовностей на основі дискретного відображення /О.В. Гресь, В.М. Косован // Міжнародна наукова інтернет конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення", 6-7 липня 2023. – Тернопіль, Україна – Переворськ, Польща. Випуск 79, С. 12-15. http://www.konferenciaonline.org.ua/ua/article/id-1243/ 8. Методи і засоби ТЗІ: методичні вказівки до курс. проектування/ укл.: Ластівка Г. І., Гресь О. В. [Навч. ел. видання] – Чернівці: Чернівецький нац. університет, 2022. – 90 с. https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view	університет радіоелектроніки, 2020 р. Свідоцтво про підв. квал. №АА 02071197/000002-20 від 19 лютого 2020 року Підвищення кваліфікації на тему: "Виявлення закладних пристроїв", ("Development of pocket devices", Харківський нац. університет радіоелектроніки, 2020 р. Свідоцтво про підв. квал. №АА 02071197/000008-20 від 21 лютого 2020 року Захист кандидатської дисертації, 2020 р.

					Виконання функцій члена редакційної колегії наукового видання, включеного до переліку фахових видань України. (з жовтня 2022 року): наукове фахове видання України (Категорія Б), науково-технічний журнал: “Вимірювальна та обчислювальна техніка в технологічних процесах” https://vottp.khmnu.edu.ua/index.php/vottp/about/editorialTeam	
Стейкхолдери:						
Савчук Ростислав Юрійович	Інженер з кібербезпеки компанії «Datami» (м. Чернівці)	Чернівецький національний університет імені Юрія Федьковича, 2021 р., „Кібербезпека”, бакалавр з кібербезпеки.				
Зайцева Вікторія Владиславівна	Інженер з кібербезпеки компанії «Datami» (м. Чернівці)	Чернівецький національний університет імені Юрія Федьковича, 2023 р., „Кібербезпека”, бакалавр з кібербезпеки.				
Здобувачі освіти:						
Авасилоає Олена Георгіївна	Студентка 325 групи ННІФТКН ЧНУ, здобувачка освіти першого (бакалаврського)					

	рівня вищої освіти ОПП «Кібербезпека» за спеціальністю 125 – Кібербезпека та захист інформації галузі знань 12 – Інформаційні технології					

Профіль освітньо-професійної програми «Кібербезпека»
зі спеціальності 125 – Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Чернівецький національний університет імені Юрія Федьковича Навчально-науковий інститут фізико-технічних та комп'ютерних наук Кафедра радіотехніки та інформаційної безпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Перший (бакалаврський) Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, обсяг освітньої програми та термін навчання: – на базі повної загальної середньої освіти з терміном навчання 11 років становить 240 кредитів ЄКТС (термін навчання 3 роки 10 місяців); – на основі диплома молодшого спеціаліста становить 120 кредитів ЄКТС (термін навчання 1 рік 10 місяців); – на основі диплома фахового молодшого бакалавра становить 180 кредитів ЄКТС (термін навчання 2 роки 10 місяців).
Наявність акредитації	Сертифікат про умовну (відкладену) акредитацію ОПП «Кібербезпека», № 7361, виданий НАЗЯВО 28.03.2024), строк дії 26.03.2025 р.
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень
Передумови	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення опису освітньої програми	http://radiotech.chnu.edu.ua/educationprograms/
2 – Мета освітньої програми	
Підготувати високопрофесійних, конкурентоспроможних, висококваліфікованих фахівців у галузі інформаційних технологій зі спеціальності 125 – Кібербезпека та захист інформації, здатних активно діяти в умовах ринкової економіки та соціального партнерства, а також вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів окремих суб'єктів або держави в цілому від ризику стороннього кібернетичного впливу. ОПП «Кібербезпека» відповідає місії ЧНУ, що передбачає інноваційність, збалансованість, успіх і реалізується через розвиток системи освіти та наукової діяльності шляхом підготовки високопрофесійних, конкурентоспроможних фахівців, здатних активно діяти в умовах ринкової економіки та соціального партнерства; розвиток наукових пріоритетів, наукових шкіл, інноваційної складової.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності**))**	Галузь знань: 12 – Інформаційні технології Спеціальність: 125 – Кібербезпека та захист інформації Об'єкти вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; – об'єкти інформаційної діяльності, в тому числі інформаційні та

	інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне і спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації. Ключові слова: інформаційна безпека, кібербезпека, технічний захист інформації.
Особливості програми	Освітньо-професійна програма передбачає підготовку висококваліфікованих, конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації на основі співпраці з підприємствами, організаціями та державними установами Західного регіону, науково-дослідними та освітніми закладами України та інших країн, з урахуванням індивідуальних потреб здобувачів. Особливостями програми є ґрунтовна підготовка з англійської мови, можливість отримати базові знання та практичні навички щодо методів і засобів забезпечення захисту інформації, а також інформаційно-телекомунікаційних систем і мереж, що відповідає запитам стейкхолдерів.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації. Відповідно до Державного класифікатора професій ДК 003:2010: випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 Фахівець з криптографічного захисту інформації. 2139.2 Фахівець з реагування на інциденти кібербезпеки 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець з технічного захисту інформації 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець сфери захисту інформації Освітньо-професійна програма розроблена з орієнтацією на професійну кваліфікацію 2139.2 – Фахівець сфери захисту інформації, проте права випускників на працевлаштування не обмежуються.
Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.

5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, семінари, ознайомча та виробничо-технологічна практики, самостійна робота (підготовка презентацій, рефератів, розрахункових та курсових робіт), в тому числі проведення занять за допомогою технологій дистанційного навчання.
Оцінювання	Екзамени та заліки в усній або письмовій формі, тести, захист практик, курсових робіт/проектів.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності.
	ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.
	ЗК 4. Здатність спілкуватися іноземною мовою.
	ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.
	ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
	ЗК 7. Здатність ухвалювати рішення і діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
	ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, предметні) компетентності	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
	СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
	СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
	СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
	СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
	СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
	СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

	СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.
	СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Програмні результати навчання	
	РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.
	РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
	РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
	РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
	РН 5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
	РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
	РН 7. Застосовувати і адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній дільності.
	РН 8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
	РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
	РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
	РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.
	РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
	РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
	РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

	РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
	РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
	РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
	РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
	РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
	РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
	РН 22. Забезпечувати супровід систем захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, брати участь у розробці нормативної документації та стандартів щодо систем інформаційної та/або кібербезпеки англійською мовою.
	РН 23. Зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історичних подій, закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя, а також виконувати завдання, пов'язані із застосуванням теорії та базових практичних навичок загальновійськової підготовки.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Характеристика кадрового забезпечення: 1. Випусковою є кафедра радіотехніки та інформаційної безпеки Навчально-наукового інституту фізико-технічних і комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича. 2. Робоча група ОПП складається з 6 кандидатів технічних та фізико-математичних наук, 3 з яких мають вчене звання доцента. 3. Гарант освітньої програми – Ластівка Галина Іванівна, кандидат технічних наук, доцент кафедри радіотехніки та інформаційної безпеки. 4. Проведення лекцій, практичних, семінарських та лабораторних занять, наукове керівництво випускними кваліфікаційними роботами здійснюється науково-педагогічними працівниками, які відповідають вимогам Ліцензійних умов провадження освітньої діяльності закладів освіти. До проведення занять залучаються фахівці-практики у сфері інформаційної та кібербезпеки.

Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності закладів освіти.
Інформаційне та навчально-методичне забезпечення	Обсяг, склад та якість інформаційного та навчально-методичного забезпечення відповідають Ліцензійним умовам провадження освітньої діяльності закладів вищої освіти згідно з діючим законодавством України - інформаційне забезпечення: 1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявний доступ до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. На офіційному веб-сайті закладу освіти розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація. 4. Електронний ресурс закладу освіти (Moodle) містить навчально-методичні матеріали з навчальних дисциплін навчального плану. - наявність навчально-методичного забезпечення: 1. Освітня програма, навчальний план, робочі програми, силабуси з усіх навчальних дисциплін навчального плану. 2. Програми практичної підготовки. 3. Навчальні матеріали з кожної навчальної дисципліни навчального плану, в тому числі підручники, навчальні посібники, конспекти лекцій (в тому числі в електронній формі), методичні вказівки щодо виконання лабораторних та практичних робіт. 4. Методичні матеріали для проведення атестації здобувачів.
9 – Академічна мобільність	
Національна кредитна мобільність	Укладені угоди про академічну мобільність на основі двосторонніх договорів між Чернівецьким національним університетом імені Юрія Федьковича та ЗВО України.
Міжнародна кредитна мобільність	Укладені угоди про міжнародну академічну мобільність (Еразмус+) на основі двосторонніх договорів між Чернівецьким національним університетом імені Юрія Федьковича та ЗВО країн-партнерів.
Навчання іноземних здобувачів вищої освіти	В рамках ліцензії передбачається підготовка іноземців.

