ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет імені Олеся Гончара

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА ТА СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ»

рівень вищої освіти	***перший (бакалаврський)***
спеціальність	***F5 Кібербезпека та захист інформації***
галузь знань	***F Інформаційні технології***

ЗАТВЕРДЖЕНО:
вченою радою Дніпровського національного університету імені Олеся Гончара
протокол №___ від ___.___.2026 р.

Ректор Дніпровського національного університету імені Олеся Гончара
_____ Сергій ОКОВИТИЙ
(наказ №___ від ___.___.2026 р.)

Вводиться в дію з 01.09.2026 р.

Дніпро
2026

ПЕРЕДМОВА

1. Внесено: кафедра кібербезпеки та комп'ютерно-інтегрованих технологій фізико-технічного факультету.

2. Розробники (робоча група):
1. Клим Вікторія Юрійовна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерно інтегрованих технологій;
2. Клименко Світлана Володимирівна, кандидат технічних наук, доцент, завідувачка кафедри кібербезпеки та комп'ютерно інтегрованих технологій;
3. Петренко Олександр Миколайович, доктор технічних наук, професор, професор кафедри кібербезпеки і комп'ютерно-інтегрованих технологій;
4.Мазуренко Валерій Борисович – кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерно інтегрованих технологій.

3. При розробці враховані вимоги:
Освітнього стандарту спеціальності:
Стандарт вищої освіти зі спеціальності 125 Кібербезпека та захист інформації за першим (бакалаврським) рівнем вищої освіти, **затверджений** наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547, **вводиться в дію** з 2024/2025 навчального року.
Постанови КМУ від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» (зі змінами).
Професійного стандарту:
Професійний стандарт «Фахівець з технічного захисту інформації», професійний стандарт «Фахівець сфери захисту інформації», професійний стандарт «Фахівець з питань безпеки (інформаційно-комунікаційні технології)», професійний стандарт «Фахівець з криптографічного захисту інформації», професійний стандарт «Аудитор інформаційних технологій (з кібербезпеки)»: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 23 січня 2024 року № 38

4. Рецензії-відгуки стейкхолдерів (додаються):
Роботодавці:
1. Данченко Дмитро Валерійович, Начальник 2-го сектору (організації технічного супроводження) Управління протидії кіберзлочинам в Дніпропетровській області ДКП НП України;
2. Богун Микола Олександрович, директор ТОВ «Каньйон Інжиніринг»;
3. Кулик Сергій Володимирович, начальник відділу технічної охорони в м. Дніпро, «Охоронний холдінг».
4. Мага Сергій Вікторович, фахівець Служба Безпеки України.
5. Артеменко Юлія Федорівна, провідний фахівець-аналітик з дослідження та моделювання ринку, ТОВ «Метал кур'єр»
6. Веретюк Сергій Вікторович, к.т.н., доцент, викладач кафедри комп'ютерних технологій та моделювання систем Поліський національний університет (м. Житомир), керівник інжинірингової школи Noosphere Engineering School
Здобувачі вищої освіти:
7. Коломойченко Руслан Андрійович, ДНУ, 2022 р.н., здобувач першого (бакалаврського) рівня вищої освіти, спеціальність 125 Кібербезпека, ОП «Кібербезпека».

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

«Кібербезпека та системи технічного захисту»

Рекомендовано:
вчена рада фізико-технічного факультету:
протокол №_3_ від «_24_» __лютого__2026 р.

Голова вченої ради _____ Сергій ДАВИДОВ

Погоджено:
Рада із забезпечення якості вищої освіти та освітньої діяльності ДНУ:
протокол №____ від «__» _____2026р.

Голова РЗЯВО _____ Валентина СІЛІЧ-БАЛГАБАЄВА

Затверджено та надано чинності рішенням вченої ради Дніпровського національного університету імені Олеся Гончара:
від ___.___.2026 р., протокол № ___ (редакція для набору 2026/2027 н.р.).

