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

ЗАТВЕРДЖУЮ
Голова Атестаційної комісії
Фізико-технічного інституту
Директор _____ Олексій НОВІКОВ
« 12 » « 02 » 2021 р.
М.П.

ПРОГРАМА

комплексного фахового випробування

для вступу на освітні програми підготовки магістра
«Системи, технології та математичні методи кібербезпеки»
за спеціальністю 125 Кібербезпека

Програму рекомендовано:
кафедрою інформаційної безпеки
Протокол № 2/2021 від « 10 » « 02 » 2021 р.
В.о. завідувача кафедри _____ Микола ГРАЙВОРОНСЬКИЙ

Київ – 2021

ВСТУП

Програма комплексного фахового випробування для вступу на освітню програму підготовки магістра “Системи, технології та математичні методи кібербезпеки” за спеціальністю 125 Кібербезпека складена на основі відповідної бакалаврської освітньої програми.

Програма побудована з наступних розділів: загальна (спільна) частина, та варіативні частини, які забезпечують можливість вибору для вступників відповідно до обраних ними індивідуальних траєкторій навчання.

Програма розроблена згідно з навчальними програмами навчальних дисциплін:

– «Вища математика»,
– «Теорія ймовірностей та математична статистика»,
– «Операційні системи»,
– «Комп’ютерні мережі»,
– «Бази даних та інформаційні системи»,
– «Теоретичні основи захисту інформації»,
– «Системи та технології кібернетичної безпеки»,
– «Безпека операційних систем та комп’ютерних мереж»,
– «Криптографія»,
– «КСЗІ: створення, впровадження, супровід»,
– «Безпека інтернет-ресурсів»,
– «Теорія безпеки та конкурентна розвідка»,
– «Моделі та методи прийняття рішень».

Комплексне фахове випробування здійснюється в письмовій формі. Білет містить п’ять завдань:

1. Питання з математики (теорія).
2. Питання з дисциплін професійної та практичної підготовки (теорія).
3. Задача з дисциплін професійної та практичної підготовки.
4. Питання з дисциплін професійної та практичної підготовки (теорія, варіативна частина).
5. Питання з дисциплін професійної та практичної підготовки (теорія, варіативна частина).

Абітурієнт обирає для відповіді чотири завдання (два теоретичні та задачу із загальної частини, і одне з двох теоретичних питань з варіативної частини).

Тривалість комплексного фахового випробування – 2 астрономічні години, перерви немає. Екзаменований вільно розподіляє свій час між всіма завданнями.

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 — ЗАГАЛЬНА ЧАСТИНА»

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. Модель взаємодії відкритих систем. Завдання кожного з рівнів.
20. Логічна структуризація мереж. Віртуальні локальні мережі. Алгоритм прозорого мосту. Алгоритм і протокол STP.
21. Маршрутизація – завдання, принципи, протоколи.
22. Стек протоколів TCP/IP. Протокол IP. Адресація. Протоколи UDP і TCP.
23. Реляційна модель даних (РМД). Структуризація даних в РМД. Обмеження цілісності. Функціональні залежності в РМД. Декомпозиція відносин за функціональними залежностями.
24. Транзакція як механізм забезпечення несуперечності даних. Властивості транзакції.
25. Захист даних в БД від несанкціонованого доступу. Основні механізмі захисту в БД: автентифікація, керування доступом, реєстрація і аудит.
26. Основні види вразливостей програмного забезпечення. Вразливості веб-застосунків. Міжнародні класифікатори вразливостей.
27. Модель загроз програмного забезпечення. Етапи побудови моделі. Класифікація загроз за методикою STRIDE. Оцінка ризиків за методикою DREAD. Моделювання загроз за допомогою дерева атаки.
28. Структура файлів що виконуються. Особливості ураження файлів, що виконуються комп’ютерним вірусом. Типи комп’ютерних вірусів. Особливості поліморфних вірусів.

