НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»

Затверджую

Голова Приймальної комісії
Ректор
_____ Анатолій МЕЛЬНИЧЕНКО
підпис
28 березня 2025 р.
дата

Навчально-науковий фізико-технічний інститут

повна назва факультету/навчально-наукового інституту

ПРОГРАМА
фахового іспиту
для вступу на освітні програми підготовки магістра
«Системи, технології та математичні методи кібербезпеки»

за спеціальністю F5 Кібербезпека та захист інформації

Програму ухвалено:
Вченою Радою Навчально-наукового
фізико-технічного інституту
Протокол № 3 від 24 березня 2025 р.
Голова Вченої Ради
_____ Олексій НОВІКОВ

Київ – 2025

ВСТУП

Програма фахового іспиту визначає форму організації, зміст та особливості проведення вступного фахового іспиту для вступу на освітні програми підготовки магістра «Системи, технології та математичні методи кібербезпеки» за спеціальністю F5 Кібербезпека та захист інформації.

Метою програми фахового іспиту для вступу на освітні програми підготовки магістра «Системи, технології та математичні методи кібербезпеки» за спеціальністю F5 Кібербезпека та захист інформації є перевірка набуття вступником компетентностей та результатів навчання, що визначені стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти.

Освітні програми "Системи, технології та математичні методи кібербезпеки" відповідають місії та стратегії КПІ ім. Ігоря Сікорського, за якими стратегічним пріоритетом університету є фундаменталізація підготовки фахівців. Особливості освітніх програм враховані шляхом обрання відповідних розділів програми фахового іспиту. Проведення фахового іспиту має виявити рівень підготовки вступника з обраної для вступу спеціальності.

Програма побудована з наступних розділів: математична частина, загальна частина та професійна частина.

Фаховий іспит здійснюється в письмовій формі в аудиторії або дистанційно засобами Moodle. Білет містить чотири завдання:

1. Питання з Розділу I (теорія).
2. Питання з Розділу II (теорія).
3. Питання з Розділу III (теорія).
4. Задача з Розділу III.

Тривалість фахового іспиту – 2 (дві) астрономічні години, перерви немає. Екзаменований вільно розподіляє свій час між всіма завданнями.

ОСНОВНИЙ ВИКЛАД

Розділ I.

1. Алгебра матриць (лінійні операції, множення, обернена та алгоритми її відшукання). Матриця лінійного оператора та її перетворення при заміні базису. Жорданова форма матриці.
2. Визначники *n*-го порядку, їх властивості. Техніка обчислення визначників.
3. Формули Крамера для розв'язків системи лінійних алгебричних рівнянь. Метод Ґаусса.
4. Системи лінійних алгебричних рівнянь. Теорема Кронекера-Капеллі. Фундаментальна система розв'язків.
5. Власні вектори та власні значення матриці. Алгоритм їх відшукання. Властивості власних векторів та власних значень симетричних матриць.

