МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

ЗАТВЕРДЖУЮ

Голова приймальної комісії
Національного аерокосмічного університету
ім. М. Є. Жуковського
«Харківський авіаційний інститут»
_____ Олексій ЛИТВИНОВ
«___» _____ 2025 р.

ПРОГРАМА
ВСТУПНОГО ВИПРОБУВАННЯ

для здобуття освітнього ступеня доктор філософії

за освітньо-науковою програмою

за спеціальністю

F5 «Кібербезпека та захист інформації»
(код та найменування)

освітньо-наукова програма

Кібербезпека
(найменування)

у **2025** році

Харків 2025

ВСТУП

Вступне випробування для здобуття освітнього ступеня доктора філософії за

освітньо-науковою програмою зі спеціальності F5 «Кібербезпека та захист інформації» (освітньо-наукова програма Кібербезпека

(код та найменування)

(найменування)

відбувається відповідно до «Правил прийому на навчання до Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» у 2025 році у формі індивідуального письмового іспиту, який приймає фахова екзаменаційна комісія з певної спеціальності (освітньої програми), склад якої затверджується наказом ректора Університету.

До фахового іспиту входять питання за темами:

- законодавча та нормативно-правова база і стандарти в галузі інформаційної та/або кібербезпеки;
- безпека інформаційно-комунікаційних систем;
- комплексні системи захисту інформації;
- криптографічний захист інформації;
- технічний захист інформації.

Перелік питань за темами наведений у програмі

Критерії оцінювання знань

1. Результат фахового іспиту визначається за шкалою від 80 до 200 балів.
2. Фаховий іспит проводиться у формі індивідуального письмового іспиту. Екзаменаційний білет складається з трьох питань, що входять до програми фахового іспиту.
3. Результат фахового іспиту розраховується за формулою $80 + 3*k$, де k – кількість балів за відповідь ($k = 0 – 40$).
4. Якщо вступник отримав менше 100 балів, то вважається, що він не склав іспит і до участі в конкурсі не допускається.

1.Питання за темою «Законодавча та нормативно-правова база і стандарти в галузі кібербезпеки»

1. Терміни та визначення.
2. Загальні положення щодо захисту інформації в ІТС.
2. Критерії оцінки захищеності інформації в комп'ютерних системах.
3. Модель загроз.
4. Модель порушника.
5. Політика безпеки.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
2. Закон України «Про основні засади забезпечення кібербезпеки України».
3. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»
4. ДСТУ 3396.0,1,2-97.
5. ДСТУ ISO/IEC 15408-1:2017.
6. НД ТЗІ 1.1-002-99. «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
7. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».
8. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»
9. НД ТЗІ 1.4-001-2000. «Типове положення про службу захисту інформації в автоматизованій системі»
10. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601
11. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

2. Питання за темою «Безпека інформаційно-комунікаційних систем»

1. Захист інформації, що обробляється та зберігається в ІКС.
2. Процедури ідентифікації, автентифікації, авторизації користувачів.
3. Програмні та програмно-апаратні комплекси ЗЗІ.
4. Шкідливе програмне забезпечення.
5. Антивіруси та міжмережеві екрани.
6. Організаційно-технічні заходи відновлення функціонування ІКС.
7. Політики резервного копіювання даних.
8. Моніторинг процесів функціонування ІКС.
9. Механізми безпеки комп'ютерних мереж.
10. Віртуальні приватні мережі

Література

1. Гайворонський М.В., Новиков О.М. Безпека інформаційно комунікаційних систем. К.: вид. група BHV, 2009. – 608 с.
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП ІНТЕРСЕРВІС», 2009. – 716 с.
3. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.

3. Питання за темою «Комплексні системи захисту інформації»

1. Формування загальних вимог до КСЗІ
2. Дослідження середовищ функціонування ІС
3. Вибір методів та засобів забезпечення необхідного рівня ІБ
4. Розробка політики безпеки в ІТС
5. Оцінка захищеності інформації в ІТС
6. Оцінка ризиків
7. Функціональна безпека та кібербезпека

Література

1. Лісовська Ю. П. Кібербезпека: ризики та заходи: посібник.-К. Видавничий дім «Кондор», 2019. -.272 с.
2. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник/ В. Д. Козюра, В. О. Хорошко, М .Є. Шелест, Ю. М. Ткач, С. В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. - 240 с.
3. Проектування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів: Вид. Львівська політехніка, 2020. – 320 с.

4. Питання за темою «Криптографічний захист інформації»

1. Криптосистеми: базові поняття, призначення, класифікація.
2. Криптопротоколи: базові поняття, призначення, класифікація.
3. Симетричні алгоритми.
4. Асиметричні алгоритми.
5. Цифровий підпис.
6. Автентифікація користувачів.
7. Розподіл ключів.
8. Методи криптоаналізу
9. Сучасні криптосистеми.
10. Постквантова криптографія

Література

1. Криптографія від історії до сучасних стандартів: навч.посібник/ Г. Л. Козіна. Запоріжжя: НУ «Запорізька». 2020. – 192 с.
2. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.
3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с

4. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
5. Моргун О.М. Кріптографічні методи захисту інформації: Навч. посібник. – Черкаси: АПБ ім. Героїв Чорнобиля, 2008. – 97с.

Література

1. Браіловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах інформаційної діяльності/ За ред. Проф. В.О. Хорошка. -К.:ДУІКТ, 2007
2. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.
3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с
4. Єфремов В.П., Кононович В.Г., Тардаскін М.Ф. Технічна експлуатація систем захисту інформації. Част. 2. Експлуатація безпечних інформаційних технологій: навч. посіб./ за ред. М.В. Захарченка. Одеса: ОНАЗ, 2003. – С. 248.
5. Тардаскін М.Ф., Кононович В.Г. Технічний захист комерційної таємниці підприємства зв'язку: навч. посіб./ за ред. М.В. Захарченка. Одеса: ОНАЗ, 2002. – 76 с

Гарант освітньо-наукової програми «Кібербезпека інформації» _____ Володимир ПЄВНЄВ

Програму розглянуто й узгоджено на випусковій кафедрі комп'ютерних систем, мереж і кібербезпеки.

Протокол № 9 від « 11 »березня 2025 р.

Завідувач кафедри 503 _____ Вячеслав ХАРЧЕНКО

ПОГОДЖЕНО

Проректор з науково педагогічної роботи Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» _____ Андрій ГУМЕННИЙ

Завідувач відділу аспірантури і докторантури _____ Володимир СЕЛЕВКО