29. Зловмисне програмне забезпечення типу комп’ютерний черв'як і троянський кінь: структура, методи розповсюдження. Методи виявлення.
30. Програмно-апаратні засоби захисту прикладних програм від несанкціонованого використання. Методи захисту програмного забезпечення від зворотного аналізу.
31. Дискреційні моделі керування доступом. Модель HRU. Властивості моделі та теореми розв'язності задачі безпеки. Модель TAM та її властивості.
32. Модель Take-Grant. Формалізація санкціонованого отримання прав доступу та крадіжки прав доступу. Розширена модель Take-Grant. Правила де-юре та де-факто.
33. Моделі тематичного керування доступом. Модель решітки цінностей. Решітка MLS.
34. Моделі мандатного керування доступом. Властивості мандатного керування доступом. Модель Белла-ла-Падули. Основна теорема безпеки.
35. Проблеми мандатного керування доступом. Розвиток моделі Белла-лаПадули: Z-система Мак-Ліна, модель Low-Watermark.
36. Рольові моделі керування доступом.
37. Моделі забезпечення цілісності даних (Біба, Кларка-Вілсона та похідні моделі).

Розділ «ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ ТА ПРАКТИЧНОЇ ПІДГОТОВКИ — ВАРІАТИВНА ЧАСТИНА — СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ»

1. Стандарт ISO 15408 (Common Criteria).
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ).
3. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки. Вразливості протоколів Інтернету — IP, TCP, ICMP, і атаки на ці протоколи.
4. Система DNS, вразливості і можливі атаки. Методи захисту.
5. Приклади атак на IAAA в веб-застосунках. Методи та технології унеможливлення.
6. Вразливості механізмів керування сесіями в веб-застосунках та їх експлуатація.
7. DoS/DDoS атаки на веб-застосунки. Temporal та pers). is). tent DoS. Об'єкти атаки на відмову в обслуговуванні.
8. Типи та приклади SQL-ін'єкцій. Можливості атакуючих щодо взаємодії з операційними системами через SQL-ін'єкції.
9. Причини та механізми експлуатації XML-ін'єкцій. Типи XML-парсерів.
10. Вразливості веб-серверів.
11. Міжмережне екранування (firewalling) як метод захисту комп’ютерних) як метод захисту комп’ютерних мереж. Класифікація і можливості міжмережних екранів.

12. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Основні протоколи.
13. Засоби IPSec: призначення, архітектура засобів, основні протоколи, формати мережних пакетів. Транспортний і тунельний режими.
14. Засоби VPN віддаленого доступу. Призначення, вимоги. Порівняння SSL/TLS і SSH.
15. Модель загроз для операційної системи. Типова архітектура комплексу засобів захисту операційних систем.
16. Склад і архітектура засобів захисту ОС Windows). .
17. Реалізація дискреційного і мандатного керування доступом в ОС Windows).
18. Склад і архітектура засобів захисту ОС Linux.
19. Реалізація дискреційного і мандатного керування доступом в ОС Linux.

Розділ «ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ ТА ПРАКТИЧНОЇ ПІДГОТОВКИ — ВАРІАТИВНА ЧАСТИНА — МАТЕМАТИЧНІ МЕТОДИ КІБЕРБЕЗПЕКИ»

1. Поняття «безпека», «загроза» та «ризик» як системоутворюючі категорії загальної теорії безпеки
2. Безпека як властивість складних систем
3. Методи побудови F/N-діаграм
4. Загальносистемні закони безпеки складних систем
5. Гомеостазис як модель оцінки стану захищеності складних систем
6. Аналітична процедура моніторингу конкурентної розвідки: аналіз *Z*-діаграм. Кількісна оцінка конкурентного середовища за допомогою *M*-діаграм («павук»-діаграми)
7. Google-аналітика як засадничий метод дослідження конкурентної розвідки
8. Невизначеність та ризик
9. Оцінка індивідуальних ризиків
10. Оцінка колективних ризиків
11. Матриця прогнозованого ризику: застосування та методи побудови
12. Управління ризиком: концепція «прийнятного ризику»
13. Стратегія оцінки ризикованих альтернатив
14. Багатокритеріальні рішення. Метод лінійної згортки. Домінування за Парето,
    множина Парето її властивості та побудова.
15. Функції вибору (ФВ) та БВ. Механізми вибору за блокуванням та домінуванням, скалярний та сукупно-екстремальний, мажорітарний та лексікографічний, відповідні функції вибору.
16. Нормальні ФВ. Теорема о непорожності нормального вибору. Структура нормального вибору, число НФВ.
17. Колективні рішення, вибір за більшістю. Парадокс Кондорсе і метод Борда. Аксіоми Ерроу, теорема неможливості і правило диктатора.

