ЗАТВЕРДЖУЮ
Голова приймальної комісії НТУ «ДП»,
ректор _____ О.О. Азюковський
« 15 » березня 2024 р.

ПРОГРАМА

фахового іспиту зі спеціальності
125 «Кібербезпека та захист інформації»
для вступу на навчання за ступенем магістра

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. Здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. 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** 1.1 Понятійна база інформаційної безпеки 1.2 Нормативно-правове забезпечення в сфері інформаційної та кібербезпеки 1.3 Управління інформаційною безпекою 1.4 Організаційне забезпечення захисту інформації
Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. Забезпечувати захист інформації, що обробляється в АС з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Вирішувати задачі захисту потоків даних в АС. Виконувати моніторинг процесів функціонування АС згідно встановленої політики інформаційної та/або кібербезпеки.	**2 Кіберзахист** 2.1 Програмні та програмно-апаратні комплекси захисту ІТС 2.2 Забезпечення захисту ресурсів і процесів в ІТС на основі моделей безпеки 2.3 Задачі супроводу системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в ІТС 2.4 Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в ІТС
Впроваджувати та забезпечувати функціонування комплексних систем захисту інформації. Виконувати аналіз та декомпозицію ІТС. Розробляти моделі загроз та порушника. Використовувати програмних та програмно-апаратних КЗЗ інформації в АС. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в АС в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки. Вирішувати задачі забезпечення та супроводу КСЗІ.	**3 Комплексні системи захисту інформації** 3.1 Передпроектні роботи із створення комплексних систем захисту інформації (КСЗІ) 3.2 Проектні роботи із створення КСЗІ 3.3 Випробування та Державна експертиза КСЗІ 3.4 Супровід та експлуатація КСЗІ

Уміння, що контролюються	Зміст програми
Застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. Виявляти небезпечні сигнали технічних засобів. Вимірювати параметри небезпечних та завадових 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.	**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
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.	**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

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.

10.Засоби та системи технічного захисту інформації : навч. посіб. для студ. спец. 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов та ін. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2019. 216с.

Критерії оцінювання окремих завдань білета

Кожне теоретичне тестове завдання білета оцінюється 1 або 2 балами, а практичне та завдання на відповідність – 5 балами, виходячи з критеріїв:

а) однобальний теоретичний тест:

0 – вибір варіанта відповіді помилковий або обрано більш одного варіанта відповіді;
1 – обраний правильний варіант відповіді.

б) двобальний теоретичний тест:

0 – вибір варіантів відповідей помилковий або обрано більш трьох варіантів;
1 – лише один правильний варіант відповіді з двох обраних або два з трьох обраних;
2 – обрані тільки правильні варіанти відповідей.

в) практичне розрахункове завдання (задача):

0 – задача не вирішувалася, або були використані формули з грубими помилками, або як такі, що не належать до суті задачі;
1 – задача вирішувалася, але в підсумку були приведені тільки загальні формули та міркування або допущені грубі помилки у використанні формул;
2 – задача вирішувалася, але допущена груба помилка у формулі або в її використанні;
3 – задача вирішена в загальному виді, або містить грубу помилку в розрахунках, або ж відсутня пряма відповідь на запитання;
4 – задача вирішена в цілому правильно, але без відповідних пояснень, або допущена незначна помилка (неточність);
5 – задача вирішена правильно з відповідними поясненнями.

Структура білета

Білет містить 30 однобальних теоретичних тестів, 5 двобальних та 12 п'ятибальних практичних розрахункових завдань, які охоплюють всі змістовні модулі програми іспиту. У підсумку максимальна сума балів білета складає 100 балів: 40 – за теоретичну частину та 60 – за практичну.

Шкала оцінювання білета

Фаховий іспит оцінюється за шкалою 100-200 балів. Мінімальний позитивний результат іспиту за виконання завдань білета (кваліфікаційний мінімум) складає 25 балів. Ця кількість балів відповідає екзаменаційній оцінки 100 шкали оцінювання. Переведення балів за виконання завдань білета вступного випробування до шкали 100-200 виконується відповідно до таблиці 5.20 додатка 5 Правил прийому до НТУ «Дніпровська політехніка». Вступники, які за резуль-

татами іспиту набрали менш ніж кваліфікаційний мінімум, позбавляються права участі в конкурсі.

Приклади екзаменаційних завдань білета

а) однобальний теоретичний тест:

Стандарт з управління інформаційною безпекою ISO 27001 є:
а) стандартом верхнього рівня, що описує безпеку ІС в цілому і принципи управління процесом забезпечення ІБ,
б) стандартом верхнього рівня, що описує безпеку ІС на технологічному і організаційному рівні, принципи, вимоги та інструкції з управління процесом забезпечення ІБ,
в) стандартом управління ризиками інформаційної безпеки,
г) стандартом управління інцидентами інформаційної безпеки.

б) двобальний теоретичний тест:

До складу технічного каналу витоку інформації в загальному випадку входить:
а) радіоефір,
б) технічний засіб захисту інформації,
в) порушник,
г) джерело інформації,
д) технічний засіб розвідки,
е) джерело загрози.

в) практичне розрахункове завдання (задача):

Визначити відношення сигнал/шум на межі контрольованої зони у децибелах, якщо рівень акустичного сигналу становить 0,2 Па, при проходженні у вільному просторі до межі контрольованої зони сигнал згасає на 10 дБ, та на шляху проходження сигналу зустрічається огороджувальна конструкція із звукоізоляцією 15 дБ. Рівень завад на межі контрольованої зони 20 дБ.

Переведення абсолютних величин в абсолютні виконується за формулою $N_{дБ} = 20 \cdot \lg \frac{P}{P_0}$,

де P - рівень сигналу в абсолютних величинах, P_0 - порогове значення.