

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»



ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

Євген СОКОЛ

« 29 » квітня 2022 р.

ПРОГРАМА

вступного випробування зі спеціальності

125 “Кібербезпека”

(шифр та назва спеціальності)

на навчання для здобуття ступеня доктора філософії
за освітньо-науковою програмою

Кібербезпека

(назва ОНП)

Схвалено вченою радою інституту

Комп’ютерних наук та інформаційних технологій

протокол № 3 від « 22 » квітня 2022 р.

Директор  Михайло ГОДЛЕВСЬКИЙ

Харків 2022

АНОТАЦІЯ

Програма складена відповідно до вимог Міністерства освіти і науки України, закону України від 06 вересня 2014 р. «Про вищу освіту», постанови КМ України від 23 березня 2016 р. № 261 «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)» зі змінами та наказу Міністерства освіти і науки України від 13.10.2021 р. № 1098 «Умови прийому на навчання для здобуття вищої освіти в 2022 році», Положення про підготовку здобувачів вищої освіти ступеня доктора філософії в аспірантурі, правил прийому до аспірантури Національного технічного університету «Харківський політехнічний інститут» наказ № 31 ОД від 21 січня 2022 року.

Метою вступного випробування є комплексна перевірка знань вступників, які вони отримали у результаті вивчення циклу дисциплін, передбачених освітньо-професійною програмою та навчальними планами в обсязі програми вищої освіти магістра зі спеціальності “Кібербезпека”. Вступник повинен продемонструвати фундаментальні та професійно-орієнтовані уміння і знання щодо узагальненого об’єкта дослідження, а також здатність вирішувати типові професійні завдання відповідного рівня.

ЗМІСТ ПРОГРАМИ

Тема “СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ”

1.1 Основи теорії чисел. Поняття подільності чисел. Ділення із залишком. НСД двох чисел. Знаходження НСД двох чисел. Спільне найменше кратне. Прості числа. Великі прості числа. Методи побудови “великих” простих чисел. Псевдопрості числа, головні методи їх побудови. Функція Ейлера. Узагальнена функція Ейлера. Визначення та головні властивості.

1.2 Основи теорії груп, кілець та полів. Групи, головні поняття та визначення. Мультиплікативні групи. Підстановки. Групи підстановок. Підгрупи. Кільця, визначення та властивості. Кільце з одиницею. Ізоморфні кільця. Поля, визначення та властивості. Прості та поширені поля. Еліптичні криві, визначення та властивості.

1.3 Теорія ймовірності та математична статистика. Дискретно-ймовірнісний простір. Події та ймовірності, їх визначення та властивості. Приклади розподілів. Випадкові величини. Мат. очікування. Незалежні випадкові величини. Основні поняття мат. статистики. Закони розподілу ймовірностей. Біноміальний, показовий, рівномірний та нормальний розподіл. Перевірка статистичних гіпотез. Схема іспитів Бернуллі, критерій знаків для однієї вибірки. Критерій згоди Колмогорова, χ^2 – квадрат Пірсона.

1.4 Спеціальний розділ теорії інформації. Умовна та безумовна ентропія. Умовна апостеріорна ентропія. Середня взаємна інформація. Блокові та неблокові коди. Норми, метрики та кодові відстані. Лінійні коди, згорткові коди, збиткові коди. Псевдовипадкові послідовності. Лінійні та нелінійні рекурентні послідовності, їх властивості.

1.5 Алгоритмічні основи криптографії. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності. Методи побудування “великих” простих чисел та незвідних поліномів, складність та реалізація алгоритмів. Афінний та проєктивний базиси скалярного множення в групі точок еліптичних кривих. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих. Методи розв’язку дискретних логарифмічних рівнянь в групі точок еліптичних кривих та порівняльна оцінка їх складності

Рекомендована література:

1. Кузнецов О.О., Євсєєв С.П., Кавун С.В., та Король О.Г. Сигнали і коди. Алгебраїчні методи синтезу. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.
2. Кузнецов О.О., Євсєєв С.П., та Кавун С.В. Захист інформації та економічна безпека підприємства. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.
3. Теорія інформації: підручник для слухачів, курсантів та студентів вищих навчальних закладів / І.В. Рубан, С.І. Хмелевський, О.В. Сєверінов та ін. – Харків: ХНУПС, 2018. – 276 с.

4. Кузнецов О.О., Євсєєв С.П., Король О.Г. Захист інформації в ІС. Харків: Вид. ХНЕУ, 2011. –510 с.