1. Профіль освітньої програми зі спеціальності F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Дніпровський національний університет імені Олеся Гончара Факультет фізико-технічний Кафедра кібербезпеки і комп'ютерно-інтегрованих технологій
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та системи технічного захисту»
Офіційна назва освітньої програми (англійською мовою)	Educational and professional program «Cyber Security and technical protection systems»
Спеціальність	F5 Кібербезпека та захист інформації
Галузь знань	F Інформаційні технології
Ступінь вищої освіти	Бакалавр
Освітня кваліфікація мовою оригіналу	бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь: бакалавр Спеціальність: F5 Кібербезпека та захист інформації Освітня програма: Кібербезпека та системи технічного захисту
Кваліфікація в дипломі (англійською мовою)	Degree: Bachelor Specialty: F5 Cyber Security and protection systems Educational program: Cyber Security and technical protection systems
Професійна кваліфікація	не надається Процедура присвоєння професійної кваліфікації регламентується «Порядком про присвоєння професійної кваліфікації у Дніпровському національному університеті імені Олеся Гончара»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців; 180 кредитів ЄКТС, термін навчання 2 роки 10 місяців Для здобуття бакалаврського ступеня вищої освіти на основі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше 120 кредитів ЄКТС, отриманих у межах попередньої освітньої програми; для здобуття бакалаврського ступеня вищої освіти на основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти»
Наявність акредитації	Міністерство освіти і науки України Сертифікат з акредитації спеціальності 125 Кібербезпека рівень перший (бакалаврський) НД № 0495177 від 19 жовтня 2017 р. Термін дії до 01.07.2023 р.*
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень

Передумови	повна загальна середня освіта або ступінь молодшого бакалавра або ступінь фахового молодшого бакалавра (ОКР молодшого спеціаліста)
Форми навчання	денна, заочна
Мова(и) викладання	українська
Термін дії освітньої програми	На період дії сертифікату з акредитації спеціальності до 31.12.2027 р. (відповідно до постанови КМУ від 16 березня 2022р. № 295*) або до проходження первинної акредитації освітньої програми
Інтернет-адреса постійного розміщення опису освітньої програми	www.dnu.dp.ua
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати системи технічного захисту інформації, технології інформаційної та кібербезпеки, формування та розвиток загальних і професійних компетентностей із впровадження та застосування у професійній діяльності інтеграції програмних та апаратних засобів виявлення, моніторингу й забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності, з акцентом на реалізацію комплексних систем технічного захисту інформації.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	галузь знань F Інформаційні технології, спеціальність F5 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 та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проєктування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних

	(інформаційних потоків). Ліцензійні версії програмного забезпечення (офіс 365:Тімс, Word, Excel, PowerPoint, OneDrive, Outlook, та ін.), доступ до ліцензійного програмного забезпечення за професійним спрямуванням (CISCO).
Відповідна деталізована галузь Міжнародної стандартної класифікації освіти ISCED-F 2013	0612 Database and network design and administration
Орієнтація освітньої програми	Освітньо-професійна програма має прикладну орієнтацію. Програма інтегрує програмно-апаратні засоби виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі F Інформаційні технології, спеціальності F5 Кібербезпека та захист інформації Освітня програма «Кібербезпека та системи технічного захисту» здобуття вищої освіти в галузі інформаційних технологій спеціальності «Кібербезпека та захист інформації» сфокусована на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої обґрунтованості, технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації та систем технічного захисту. **Ключові слова**: інформаційні технології, кібербезпека, автоматизація, система керування, система автоматизації, комп'ютеризовані системи управління, процеси керування, інформаційно-комунікаційні системи, проєктування, системи технічного захисту, комп'ютерні мережі, криптографія, шифрування, кодування.
Особливості програми	Програма передбачає обов'язковою умовою проходження навчальної та виробничої практики зі спеціальності на передових підприємствах, що експлуатують або розробляють інформаційні технології, системи технічного захисту інформації (Облдержадміністрація м. Дніпро, Департамент цифрової трансформації інформаційних технологій та електронного урядування; ТОВ «Каньйон Інжиніринг», департамент кіберполіції національної поліції Украйни та ін.). Дисципліни програми засновані на вивченні апаратних, програмних, криптографічних та комбінованих засобах захисту інформації; особливостях нормативних та організаційних методах захисту інформації; захисту в мережі інтернет; системах технічного захисту приміщень. Здобувачі мають доступ до безкоштовних ліцензійних версій програмного забезпечення (офіс 365:Тімс, Word, Excel, PowerPoint, OneDrive, Outlook, та ін.) та ліцензійного програмного забезпечення за професійним спрямуванням - CISCO.

