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

ЗАТВЕРДЖЕНО
Вченою радою
Фізико-технічного інституту
Протокол № ___ від ____ лютого 2018 р.

Голова вченої ради _____ О.М.Новіков

М.П.

# ПРОГРАМА

додаткового вступного випробування
для вступу на програму підготовки магістра
*за спеціальністю 125 Кібербезпека*

Програму рекомендовано кафедрами

*Інформаційної безпеки*
Протокол № ___ від ___ _____ 2018 р.

в.о. завідувача кафедри _____М.В.Грайворонський

*Фізико-технічних засобів захисту інформації*
Протокол № ___ від ___ _____ 2018 р.

завідувач кафедри _____Є.А.Мачуський

Київ – 2018

## ВСТУП

Програма додаткового вступного випробування для вступу на освітньо-професійну програму підготовки магістра за спеціальністю 125 Кібербезпека (для вступників, що мають диплом бакалавра інших напрямів підготовки) складена на основі освітньо-професійних програм напрямів підготовки 6.170101 “Безпека інформаційних і комунікаційних систем” і 6.170102 “Системи технічного захисту інформації”.

Програма розроблена згідно з навчальними програмами нормативних навчальних дисциплін.

Додаткове вступне випробування здійснюється в письмовій формі. Кожний білет містить три завдання:

1. Питання з математики (теорія).
2. Питання з дисциплін професійної та практичної підготовки (теорія).
3. Задача з математики.

Тривалість додаткового вступного випробування – 1,5 астрономічні години, перерви немає.

## ОСНОВНИЙ ВИКЛАД

### Розділ «ВИЩА МАТЕМАТИКА, ТЕОРІЯ ЙМОВІРНОСТЕЙ ТА МАТЕМАТИЧНА СТАТИСТИКА»

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 – Ляйбниця. 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. Ряд Фур'є періодичної функції. Дійсна та комплексна форма ряду Фур'є. Інтеграл та перетворення Фур'є.
17. Диференційовність функції декількох змінних. Часткові похідні та диференціал. Вигляд диференціалу $n$-го порядку для функції декілької змінних.
18. Локальні та глобальні екстремуми функції декількох змінних. Алгоритм їх відшукання.
19. Кратні інтеграли. Теорема Фубіні (Зведення кратних інтегралів до повторних). Заміна змінних у кратному інтегралі.
20. Криволінійні та поверхневі інтеграли 1-го і 2-го роду: означення і властивості, способи обчислення.
21. Основні інтегральні формули аналізу (Ґріна на площині, Остроградського – Ґаусса та Стокса у просторі).
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, ґауссовий). Їх числові характеристики – математичне очікування, дисперсия, моменти.
24. Теорема Чебишева про закон великих чисел. Інтегральна гранична теорема Муавра-Лапласа.
25. Інтервальне оцінювання. Оцінка середнього та дисперсії ґауссового розподілу.

Розділ «ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ ТА ПРАКТИЧНОЇ ПІДГОТОВКИ»

1. Операційні системи – визначення, основні компоненти, особливості функціонування. Класифікація за призначенням і приклади сучасних ОС кожного типу. Вимоги до сучасних ОС.
2. Відкриті системи. Джерела стандартів. Модель взаємодії відкритих систем. Завдання кожного з рівнів.
3. Стек протоколів TCP/IP. Протокол IP. Адресація. Протоколи UDP і TCP.
4. Зловмисне програмне забезпечення — вірус, черв'як, троянський кінь. Класифікація, методи розповсюдження. Методи виявлення і протидії.