Тема “МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ. КРИПТОГРАФІЧНІ СИСТЕМИ”

2.1 Основи теорії захисту інформації. Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу. Концепція захищеної комп'ютерної системи (мережі). Політики безпеки інформації та їх впровадження.

2.1.2. Основні функції криптографічних систем. Криптографія та криптографічний аналіз. Класифікація криптографічних систем по стійкості. Теоретично недешифруємі системи й умови їх реалізації. Обчислювально-стійкі та доказово стійкі системи й умови їхньої реалізації. Інформаційні характеристики джерел повідомлень, криптограм і ключів. Класифікація шифрів. Симетричні та несиметричні алгоритми шифрування. Блокові та потокові алгоритми шифрування, та їх властивості. Генератори псевдовипадкових послідовностей. Несиметричні алгоритми шифрування та їх властивості. Умови реалізації та галузі застосування систем шифрування. Автентифікація. Погрози порушення автентичності. Модель взаємної довіри, взаємної недовіри та взаємного захисту. Методи автентифікації в поточкових системах шифрування, оцінка їх ефективності. Цифровий підпис, оцінка ефективності електронних підписів. Класифікація методів криптографічного аналізу та умови здійснення.

2.2 Криптографічні системи. Класифікація та характеристика симетричних криптографічних систем. Основні вимоги та склад симетричних криптографічних систем. Основні принципи та режими симетричного шифрування. Класифікація та характеристика несиметричних криптографічних систем. Основні протоколи встановлення таємниці та ключів. Аналіз рівнів безпеки. Алгоритми цифрового підпису та порівняльний аналіз їх властивостей. Алгоритм цифрового підпису в групі точок еліптичних кривих. Криптографічна стійкість та складність перетворень. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.

2.3 Проектування та використання систем і засобів захисту інформації. Нормативна база, яка визначає процеси розробки та створення комплексних систем захисту інформації. Вимоги до перспективних симетричних криптографічних систем. Стандарти симетричного блокового шифрування. Стійкість симетричних блокових криптосистем. Методика оцінки та порівняльного аналізу. Розробка програмних і апаратних засобів криптографічного захисту інформації. Основні вимоги. Принципи програмної та апаратної реалізації. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування.

2.4 Технічний захист інформації. Технічні канали витоку інформації. Радіоелектронні, вібро-акустичні та візуально-оптичні канали витоку

інформації. Канали витоку інформації і їх структура та загальна характеристика. Сигнали як носії інформації. Способи і засоби отримання інформації по вібро-акустичному каналу. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії. Методи та засоби захисту мовної інформації. Засоби протидії підслуховуванню: інформаційне приховування та енергетичне приховування. Класифікація технічних засобів закриття. Аналогове скремблювання: частотна інверсія, часова і частотна перестановка, цифрове шифрування. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів. Демаскуючі признаки закладних приладів. Апаратно-програмні комплекси викриття, ідентифікації та локалізації радіоакустичних закладних пристроїв. Основні характеристики і властивості радіоелектронного каналу витоку інформації. Джерела електромагнітних сигналів як носіїв інформації, їх властивості та особливості поширення. Побічні електромагнітні випромінювання технічних засобів. Екранування та заземлення технічних засобів передачі інформації. Вимоги та методи забезпечення захисту інформації від витоку по технічним каналам в АС 1 та АС2. Вимоги нормативних документів та захист електронних засобів інформаційно-телекомунікаційних систем від зовнішнього впливу.

2.5 Системи керування захистом інформації. Архітектура системи безпеки операційних систем (ОС). Диспетчер облікових записів (ДОЗ). Паролі, відновлення паролів. Захист файлів і компоненти (NTFS). Права доступу. Дозволи NTFS. Захист реєстру. Інформація про безпеку реєстру. Захист від локального та віддаленого доступу. Аудит реєстру.

Рекомендована література:

1. Ленков С. В., Перегудов Д. А., и Хорошко В. А., *Методы и средства защиты информации : монография* [в 2-х т.] Т. 2. Информационная безопасность. К. : Арий, 2008.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво “Форт”, 2013. – 880 с.
3. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво “Форт”, 2015. – 960 с.
4. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678.
5. Євсєєв С.П., Йохов О.Ю., та Король О.Г. Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.
6. Задірака В., Олексик О. Комп’ютерна криптологія. – Київ, 2002. – 502 с.

7. 29. Тимошенко Л.П. Схемотехніка пристроїв технічного захисту інформації: навч. посіб. [Ч.1] / Л.П. Тимошенко; за ред. В.М. Карташова. – Харків: СМІТ, 2012. – 340 с.

