МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖУЮ:
Голова приймальної комісії
Харківського національного
економічного університету
імені Семена Кузнеця

_____ Володимир ПОНОМАРЕНКО
«14» травня 2022 р.

ПРОГРАМА ФАХОВОГО ІСПИТУ

освітній ступінь «МАГІСТР»

спеціальність 125 «КІБЕРБЕЗПЕКА»
освітньо-професійна програма «Кібербезпека»

Харків
2022

Програма фахового вступного випробування розроблена для абітурієнтів, які вступають на навчання за освітнім ступенем магістр за спеціальністю 125 «Кібербезпека». Завдання фахового вступного випробування складено з метою виявлення знань, вмінь, компетентностей, якими володіє бакалавр за галуззю знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека» (табл. 1).

Таблиця 1 – Основні компетентності, якими повинен володіти бакалавр за галуззю знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека»

Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною

	безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати

методи та засоби криптографічного та технічного 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.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ЗМІСТ ФАХОВИХ ВСТУПНИХ ВИПРОБУВАНЬ

1. Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки

1.1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки.

1.1.1. ЗУ про інформацію, про науково-технічну інформацію.

1.1.2. ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах».

1.1.3. ЗУ «Про доступ до публічної інформації».

1.1.4. ЗУ «Про державну таємницю».

1.1.5. ЗУ «Про основні засади забезпечення кібербезпеки України».

1.1.6. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

1.2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки.

1.2.1. Регламенти ЄС в галузі кібербезпеки.

1.2.2. ДСТУ ISO 27001.

2. Інформаційні технології в інформаційній та/або кібербезпеці

2.1. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.

2.1.1 Мережева модель OSI. Основні протоколи стеку TCP/IP.

2.1.2. Віртуалізація (принципи, гіпервізори).

2.1.3. Архітектура комп'ютерів.

2.2. Методи і засоби обробки інформації.

2.2.1. Алгоритмізація та програмування (без прив'язки до конкретної мови програмування).

2.2.2. Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Делегати, Узагальнення).

2.2.3. Методи сортування та пошуку даних.

2.2.4. Кількісна міра інформації.

2.2.5. Завадостійкі коди.

2.3. Операційні системи.

2.3.1. Архітектура операційних систем.

2.3.2. Процеси і потоки в операційних системах.

2.3.3. Керування пам'яттю в операційних системах.

2.3.4. Файлові системи.

2.3.5. Захисні механізми операційних систем.

2.4. Моделі безпеки в інформаційній та/або кібербезпеці.

2.4.1. Модель порушника.

2.4.2. Модель загроз.

2.4.3. Модель вразливостей.

3. Безпека інформаційно-комунікаційних систем

3.1. Захист інформації, що обробляється та зберігається в ІКС.

3.1.1. Процедури ідентифікації, автентифікації, авторизації користувачів.

3.1.2. Резервування інформації та компонентів ІКС.

3.2. Програмні та програмно-апаратні комплекси ЗЗІ.

3.2.1. Антивіруси, міжмережеві екрани.

3.2.2. IPS, IDS.

3.2.3. Системи контролю та управління доступом.

3.3. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

3.3.1. Організаційно-технічні заходи відновлення функціонування ІКС.

3.3.2. Журнал аудиту подій.

3.3.3. Політики резервного копіювання даних.

3.4. Моніторинг процесів функціонування ІКС.

3.4.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторингу.

3.4.2. Система візуалізації та управління подіями (SIEM).

3.4.3. Аналіз подій.

3.5. Механізми безпеки комп'ютерних мереж.

3.5.1. Віртуальні приватні мережі (VPN).

3.5.2. Протоколи автентифікації RADIUS.

3.5.3. Протоколи SSL/TLS.

4. Комплексні системи захисту інформації

4.1. Проєктування, створення, супровід КСЗІ.

4.1.1. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.

4.1.2. Вибір методів та засобів забезпечення необхідного рівня ІБ.

4.2. Моделі загроз та моделі порушника.

4.2.1. Загрози цілісності.

4.2.2. Загрози доступності.

4.2.3. Загрози конфіденційності.

4.2.4. Загрози через технічні канали.

4.2.5. Загрози через соціальну інженерію.

4.3. Оцінка захищеності інформації в ІКС.

4.3.1. Концептуальна схема оцінки безпеки інформації.

4.3.2. Кількісна та якісна оцінки безпеки інформації.

5. Управління інформаційною та / або кібербезпекою

5.1. Управління кіберінцидентами.

5.1.1. Поняття кіберінцидента / кібератаки.

5.1.2. Розслідування кіберінцидентів / кібератак.