	Освітня програма в рамках університетських підписаних угод щодо європейської науково-освітньої інтеграції надає змогу майбутнім бакалаврам пройти стажування за кордоном та включає в себе програму академічної мобільності.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати на первинних посадах за професіями, визначеними Національним класифікатором України: Класифікатор професій ДК 003:2010 (зі змінами і доповненнями) ***2 Професіонали*** *213 Професіонали в галузі обчислень (комп'ютеризації)* 2139.2 Аудитор інформаційних технологій (з кібербезпеки) 2139.2 Фахівець з технічного захисту інформації 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець сфери захисту інформації 2139.2 Фахівець з криптографічного захисту інформації ***3 Фахівці*** 3121 Фахівець з інформаційних технологій. 3439 Фахівець із організації захисту інформації з обмеженим доступом
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	Студентоцентроване навчання, технологія проблемного (проблемно-орієнтованого) і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системі Office 365, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції (в тому числі, мультимедійних та інтерактивних), навчання через лабораторну практику, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами.
Оцінювання	Екзамени, заліки, диференційовані заліки; презентації, звіти та захист лабораторних робіт і практик, курсових робіт. Оцінювання навчальних досягнень здобувачів освіти здійснюється за 100-бальною шкалою.
6 – Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	*Компетентності, визначені стандартом вищої освіти:* ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області і розуміння

	професійної діяльності. ЗК 3. Здатність спілкуватися державною 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 та свобод людини і громадянина в Україні. ЗК 7. Здатність ухвалювати рішення й 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\ФК)	*Компетентності, визначені стандартом вищої освіти:* СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації. СК3. Здатність забезпечувати неперервність бізнес процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів, тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних

	процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. *Компетентності, визначені закладом вищої освіти:* СК11. Здатність застосовувати знання з загальної фізики, електротехніки, електроніки і мікропроцесорної техніки, в обсязі, необхідному для розуміння процесів в системах автоматизації та комп'ютерно-інтегрованих технологіях. СК12. Володіти знаннями новітніх технологій у галузі інформаційних технологій, зокрема, проектування систем технічного захисту інформації, збору даних та їх архівування для формування бази даних параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу. СК13. Здатність обґрунтовувати вибір технічної структури та вміти розробляти прикладне програмне забезпечення для мікропроцесорних систем керування на базі локальних засобів автоматизації, промислових логічних контролерів та програмованих логічних матриць і сигнальних процесорів. СК14. Здатність розуміти комерційний та економічний контекст для проєктування систем технічного захисту інформації.
7 – Програмні результати навчання	
Результати навчання, визначені стандартом вищої освіти: **РН1.** Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків. **РН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **РН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **РН4.** 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. **РН5.** 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. **РН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **РН7.** Застосовувати й 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 діяльності. **РН8.** 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. **РН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **РН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки	

та систем захисту інформації для здійснення професійної діяльності. **РН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. **РН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **РН13.** 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. **РН14.** 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. **РН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **РН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. **РН17.** 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. **РН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. **РН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. ПР20. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. ПР21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційних ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних ресурсах. *Результати навчання, визначені закладом вищої освіти:* ПР22. Знати електротехніку, електроніку та мікропроцесорну техніку на рівні, необхідному для розв’язання типових задач і проблем автоматизації. ПР23. Вміти застосовувати знання з охорони праці в галузі професійної діяльності, основні заходи пожежної профілактики на галузевих об’єктах, систем управління охорони праці в галузі, організації робочих місць. ПР24. Вміти застосовувати знання про основні методи обробки вимірювань, цифрової обробки зображень та сигналів в інформаційних, інформаційно-комунікаційних та технічних системах. ПР25. Вміти застосовувати знання з охорони праці в галузі професійної діяльності, основні заходи пожежної профілактики на галузевих об’єктах, систем управління охорони праці в галузі, організації робочих місць.
8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Кадрове забезпечення відповідає чинним Ліцензійним умовам провадження освітньої діяльності у сфері вищої

