МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«ЗАТВЕРДЖУЮ»
Голова приймальної комісії
Олег ГРИГОР
«13» 07 2022 р.

ПРОГРАМА

фахового іспиту

при вступі на навчання для здобуття освітнього ступеня магістра

зі спеціальності 125 – Кібербезпека

(освітня програма – Безпека інформаційних і комунікаційних систем)

Черкаси 2022

1 ПРОГРАМА ВСТУПНИХ ВИПРОБУВАНЬ

Програма фахового іспиту складена на підставі Порядку прийому на навчання для здобуття вищої освіти в 2022 році, затверджених Наказом Міністерства освіти і науки України 27 квітня 2022 року № 392, зареєстрованого в Міністерстві юстиції України 03 травня 2022 р. за №487/37823.

1.1 ВИМОГИ ДО РІВНЯ ПІДГОТОВКИ ВСТУПНИКІВ

До участі у конкурсі щодо зарахування на навчання для здобуття освітнього ступеня магістра **зі спеціальності 125 - Кібербезпека (освітня програма – Безпека інформаційних і комунікаційних систем)** згідно переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266, допускаються особи, які здобули освітній ступінь бакалавра чи магістра або освітньо-кваліфікаційний рівень спеціаліста за спеціальностями згідно Додатку 5 Правил прийому до Черкаського державного технологічного університету в 2022 р.

Вступник має виявити базові знання з теорії та практики дисциплін, що виносяться на вступне випробування.

1.2 МЕТА ТА ЗАВДАННЯ ВСТУПНИХ ВИПРОБУВАНЬ

Перевірити відповідність знань, умінь, навичок вступників вимогам програми.

Оцінити ступінь підготовки вступників для навчання на здобуття ступеня магістра **зі спеціальності 125 – Кібербезпека (освітня програма – Безпека інформаційних і комунікаційних систем).**

1.3 ПЕРЕЛІК ДИСЦИПЛІН ТА РОЗДІЛІВ З НИХ, ЯКІ ВИНОСЯТЬСЯ НА ВСТУПНІ ВИПРОБУВАННЯ

На іспит виносяться питання з навчальних програм наступних дисциплін: «Інформаційно-комунікаційні системи», «Прикладна криптологія», «Нормативно-правове забезпечення інформаційної безпеки», «Захист інформації в інформаційно-комунікаційних системах», «Моніторинг і аудит безпеки

інформаційно-комунікаційних систем», «Комплексні системи захисту інформації».

Перелік тем з навчальних дисциплін, що виносяться на іспит:

1.3.1 Дисципліна «Інформаційно-комунікаційні системи»:

1. Знайомство з основними поняттями.
2. Налаштування мережевої операційної системи.
3. Мережеві протоколи і комунікації.
4. Мережевий доступ.
5. Мережа стандарту Ethernet.
6. Мережевий рівень.
7. IP-адресація.
8. Поділ IP-мереж на підмережі.
9. Транспортний рівень. Рівень додатків.
10. Проектування мережі.

1.3.2 Дисципліна «Прикладна криптологія»:

1. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.
2. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.
3. Основи теорії секретних систем (конфіденційності).
4. Симетричні криптографічні перетворення та їх властивості.
5. Джерела ключів та ключової інформації, вимоги до них.
6. Вступ в теорію асиметричних крипто-перетворень.
7. Асиметричні крипто-перетворення в групах точок еліптичних кривих.
8. Джерела ключів асиметричних криптосистем та вимоги до них. Методи та механізми автентифікації в криптосистемах.
9. Методи та механізми захисту від несанкціонованого доступу.
10. Методи та механізми імітозахисту в радіосистемах.
11. Електронні цифрові підписи з додатком.

12. Електронні цифрові підписи з відновлення повідомлень.

13. Властивості та основи застосування електронних цифрових підписів.

14. Криптографічні механізми та протоколи управління ключами.

15. Криптографічні механізми та протоколи автентифікації.

16. Синтез та аналіз криптографічних протоколів.

17. Квантова криптографія та криптоаналіз.

18. Вступ в теорію криптоаналізу в симетричних криптосистемах.