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОПП

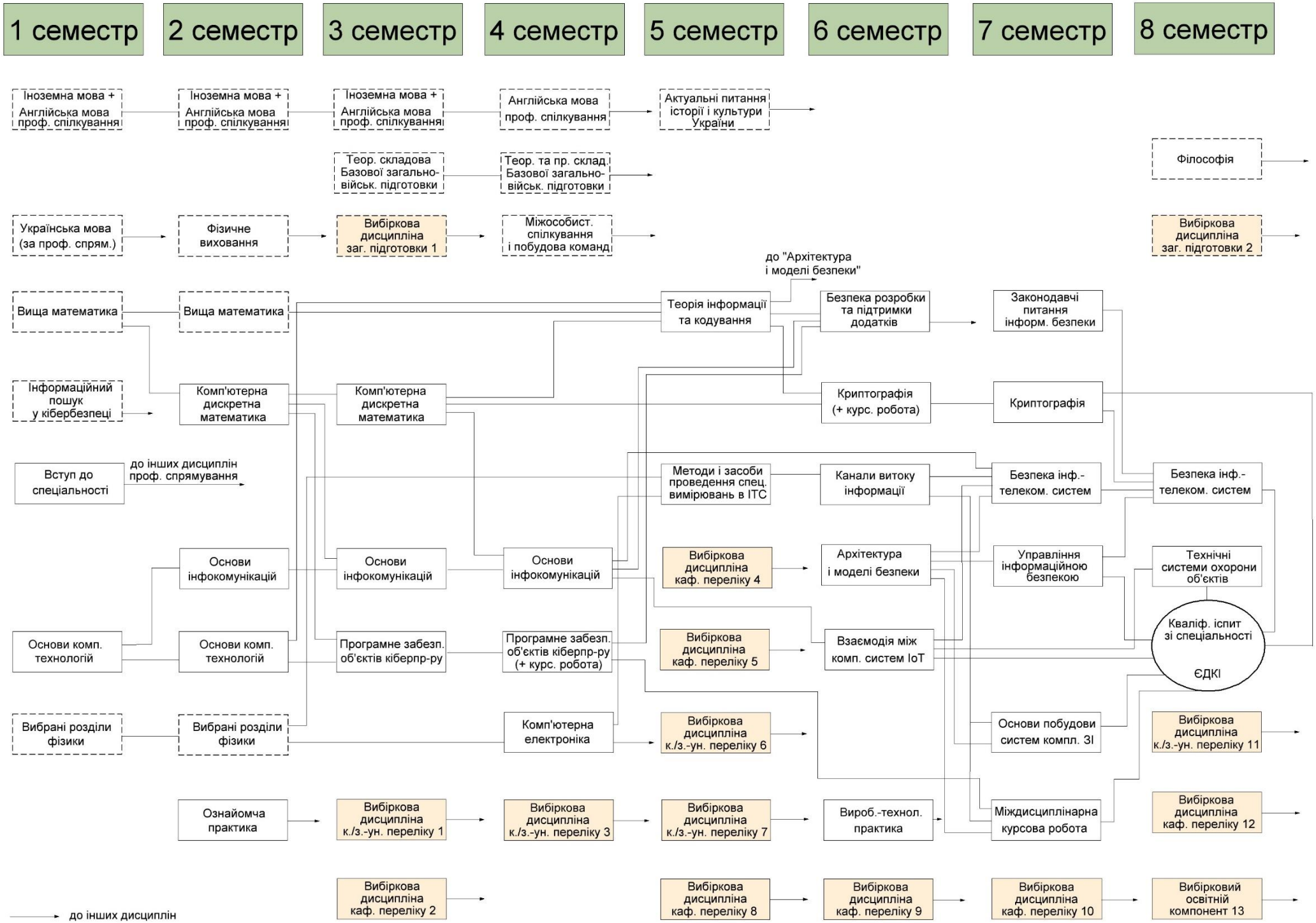
Код н/д (в т.ч. в навч. плані)	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК 1 (ЗПО1)	Іноземна мова (за професійним спрямуванням)	6	Залік, екзамен
ОК 2 (ЗПО2)	Англійська мова професійного спілкування	24	Залік, екзамен
ОК 3 (ЗПО3)	Українська мова (за професійним спрямуванням)	3	Залік
ОК 4 (ЗПО4)	Інформаційний пошук у кібербезпеці	3	Залік
ОК 5 (ЗПО5)	Вибрані розділи фізики	7	Екзамен
ОК 6 (ЗПО6)	Вища математика	6	Екзамен
ОК7 (ЗПО8)	Міжособистісне спілкування і побудова команд	3	Залік
ОК 8 (ЗПО9)	Актуальні питання історії і культури України	3	Екзамен
ОК 9 (ЗПО10)	Філософія	4	Екзамен
ОК 10 (ППО1)	Вступ до спеціальності	3	Залік
ОК11 (ППО2)	Основи комп'ютерних технологій	9	Екзамен
ОК12 (ППО3)	Комп'ютерна дискретна математика	7	Залік, екзамен
ОК13 (ППО4)	Основи інфокомунікацій	11	Залік, екзамен
ОК14 (ППО5)	Програмне забезпечення об'єктів кіберпростору	8	Залік, екзамен
ОК15	Програмне забезпечення об'єктів кіберпростору. Курсова робота	2	Захист
ОК16 (ППО6)	Комп' ютерна електроніка	4	Екзамен
ОК17 (ППО7)	Теорія інформації та кодування	4	Екзамен
ОК18 (ППО8)	Методи і засоби проведення спеціальних вимірювань в ІТС	4	Екзамен
ОК19 (ППО9).	Безпека розробки та підтримки додатків	3,5	Екзамен
ОК20 (ППО10)	Архітектура і моделі безпеки	3,5	Екзамен
ОК21 (ППО11)	Канали витоку інформації	4	Екзамен
ОК22 (ППО12)	Взаємодія між компонентами систем IoT	3	Залік