	освіти та базується на наступних принципах: відповідності наукових спеціальностей науково-педагогічних працівників освітнім галузі знань та спеціальності; обов'язковості та періодичності проходження стажування і підвищення кваліфікації викладачів; моніторингу рівня наукової активності науково-педагогічних працівників; впровадження результатів стажування та наукової діяльності в освітній процес.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення навчальних приміщень та соціальна інфраструктура університету в повному обсязі відповідає чинним Ліцензійним умовам. В освітньому процесі використовується мультимедійне обладнання для проведення лекцій, практичних та лабораторних занять (обладнання комп'ютерних лабораторій/аудиторій (із відповідним програмним забезпеченням) з доступом до мережі Internet). У разі використання технологій дистанційного навчання передбачається використання платформи MS Office 365.
Інформаційне та навчально-методичне забезпечення	Університет має власний веб сайт за адресою http://dnu.dp.ua, де розміщено інформацію щодо інформаційного та навчально-методичного забезпечення освітнього процесу. Інформаційне забезпечення ґрунтується на використанні ресурсів: бібліотеки (з вільним доступом до різноманітних джерел інформації, також до наукометричних баз Scopus, Web of Science Core Collection), мережі Internet з вільним доступом, цифрового репозиторію. Навчально-методичне забезпечення засновано на розроблених робочих програмах для кожного освітнього компоненту, а також програмах практичної підготовки. В наявності завдання для самостійної (індивідуальної) роботи студентів, методичні рекомендації для виконання курсових та кваліфікаційних робіт. Критерії оцінювання знань та вмінь студентів розроблено для поточного та семестрового контролю з кожного освітнього компоненту, а також для підсумкової атестації. Для формування та дотримання принципів академічної доброчесності в освітньому процесі застосовується академічна антиплагіатна система відповідно до діючої угоди.
9 – Академічна мобільність	
Національна (внутрішня) кредитна мобільність	На основі угод/договорів між ДНУ та університетами України
Міжнародна кредитна мобільність	На основі угод/договорів між ДНУ та університетами інших країн
Навчання іноземних здобувачів вищої освіти	Можливе за умови вивчення студентом української мови

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

2.1. Перелік компонент ОП

240 кредитів ЄКТС, термін навчання 3 роки 10 місяців

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Послідовність вивчення, семестр
1	2	3	4	5
Обов'язкові компоненти:				
І Цикл загальної підготовки				
ОК 1.1	Фізичне виховання та здоровий спосіб життя	3,0	залік	1, 2, 3
ОК 1.2	Безпека праці та життєдіяльності	3,0	диф. залік	5
ОК 1.3	Історія та культура України	4,0	диф. залік	1
ОК 1.4	Філософія та етика	3,0	екзамен	3
ОК 1.5	Іноземна мова (англійська/ німецька/ французька)	6,0	залік	2,3
ОК 1.6	Сучасна українська мова	3,0	диф. залік	1
ОК 1.7	Реалізація прав, свобод і обов'язків громадянина України	3,0	залік	5
ОК 1.8	Менеджмент та підприємство	3,0	залік	1
Всього І		**28**		
ІІ Цикл професійної підготовки				
ОК 2.1	Вища математика	9,0	екзамен	1,2
ОК 2.2	Фізика	6,0	залік	1,
			екзамен	2
ОК 2.3	Охорона праці в галузі	3,0	залік	6
ОК 2.4	Основи програмування	10,0	екзамен	1,2
ОК 2.5	Електротехніка	4,0	екзамен	3
ОК 2.6	Мікропроцесорні інформаційні системи	7,0	екзамен	6,7
ОК 2.7	Електроніка	3,0	екзамен	4
ОК 2.8	Бази даних та бази знань	3,0	екзамен	4
ОК 2.9	Методи цифрової обробки зображень та сигналів	6,0	екзамен	7,
			диф.залік	8
ОК 2.10	Вступ до спеціальності "Кібербезпека та захист інформації"	4,0	диф.залік	1
ОК 2.11	Моніторинг процесів функціонування інформаційно-комунікаційних систем	3,0	екзамен	4
ОК 2.12	Організаційне та нормативно-правове забезпечення кібербезпеки	8,0	залік	2
			екзамен	3
ОК 2.13	Механізми безпеки комп'ютерних мереж	4,0	залік	2
ОК 2.14	Управління інформаційною безпекою	3,0	екзамен	3
ОК 2.15	Методи та засоби технічного захисту інформації	8,0	екзамен	5,6
ОК 2.16	Технічні канали витоку інформації	3,0	екзамен	4
ОК 2.17	Безпека інформаційних систем та хмарних технологій	7,0	екзамен	5,6
ОК 2.18	Криптографія та стеганографія	10,0	диф.залік	4
			екзамен	5
ОК 2.19	Курсова робота з дисципліни «Криптографія та стеганографія»	1,0	диф.залік	5