5. Методики захисту мереж: Міжмережне екранування (firewalling), Віртуальні приватні мережі (VPN).
6. Несанкціонований доступ (НСД) до інформації. Способи та види НСД. Види технічних каналів витоку інформації.
7. Джерела загроз, модель загроз, модель порушника. Категорії порушників.
8. Політика безпеки (ПБ) інформації. Види ПБ. Призначення і основні складові політики безпеки.
9. Ідентифікація та автентифікація (ІА). Методи ІА.
10. Система нормативних документів України із захисту інформації.
11. Класифікація інформації за режимом доступу та за правовим режимом. Види інформації, захист якої гарантується державою.
12. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Види критеріїв, їх призначення. Рівні оцінок за критеріями.
13. Міжнародний стандарт з оцінки безпеки інформаційних технологій ISO/IEC 15408 (Common Criteria).
14. Система міжнародних стандартів ISO 27000. Перелік основних стандартів, сфера застосування.
15. Класи і категорії автоматизованих інформаційних систем. Стандартні функціональні профілі захищеності інформації, що обробляється, від несанкціонованого доступу.
16. Етапи побудови комплексної системи захисту інформації (КСЗІ). Зміст робот, що виконуються на окремих етапах. Документи, що розробляються для кожного етапу створення КСЗІ.
17. Оцінка ризиків порушення інформаційної безпеки. Методи, рекомендації, стандарти.
18. Основні теоретичні моделі інформаційної безпеки. Моделі керування доступом.
19. Основні поняття криптології. Теорія зв'язку в секретних системах Шеннона.
20. Узагальнені методи контурних струмів та вузлових напруг.
21. Частотні характеристики коливальних контурів (послідовного, паралельного, зв'язаних).
22. Спектральний аналіз і синтез сигналів. Перетворення Фур'є. Спектри періодичних сигналів. Спектральне представлення неперіодичних сигналів. Теореми про спектри (основні властивості перетворення Фур'є).
23. Кореляційний аналіз сигналів. Автокореляційна функція (АКФ). Взаємокореляційна функція (ВКФ). Зв'язок між енергетичним спектром і АКФ сигналу.
24. Основні об'єкти захисту інформації. Перелік та визначення.
25. Основні методи та засоби захисту об'єктів інформаційної діяльності від витоку інформації каналами побічного електронного випромінювання та наведення.

## ПРИКІНЦЕВІ ПОЛОЖЕННЯ

### ВИКОРИСТАННЯ ДОПОМІЖНОГО МАТЕРІАЛУ

Під час відповідей на теоретичні питання користуватися додатковою 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

додаткового вступного випробування для вступу
на програму підготовки магістра за спеціальністю 125 Кібербезпека

Відповідь на перше і друге (теоретичні) питання комплексного фахового випробування оцінюється за бальною шкалою за таким порядком визначення (максимальний ваговий бал 33):

- 32-33 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 28-31 – повна відповідь (містить не менше 85% потрібної інформації);
- 25-27 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 22-24 – задовільна відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 20-21 – неповна, неточна, але мінімально достатня відповідь (містить не менше 60% потрібної інформації);
- 1-19 – незадовільна відповідь;
- 0 — відсутність відповіді.

Система оцінювання задачі (максимальний ваговий бал 34):

- 33…34 – повне, безпомилкове, відмінне розв’язання завдання, обсяг виконання 95-100%;
- 30…32 – повне розв’язання завдання з несуттєвими похибками, містить не менше 85% потрібної інформації;
- 27…29 – розв’язання завдання з похибками, містить не менше 75% потрібної інформації;
- 26…29 – завдання виконане задовільно, з невеликими помилками, містить не менше 65% потрібної інформації;
- 24…25 – завдання виконане задовільно, з помилками, містить не менше 60% потрібної інформації;
- 1-24 – завдання не виконано;
- 0 — спроби розв’язання задачі відсутні.

Кінцева кількість балів – проста арифметична сума балів, отриманих за відповіді на кожне з трьох вищезазначених завдань. Максимальна кількість балів – 100.