ОК23 (ППО13)	Криптографія	8	Залік, екзамен
ОК24	Криптографія. Курсова робота	2	Захист
ОК25 (ППО14)	Управління інформаційною безпекою	4	Екзамен
ОК26 (ППО15)	Законодавчі питання інформаційної безпеки	3	Залік
ОК 27 (ППО16)	Основи побудови систем комплексного захисту інформації	4	Залік
ОК 28 (ППО17)	Безпека інформаційно-телекомунікаційних систем	10	Екзамен
ОК 29 (ППО18)	Технічні системи охорони об'єктів	4	Залік
ОК30	Міждисциплінарна курсова робота	3	Захист
ОК 31 (ППО19)	Ознайомча практика	4	Залік
ОК 32 (ППО20)	Виробничо-технологічна практика	5	Залік
ОК 33 (ППО21)	Кваліфікаційний іспит зі спеціальності	2	Екзамен
ОК 34 (ЗПО7)	Фізичне виховання	3	Залік
ОК 35 (ЗПО11)	Теоретична складова Базової загальновійськової підготовки	3	Залік
ОК 36 (ЗПО12)	Практична складова Базової загальновійськової підготовки*	7*	
Загальний обсяг обов'язкових компонент:		**180 кредитів**	
Вибіркові компоненти ОП			
ВБ 1 (ЗПВ1).	Вибіркова дисципліна загальної підготовки 1	3	Залік
ВБ 2 (ЗПВ2).	Вибіркова дисципліна загальної підготовки 2	4	Залік
ВБ 3 (ЗПВ3).	Військова підготовка*	29*	
ВБ 4 (ППВ1).	Вибіркова дисципліна каф./загальноуніверситетського переліку 1	3	Залік
ВБ 5 (ППВ2).	Вибіркова дисципліна кафедрального переліку 2	5	Залік
ВБ 6 (ППВ3).	Вибіркова дисципліна кафедрального переліку 3	4	Залік
ВБ 7 (ППВ4).	Вибіркова дисципліна кафедрального переліку 4	4	Залік
ВБ 8 (ППВ5).	Вибіркова дисципліна кафедрального переліку 5	4	Залік
ВБ 9 (ППВ6).	Вибіркова дисципліна каф./загальноуніверситетського переліку 6	3	Залік
ВБ 10 (ППВ7).	Вибіркова дисципліна каф./загальноуніверситетського переліку 7	3	Залік
ВБ 11 (ППВ8).	Вибіркова дисципліна кафедрального переліку 8	6	Залік
ВБ 12 (ППВ9).	Вибіркова дисципліна кафедрального переліку 9	4	Залік
ВБ 13	Вибіркова дисципліна каф./загальноуніверситетського	3	Залік

(ППВ10).	переліку 10		
ВБ 14 (ППВ11).	Вибіркова дисципліна кафедрального переліку 11	5	Залік
ВБ 15 (ППВ12).	Вибірковий ОК кафедрального переліку 11	6	Залік
ВБ 16 (ППВ13)	Вибірковий освітній компонент 12	3	Залік
Загальний обсяг вибіркових компонент:		**60 кредитів**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240 кредитів**	

Вибір здобувачами освіти компонент блоку вибіркових компонент ОП здійснюється із запропонованого переліку, розміщеного на сайті випускової кафедри http://radiotech.chnu.edu.ua/ (вкладка «Силабуси навчальних дисциплін») та загальноуніверситетського каталогу вибіркових дисциплін (https://www.chnu.edu.ua/navchannia/dlia-studentiv/kataloh-kursiv/).