ОК 2.20	Сучасні методи, моделі та інформаційні технології кібербезпеки	4,0	екзамен	1
ОК 2.21	Тестування інформаційно-комунікаційних технологій	3,0	залік	4
ОК 2.22	Комплексні системи технічного захисту інформації	6,0	залік	7
			екзамен	8
ОК 2.23	Теорія інформації та кодування	6,0	залік	6
			екзамен	7
ОК 2.24	Курсова робота з дисципліни «Теорія інформації та кодування»	1,0	диф.залік	7
ОК 2.25	Проєктування систем технічного захисту	8,0	залік	7
			екзамен	8
ОК 2.26	Сучасні програмні та програмно-апаратні комплекси	7,0	екзамен	7
			диф.залік	8
ОК 2.27	Навчальна практика: обчислювальна	3,0	диф. залік	2
ОК 2.28	Виробнича практика: технологічна	3,0	диф. залік	6
ОК 2.29	Виробнича практика: зі спеціальності	6,0	диф. залік	8
Всього ІІ		**149**		
Разом		**177**		
Вибіркові компоненти:				
2 курс				
ВК 1	Дисципліна 1 Базова загальновійськова підготовка (курс теоретичної підготовки) / Цивільний захист та основи медичних знань*	3,0	диф. залік	3
ВК 2	Дисципліна 2	5,0	диф. залік	3
ВК 3	Дисципліна 3	5,0	диф. залік	3
ВК 4	Дисципліна 4	5,0	диф. залік	4
ВК 5	Дисципліна 5	5,0	диф. залік	4
3 курс				
ВК 6	Дисципліна 6	5,0	диф. залік	5
ВК 7	Дисципліна 7	5,0	диф. залік	5
ВК 8	Дисципліна 8	5,0	диф. залік	6
ВК 9	Дисципліна 9	5,0	диф.залік	6
4 курс				
ВК 10	Дисципліна 10	5,0	диф.залік	7
ВК 11	Дисципліна 11	5,0	диф.залік	7
ВК 12	Дисципліна 12	5,0	диф.залік	8
ВК 13	Дисципліна 13	5,0	диф.залік	8
Загальний обсяг обов'язкових компонент				**177 (74%)**
Загальний обсяг вибіркових компонент (дисциплін вибору студента)				**63 (26%)**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ				**240**

Примітка:

- здобувачі вищої освіти обирають дисципліни за вибором відповідно до «Положення про порядок обрання здобувачами вищої освіти дисциплін за вибором у ДНУ» **(**перелік дисциплін розміщується на сайті університету);
- здобувачі, які обирають можливості академічної чи національної мобільності та/або поновлюються/переводяться мають право у сукупності набирати кількість кредитів з вибіркових компонентів на рік (семестр) навчання у відповідності до визначеної кількості кредитів у ОП.

*** -** позначені вибіркові компоненти, які обираються з урахуванням вимог виконання відповідно до пункту 8 Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21 червня 2024 р. № 734.