Переведення значення бальної шкали в екзаменаційну оцінку здійснюється за такою системою співвідношення згідно критеріїв ECTS:

| Сумарна кількість балів | Оцінка |
|---|---|
| 95…100 | **Відмінно** |
| 85…94 | **Дуже добре** |
| 75…84 | **Добре** |
| 65…74 | **Задовільно** |
| 60…64 | **Достатньо** |
| Менше 60 | **Незадовільно** |

## СПИСОК ЛІТЕРАТУРИ

Розділ “ВИЩА МАТЕМАТИКА”


1. В.А. Ильин, Э.Г. Позняк. Аналитическая геометрия. М.: Наука, 1988.
2. В.А. Ильин, Э.Г. Позняк. Линейная алгебра. М.: Наука, 1974.
3. А.Г. Курош. Курс высшей алгебры. М.: Наука, 1975.
4. Г.М. Фихтенгольц. Курс дифференциального и интегрального исчисления. Т. 1,2,3. М., «Наука», 1966.
5. В.А. Ильин, Э.Г. Позняк. Основы математического анализа. Ч. 1,2. М. «Наука», 1980.
6. Г.Е. Шилов. Математический анализ. М., «Наука», 1970.
7. Дубовик В.П., Юрик І.І. Вища математика. Навч. посібник. К.: Вища школа. – 1993. – 648 с.
8. В.П. Чистяков. Курс теории вероятностей. М.: Наука, 1978.
9. Е.С. Вентцель, Л.А. Овчаров. Теория вероятностей и ее инженерные приложения. М.: Наука, 1988.
10. Б.В. Гнеденко. Курс теории вероятностей. М.: Наука, 1988.
11. А.Д. Вентцель. Курс теории случайных процес сов. М.: Наука, 1975.
12. Г.И. Ивченко, Ю.И. Медведев. Математическая статистика. М.: Высшая школа, 1984.


Розділ “ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ ТА ПРАКТИЧНОЇ ПІДГОТОВКИ”


1. Таненбаум Э. Архитектура компьютера. 5-е изд. – СПб.: Питер, 2007. – 844 с.
2. Шеховцов В. А. Операційні системи – К.: Видавнича група BHV, 2005. – 576 с.
3. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. – СПб.: Питер, 2015. – 1120 с.
4. Дейт, К., Дж. Введение в системы баз данных. 6-е изд. – К.; М., СПб.: «Вильямс», 2000. – 848 с.
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.
7. Багатоканальний електрозв’язок та телекомунікаційні технології / За редакцією Поповського В.В. – Харків: “Компанія СМІТ”, 2003. – 512 с.

8. Цифровые и аналоговые системы передачи / Под ред. В. И. Иванова. – М.: Горячая линия – Телеком, 2003. – 232 с.
9. Айри Пол. Объектно-ориентированное программирование с использованием C++. – К.: НИПФ “ДиаСофт Лтд.”, 1999.
10. Ховард М., Лебланк Д. Защищенный код. – М: «Русская редакция», 2003. – 704 с.
11. Казарин О.В. Теория и практика защиты программ. – М.: 2004. – 450 с.
12. М. В. Грайворонський, О.М. Новіков. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
13. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М. Изд. центр “Академия”, 2005 – 144 с.
14. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. – Екатеринбург: 2008. – 212 с.
15. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001.
16. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998
17. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
18. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
19. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
20. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
21. 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»
22. Диффи У., Хеллман М. Защищенность и имитостойкость. / ТИИЭР. – 1979. – Т.67, №3.
23. Месси Дж.Л. Введение в современную криптологию. / ТИИЭР. – 1988. – Т.76, №5.
24. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003.
25. Симмонс Г.Дж. Обзор методов аутентификации информации. ТИИЭР. – 1988. – Т.76, №5.
26. Бакалов В.П. Основы теории цепей / Бакалов В.П., Дмитриков В.Ф., Крук Б.И. – М.: Радио и связь, 2000. – 592 с.: ил.
27. Нефедов В.И. Основы радиоэлектроники и связи: Учебник для вузов / Нефедов В.И. – М.: Высшая школа, 2005. – 510с.
28. 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.

## РОЗРОБНИКИ ПРОГРАМИ

_____ д.т.н. професор Архипов О. Є.

_____ к.ф.-м.н. доцент Грайворонський М. В.

_____ к.т.н. доцент Демчинський В. В.

_____ к.ф.-м.н. доцент Южакова Г. О.

_____ к.т.н. доцент Коломицев М. В.

_____ к.т.н. ст. викладач Яковлев С.В.

_____ к.т.н. доцент Прогонов Д.О.