19. Методи криптоаналізу блокових симетричних криптосистем.

20. Методи криптоаналізу потокових симетричних криптосистем.

1.3.3 Дисципліна «Нормативно-правове забезпечення інформаційної безпеки»:

1. Інформація як об'єкт правового регулювання.

2. Законодавство України в області інформаційної безпеки.

3. Міжнародне законодавство в області захисту інформації.

4. Правовий режим захисту державної таємниці.

5. Основи захисту конфіденційної інформації.

6. Правовий захист інтелектуальної власності.

7. Сфера криптографічного захисту інформації.

8. Нормативно-правові основи здійснення криптографічного захисту в Україні.

9. Захист інформації в автоматизованих системах.

10. Захист інформації в комп'ютерних системах та мережах.

1.3.4 Дисципліна «Захист інформації в інформаційно-комунікаційних системах»:

1. Основні поняття й положення захисту інформації в комп'ютерних системах

2. Криптографічні методи захисту інформації

3. Біометричні системи захисту та ідентифікації.

4. Комп'ютерні віруси й механізми боротьби з ними.

5. Захист інформації в розподілених КС.

6. Побудова захищених корпоративних мереж.

7. Побудова й організація функціонування систем захисту інформації в комп'ютерних системах.

1.3.5 Дисципліна «Моніторинг і аудит безпеки інформаційно-комунікаційних систем»:

1. Кібербезпека і центр моніторингу та управління безпекою.
2. Операційна система Windows.
3. Операційна система Linux.
4. Мережеві протоколи і служби
5. Мережева інфраструктура
6. Принципи забезпечення безпеки мережі
7. Мережеві атаки
8. Захист мережі
9. Криптографія і інфраструктура загальних ключів
10. Захист і аналіз кінцевих пристроїв
11. Моніторинг безпеки
12. Аналіз даних вторгнень
13. Реагування на інциденти і їх обробка

1.3.6 Дисципліна «Комплексні системи захисту інформації»:

1. Сутність і задачі комплексної системи захисту інформації.
2. Методологічні основи комплексної системи захисту інформації.
3. Принципи створення комплексної системи захисту інформації.
4. Несанкціонований доступ до інформації і способи його здійснення.
5. Методи, засоби та заходи захисту інформації в інформаційно телекомунікаційних системах від несанкціонованого доступу.
6. Технічні канали витоку та руйнування інформації.

7. Захист інформації в інформаційно телекомунікаційних системах від витоку та руйнування.

1.4 СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1.4.1 Дисципліна «Інформаційно-комунікаційні системи»:

1. Wendell Odom. CCNA 200-301 Official Cert Guide. Volume 1-2 Cisco Press, 2019. — 1095 p.
2. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. - К.: Видавнича група «АТОПОЛ», 2014. - 262 с.
3. Загальні принципи функціонування комп'ютерних мереж. Навчальний посібник. / С.В. Мінухін, С.В. Кавун, С.В. Знахур. – Харків: Вид. ХНЕУ, 2008. – 210 с.
4. Лосев Ю.І. Комп'ютерні мережі: навчальний посібник / Ю.І. Лосев, К.М. Руккас, С.І. Шматков / За ред. Ю.І. Лосева. – Х.: ХНУ імені В.Н. Каразіна, 2013. – 248с.

1.4.2 Дисципліна «Прикладна криптологія»

1. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. — К.: «Центр учбової літератури», 2018. — 558 с., іл.
2. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавницт-во "Форт", 2012. – 880 с.: іл.
3. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 368 с.
4. Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Системи ЕЦП. Теорія та практика. Харків. Форт. 2010, 593 с.
5. Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.: іл.

1.4.3 Дисципліна «Нормативно-правове забезпечення інформаційної безпеки»

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102.
2. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія; НАПрН України, НДІІП, НАН України, Нац. б-ка ім. В.І. Вернадського. – Київ, 2015. – 388 с.
3. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.
4. Богуш В.М., Юдін О.К. Інформаційна безпека держави: навчальний посібник/ В.М. Богуш, О.К. Юдін. – К.: «Мк-Пресс», 2005. – 432 с.
5. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В. Гайворонський, О.М. Новіков. – К.: Видавництво ТОВ НВП «Інтерсервіс», 2009. – 714 с.
6. Дахно І.І. Право інтелектуальної власності: навчальний посібник/ І.І. Дахно.- К: «Либідь», 2003. – 199 с.
7. Правове забезпечення інформаційної діяльності в Україні/ За заг. ред. Ю.С. Шемшученка, І.С. Чижа.- К.: ТОВ «Видавництво «Юридична думка», 2006. – 378 с.