18. Правила вибору, змістовні за Кондорсе: Копленда, Сімпсона, Шульце. Утилітаризм та егалітаризм, колективні функції корисності.
19. Функції корисності (ФК) в задачах вибору. Задачі з урнами. Згортання дерева рішень.
20. Криві та мапи байдужості, локальні коефіцієнти заміщення (ЛКЗ). Побудова ФК та прийняття рішення за ЛКЗ.

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
комплексного фахового випробування
для вступу на освітню програму підготовки магістра
«Системи, технології та математичні методи кібербезпеки»
за спеціальністю 125 Кібербезпека

Вступник дає відповіді на питання з математики, два теоретичних питання з дисциплін професійної та практичної підготовки, і розв’язує одну задачу. Відповідь на кожне з теоретичних питань комплексного фахового випробування оцінюється за бальною шкалою 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);
- менше 15 – незадовільна відповідь.

Система оцінювання практичного запитання (задачі):

- 24…25 – повне (обсяг виконання 95-100%), безпомилкове, відмінне розв’язання завдання;
- 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;
- менше 15 – завдання не виконано.

Кінцева кількість балів – сума балів, отриманих за відповіді на кожне з трьох вищезазначених питань. Максимальна кількість балів – 100. Мінімальна кількість балів, що дає право продовжувати участь у конкурсному відборі – 60.

Отримана оцінка перераховується в оцінку за 200-бальною шкалою (100...200) згідно таблиці відповідності.

Таблиця відповідності оцінок рейтингової системи оцінювання (РСО, 60...100) балам 200-бальної шкали (100...200)

Оцінка РСО	Бали 100...200	Оцінка РСО	Бали 100...200	Оцінка РСО	Бали 100...200	Оцінка РСО	Бали 100...200
60	100,0	70	125,0	80	150,0	90	175,0
61	102,5	71	127,5	81	152,5	91	177,5
62	105,0	72	130,0	82	155,0	92	180,0
63	107,5	73	132,5	83	157,5	93	182,5
64	110,0	74	135,0	84	160,0	94	185,0
65	112,5	75	137,5	85	162,5	95	187,5
66	115,0	76	140,0	86	165,0	96	190,0
67	117,5	77	142,5	87	167,5	97	192,5
68	120,0	78	145,0	88	170,0	98	195,0
69	122,5	79	147,5	89	172,5	99	197,5
						100	200,0

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

СПИСОК ЛІТЕРАТУРИ

Розділ “ВИЩА МАТЕМАТИКА”

1. В. А. Ильин, Э. Г. Позняк. Аналитическая геометрия. – М.: из-во “Наука”, 1988.
2. В. А. Ильин, Э. Г. Позняк. Линейная алгебра. – М.: из-во “Наука”, 1974.
3. А. Г. Курош. Курс высшей алгебры. – М.: из-во “Наука”, 1975.
4. Г. М. Фихтенгольц. Курс дифференциального и интегрального

исчисления. Т. 1,2,3. – М.: из-во “Наука”, 1966.
5. В. А. Ильин, Э. Г. Позняк. Основы математического анализа. Ч. 1,2. – М.: из-во “Наука”, 1980.
6. Г. Е. Шилов. Математический анализ. – М.: из-во “Наука”, 1970.
7. Дубовик В. П., Юрик І. І. Вища математика / Навч. посібник. – К.: ви-во «Вища
Школа». – 1993. – 648 с.
8. В. П. Чистяков. Курс теории вероятностей. – М.: из-во “Наука”, 1978.
9. Е. С. Вентцель, Л. А. Овчаров. Теория вероятностей и ее инженерные приложения. – М.: из-во “Наука”, 1988.
10. Б. В. Гнеденко. Курс теории вероятностей. – М.: из-во “Наука”, 1988.
11. А. Д. Вентцель. Курс теории случайных процессов. – М.: из-во “Наука”, 1975.
12. Г. И. Ивченко, Ю. И. Медведев. Математическая статистика. – М.: Высшая школа, 1984.