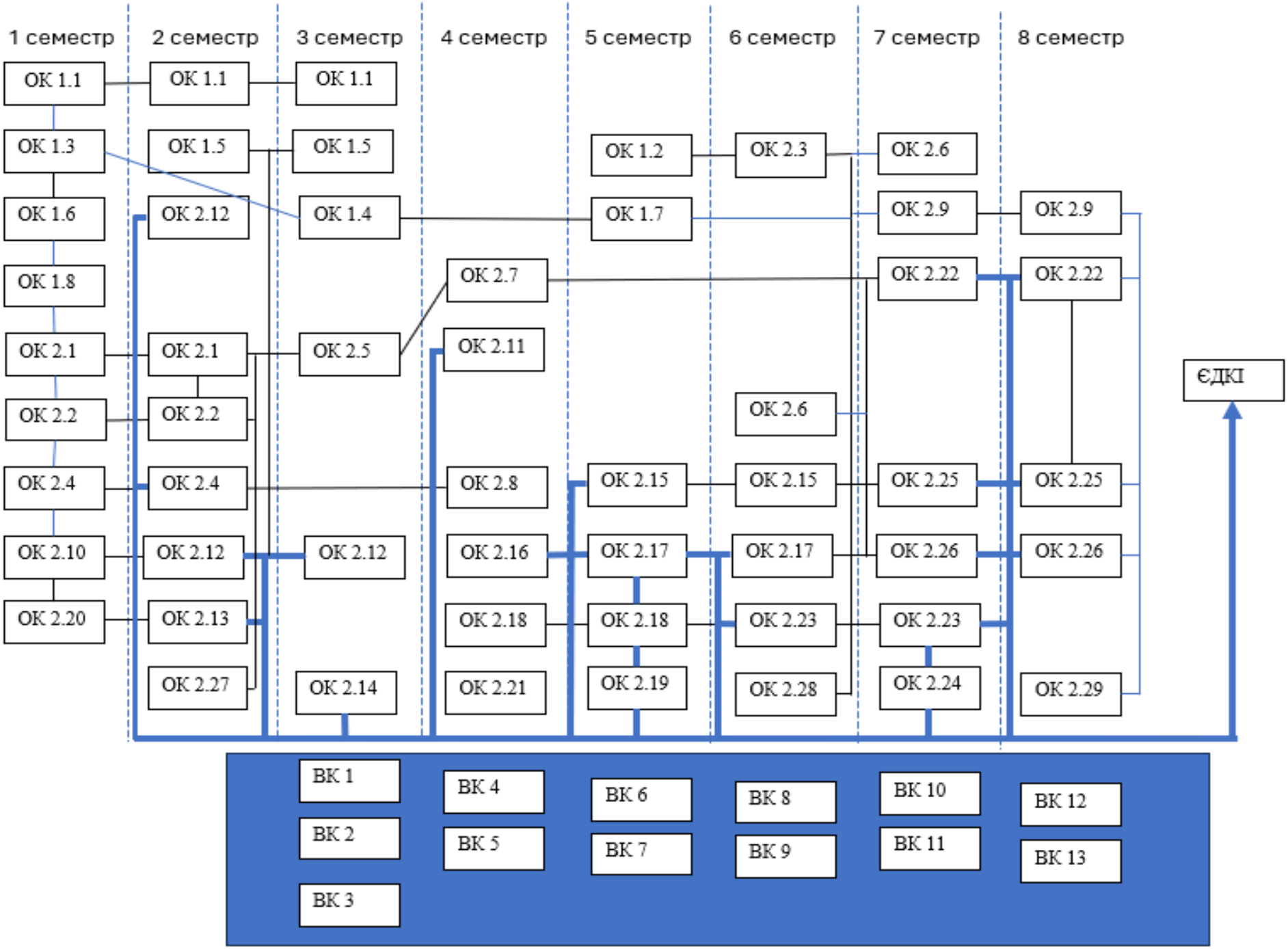
- ОК «Практична підготовка базової загальновійськової підготовки» обсягом 7 кредитів ЄКТС, включається до індивідуальних навчальних планів здобувачів вищої освіти – громадян України чоловічої статі (жіночої статі – добровільно), які навчаються за денною або дуальною формою здобуття освіти, згідно з Порядком проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21 червня 2024 р. № 734 та організовується і проводиться Міністерством оборони України, а його обсяг не враховується в загальному обсязі кредитів ЄКТС, необхідному для опанування ОП.