6. Векторна алгебра. Скалярний, векторний, мішаний добуток векторів та їх властивості.
7. Аналітична геометрія: рівняння основних геометричних об’єктів на площині та у просторі.
8. Поняття послідовності. Збіжні та розбіжні послідовності, границя збіжної послідовності. Критерій Коші існування границі. Нескінченно малі послідовності та їх основні властивості.
9. Означення границі функції у точці мовою послідовностей (за Гейне) та мовою нерівностей (за Коші). Критерій існування границі мовою односторонніх границь. Неперервні функції, класифікація точок розриву неперервної функції.
10. Граничний перехід у сумі, добутку, частці та у нерівностях для функцій. Невизначеності, їх види та способи розкриття. Порівняння функцій в околі точки. Таблиця еквівалентних нескінченно малих при $x \to 0$ функцій.
11. Поняття похідної та диференціалу функції. Інваріантність першого диференціалу та його застосування до наближених обчислень. Похідні та диференціали вищих порядків.
12. Формула Ньютона-Ляйбніця. Застосування визначеного інтеграла для знаходження геометричних та фізичних величин (площ, об’ємів, центрів мас, моментів інерції тощо).
13. Поняття числового ряду та його суми. Ознаки збіжності числових рядів.
14. Поняття функціонального ряду та його області збіжності. Вигляд області збіжності степеневого ряду. Степеневий ряд Тейлора.
15. Формула Тейлора та ряди Тейлора для найважливіших елементарних функцій.
16. Поняття множини. Основні операції на множинах. Покриття і розбиття множини. Булеан множини. Декартів добуток множин.
17. Поняття відношення, операції: добуток відношень; обернене до даного.
18. Основні властивості та види відношень. Відношення еквівалентності, часткового порядку. Лінійний та повний порядки; лексико-графічний порядок.
19. Напівгрупи, групи, кільця, поля. Приклади.
20. Поняття алгебри, підалгебри. Гомоморфізми та ізоморфізми алгебр.
21. Булеві алгебри. Решітки.
22. Поняття імовірнісного простору. Геометрична та класична модель. Модель Бернуллі.
23. Поняття дискретної та неперервної випадкової величини. Основні дискретні та неперервні розподіли (Бернуллі, Пуассона, геометричний, експоненціальний, Коші, гаусовий). Їх числові характеристики – математичне очікування, дисперсія, моменти.
24. Теорема Чебишева про закон великих чисел. Інтегральна гранична теорема Муавра-Лапласа.
25. Довірча ймовірність, інтервальне оцінювання. Оцінка середнього та дисперсії гаусового розподілу.

Розділ ІІ.

1. Політика безпеки. Призначення і основні складові політики безпеки.
2. Система нормативних документів України із захисту інформації.
3. Класифікація інформації за режимом доступу та за правовим режимом. Види інформації, захист якої гарантується державою.
4. Етапи побудови комплексної системи захисту інформації (КСЗІ). Зміст робіт, що виконуються на окремих етапах. Документи, що розробляються для кожного етапу створення КСЗІ.
5. Основні поняття криптології. Теорія зв'язку в секретних системах Шеннона. Цілком таємні шифри, границя Шеннона. Шифр одноразового блокноту.
6. Принципи побудови сучасних блокових шифрів. Алгоритми шифрування DES та ДСТУ ГОСТ 28147:2009: схема роботи, параметри.
7. Алгоритми шифрування AES та ДСТУ 7624:2014 «Калина»: схема роботи, параметри.
8. Регістри зсуву з лінійним оберненим зв'язком: означення, характеристичні поліноми, обчислення періоду гами. Застосування регістрів зсуву у криптографії, потокові шифри.
9. Важкооборотні функції та важкооборотні функції із секретом. Схема вироблення спільного секрету Діффі-Хеллмана: опис, обґрунтування стійкості. Система шифрування RSA: генерування ключів, шифрування, розшифрування.
10. Криптографічні геш-функції: означення, властивості, основні параметри стійкості. Цифрові підписи: означення, задачі. Схема RSA цифрового підпису із геш-функцією.
11. Схема шифрування Ель-Гамаля; схема цифрового підпису Ель-Гамаля (опис, обґрунтування стійкості).
12. Задача автентифікації користувачів. Криптографічні алгоритми автентифікації: схеми на одноразових паролях, схеми на цифрових підписах.
13. Типи ядер операційних систем: монолітне, модульне, гібридне, мікроядро, наноядро, екзоядро. Приклади ОС з різними ядрами.
14. Процеси і потоки: визначення, моделі, схеми багатопотоковості, опис процесів і потоків у системі. Приклади реалізації у різних ОС (Linux, Windows).
15. Стани потоків і переходи між станами, завдання і алгоритми планування процесів (потоків). Приклади реалізації у різних ОС (Linux, Windows).
16. Керування пам'яттю: завдання, методи розподілу пам'яті, віртуальна пам'ять. Сегментний і сторінковий розподіл пам'яті у процесорах x86.
17. Організація пристроїв введення-виведення. Контролер, драйвер, оброблення переривань. Структура драйверів в Linux і Windows.
18. Файлові системи: визначення, атрибути файлів, опис розміщення файлів на диску. Приклади файлових систем (FAT32, NTFS, ext2/3).
19. Дискреційні моделі керування доступом. Модель HRU. Властивості моделі та теореми розв'язності задачі безпеки. Модель TAM та її властивості.