Тема “ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ І МЕРЕЖАХ”

3.1 Стандартизація та сертифікація систем і засобів захисту інформації. Основні положення безпеки інформації. Сутність вимог основних стандартів по забезпеченню безпеки інформації. Призначення та ціль розробки стандарту. Етапи розробки стандартів. Порядок сертифікації засобів захисту. Основні вимоги стандартів по управлінню ключами. Функції центрів управління та сертифікації ключів. Стандарти ЦП та їх застосування. Стандартні криптографічні протоколи розподілу таємниці. Властивості та реалізація. Стандарти гешування, властивості та застосування.

3.2 Захист інформації в комп’ютерних системах і мережах. Методи та засоби генерації та розподілу системних параметрів і ключів. Захист інформації із використанням цифрового підпису та коду автентифікації. Криптографічні методи та засоби захисту інформації в локальних та глобальних мережах. Криптографічні протоколи встановлення ключів та оцінка їх якості. Принципи забезпечення основних послуг – цілісності, конфіденційності, доступності й автентичності в локальних та глобальних мережах. Принципи побудування та функціонування інфраструктур з відкритими ключами. Порядок надання послуг з ЦП. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.

Рекомендована література:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво “Форт”, 2013. – 880 с.
2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво “Форт”, 2015. – 960 с.
3. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П., Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678.
4. Євсєєв С.П., Йохов О.Ю., та Король О.Г. Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.
5. Задірака В., Олексик О. Комп’ютерна криптологія. – Київ, 2002. – 502 с.
6. Сенів М.М. Безпека програм та даних: навч. посіб. / М.М. Сенів, В.С. Яковина; М-во освіти і науки України, Нац. ун-т “Львівська політехніка”. – Львів: Вид-во Львівської політехніки, 2015. – 256 с.
7. ISO/IEC 11700-1, 2, 3. Information technology – Security techniques – Key management.
8. ISO/IEC 15946-1, 2, 3. Information technology – Security techniques – Cryptographic techniques based on elliptic curves.
9. ISO/IEC 9798-1, 2, 3, 4, 5. IT Security techniques – Entity authentication.

10. ISO/IEC 9797-1, 2, 3. Information technology – Security techniques – Message Authentication Codes (MACs).
11. ISO/IEC 13888-1.2.3. Information security – Non-repudiation.
12. ISO/IEC 14888- 1.2.3. IT Security techniques – Digital signatures with appendix.
13. ISO/IEC 9594-8. Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks.
14. ISO/IEC 18031. Information technology – Security techniques – Random bit generation.
15. ISO/IEC 18032. Information technology – Security techniques – Prime number generation.
16. ISO/IEC 18033 – 1, 2, 3, 4. Information technology – Security techniques – Encryption algorithms.
17. Edited by Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
18. Hryshchuk R., Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko //– Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

Тема “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

- 4.1. Системи аналізу вразливостей та принципи етичного хакінгу.
- 4.2. Методи виявлення та аналізу шкідливого програмного забезпечення.
- 4.3. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.
- 4.4. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення; патерни безпеки: керування ідентифікацією, автентифікація, моделі доступу, керування сесіями та ін.
- 4.5. Аспекти адміністрування, аудит та безпека інформаційних служб Internet.
- 4.6. Методи проведення цифрової криміналістики.

Рекомендована література:

1. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
2. Богуш В.М. Інформаційна безпека держави: [навч. посіб.] / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.
3. Бурячок В.Л., Гришук Р.В., та Хорошко В.О., під заг. ред. проф. В. О. Хорошка, “Політика інформаційної безпеки”, ПВП “Задруга”, 2014.
4. Гришук Р.В., та Даник Ю.Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

5. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій.
6. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій
7. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.
8. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибір засобів захисту
9. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою
10. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD).
11. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)
12. Юдін О.К. “Інформаційна безпека. Нормативно-правове забезпечення”, К. : НАУ, 2011.
13. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model.
14. ISO/IEC 15408-2:2005– Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
15. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements
16. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements
17. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls.
18. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
19. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity
20. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity.

Тема “МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СИСТЕМ БЕЗПЕКИ”

5.1 Принципи побудови математичних моделей. Основні види моделювання. Формальні методи побудови моделей. Формальні методи

побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід. Ідентифікація параметрів математичної моделі. Адекватність, чутливість, непротирічність моделі.

