

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Ректор ВНТУ

_____ Віктор БІЛЧЕНКО

Наказ ВНТУ № _____ від « ___ » _____ 2024р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Адміністрування та штучний інтелект у кібербезпеці

Administration and artificial intelligence in cybersecurity

Рівень вищої освіти	перший (бакалаврський)
Спеціальність	F5 Кібербезпека та захист інформації
Галузь знань	F Інформаційні технології
Освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації

Розглянуто та схвалено
на засіданні Вченої Ради ВНТУ
Протокол № _____ від
« ___ » _____ 2024 р.

Вінниця, 2024

ЛИСТ ПОГОДЖЕННЯ

ОПП Адміністрування та штучний інтелект у кібербезпеці

Рівень вищої освіти перший (бакалаврський)

Спеціальність F5 Кібербезпека та захист інформації

Гарант ОПП

к.т.н., доц. кафедри ВМ _____ Наталія САЧАНЮК-КАВЕЦЬКА

Директор Центру

забезпечення якості

освіти ВНТУ _____ Станіслав ТУЖАНСЬКИЙ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри менеджменту та безпеки інформаційних систем; протокол №7 від «05» листопада 2024 р.

Завідувач кафедри _____ Василь КАРПІНЕЦЬ

ОПП розглянуто після надходження всіх зауважень та пропозицій та схвалено на:

засіданні Вченої ради факультету менеджменту та інформаційної безпеки; протокол №__ від «__» _____ 2024 р.

Голова _____ Алла КРАЄВСЬКА

засідання Ради з якості освіти ВНТУ,
протокол №__ від «__» _____ 2024 р.

Голова _____ Олександр ПЕТРОВ

ПРЕАМБУЛА

ОПП АДМІНІСТРУВАННЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ

Рівень вищої освіти перший (бакалаврський)

Спеціальність F5 Кібербезпека та захист інформації

Розроблена на основі стандарту вищої освіти (наказ №1547 від «29» жовтня 2024р.)

РОЗРОБНИКИ

Гарант ОПП, к.т.н., доц. кафедри ВМ

Наталія САЧАНЮК-КАВЕЦЬКА

Завідувач кафедри МБІС, к.т.н., доцент

Василь КАРПІНЕЦЬ

Голова секції УБ кафедри МБІС, д.т.н., професор

Юрій ЯРЕМЧУК

Освітньо-професійну програму розглянуто та схвалено на засіданні Студентської ради факультету менеджменту та інформаційної безпеки;

протокол №__ від «__» _____ 2024 р.

Голова _____

Анастасія ГАЙДАЙ

РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Грималовський Микола Миколайович, начальник 3-го відділу Управління Державної служби спеціального зв'язку та захисту інформації у Вінницькій області

Прокоф'єв Михайло Іванович, доктор технічних наук, директор Науково-дослідного центру систем технічного захисту інформації "ТЕЗІС" НТУУ «КПІ ім. Ігоря Сікорського», віце-президент Асоціації захисників інформації "АЗІС", Заслужений працівник освіти України

Волинець Олександр Юрійович, керівник проєктів в ІТ компанії Morebis, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

Безпалій Кирило Валерійович, старший інженер розробник в ІТ компанії Exadel, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

ВСТУП

Освітньо-професійна програма (далі – ОПП) підготовки бакалаврів за спеціальністю F5 «Кібербезпека та захист інформації» розроблена із врахуванням стандарту вищої освіти (наказ №1547 від «29» жовтня 2024р.).

1 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем
Ступінь вищої освіти та назва освітньої кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Адміністрування та штучний інтелект у кібербезпеці
Тип диплому, форми здобуття освіти та обсяг освітньої програми	Диплом бакалавра; 240 кредитів ЄКТС (на основі ПЗСО), термін навчання – 3 роки 10 місяців (очна (денна), заочна); 180 кредитів ЄКТС (на основі НРК 5), термін навчання – 2 роки 10 місяців (очна (денна), заочна).
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Адміністрування та штучний інтелект у кібербезпеці
Цикл/рівень	6 рівень НРК України, перший цикл FQ-EHEA, 6 рівень EQF-LLL
Передумови	Повна загальна середня освіта або освітньо-кваліфікаційний рівень «молодший спеціаліст» (ступінь «молодший бакалавр»)
Мова (и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої програми	https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html
2 – Мета освітньої програми	
Формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з адміністрування та штучного інтелекту у кібербезпеці, інтелектуальний потенціал, навички практичного досвіду та інноваційної діяльності в галузі кібербезпеки та захисту інформації, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі ¹ .	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань – F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації

Об'єкти професійної діяльності випускників	- 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 забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.
Орієнтація освітньої програми	ОПП орієнтована на принципи супроводу систем та комплексів кібербезпеки; теорії, моделі та принципи управління доступом до інформаційних ресурсів; методи та засоби виявлення, управління та ідентифікації ризиків; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації; методи та засоби технічного та криптографічного захисту інформації; сучасні інформаційно-комунікаційні технології; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
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 проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Основний фокус освітньої програми та спеціалізації	Загальна освіта зі спеціальності кібербезпеки. Акцент робиться на формуванні та розвитку професійних компетентностей щодо захисту інформації на об'єктах інформаційної діяльності; вивченні теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації.
Особливості програми	Формування відповідних компетентностей у сфері інформаційної та кібернетичної безпеки, насамперед, адміністрування та штучного інтелекту у кібербезпеці, в умовах нестабільності інформаційного середовища на

	<p>основі принципів інноваційного розвитку та сучасних інформаційних технологій, поєднуючи ґрунтовну фундаментальну підготовку із сучасною професійною підготовкою, використовуючи при цьому весь науково-технічний потенціал університету в цій сфері, у першу чергу, залучення науково-педагогічного персоналу, апаратури та обладнання відповідних науково-дослідних лабораторій та навчально-наукових центрів, у тому числі тих, що здійснюють свою діяльність відповідно до ліцензії Державної служби спеціального зв'язку та захисту інформації України з надання науково-технічних послуг та виконання наукових-дослідних робіт у галузі криптографічного та технічного захисту інформації. Важливим також є орієнтація ОПП на міжнародні професійні програми, включаючи сертифіковані, від провідних компаній-виробників комп'ютерного та мережевого обладнання, програмного забезпечення, технологій та рішень з кібербезпеки, зокрема таких компаній як Microsoft, Cisco, IBM, HCL Technologies, Spuse та ін.</p>
<p>4 – Придатність випускників до працевлаштування та подальшого навчання</p>	
<p>Працевлаштування випускників</p>	<p>На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації.</p> <p>Фахівець з адміністрування та штучного інтелекту у кібербезпеці може займати такі первинні посади відповідно до затверджених професійних стандартів, зокрема:</p> <ul style="list-style-type: none"> – 2139.2 Адміністратор безпеки мереж і систем – 2139.2 Фахівець сфери захисту інформації – 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) – 2132.2 Конструктор систем кібербезпеки – 2139.2 Фахівець з підтримки інфраструктури кіберзахисту – 2139.2 Фахівець з реагування на інциденти кібербезпеки – 2139.2 Фахівець з криптографічного захисту інформації – 2139.2 Фахівець з технічного захисту інформації – 2139.2 Фахівець з тестування систем захисту інформації – 2139.2 Аудитор інформаційних технологій (з кібербезпеки) – 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки)

	Права випускників на працевлаштування не обмежуються.
Академічні права випускників	Мають право на здобуття освіти за другим (магістерським) рівнем вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсових робіт, дослідницькі лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації із викладачами, наукові семінари, демонстраційні класи, елементи дистанційного (онлайн, електронного) навчання проходження практики на підприємствах та в науково-дослідних установах, підготовка кваліфікаційної роботи.
Оцінювання	Методи оцінювання – екзамени, тести, практика, контрольні, курсові роботи, есе, презентації. Формативні (вхідне тестування та поточний контроль): тестування знань або умінь; усні презентації; звіти про лабораторні роботи; аналіз текстів або даних; звіти про практику; огляд літератури тощо). Сумативні (підсумковий контроль): екзамен (письмовий з подальшим усним опитуванням); залік (за результатами формативного контролю).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	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 та 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

	<p>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.</p>
<p>Спеціальні (фахові, предметні) компетентності (СК)</p>	<p>СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p>СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p>СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.</p> <p>СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та пошкодження.</p> <p>СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).</p> <p>СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>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.</p> <p>СК 11. Здатність використовувати основні технології штучного інтелекту для розробки інтелектуальних систем у кібербезпеці.</p> <p>СК 12. Здатність використовувати методи та засоби</p>