20. Модель Take-Grant. Формалізація санкціонованого отримання прав доступу та крадіжки прав доступу. Розширена модель Take-Grant. Правила де-юре та де-факто.
21. Моделі тематичного керування доступом. Модель решітки цінностей. Решітка MLS.
22. Моделі мандатного керування доступом. Властивості мандатного керування доступом. Модель Белла-ЛаПадули. Основна теорема безпеки.
23. Проблеми мандатного керування доступом. Розвиток моделі Белла-ЛаПадули: Z-система Мак-Ліна, модель Low-Watermark.
24. Рольові моделі керування доступом.
25. Моделі забезпечення цілісності даних (Біба, Кларка-Вілсона та похідні моделі).

Розділ ІІІ.

1. Стандарт ISO 15408 (Common Criteria).
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ).
3. Реляційна модель даних (РМД). Структуризація даних в РМД. Обмеження цілісності. Функціональні залежності в РМД. Декомпозиція відносин за функціональними залежностями.
4. Транзакція як механізм забезпечення несуперечності даних. Властивості транзакції.
5. Захист даних в БД від несанкціонованого доступу. Основні механізмі захисту в БД: автентифікація, керування доступом, реєстрація і аудит.
6. Основні види вразливостей програмного забезпечення. Вразливості веб-застосунків. Міжнародні класифікатори вразливостей.
7. Модель загроз програмного забезпечення. Етапи побудови моделі. Класифікація загроз за методикою STRIDE. Оцінка ризиків за методикою DREAD. Моделювання загроз за допомогою дерева атаки.
8. Структура файлів що виконуються. Особливості ураження файлів, що виконуються комп’ютерним вірусом. Типи комп’ютерних вірусів. Особливості поліморфних вірусів.
9. Зловмисне програмне забезпечення типу комп’ютерний черв'як і троянський кінь: структура, методи розповсюдження. Методи виявлення.
10. Програмно-апаратні засоби захисту прикладних програм від несанкціонованого використання. Методи захисту програмного забезпечення від зворотного аналізу.
11. Модель взаємодії відкритих систем. Завдання кожного з рівнів.
12. Стек протоколів TCP/IP. Протокол IP. Адресація. Протоколи UDP і TCP.
13. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки. Вразливості протоколів Інтернету — IP, TCP, ICMP, і атаки на ці протоколи.
14. Система DNS, вразливості і можливі атаки. Методи захисту.

15. Міжмережне екранування (firewalling) як метод захисту комп'ютерних мереж. Класифікація і можливості міжмережних екранів.
16. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Основні протоколи.
17. Засоби IPSec: призначення, архітектура засобів, основні протоколи, формати мережних пакетів. Транспортний і тунельний режими.
18. Засоби VPN віддаленого доступу. Призначення, вимоги. Порівняння SSL/TLS і SSH.
19. Модель загроз для операційної системи. Типова архітектура комплексу засобів захисту операційних систем.
20. Склад і архітектура засобів захисту ОС Windows.
21. Реалізація дискреційного керування доступом в ОС Windows.
22. Склад і архітектура засобів захисту ОС Linux.
23. Реалізація дискреційного керування доступом в ОС Linux.
24. Реалізація мандатного керування доступом в ОС Linux.
25. Реалізація засобів фільтрування мережного трафіку в ОС Linux.

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

ВИКОРИСТАННЯ ДОПОМІЖНОГО МАТЕРІАЛУ

Під час відповідей на теоретичні питання користуватися літературою та будь-якими електронними пристроями забороняється. Для розв'язання задачі дозволяється користуватися калькулятором, але не таким, що входить до складу програмного забезпечення мобільного телефону, смартфону, планшету або портативного комп'ютера.