2.2. Структурно-логічна схема ОП


1 семестр
2 семестр
3 семестр
4 семестр
5 семестр
6 семестр
7 семестр
8 семестр
Іноземна мова + Англійська мова проф. спілкування
Іноземна мова + Англійська мова проф. спілкування
Іноземна мова + Англійська мова проф. спілкування
Англійська мова проф. спілкування
Актуальні питання історії і культури України
Філософія
Теор. складова Базової загально-військ. підготовки
Теор. та пр. склад. Базової загально-військ. підготовки
Українська мова (за проф. спрям.)
Фізичне виховання
Вибіркова дисципліна заг. підготовки 1
Міжособист. спілкування і побудова команд
Вибіркова дисципліна заг. підготовки 2
до "Архітектура і моделі безпеки"
Вища математика
Вища математика
Теорія інформації та кодування
Безпека розробки та підтримки додатків
Законодавчі питання інформ. безпеки
Інформаційний пошук у кібербезпеці
Комп'ютерна дискретна математика
Комп'ютерна дискретна математика
Криптографія (+ курс. робота)
Криптографія
Вступ до спеціальності
до інших дисциплін проф. спрямування
Методи і засоби проведення спец. вимірювань в ІТС
Канали витоку інформації
Безпека інф.-телеком. систем
Безпека інф.-телеком. систем
Основи інфокомунікацій
Основи інфокомунікацій
Основи інфокомунікацій
Вибіркова дисципліна каф. переліку 4
Архітектура і моделі безпеки
Управління інформаційною безпекою
Технічні системи охорони об'єктів
Основи комп. технологій
Основи комп. технологій
Програмне забезп. об'єктів кіберпр-ру
Програмне забезп. об'єктів кіберпр-ру (+ курс. робота)
Вибіркова дисципліна каф. переліку 5
Взаємодія між комп. систем IoT
Кваліф. іспит зі спеціальності
ЄДКІ
Вибрані розділи фізики
Вибрані розділи фізики
Комп'ютерна електроніка
Вибіркова дисципліна к./з.-ун. переліку 6
Основи побудови систем компл. ЗІ
Вибіркова дисципліна к./з.-ун. переліку 11
Ознайомча практика
Вибіркова дисципліна к./з.-ун. переліку 1
Вибіркова дисципліна к./з.-ун. переліку 3
Вибіркова дисципліна к./з.-ун. переліку 7
Вироб.-технол. практика
Міждисциплінарна курсова робота
Вибіркова дисципліна каф. переліку 12
Вибіркова дисципліна каф. переліку 2
Вибіркова дисципліна каф. переліку 8
Вибіркова дисципліна каф. переліку 9
Вибіркова дисципліна каф. переліку 10
Вибірковий освітній компонент 13
до інших дисциплін

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Кібербезпека» спеціальності 125 – Кібербезпека та захист інформації здійснюється у формі єдиного кваліфікаційного іспиту та кваліфікаційного іспиту зі спеціальності.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених відповідним стандартом освіти.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Атестація випускників освітньої програми «Кібербезпека» спеціальності 125 – Кібербезпека та захист інформації завершується видачею документу встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: **бакалавр з кібербезпеки та захисту інформації.**

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Освітні компоненти / Компет.	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36
Загальні компетентності																																				
ЗК 1																																				
ЗК 2																																				
ЗК 3																																				
ЗК 4																																				
ЗК 5																																				
ЗК 6																																				
ЗК 7																																				
ЗК8																																				
Спеціальні (фахові, предметні) компетентності																																				
СК1																																				
СК2																																				
СК3																																				
СК4																																				
СК5																																				
СК6																																				
СК7																																				
СК8																																				
СК9																																				
СК10																																				

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

Освітні компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36
РН 1																																				
РН 2																																				
РН 3																																				
РН 4																																				
РН 5																																				
РН 6																																				
РН 7																																				
РН 8																																				
РН 9																																				
РН 10																																				
РН 11																																				
РН 12																																				
РН 13																																				
РН 14																																				
РН 15																																				
РН 16																																				
РН 17																																				
РН 18																																				
РН 19																																				
РН 20																																				
РН 21																																				
РН 22																																				
РН 23																																				