	<p>штучного інтелекту для захисту інформаційних систем та конфіденційних даних від внутрішніх та зовнішніх загроз, шляхом виявлення потенційних ризиків у програмно-апаратних комплексах, моніторингу, виявлення, розслідування, аналізу та реагування на події безпеки, тим самим зменшуючи ризики в режимі реального часу.</p> <p>СК 13. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для адміністрування кібербезпекою.</p>
--	---

7 – Програмні результати навчання

	<p>РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.</p> <p>РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.</p> <p>РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.</p> <p>РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язування складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p>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.</p> <p>РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>РН 7. 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.</p> <p>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.</p> <p>РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.</p> <p>РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної</p>
--	--

діяльності.

PH11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

PH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

PH13. 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.

PH14. 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.

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

PH17. 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.

PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

PH20. 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

	<p>захисту інформації.</p> <p>РН21. 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.</p> <p>РН 22. Розробляти моделі штучного інтелекту та алгоритми для створення інтелектуальних систем у кібербезпеці.</p> <p>РН 23. Впроваджувати та налаштовувати адаптивні інтелектуальні системи для виявлення вразливостей, розпізнавання аномальних активностей та ефективного реагування на кібератаки; розробляти та вдосконалювати моделі машинного навчання, які сприяють підвищенню рівня кібербезпеки, забезпечуючи надійний захист цифрових систем та даних від потенційних загроз.</p> <p>РН 24. Проектувати системи для адміністрування кібербезпекою на основі використання сучасних принципів, способів та методів теорії захищених систем.</p>
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	<p>Кадрове забезпечення ОПП формується, в основному за рахунок кафедри менеджменту та безпеки інформаційних систем. До викладання дисциплін залучаються також інші кафедри факультету менеджменту та безпеки інформаційних систем, і університету. Керівник проектної групи освітньої програми та викладацький склад, який забезпечує її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.</p>
Матеріально-технічне забезпечення	<p>Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає в себе сучасні лабораторії Центру інформаційних технологій та захисту інформації, зокрема комп'ютерні класи мережевої академії Cisco та ІТ Академії Microsoft, Науково-дослідну лабораторію технічного захисту інформації.</p>
Інформаційне та навчально-методичне забезпечення	<p>Відповідно до вимог Ліцензійних умов провадження освітньої діяльності включає в себе бібліотечні ресурси, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація</p>

	щодо освітньої діяльності за ОП.
9 – Академічна мобільність	
Національна кредитна мобільність	Здійснюється на підставі укладення угод про співробітництво між Університетом та закладами вищої освіти України.
Міжнародна кредитна мобільність	Здійснюється на підставі укладення угод між Університетом та групою закладів вищої освіти різних країн за узгодженими та затвердженими у встановленому порядку індивідуальними навчальними планами студентів та програмами навчальних дисциплін, а також в рамках міжурядових угод про співробітництво в галузі освіти, міжнародних проектів, в яких Університет приймає участь, грантів та ін.
Навчання іноземних здобувачів вищої освіти	За даною освітньою програмою не передбачено навчання іноземних здобувачів вищої освіти

