



ЗАТВЕРДЖУЮ

Голова приймальної комісії НТУ «ДП»,
ректор

Г.Г. Півняк
Г.Г. Півняк

лютого
2020 р.

ПРОГРАМА

вступного фахового екзамену за ступенем магістра спеціальності

125 Кібербезпека

на основі ступеня (освітньо-кваліфікаційного рівня) бакалавра (спеціаліста)

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

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

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. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: підруч. / С.М. Головань та ін. Львів : Видавництво Національного університету «Львівська політехніка», 2005. 288 с.
3. Диогенес Ю., Озкая Э. Кибербезопасность. Стратегии атак и обороны : учеб. пособ. Москва : ДМК-Пресс, 2019. 326 с.
4. Магауенов Р.Г. Системы охранной сигнализации: основы теории принципы построения : учеб. пособ. Москва : Горячая линия-Телеком, 2004. 367 с.
5. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом : підручник / Головань С.М. та ін. Львів : Видавництво Національного університету «Львівська політехніка», 2005. 288 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. С-Пб. : НиТ, 2004. 384 с.
7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група ВНУ, 2009. 608 с.
8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособ. для ВУЗов. Москва : Горячая линия – Телеком, 2004. 280 с.
9. Сушко С.О., Кузнецов Г.В., Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу : навч. посіб. Дніпропетровськ : НГУ, 2010. 465 с.
10. Основы криптографии : учеб. пособ. / А.П. Алферов и др. Москва : Гелиос, 2002. 480 с.