ЗАТВЕРДЖУЮ
Голова приймальної комісії НТУ «ДП»,
ректор _____ О.О. Азюковський
« 18 » квітня 2023 р.

# ПРОГРАМА

фахового іспиту за ступенем магістра зі спеціальності
**125 «Кібербезпека та захист інформації»**
на основі ступеня (освітньо-кваліфікаційного рівня) бакалавра (спеціаліста)

| Уміння, що контролюються | Зміст програми |
|---|---|
| Застосовувати законодавчу та нормативно-правову базу, державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.<br>Здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.<br>Аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. | **1 Основи забезпечення безпеки інформації**<br>1.1 Понятійна база інформаційної безпеки<br>1.2 Нормативно-правове забезпечення в сфері інформаційної та кібербезпеки<br>1.3 Управління інформаційною безпекою<br>1.4 Організаційне забезпечення захисту інформації |
| Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.<br>Забезпечувати захист інформації, що обробляється в АС з метою реалізації встановленої політики інформаційної та/або кібербезпеки.<br>Вирішувати задачі захисту потоків даних в АС.<br>Виконувати моніторинг процесів функціонування АС згідно встановленої політики інформаційної та/або кібербезпеки. | **2 Кіберзахист**<br>2.1 Програмні та програмно-апаратні комплекси захисту ІТС<br>2.2 Забезпечення захисту ресурсів і процесів в ІТС на основі моделей безпеки<br>2.3 Задачі супроводу системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в ІТС<br>2.4 Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в ІТС |
| Впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.<br>Виконувати аналіз та декомпозицію ІТС.<br>Розробляти моделі загроз та порушника.<br>Використовувати програмних та програмно-апаратних КЗЗ інформації в АС.<br>Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в АС в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.<br>Вирішувати задачі забезпечення та супроводу КСЗІ. | **3 Комплексні системи захисту інформації**<br>3.1 Передпроектні роботи із створення комплексних систем захисту інформації (КСЗІ)<br>3.2 Проектні роботи із створення КСЗІ<br>3.3 Випробування та Державна експертиза КСЗІ<br>3.4 Супровід та експлуатація КСЗІ |

| Уміння, що контролюються | Зміст програми |
|---|---|
| Застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.<br>Виявляти небезпечні сигнали технічних засобів.<br>Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів ЗІ та визначати ЗІ від витоку технічними каналами відповідно до вимог НД ТЗІ.<br>Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог НД ТЗІ.<br>Здійснювати оцінювання можливості НСД до елементів ІТС. | **4 Системи технічного захисту інформації**<br>4.1 Технічні канали витоку інформації<br>4.2 Методи, технічні засоби та контроль ефективності захисту інформації від витоку технічними каналами<br>4.3 Технічні засоби виявлення закладних пристроїв<br>4.4 Технічні системи охорони об'єктів |
| Застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.<br>Вирішувати задачі захисту інформації, що обробляється ІТС з використанням сучасних методів та засобів криптографічного захисту інформації.<br>Використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС. | **5 Прикладна криптологія**<br>5.1 Математичні основи криптології<br>5.2 Симетричні криптографічні системи<br>5.3 Асиметричні криптосистеми та їх криптоаналіз<br>5.4 Криптографічні механізми та протоколи |

**Рекомендована література**


1. НД ТЗІ 1.1-002; НД ТЗІ 1.1-003; НД ТЗІ 3.7-003; НД ТЗІ 2.5-004; НД ТЗІ 2.5-005; НД ТЗІ 3.6-001; НД ТЗІ 3.7-001; НД ТЗІ 2.5-008; НД ТЗІ 2.5-010; НД ТЗІ 1.4-001; НД ТЗІ 1.5-002; НД ТЗІ 2.6-001; НД ТЗІ 2.6-002; НД ТЗІ 1.6-005; ДСТУ ISO/IEC 27000; ДСТУ ISO/IEC 27001; ДСТУ ISO/IEC 27002; ДСТУ 3396.1-96.
2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект : підруч. / за заг. ред. проф. В.Б. Толубка. Київ : ДУТ, 2015. 288 с.
3. Христич В.В., Дерев'янко О.А., Бондаренко С.М., Антошкін О.А. Системи пожежної та охоронної сигналізації : навч. посіб. Харків : АПБУ МВС України, 2008. 87 с.
4. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: підруч. / С.М. Головань та ін. Львів : Видавництво Національного університету «Львівська політехніка», 2005. 288 с.
5. Вакалюк Т.А. Захист інформації в комп'ютерних системах : навч. посіб. Житомир : Видавництво ЖДУ, 2013. 136 с.
6. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2009. 608 с.
7. Інформаційна безпека : підруч. / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін. ; під ред. В.В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.
8. Сушко С.О., Кузнецов Г.В., Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу : навч. посіб. Дніпропетровськ : НГУ, 2010. 465 с.
9. Остапов С.Е., Валь Л.О. Глинчук Л.Я. Основи криптографії : навч. посіб. Луцьк : Вежа-Друк, 2014. 164 с.