1.4.4 Дисципліна «Захист інформації в інформаційно-комунікаційних системах»:

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. –Х. : Вид. ХНЕУ, 2011. –510 с.

2. Гуз А.М., Довгань О.Д., Марущак А.І. Організація захисту інформації з обмеженим доступом. -К. : Наук.-вид. відділ НА СБ України, 2015. -378 с.

3. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.

1.4.5 Дисципліна «Моніторинг і аудит безпеки інформаційно-комунікаційних систем»:

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. Allan Johnson. CCNA Cybersecurity Operations Companion Guide. – San Jose: Cisco Press, 2018. – 651 p.
3. Bejtlich Richard. The practice of network security monitoring: understanding incident detection and response / by Richard Bejtlich.. – San Francisco: No Starch Press, 2018. – 380 p.
4. William M. Hancock Cybersecurity Operations Handbook. – ELSEVIER INDIA, 2008. – 1287 p.

1.4.6 Дисципліна «Комплексні системи захисту інформації»

1. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
2. Хорошко В.О. Проектування комплексних систем захисту інформації: підручник / В.О.Хорошко, І.М.Павлов, Ю.Я.Бобало, В.Б.Дудикевич, О.Р.Опірський, Л.Т. Пархуць. – Львів: Львівська політехніка, 2020. – 320 с.
3. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

2 ПОЯСНЮВАЛЬНА ЗАПИСКА ДО ВСТУПНИХ ВИПРОБУВАНЬ

Вимоги до фахового іспиту відповідають вимогам чинних навчальних програм згідно стандарту вищої освіти **за спеціальністю 125 – «Кібербезпека» (освітня програма – Безпека інформаційних і комунікаційних систем).**

Час тестування – 2 астрономічні години (120 хвилин).

Вступні випробування проводяться у формі тестування в письмовій формі.

Тестове завдання складається з двох блоків. Блок 1 – 10 завдань. Блок 2 – 10 завдань.

Блоки 1 та Блок 2 містять завдання відкритого типу.

Для тестового Блоку 1 подано 4 варіантів відповідей, Блоку 2 – 4 варіантів відповідей, з яких тільки одна правильна. Тестове питання вважається виконаним правильно, якщо вступник вказав саме правильну відповідь.

Правильність виконання завдань оцінюється відповідно до критеріїв оцінювання знань.

Екзаменатор не зобов'язаний читати розв'язання завдань, що наведені вступником в чернетці.

Результати фахового іспиту оцінюються за шкалою від 100 до 200 балів.

Особи, які набрали на вступних випробуваннях менше ніж 125 бали, позбавляються права участі в конкурсі за спеціальністю (освітньою програмою).

3 КРИТЕРІЇ ОЦІНЮВАННЯ ВСТУПНИХ ВИПРОБУВАНЬ

1. Результати фахового іспиту оцінюються за шкалою від 100 до 200 балів і є результатом додавання до 100 балів суми балів, отриманих за виконання кожного завдання тесту:

за правильне розв'язання кожного з тестових питань *Блоку 1* вступник одержує по 4 бали (всього 40 балів), *Блоку 2* вступник одержує по 6 балів (всього 60 балів). За неправильну відповідь на тестове завдання вступник отримує – 0 балів.

2. Особи, які набрали на вступних випробуваннях менше ніж 125 бали, позбавляються права участі в конкурсі зі спеціальності **125 – «Кібербезпека» (освітня програма – Безпека інформаційних і комунікаційних систем)**.

Голова фахової атестаційної комісії
зі спеціальності 125 – «Кібербезпека»,
(освітня програма – Безпека
інформаційних і комунікаційних
систем)

д.т.н., професор В.В. Палагін