5.2 Математичні основи моделей безпеки. Поняття автомата. Елементи теорії графів. Алгоритмічно розв'язні і алгоритмічно нерозв'язні проблеми. Модель решітки. Основні види формальних моделей безпеки. Проблема адекватності реалізації моделі безпеки в реальному комп'ютерній системі.

5.3 Моделі з дискреційним управлінням доступу. Модель матриці доступу Харрісона-Руззо-Ульмана. Опис моделі. Аналіз безпеки систем ХРУ. Модель типизованої матриці доступу. Модель поширення прав доступу Take-Grant. Основні положення класичної моделі Take-Grant. Розширена модель Take-Grant. Подання систем Take-Grant системами ХРУ. Дискреційні ДП-моделі. Базова ДП-модель. ДП-модель без кооперації довірених і недовірених суб'єктів.

5.4 Моделі ізольованого програмного середовища. Суб'єктно-орієнтована модель ізольованого програмного середовища. Коректність суб'єктів в ДП-моделях КС з дискреційним управлінням доступом. ДП-модель з функціонально асоційованими з суб'єктами сутностями. ДП-модель для політики безпечного адміністрування. ДП-модель для політики абсолютного поділу адміністративних і призначених для користувача повноважень. ДП-модель з функціонально або параметрично асоційованими з суб'єктами сутностями. Застосування ФАС ДП-моделі для аналізу безпеки веб-систем.

5.5 Моделі з мандатним управлінням доступу. Модель Бела-ЛаПадули. Модель мандатної політики цілісності інформації Віба. Модель систем військових сполучень. Загальні положення та основні поняття. Неформальне опис моделі СВС. Формальний опис моделі СВС. Мандатна ДП-модель.

5.6 Моделі безпеки інформаційних потоків. Автоматна модель безпеки інформаційних потоків. Програмна модель контролю інформаційних потоків. Імовірнісна модель безпеки інформаційних потоків. ДП-моделі безпеки інформаційних потоків за часом. ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з ототожненням породжених суб'єктів.

5.7 Моделі рольового управління доступом. Базова модель рольового управління доступом. Модель адміністрування рольового управління доступом. Основні положення. Адміністрування множин авторизованих ролей користувачів. Адміністрування множин прав доступу, якими володіють ролі. Адміністрування ієрархії ролей. Модель мандатної рольового управління доступом. Захист від загрози конфіденційності інформації. Захист від загроз конфіденційності та цілісності інформації. Мандатна сутнісно-рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux.

Рекомендована література:

1. Грищук Р.В., та Даник Ю.Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
2. Кібербезпека мереж наступного покоління : навч. посіб. / О. О. Вараксін, Є. В. Васіліу, С. М. Горохов и др. ; за ред. В. Г Кононовича ; М-во освіти і науки України, Одеська нац. академія зв'язку ім. О. С. Попова. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 240 с.
3. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с
4. Махней О. В. Математичне моделювання : навчальний посібник / О. В. Махней. – Івано-Франківськ : Супрун В. П., 2015. – 372 с.
5. Олейніков А.М. Методи та засоби захисту інформації. Навчальний посібник для студентів вищих навчальних закладів // Харків: НТМТ , 2014. – 298 с.

Тема “ЗАХИСТ ІНФОРМАЦІЇ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ”

6.1 Централізовані та децентралізовані мережі. Принципи формування систем безпеки. Технологія блокчейн. Технології майнінга. Моделі знаходження консенсусу. Криптографічні протоколи гешування.

6.2. Основи смарт-контрактів. Принципи формування смарт-контрактів. Принципи токенизації. Принципи формування та особливості Bitcoin Script. Принципи формування протоколу Bitshares. Формування SmartCoins. Облікова система Atomic Swap. Принципи створення Stablecoin. Проведення транзакцій та формати ключів у BitCoin.

Рекомендована література:

1. Кравченко П., Скрыбін Б. Блокчейн та децентралізовані системи. Ч. 1. Харків: Промарт, 2018. – 400 с.
2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 2 – Харків: ПРОМАРТ, 2019. – 452 с.
3. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.
4. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво “Форт”, 2015. – 960 с.
5. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П., Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678.
6. Wanjala Peter. A Beginner’s Journey to Ethereum’s Smart Contracts. [Peter Namisiko Wanjala], 2018. – 189 p.

7. Vaneetvelde Kenny. Ethereum Projects for Beginners (code).Packt Publishing, 2018. – 92 p.
8. Skvorc Bruno. Learn Ethereum: The Collection. SitePoint, 2018. – 447 p.