КРИТЕРІЇ ОЦІНЮВАННЯ
фахового іспиту
для вступу на освітні програми підготовки магістра
«Системи, технології та математичні методи кібербезпеки»
за спеціальністю 125 «Кібербезпека та захист інформації»

Вступник дає відповіді на питання з Розділу І, два теоретичних питання з Розділу ІІ і ІІІ, розв'язує одну задачу. Відповідь на кожне з теоретичних питань фахового іспиту оцінюється за бальною шкалою рейтингової системи оцінювання (РСО) за таким порядком визначення (з максимальним ваговим балом 25):

- 24…25 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 21…23 – повна відповідь (містить не менше 85% потрібної інформації);
- 19…20 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 17…18 – достатня відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 15…16 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації або окремі помилки);
- 1...15 – незадовільна відповідь;
- 0 — відповідь відсутня.

Шкала оцінювання задачі за РСО (максимальний ваговий бал 25):

- 24…25 – повне, безпомилкове, відмінне розв'язання завдання, обсяг виконання 95-100%;
- 21…23 – повне розв'язання завдання з несуттєвими похибками, містить не менше 85% потрібної інформації;
- 19…20 – розв'язання завдання з похибками, містить не менше 75% потрібної інформації;
- 17…18 – завдання виконане задовільно, з невеликими помилками, містить не менше 65% потрібної інформації;
- 15…16 – завдання виконане задовільно, з помилками, містить не менше 60% потрібної інформації;
- 1...15 – завдання не виконано;

- 0 — спроби розв’язку задачі відсутні.

Кінцева кількість балів – проста арифметична сума балів, отриманих за відповіді на кожне з чотирьох вищезазначених завдань. Максимальна кількість балів РСО – 100. Мінімальна кількість балів, що дає право продовжувати брати участь у конкурсному відборі — 60.
Отримана оцінка перераховується в оцінку за 200-бальною шкалою (100...200) згідно таблиці:

Таблиця відповідності оцінок РСО (60…100 балів)
оцінкам 200-бальної шкали (100…200 балів)

шкала РСО	шкала 100…200		шкала РСО	шкала 100…200		шкала РСО	шкала 100…200		шкала РСО	шкала 100…200
60	100		70	140		80	160		90	180
61	105		71	142		81	162		91	182
62	110		72	144		82	164		92	184
63	115		73	146		83	166		93	186
64	120		74	148		84	168		94	188
65	125		75	150		85	170		95	190
66	128		76	152		86	172		96	192
67	131		77	154		87	174		97	194
68	134		78	156		88	176		98	196
69	137		79	158		89	178		99	198
									100	200

Якщо згідно РСО отримано менше 60 балів, оцінка за 200-бальною шкалою прирівнюється до нуля.

СПИСОК ЛІТЕРАТУРИ

Розділ І.

1. Хмельницький М. О. Алгебра та геометрія. – К.: КПІ ім. Ігоря Сікорського, 2022. – 171 с. https://ela.kpi.ua/handle/123456789/48441
2. Безущак О. О., Ганюшкін О. Г., Кочубинська Є. А. Навчальний посібник з лінійної алгебри для студентів механіко-математичного факультету. – К.: ВПЦ "Київський університет", 2019. – 224 с.
3. Федір Лиман, Віталій Власенко, Світлана Петренко. Вища математика. Навчальний посібник. У 2-х частинах. – К.: Університетська книга, 2018.
4. Є. П. Зайцев. Вища математика. Інтегральне числення функції однієї та багатьох змінних. Звичайні диференціальні рівняння. Ряди. – К.: Алерта, 2018. – 154 с.
5. Галицька І. Є. Математичний аналіз 2. Дистанційний курс для спец. 125 «Кібербезпека», ОП «Системи, технології та математичні методи кібербезпеки». – К.: КПІ ім. Ігоря Сікорського, 2022.
6. В. Ю. Клепко, В. Л. Голець. Вища математика в прикладах і задачах. – К.:

