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

ПРОГРАМА

вступного екзамену зі спеціальності
125 «Кібербезпека та захист інформації»
для вступу на навчання за ступенем доктора філософії

Уміння, що контролюються	Зміст програми
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. Обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах.	**1 Організаційно-технічні та правові основи забезпечення кібербезпеки та захисту інформації** 1.1 Терміни в галузі кібербезпеки та захисту інформації 1.2 Нормативно-правове забезпечення в сфері кібербезпеки та захисту інформації 1.3 Управління інформаційною безпекою 1.4 Організаційне забезпечення захисту інформації
Забезпечувати процеси захисту ІКС шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; розробляти та аналізувати проекти ІКС, базуючись на стандартизованих технологіях та протоколах передачі даних. Забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. Застосовувати в професійній діяльності знання, навички та практики щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації.	**2 Забезпечення безпеки інформації в інформаційно-комунікаційних системах (ІКС)** 2.1 Комплекси захисту ІКС 2.2 Моделі безпеки. Забезпечення захисту ресурсів та процесів в ІКС 2.3 Управління доступом відповідно принципам і критеріям доступу та прийнятої політики безпеки в ІКС 2.4 Методи та заходи захисту інформації в ІКС
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. Проектувати КСЗІ в автоматизованих системах відповідно до вимог нормативних документів системи технічного захисту інформації. Вирішувати задачі захисту потоків даних та визначати	**3 Системи захисту інформації** 3.1 Роботи зі створення комплексних систем захисту інформації (КСЗІ) 3.2 Випробування та експлуатація КСЗІ 3.3 Методи, технічні засоби та оцінка ефективності захисту

Уміння, що контролюються	Зміст програми
рівень захищеності інформаційних ресурсів в ІКС. Застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	інформації від витоку технічними каналами 3.4 Технічні системи охорони об'єктів
Використовувати методи та засоби криптографічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. Використовувати криптографічний захист для забезпечення необхідного рівня захищеності інформації в ІКС.	**4 Криптографічний захист інформації** 4.1 Математичні основи шифрування 4.2 Симетричні криптографічні системи 4.3 Асиметричні криптографічні системи та їх аналіз 4.4 Криптографічні алгоритми та протоколи

Рекомендована література

1. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. К.: НАУ, 2011. 620 с.
2. Корченко О.Г., Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів. Житомир: ЖВІ НАУ, 2010. 280 с.
3. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. професора В.Б. Толубка. К.: ДУТ, 2015. 288 с.
4. Христич В.В., Дерев'янко О.А., Бондаренко С.М., Антошкін О.А. Системи пожежної та охоронної сигналізації. Навчальний посібник. Харків: АПБУ МВС України, 2008. 87 с.
5. Головань С. М. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом. Підручник / С. М. Головань, В. Б. Дудикевич, В. С. Зачепило, Л. Т. Пархуць, В. О. Хорошко, Л. М. Щербак. Львів: Видавництво Львівської політехніки, 2005. 288 с.
6. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчальний посібник. Житомир: Видавництво ЖДУ, 2013. 136 с.
7. Грайворовський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. К.: Видавнича група BHV, 2009. 608 с.
8. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова К.: Видавництво Ліра-К, 2021. 412 с.
9. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних : підруч. К. : Вид-во DIRECTLINE, 2009. 714 с.
10. Сушко С.О., Кузнецов Г.В., Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу : навч. посіб. Дніпропетровськ : НГУ, 2010. 465 с.
11. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Х. : Видавництво «Форт», 2012. 870 с.
12. Остапов С.Е., Валь Л.О. Глинчук Л.Я. Основи криптографії. Навчальний посібник. Луцьк: Вежа-Друк, 2014. 164 с.

Критерії оцінювання окремих завдань білета

Кожне теоретичне тестове завдання білета оцінюється 1 або 2 балами, а практичне завдання – 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.

Шкала оцінювання білета

Іспит оцінюється за шкалою 100-200 балів (сума балів за виконання завдань білета плюс сто балів). Позитивним результатом складання іспиту є оцінка в межах 124 – 200 балів. Вступники, які набрали на іспиті менш ніж 124 бала, позбавляються права участі в конкурсі.

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.

Приклади екзаменаційних завдань білета

а) однобальний теоретичний тест:

Сукупність носія інформації, середовища його поширення та засобу технічної розвідки (згідно ДСТУ 3396.2) це:

а) інформативний сигнал,

б) технічний канал витоку інформації,

в) технічна розвідка,

г) захист інформації.

б) двобальний теоретичний тест:

До основних принципів політики безпеки не відноситься:

а) системність,
б) комплексність,
в) максимальність захисту,
г) неперервність захисту,
д) жорстке керування системою захисту,
е) відкритість алгоритмів і механізмів захисту.

в) практичне розрахункове завдання (задача):

Розділити секрет $C = 11$ за $(3,5)$ – пороговою схемою Шаміра, в якій будь-які 3 з 5 користувачів можуть відновити секрет. Використано поле $GF(13)$, секретний поліном $f(x) = 7x^2 + 8x + 11 (\mathrm{mod} 13)$, несекретні ненульові елементи поля $r_1 = 1, r_2 = 2, r_3 = 3, r_4 = 4, r_5 = 5$.