5.2. Управління ризиками в інформаційній та / або кібербезпеці.

5.2.1. Ризики інформаційної безпеки.

5.2.2. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику.

5.3. Аудит інформаційної та/або кібербезпеки.

5.3.1. Етапи проведення аудиту.

5.3.2. Аудит на основі аналізу ризиків.
5.3.3. Аудит на основі стандартів ІБ.
5.3.4. Аудит на основі експериментальних досліджень ІС.
5.4. Забезпечення безперервності бізнес-процесів.
5.4.1. Поняття бізнес-процесу.
5.4.2. Модель бізнес-процесу.
6. Криптографічний захист інформації
6.1. Математичні основи криптографії та стеганографії.
6.1.1. Модулярні обчислення.
6.1.2. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях.
6.1.3. Умови стійкості шифрів.
6.1.4. Однонаправлені функції, функції гешування.
6.1.5. Псевдовипадкові послідовності в криптосистемах.
6.1.6. Обчислення в системі чисел з плаваючою точкою.
6.2. Симетричні криптосистеми.
6.2.1. Модель симетричної криптосистеми.
6.2.2. Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування.
6.2.3. Блокові шифри. DES, AES, ГОСТ 28147, DSTU7624. В 6.2.3.1. DES 6.2.3.2. AES
6.2.3.3. ДСТУ ГОСТ 28147-2009
6.2.3.4. ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість).
6.2.4. Потокові шифри. RC4, STRUMOK. А 6.2.4.1. RC4 6.2.4.2. ДСТУ 8845:2019 (довжина ключів, крипостійкість).
6.3. Асиметричні криптосистеми.
6.3.1. Модель асиметричної криптосистеми.
6.3.2. Шифри RSA, EG.
6.3.3. Генерація спільних секретів DH.
6.3.4. Електронний цифровий підпис DSA.
6.4. Криптографічні протоколи.
6.4.1. Протоколи захисту мережевого трафіку IPSec.
6.4.2. Протоколи безпечної передачі даних прикладного рівня: https.
6.5. Цифрова стеганографія.
6.5.1. Поняття цифрової стеганографії.
6.5.2. Модель стеганосистеми. Основні вимоги до стеганосистеми.
6.5.3. Відкриті, напівзакриті, закриті стеганосистеми.
6.5.4. Поняття ЦВЗ, класифікація.
6.5.5. Метод модифікації найменшого значущого біта.
6.5.6. Атаки на стеганосистеми.
7. Технічний захист інформації
7.1. Технічні канали витоку інформації.
7.1.1. Акустичний (мовний) канал витоку інформації.
7.1.2. Електричний канал витоку інформації.

7.1.3. Електромагнітний канал витоку інформації.

7.1.4. Оптичний та оптоелектронний канал витоку інформації.

7.1.5. Параметричний канал витоку інформації.

7.2. Методи та засоби технічного захисту інформації.

7.2.1. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.

7.2.2. Системи відеоспостереження.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. SQL Server 2008: ускоренный курс для профессионалов / Р.Э. Уолтерс, М.Коулс, Р.Рей и др. – М.: Изд. дом «Вильямс», 2008. – 768 с.

2. Абрамов В.О. Архітектура електронно-обчислювальних машин. Навчальний посібник. – К.: КМПУ імені Б.Д.Грінченка, 2007. – 84 с.

3. Антонов В.М. Сучасні комп'ютерні мережі. – К.: МК-Прес, 2015.– 480 с.

4. Керниган Б., Ричи Д. Язык программирования Си: Пер. с англ. / Под ред. В.С. Штаркмана. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 1992. – 272 с.

5. Хеник Б. HTML и CSS. Путь к совершенству (HTML и CSS: The Good Parts).

6. Билл Кеннеди, Чак Муссиано – «HTML и XHTML. Подробное руководство (HTML & HXTML. The Definitive Guide)».

7. Буров Є. В. Комп'ютерні мережі: підруч. – Львів: Магнолія-плюс, 2006. – 262 с.

8. Герберт, Шилдт Java 2 v5.0 (Tiger). Новые возможности; СПб: БХВ-Петербург, 2013. – 208 с.

9. Григорьев, А.Б. О чем не пишут в книгах по Delphi; БХВ-Петербург, 2012. – 576 с.

10. Семенов С.Г. Давидов В.В., Далека В.Д., Кучук Н.Г. Бульба С.С. Сучасні технології безпечного програмування: навчально-методичний посібник. – Харків: НТУ «ХПІ», 2021. – 112 с.

Голова атестаційної комісії Сергій СЕМЕНОВ