Центр навчальної літератури, 2017.
7. Дубовик В. П. Вища математика: навч. посіб. для студ. вищ. навч. закл./ В. П Дубовик, І. І. Юрик. – 4-те вид. – К.: Ігнатекс-Україна, 2013.
8. Капітонова Ю. В., Кривий С. Л. Летичевський О. А., Луцький Г. М., Печурін М. К. Основи дискретної математики. – К.: Наукова думка, 2002, 560 с.
9. Дискретний аналіз 1. Множини та відношення: методичні вказівки до практичних занять для студентів напрямів підготовки «Безпека інформаційних і комунікаційних систем» та «Прикладна математика» / уклад. А. А. Шумська. – Київ: КПІ ім. Ігоря Сікорського, 2010. https://ela.kpi.ua/handle/123456789/567
10. Дискретний аналіз. Ч. 4: Елементи загальної алгебри: курс лекцій для студентів спеціальності, пов'язаних з інформаційними технологіями та захистом інформації/уклад. М. К. Мороховець. – Київ: КПІ ім. Ігоря Сікорського, 2015. – 81 с. https://ela.kpi.ua/handle/123456789/11994
11. Спекторський І. Я. Дискретна математика. – К.: в-во «Політехніка КПІ ім. Ігоря Сікорського», 2004. – 219 с.
12. Гнєденко Б. В. Курс теорії ймовірностей. – К.: в-во «Київський університет», 2010. – 463 с.
13. Кузнєцов М. Ю., Шумська А. А. Теорія ймовірностей та математична статистика. Збірник завдань до практичних занять. Гриф надано Методичною радою КПІ ім. Ігоря Сікорського, прот. № 7 від 13.05.2021. – 28 с.
14. Кузнєцов М. Ю., Шумська А. А. Теорія ймовірностей та математична статистика. Методичні вказівки до розв'язання задач. Гриф надано Методичною радою КПІ ім. Ігоря Сікорського, прот. № 7 від 13.05.2021. – 64 с.

Розділи II, III.

Основна література:

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ/ Грайворонський М. В., Новіков О. М. – К.: Видавнича група BHV, 2009. – 608 с.
2. Богуш В. М. Інформаційна безпека від А до Я / Богуш В. М., Кудін А. М. – К.: МОУ, 1999. – 456 с.
3. Шеховцов В. А. Операційні системи – К.: Видавнича група BHV, 2005. – 576 с.

4. Буров Є. В. Комп’ютерні мережі / 2-е вид., оновл. і доп. – Львів: Бак, 2003.
5. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л. О., Савчук М. М. – К.:КПІ ім. Ігоря Сікорського, 2008. – 128 с.
6. Вербіцький О. В. Вступ до криптології. – Львів: в-во «Науково-технічна література», 1998. – 248 с.
7. Пасічник В. В. Організація баз даних та знань: підручник для ВНЗ / В. В. Пасічник, В. А. Резніченко. – К.: Видавнича група BHV, 2006. – 384с.
8. Антонюк А. О. Основи захисту інформації в автоматизованих системах: Навч. посіб. – К: Видавничий дім «КМ Академія», 2003. – 243 с.

Додаткова література:

1. Закон України "Про захист персональних даних".
2. Закон України “Про інформацію”.
3. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”.
4. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 № 1126.
5. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
6. Постанова Кабінету Міністрів України від 29.03.06 № 373 "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".
7. Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 № 93, зареєстровано в Міністерстві юстиції України 16.07.07 за № 820/14087.
8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
11. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
12. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
13. НД ТЗІ 2.5-010-2003 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу.
14. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах

15. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
16. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною № 1, затвердженою наказом ДСТСЗІ СБ України 18.06.02 № 37).
17. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
18. Архипов О. Є. Захист інформації в телекомунікаційних мережах та системах зв'язку: навч.-метод. посібник / Архипов О. Є., Луценко В. М, Худяков В. О. – К.: ІВЦ "Видавництво "Політехніка", 2003. – 40 с.
19. Вінницький И. П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В. П. Вінницький, В. Г. Поліщук. – К.: ІВЦ “Видавництво «Політехніка»”, 2004. – 436 с.
20. Khan S. A., Kumar R., Khan R. A. Software Security: Concepts & Practices. 2023 – 330 c.
21. Sirapat Boonkrong, Nakhon Ratchasima. Authentication and Access Control. Practical Cryptography Methods and Tools. – 242 p.
22. Alexey Kleymenov Amr Thabet. Mastering Malware Analysis – 573 p.
23. Threat Modeling A Practical Guide for Development TeamsYvonne Wilson Abhishek Hingnikar. Solving Identity Management in Modern Applications. – 398 p.
24. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications – 330 p.
25. Організація комп’ютерних мереж [Електронний ресурс]: підручник: для спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки»/ Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7Мбайт). – К.: КПІ ім. Ігоря Сікорського, 2018. – 259 с.
26. Tanenbaum, Andrew S., Computer networks / Andrew S. Tanenbaum, David J. Wetherall. – 5th ed. – Pearson Education, Inc., 2011. – 816 p. – ISBN-13: 978-0-13-212695-3.
27. Kurose, James F., Computer Networking: A Top-Down Approach / James F. Kurose, Keith W. Ross. – 7th ed. – Pearson Education, Inc., 2017. – 864 p. – ISBN-13: 978-0-13-359414-0.
28. Windows Internals, Seventh Edition, Part 1: System architecture, processes, threads, memory management, and more by Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, and David A. Solomon. – Microsoft Press, 2017. – ISBN: 978-0-7356-8418-8.
29. Windows Internals, Seventh Edition, Part 2 by Andrea Allievi, Alex Ionescu, Mark E. Russinovich, and David A. Solomon. – Microsoft Press, 2021. – ISBN: 978-0-13-546240-9.
30. Andrew S. Tanenbaum, Herbert Bos, Modern Operating Systems, 5th edition. – Pearson, 2022 – ISBN-13: 9780137618873.

ПРИКЛАД ЕКЗАМЕНАЦІЙНОГО БІЛЕТУ

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий фізико-технічний інститут

Фаховий іспит

Ступінь вищої освіти магістр
(назва)

Спеціальність F5 Кібербезпека та захист інформації
(код і назва спеціальності)

Освітня програма Системи, технології та математичні методи кібербезпеки
(назва)

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 999

1. Теорема Чебишева про закон великих чисел. Інтегральна гранична теорема Муавра-Лапласа.
2. Процеси і потоки: визначення, моделі, схеми багатопотоковості, опис процесів і потоків у системі. Приклади реалізації у різних ОС (Linux, Windows).
3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ).
4. Задача:

Нехай в моделі MLS решітка рівнів таємності (L<=M<=H) та множина тематик (A,B,C).
Відобразіть графічно співвідношення між елементами LAB, LBC, MA, MAC, HA, HAC.
Вкажіть найменшу верхню та найбільшу нижню границі для даного набору елементів.

РОЗРОБНИКИ ПРОГРАМИ

д. т. н., проф. каф. ІБ _____ Дмитро ЛАНДЕ

к. ф.-м. н., доц. каф. ІБ _____ Сергій СМИРНОВ

.

к. т. н., доц. каф. ІБ _____ Володимир ДЕМЧИНСЬКИЙ

к. т. н., доц. каф. ІБ _____ Ірина СТЬОПОЧКІНА

к. ф.-м. н., доц. каф. ММЗІ _____ Ганна ЮЖАКОВА

к. т. н., доц. каф. ІБ _____ Михайло КОЛОМИЦЕВ

к. т. н. каф. ММЗІ _____ Сергій ЯКОВЛЄВ

РЕКОМЕНДОВАНО
кафедрою інформаційної безпеки.
Протокол № 3/2025 від 18 лютого 2025 р.

Завідувач кафедри ІБ _____ Дмитро ЛАНДЕ