Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

ЄДИНОГО ДЕРЖАВНОГО КВАЛІФІКАЦІЙНОГО ІСПИТУ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Кібербезпека та захист інформації
Форма навчання	Денна
Розробник	Гришанович Тетяна Олександрівна, к.ф.-м.н. наук
Контактна інформація	Hryshanovych.Tatiana@vnu.edu.ua
Семестр, курс	4 курс, 8 семестр
Обсяг дисципліни	Загальний обсяг: 2 кредити / 60 годин. Аудиторних годин: 0 год; Самостійна робота: 56 год. Консультації: 4 год.
Форма контролю	Іспит (8 семестр)
Час занять	Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Підсумкова атестація випускників освітньо-професійної програми «Кібербезпека та захист інформації» спеціальності 125 " Кібербезпека та захист інформації " проводиться у формі єдиного державного кваліфікаційного іспиту та завершується видачею документа встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікацій: освітня кваліфікація: Бакалавр з кібербезпеки та захисту інформації; професійна кваліфікація: Фахівець сфери захисту інформації. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та освітньою програмою Кібербезпека та захист інформації.
Мета вивчення дисципліни	Метою кваліфікаційного іспиту є вимірювання та оцінювання результатів навчання, досягнутих здобувачем освіти за підсумками опанування освітньої програми
Результати навчання, які будуть оцінюватись	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **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 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. **ФК 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. **ФК 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ФК 4.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики безпеки. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **ФК 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **ФК 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **ПРН 1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **ПРН 2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **ПРН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **ПРН 4.** Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних

	проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **ПРН 5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **ПРН 6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **ПРН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. **ПРН 8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. **ПРН 9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **ПРН 10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. **ПРН 11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **ПРН 12.** Розробляти моделі загроз та порушника. **ПРН 13.** Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. **ПРН 14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень. **ПРН 15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. **ПРН 16.** Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. **ПРН 17.** Забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. **ПРН 18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **ПРН 19.** Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. **ПРН 20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. **ПРН 21.** Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах. **ПРН 22.** Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних

	документів системи технічного захисту інформації. **ПРН 38.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. **ПРН 39.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах дотримання режиму секретності із фіксуванням результатів у відповідних документах. **ПРН 40.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних- засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. **ПРН 41.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **ПРН 42.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **ПРН 43.** Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. **ПРН 44.** Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. **ПРН 45.** Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **ПРН 46.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. **ПРН 47.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. **ПРН 48.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. **ПРН 49.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. **ПРН 50.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **ПРН 51.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. **ПРН 52.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **ПРН 53.** Вирішувати задачі аналізу програмного коду на наявність можливих загроз. **ПРН 54.** Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого

	розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Загальні засади

Організаційні засади проведення атестації здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту визначає Порядок атестації здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту (постанова №497 КМУ від 19.05.2021 р). За організацію і проведення кваліфікаційного іспиту за спеціальностями відповідають визначені у переліку державні органи, до сфери управління яких належать заклади вищої освіти та/або які відповідають за формування та реалізацію державної політики у відповідній сфері. Для спеціальності 125 «Кібербезпека» це МОН, Адміністрація Держспецзв'язку, Міноборони.

Політика оцінювання

Організація і проведення кваліфікаційного іспиту базуються на таких принципах: академічна доброчесність; об'єктивність; прозорість і публічність; нетерпимість до корупційних та пов'язаних з корупцією діянь. Кваліфікаційний іспит може проводитися у формі зовнішнього незалежного оцінювання або в іншій формі та передбачати використання різних видів тестових та ситуаційних завдань, укладених відповідно до програми кваліфікаційного іспиту.

Програма кваліфікаційного іспиту розробляються за спеціальністю/групою спеціальностей та відповідним рівнем освіти на основі стандартів фахової передвищої, вищої освіти відповідного рівня та спеціальності. Програма кваліфікаційного іспиту затверджується відповідальними державними органами та оприлюднюється на офіційних веб-сайтах державного органу та закладів освіти, які здійснюють підготовку фахівців за такою спеціальністю та рівнем освіти (крім інформації з обмеженим доступом), не пізніше ніж за шість місяців до проведення кваліфікаційного іспиту.

Із проєктом єдиного державного кваліфікаційного іспиту можна ознайомитись за лінком:
https://mon.gov.ua/storage/app/media/gromadske-obgovorennya/2021/12/30/HO.Prohr.YEDKI.125-Kiberbezp.pdf

Кваліфікаційний іспит є обов'язковим компонентом індивідуального навчального плану здобувача освіти. Здобувач освіти допускається до складання кваліфікаційного іспиту за умови відсутності в нього академічної заборгованості.

У разі неуспішного складання кваліфікаційного іспиту особа вважається такою, що не виконала індивідуальний навчальний план та відраховується із закладу фахової передвищої освіти відповідно до пункту 4 частини першої статті 44 Закону України "Про фахову передвищу освіту" або закладу вищої освіти відповідно до пункту 4 частини першої статті 46 Закону України "Про вищу освіту" (крім осіб, зазначених в абзаці шостому цього пункту). Таку особу може бути поновлено на навчання для здобуття ступеня фахової передвищої або вищої освіти за такою самою спеціальністю для однократного повторного складання кваліфікаційного іспиту. Строк, до якого здобувачі освіти можуть повторно скласти кваліфікаційний іспит, визначається відповідальними державними органами.

У разі повторного неуспішного складання кваліфікаційного іспиту особа може бути

поновлена на навчання за ступенем фахової передвищої або вищої освіти за такою самою спеціальністю для повторного навчання протягом не менше як двох семестрів. Рішення про зарахування особі, яка здобуває ступінь фахової передвищої або вищої освіти, результатів контрольних заходів під час повторного навчання та надання допуску до складання кваліфікаційного іспиту ухвалюється закладом освіти. Повторне навчання та складання кваліфікаційного іспиту здійснюється виключно за рахунок коштів фізичних та/або юридичних осіб. Повторне складання кваліфікаційного іспиту проводиться за програмою та відповідно до умов проведення, що діють на дату його складання.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 28.06.2023 р.
Завідувач кафедри:  (Гришанович Т. О.)