2.2. Структурно-логічна схема ОП

240 кредитів ЄКТС, термін навчання 3 роки 10 місяців

Курс	Семестр	Компоненти освітньої програми	Кількість компонентів за семестр	Кількість компонентів за навчальний рік
1	1	ОК 1.1, ОК 1.3, ОК 1.6, ОК 1.8, ОК 2.1, ОК 2.2, ОК 2.4, ОК 2.10, ОК 2.20	9	13
	2	ОК 1.1, ОК 1.5, ОК 2.1, ОК 2.2, ОК 2.4, ОК 2.12, ОК 2.13, ОК 2.27	8	
2	3	ОК 1.1, ОК 1.4, ОК 1.5, ОК 2.5, ОК 2.12, ОК 2.14, ВК 1, ВК 2, ВК 3	9	17
	4	ОК 2.7, ОК 2.8, ОК 2.11, ОК 2.16, ОК 2.18, ОК 2.21, ВК 4, ВК 5	8	
3	5	ОК 1.2, ОК 1.7, ОК 2.15, ОК 2.17, ОК 2.18, ОК 2.19, ВК 6, ВК 7	8	14
	6	ОК 2.3, ОК 2.6, ОК 2.15, ОК 2.17, ОК 2.23, ОК 2.28, ВК 8, ВК 9	8	
4	7	ОК 2.6, ОК 2.9, ОК 2.22, ОК 2.23, ОК 2.24, ОК 2.25, ОК 2.26, ВК 10, ВК 11	9	12
	8	ОК 2.9, ОК 2.22, ОК 2.25, ОК 2.26, ОК 2.29, ВК 12, ВК 13	7	

Структурно-логічна схема послідовності вивчення (виконання) освітніх компонент ОП «Кібербезпека та захист інформації»



Структурно-логічна схема послідовності вивчення (виконання) освітніх компонент ОП «Кібербезпека та захист інформації» (240 кредитів)

<table>
<tr><th colspan="2">I курс</th><th colspan="2">II курс</th><th colspan="2">III курс</th><th colspan="2">IV курс</th></tr>
<tr><th>1 семестр</th><th>2 семестр</th><th>3 семестр</th><th>4 семестр</th><th>5 семестр</th><th>6 семестр</th><th>7 семестр</th><th>8 семестр</th></tr>
<tr><td colspan="3">Фізична культура</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Історія та культура України</td><td></td><td></td><td></td><td>Безпека праці та життєдіяльності</td><td></td><td></td><td></td></tr>
<tr><td>Менеджмент та підприємство</td><td></td><td>Філософія та етика</td><td></td><td>Реалізація прав, свобод і обов'язків громадянина України</td><td></td><td></td><td></td></tr>
<tr><td>Сучасна українська мова</td><td colspan="2">Іноземна мова (англійська/ німецька/ французька)</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Вища математика</td><td></td><td></td><td></td><td>Охорона праці в галузі</td><td></td><td></td></tr>
<tr><td colspan="2">Фізика</td><td>Електроніка</td><td>Електротехніка</td><td></td><td></td><td colspan="2">Методи цифрової обробки зображень та сигналів</td></tr>
<tr><td colspan="2">Основи програмування</td><td></td><td>Бази даних та бази знань</td><td></td><td colspan="2">Мікроконтролерна та мікропроцесорна техніка</td><td></td></tr>
<tr><td>Вступ до спеціальності "Кібербезпека та захист інформації"</td><td colspan="2">Організаційне та нормативно-правове забезпечення кібербезпеки</td><td>Засоби приймання, передавання та обробки сигналів в системах технічного захисту</td><td colspan="2">Методи та засоби технічного захисту інформації</td><td colspan="2">Комплексні системи технічного захисту інформації</td></tr>
<tr><td>Сучасні методи, моделі та інформаційні технології кібербезпеки</td><td>Безпека інформаційно-комунікаційних систем</td><td>Управління інформмаційною безпекою</td><td>Технічні канали витоку інформації</td><td colspan="2">Безпека хмарних систем та інформаційно-комунікаційних технологій</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Криптографія та стеганографія</td><td colspan="2">Теорія інформації та кодування</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Тестування інформаційно-комунікаційних технологій</td><td></td><td></td><td colspan="2">Проєктування систем технічного захисту</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Курсова робота з дисципліни «Криптографія та стеганографія»</td><td></td><td>Курсова робота з дисципліни "Теорія інформації та кодування"</td><td></td></tr>
<tr><td></td><td>Навчальна практика: обчислювальна</td><td></td><td></td><td></td><td>Виробнича практика: технологічна</td><td></td><td>Виробнича практика: зі спеціальності</td></tr>
<tr><td></td><td></td><td>ВК 1</td><td>ВК 4</td><td>ВК 6</td><td>ВК 8</td><td>ВК 10</td><td>ВК 12</td></tr>
<tr><td></td><td></td><td>ВК 2</td><td>ВК 5</td><td>ВК 7</td><td>ВК 9</td><td>ВК 11</td><td>ВК 13</td></tr>
<tr><td></td><td></td><td>ВК 3</td><td></td><td></td><td></td><td></td><td>ЄДКІ</td></tr>
<tr><td colspan="8">Позначено кольором компоненти:</td></tr>
<tr><td>Дисципліни 1 циклу</td><td>Дисципліни 2 циклу (базові дисципліни)</td><td colspan="2">Дисципліни 2 циклу (за професійним спрямуванням)</td><td>Курсові роботи</td><td>Практики</td><td>Вибіркові компоненти</td><td>Атестація</td></tr>
</table>