Розділ “ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ ТА ПРАКТИЧНОЇ ПІДГОТОВКИ”

Основна література:

1. Таненбаум Э. Архитектура компьютера. – 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. – СПб.: Питер, 2015. – 1120 с.
4. Руссинович М., Соломон Д. Внутреннее устройство Microso Windows. – СПб.:
Питер, 2013. – 800 с.
5. Дейт, К., Дж. Введение в системы баз данных. 6-е изд. – К- М-СПб.: «Вильямс», 2000. – 848 с.
6. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2012. – 960 с.
7. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.
8. Ховард М., Лебланк Д. Защищенный код. – М: «Русская редакция», 2003. – 704 с.
9. Казарин О. В. Теория и практика защиты программ. – М.: 2004. – 450 с.
10. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комуніка-ційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
11. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М. Изд. центр “Академия”, 2005 – 144 с.
12. Гайдамакин Н. А. Теоретические основы компьютерной безопасности / Учебное пособие. – Екатеринбург: 2008. – 212 с.
13. Математичні методи захисту інформації. Курс лекцій. Ч І / Укладачі Завадська Л. О., Савчук М. М. – К.: НТУУ «КПІ», 2008. – 128 с.
14. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – М.: Гелиос АРВ, 2001.

15. Вербіцький О. В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Издательство ТРИУМФ, 2003. – 816 с.
17. Menezes A., P. van Oorschot, S.Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.
18. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
19. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
20. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
21. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
22. 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

Додаткова література:

1. Юров В. Assembler. Учебник для вузов. – СПб.: Питер, 2003. – 637 с.
2. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2001. – 544с.
3. Дж. Рихтер. Windows для профессионалов. Создание эффективных WIN32-приложений с учетом специфики 64-разрядной версии Windows. – СПб.: Питер, Русская Редакция, 2001. – 752 с.
4. Ульман Дж. Основы систем БД. Пер с англ. – М.: Финансы и статистика,1983. – 334 с.
5. Карпова Т. Базы данных. Модели, разработка, реализация. – СПб.: Питер, 2001. – 304 с.
6. Джен Л. Харрингтон. Проектирование реляционных баз данных. − М.: Издательство «Лори», 2006. − 230 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. Шиндер Д.Л. Основы компьютерных сетей. – М.: Издательский дом «Вильямс», 2002. – 656 с.
9. Амато В. Основы организации сетей Cis). co, т.2. – М.: Издательский дом «Вильямс», 2002. – 464 с.
10. Куроуз Дж., Росс К. Компьютерные сети. 2-е изд. – СПб.: Питер, 2004. – 765 с.
11. Вінницький И. П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В. П. Вінницький, В. Г. Поліщук. – К.: ІВЦ "Видавництво «Політехніка»", 2004. – 436 с.

12. Макавеева М. М., Шинаков Ю. С. Системы связи с подвижными объектами. –
М.: Радио и связь, 2002. – 440 с.
13. Телекоммуникационные системы и сети, т. 1 / Б. И. Крук, В. И. Попан-
тонопуло, В. П. Шувалов и др. – М.: Горячая линия-Телеком, 2003. – 647 с.
14. Защита программного обеспечения. Пер, с англ. Д. Гроувер, Р. Сатер,
Дж. Фипс и др. Под редакцией Д. Гроувера – М.: Мир, 1992. – 285 с.
15. Хогланд Г., Мак-Гроу Г. Взлом программного обеспечения: анализ и
использование кода. – М: «Вильямс», 2005. – 384 с.
16. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения. –
СПб.: БХВ-Петербург, 2005. – 432 с.
17. Антонюк А. О. Основи захисту інформації в автоматизованих системах:
Навч. посіб. – К: Видавничий дім «КМ Академія», 2003. – 243 с.
18. Теоретические основы компьютерной безопасности / П. Н. Девянин и
др. – М.: Радио и связь, 2000. – 192 с.
19. Кузьмін Н. В., Кедрус В. А. Основы теории информации и кодирования. –
К.:
ви-во “Вища школа”, 1977.
20. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих
ошибки.
– М. “Связь”, 1979.
21. Диффи У., Хеллман М. Защищенность и имитостойкость // ТИИЭР. – 1979.
–
Т.67. – №3.
22. Месси Дж.Л. Введение в современную криптологию // ТИИЭР. – 1988. –
Т.76. – №5.
23. Фомичев В. М. Дискретная математика и криптология. – М.: ДИАЛОГ-
МИФИ, 2003.
24. Симмонс Г. Дж. Обзор методов аутентификации информации // ТИИЭР. –
1988. – Т.76, №5.

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.т.н. доцент Барановський О. М.
_____ к.ф.-м.н. доцент Южакова Г. О.
_____ к.т.н. доцент Коломицев М. В.

_____ к.т.н. доцент Яковлєв С. В.