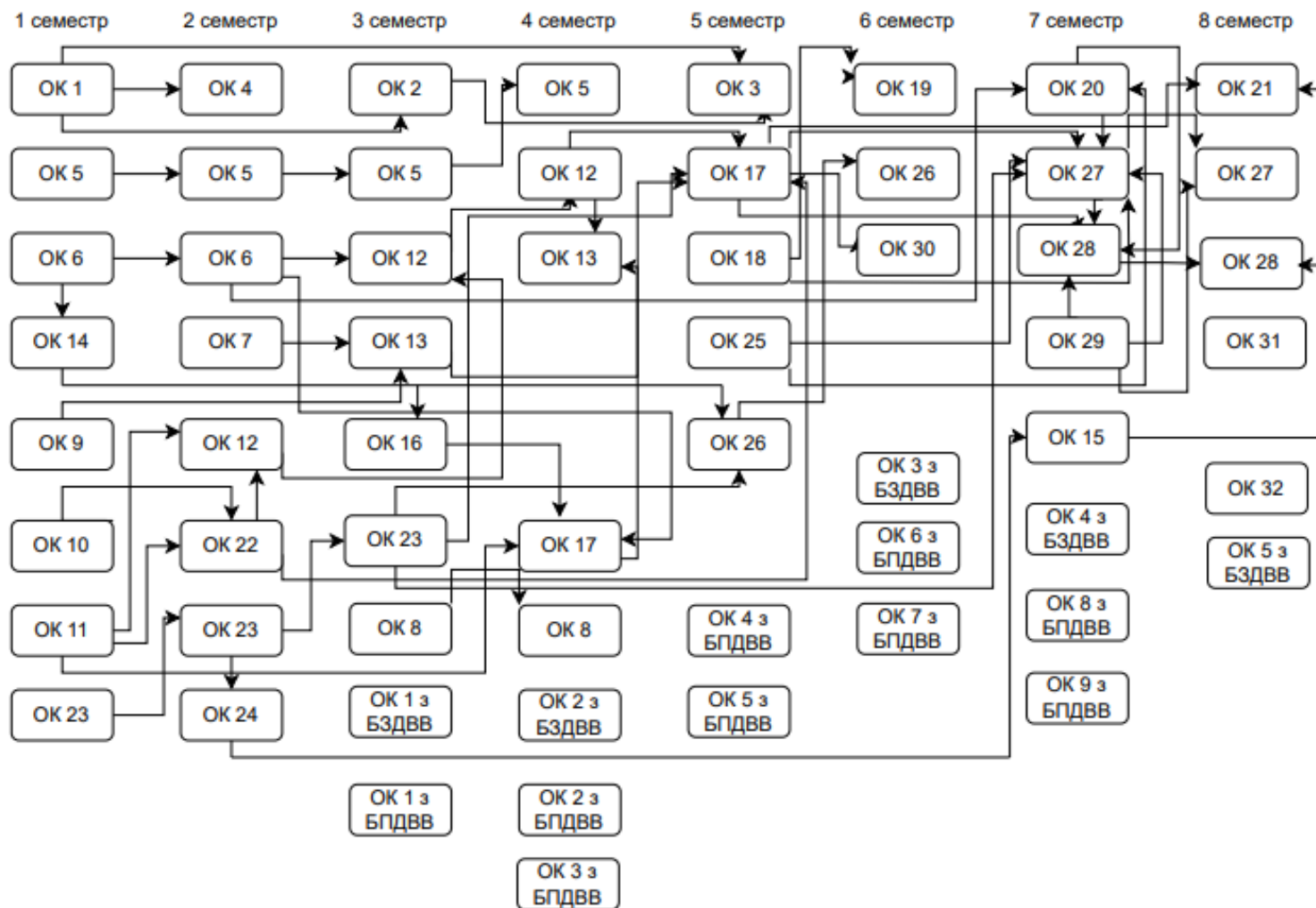
2 ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
Загальні			
1.1.	Історія та культура України	3,0	залік
1.2.	Філософія	3,0	залік
1.3.	Політологія	3,0	залік
1.4.	Українська мова за професійним спрямуванням	3,0	залік
1.5.	Іноземна мова за професійним спрямуванням	8,0	залік
1.6.	Вища математика	12,0	іспит
1.7.	Фізика	5,0	іспит
1.8.	Базова загальновійськова підготовка	3,0	залік
Професійні			
1.9.	Основи комп'ютерної техніки	3,0	іспит
1.10.	Інформаційні технології	3,0	залік
1.11.	Internet-технології та кібергігієна	4,0	іспит
1.12.	Теоретичні основи процесів у кібербезпеці	12,0	іспит
1.13.	Схемотехніка	9,0	залік, іспит
1.14.	Математичні основи криптографії	4,0	іспит
1.15.	Технології штучного інтелекту в кібербезпеці	3,0	залік
1.16.	Основи наукових досліджень, аналізу та синтезу інформації	4,0	іспит
1.17.	Управління ризиками та оцінювання захищеності інформації	7,0	іспит
1.18.	Інформаційно-телекомунікаційні системи	3,0	іспит
1.19.	Основи технічного захисту інформації	5,0	іспит
1.20.	Економіка, організація та управління бізнес процесами	3,0	залік