Примітка: УВК - дисципліни університетського вибіркового каталогу, ФВК - дисципліни факультетського вибіркового каталог

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту.	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

240 кредитів ЄКТС, термін навчання 3 роки 10 місяців

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 1.8	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ОК 2.7	ОК 2.8	ОК 2.9	ОК 2.10	ОК 2.11	ОК 2.12	ОК 2.13	ОК 2.14	ОК 2.15	ОК 2.16	ОК 2.17	ОК 2.18	ОК 2.19	ОК 2.20	ОК 2.21	ОК 2.22	ОК 2.23	ОК 2.24	ОК 2.25	ОК 2.26	ОК 2.27	ОК 2.28	ОК 2.29
ЗК 1		•			•	•			•	•	•	•	•													•	•		•			•	•		•	•	•
ЗК 2																		•		•							•						•	•			•	•
ЗК 3		•				•																					•						•			•	•
ЗК 4					•																																•
ЗК 5																				•								•					•	•			•
ЗК 6							•																														•
ЗК 7																		•									•								•	•	•
ЗК 8	•		•			•	•		•	•								•										•								•
ЗК 9																																					•
ЗК 10																																					•
СК 1																				•																•	•
СК 2																					•				•			•					•			•	•
СК 3								•																					•							•	•
СК 4																			•		•		•		•	•	•		•	•			•	•		•	•
СК 5																•			•			•								•				•		•	•
СК 6				•																										•				•	•		•
СК 7																						•								•				•		•	•
СК 8				•																		•				•	•			•	•	•			•		•
СК 9																														•			•			•	•
СК 10																								•	•				•	•			•			•	•
СК 11									•	•			•	•	•																					•	•
СК 12																			•																	•	•
СК 13														•																						•	•
СК 14								•									•		•																	•	•

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

240 кредитів ЄКТС, термін навчання 3 роки 10 місяців

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 1.8	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ОК 2.7	ОК 2.8	ОК 2.9	ОК 2.10	ОК 2.11	ОК 2.12	ОК 2.13	ОК 2.14	ОК 2.15	ОК 2.16	ОК 2.17	ОК 2.18	ОК 2.19	ОК 2.20	ОК 2.21	ОК 2.22	ОК 2.23	ОК 2.24	ОК 2.25	ОК 2.26	ОК 2.27	ОК 2.28	ОК 2.29
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		•									•																										•
РН 24																•	•																				•
РН 25		•										•																									•
РН 26	•																																				•