1.21.	Управління інцидентами інформаційної безпеки	4,0	іспит
1.22.	Основи інформаційної безпеки (вступ до фаху)	3,0	залік
1.23.	Основи програмування захищених інформаційних систем (в т.ч. курсова робота)	13,0	залік, іспит
1.24.	Введення в штучний інтелект	3,0	іспит
1.25.	Бази даних і знань (в т.ч. курсова робота)	6,0	іспит
1.26.	Основи криптографічного захисту інформації (в т.ч. курсова робота)	8,0	залік, іспит
1.27.	Проектування систем управління інформаційною безпекою (в т.ч. курсовий проект)	9,0	залік, іспит
1.28.	Адміністрування кібербезпеки	7,0	залік, іспит
1.29.	Правове та організаційне забезпечення інформ- та кібербезпеки	3,0	іспит
1.30.	Виробнича практика	9,0	залік
1.31.	Переддипломна практика	4,5	залік
1.32.	Бакалаврська кваліфікаційна робота	10,5	
Загальний обсяг обов'язкових компонент		180	
ВИБІРКОВІ КОМПОНЕНТИ ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА			
Загальні			
2.1.	Освітній компонент 1 з БЗДВВ	3,0	залік
2.2.	Освітній компонент 2 з БЗДВВ	3,0	залік
2.3.	Освітній компонент 3 з БЗДВВ	3,0	залік
2.4.	Освітній компонент 4 з БЗДВВ	3,0	залік
2.5.	Освітній компонент 5 з БЗДВВ	3,0	залік
Професійні			
2.6.	Освітній компонент 1 з БПДВВ	5,0	залік
2.7.	Освітній компонент 2 з БПДВВ	5,0	залік
2.8.	Освітній компонент 3 з БПДВВ	5,0	залік
2.9.	Освітній компонент 4 з БПДВВ	5,0	залік
2.10.	Освітній компонент 5 з БПДВВ	5,0	залік
2.11.	Освітній компонент 6 з БПДВВ	5,0	залік
2.12.	Освітній компонент 7 з БПДВВ	5,0	залік
2.13.	Освітній компонент 8 з БПДВВ	5,0	залік
2.14.	Освітній компонент 9 з БПДВВ	5,0	залік
Всього за вибірковими компонентами		60	
ЗАГАЛЬНИЙ ОБСЯГ ЗА ПЛАНОМ		240	

2.2. Структурно-логічна схема освітньо-професійної програми



3 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

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

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

Вимоги до кваліфікаційної роботи/проєкту

Кваліфікаційна робота/проєкт має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації.

Кваліфікаційна робота/проєкт має бути перевірена на плагіат.

Кваліфікаційна робота повинна бути опублікована на сайті Вінницького національного технічного університету.

4 ХАРАКТЕРИСТИКА СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПІДГОТОВКИ БАКАЛАВРА

У Вінницькому національному технічному університеті функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

- 1) визначення принципів та процедур забезпечення якості вищої освіти;
- 2) здійснення моніторингу та періодичного перегляду освітніх програм;
- 3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб;
- 4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
- 5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою чи спеціальністю;
- 6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- 7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
- 8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;
- 9) інших процедур і заходів.

5 ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЯ ПРОГРАМА

1. Закон України «Про вищу освіту» 01.07.2014 №1556-VII - [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1556-18>];
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Режим доступу: <http://zakon2.rada.gov.ua/laws/show/80/94-вр>];
3. Закон України «Про основні засади забезпечення кібербезпеки України» - відомості Верховної Ради (ВВР), 2017, №45, ст.403;
4. Постанова Кабінету Міністрів України від 30.12.2015р. №1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1187-2015-п/page>];
5. Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р.№266. [Режим доступу: <http://zakon.rada.gov.ua/laws/show/266-2015-п>];
6. Національний класифікатор України: "Класифікатор професій» ДК 003:2010 [Режим доступу: <http://www.003.com>];
7. Наказ МОН України №1547 «Про внесення змін до стандарту вищої освіти зі спеціальності F5 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти» від 29.10.2024 р.;
8. «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року №47/2017. [Режим доступу: <https://www.president.gov.ua/documents/472017-21374>];
9. Рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. №96. [Режим доступу: <https://www.president.gov.ua/documents/2422016-20141>];
10. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. №1229;
11. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 р. №505;
12. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. №373.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки бакалаврів зі спеціальності F5 «Кібербезпека та захист інформації» та програмні результати навчання, які виражають те, що студент повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 наведені матриці відповідності визначених освітньою програмою результатів навчання (компетентностей) та освітніх компонентів.

Таблиця 1. Матриця забезпечення програмних результатів навчання обов'язковими освітніми компонентами

	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		
PH 1				+																										+	+	+		
PH 2					+																													
PH 3	+	+	+					+																										
PH 4												+					+					+	+					+	+		+	+	+	
PH 5		+				+	+					+				+	+		+	+	+	+						+	+		+	+	+	
PH 6						+						+									+					+		+	+		+	+	+	
PH 7														+				+					+				+							
PH 8						+	+																											
PH 9												+							+			+						+		+	+	+	+	
PH 10										+	+	+										+	+	+				+		+	+	+	+	
PH 11																				+								+		+	+			
PH 12											+							+	+							+		+		+	+	+		
PH 13									+	+	+		+											+						+				
PH 14												+						+				+						+						
PH 15															+	+						+			+					+				
PH 16									+									+								+	+							
PH 17																	+					+						+	+					
PH 18													+														+							
PH 19																										+			+					
PH 20																				+							+							
PH 21																	+					+					+							
PH 22													+	+										+		+								
PH 23															+		+					+		+										
PH 24										+	+											+												

Таблиця 2. Матриця відповідності компетентностей обов'язковим освітнім компонентам

	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
ЗК 1		+				+	+					+		+		+	+	+	+	+	+	+				+	+	+		+	+	+
ЗК 2		+				+	+					+				+	+		+	+	+	+			+		+	+		+	+	+
ЗК 3				+																										+	+	+
ЗК 4					+																											
ЗК 5						+	+																									
ЗК 6	+	+	+					+																						+		
ЗК 7	+	+	+					+																								
ЗК 8						+						+		+				+					+			+	+					
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											+						+						+							+		

ТАБЛИЦЯ 3. ЗВЕДЕНА ТАБЛИЦЯ ФАХОВИХ КОМПЕТЕНТНОСТЕЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Фахові компетентності	Результати навчання
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації	РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК2. Здатність до використання інформаційних технологій, сучасних методів і моделей кібербезпеки та систем захисту інформації.	РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації	РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та/або інфраструктури організації в цілому.;
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та 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.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур,	РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;

практичних прийомів тощо)	
СК7. Здатність здійснювати професійну діяльність на основі впровадженій системи управління інформаційною та кібербезпекою	РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності	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.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	РН20. 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 та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти та оцінювати можливі вразливості та загрози інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
PH1	+			+															
PH2	+				+														
PH3	+						+	+											
PH4	+	+	+																
PH5	+	+	+																
PH6	+		+						+										
PH7	+	+							+										
PH8	+					+													
PH9	+						+			+									
PH10	+									+									
PH11	+										+								
PH12	+											+							
PH13	+											+							
PH14	+												+						
PH15	+												+						
PH16	+													+					
PH17	+														+				
PH18	+															+			
PH19	+															+			
PH20	+																+		
PH21	+																	+	

**Матриця відповідності визначених Стандартом компетентностей
дескрипторам НРК**

Класифікація компетентностей (результатів навчання) за НРК	Знання Зн1 Концептуальні наукові та практичні знання. Зн2 Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання.	Уміння Ум1. Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	Комунікація К1. Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації. К2. Збір, інтерпретація та застосування даних. К3. Спілкування з професійних питань, у тому числі іноземною мовою, усно та письмово.	Відповідальність та автономія АВ1. Управління складною технікою або професійною діяльністю чи проектами. АВ2. Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. АВ3. Формування суджень, що враховують соціальні, наукові та етичні аспекти. АВ4. Організація та керівництво професійним розвитком осіб та груп. АВ5. Здатність продовжувати навчання із значним ступенем автономії.
ЗК1	Зн2	Ум1		
ЗК2	Зн2	Ум1	К1	
ЗК3			К1, К3	
ЗК4			К1, К3	
ЗК5	Зн1, Зн2	Ум1	К2	АВ3
ЗК6	Зн1		К1	АВ2, АВ3, АВ4
ЗК7			К1	АВ2
ЗК8	Зн2		К2	АВ3
СК1	Зн2	Ум1	К2	
СК2	Зн1, Зн2	Ум1	К2	
СК3		Ум1		АВ1
СК4		Ум1		АВ1
СК5		Ум1	К2	АВ1, АВ2
СК6		Ум1	К1	АВ1
СК7		Ум1	К1	АВ1
СК8	Зн2	Ум1		
СК9	Зн2	Ум1		
СК10		Ум1	К2	АВ2