ПЕРЕЛІК ЗАПИТАНЬ ВСТУПНОГО ВИПРОБОВУВАННЯ

1. Знаходження НСД двох чисел. Методи побудови “великих” простих чисел.
2. Кільця, визначення та властивості.
3. Поля, визначення та властивості. Прості та поширені поля. Критерій згоди Колмогорова, χ^2 – квадрат Пірсона.
4. Еліптичні криві, визначення та властивості. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих.
5. Дискретно-ймовірнісний простір. Події та ймовірності, їх визначення та властивості.
6. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності.
7. Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу.
8. Класифікація шифрів. Класифікація криптографічних систем по стійкості.
9. Симетричні та несиметричні алгоритми шифрування. Блокові та потокові алгоритми шифрування, та їх властивості.
10. Несиметричні алгоритми шифрування та їх властивості.
11. Методи автентифікації, оцінка їх ефективності. Стандарти гешування, властивості та застосування.
12. Цифровий підпис, оцінка ефективності електронних підписів. Стандарти ЦП та їх застосування.
13. Основні принципи та режими симетричного шифрування. Класифікація та характеристика несиметричних криптографічних систем.
14. Алгоритм цифрового підпису в групі точок еліптичних кривих.
15. Криптографічна стійкість та складність перетворень. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.
16. Вимоги до перспективних симетричних криптографічних систем
17. Стандарти симетричного блокового шифрування. Стандартні криптографічні протоколи розподілу таємниці.
18. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування.
19. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування.
20. Технічні канали витоку інформації.
21. Канали витоку інформації і їх структура та загальна характеристика.
22. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії.
23. Методи та засоби захисту мовної інформації.
24. Класифікація технічних засобів закриття.
25. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів.
26. Основні характеристики і властивості радіoeлектронного каналу витоку інформації.
27. Архітектура системи безпеки операційних систем.

28. Сутність вимог основних стандартів по забезпеченню безпеки інформації.
29. Методи та засоби генерації та розподілу системних параметрів і ключів.
30. Захист інформації із використанням цифрового підпису та коду автентифікації.
31. Криптографічні протоколи встановлення ключів та оцінка їх якості.
32. Принципи побудування та функціонування інфраструктур з відкритими ключами.
33. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.
34. Системи аналізу вразливостей та принципи етичного хакінгу.
35. Методи виявлення та аналізу шкідливого програмного забезпечення.
36. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.
37. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення.
38. Аспекти адміністрування, аудит та безпека інформаційних служб Internet.
39. Методи проведення цифрової криміналістики.
40. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.
41. Математичні основи моделей безпеки. Поняття автомата. Елементи теорії графів.
42. Моделі з дискреційним управлінням доступу.
43. Моделі ізольованого програмного середовища.
44. Моделі з мандатним управлінням доступу. Модель Бела-ЛаПадули.
45. Моделі безпеки інформаційних потоків. Автоматна модель безпеки інформаційних потоків.
46. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів.
47. Мандатна ДП-модель з ототожненням породжених суб'єктів.
48. Модель адміністрування рольового управління доступом. Основні положення.
49. Модель мандатної рольового управління доступом.
50. Мандатна сутнісно-рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux.
51. Централізовані та децентралізовані мережі. Принципи формування систем безпеки.
52. Технологія блокчейн. Технології майнінга. Моделі знаходження консенсусу.
53. Базова модель рольового управління доступом.
54. Принципи майнінга та знаходження консенсусу. Криптографічні протоколи гешування.
55. Основи смарт-контрактів. Принципи формування смарт-контрактів.
56. Принципи токенизації. Принципи формування та особливості Bitcoin Script.
57. Принципи формування протоколу Bitshares. Формування SmartCoins.
58. Облікова система Atomic Swap.

- 59. Принципи створення Stablecoin.
- 60. Проведення транзакцій та формати ключів у BitCoin.
- 61. Мережа Фейстеля. Її архітектура та функціонування.
- 62. Модульна арифметика у криптографії. Порівняння за модулем. Основні операції у модульній арифметиці.
- 63. Зведення в ступінь у модульній арифметиці. Мала теорема Ферма.
- 64. Поняття про односторонні функції. Приклади. Використання в несиметричних криптосистемах.
- 65. Вимоги до криптографічних геш-функцій.

Затверджено на засіданні кафедри “Кібербезпека” від 15.04.2022 протокол № 7.

Завідувач кафедри



Сергій ЄВСЕЄВ

Гарант ОНП



Сергій ЄВСЕЄВ

Завідувач аспірантури НТУ «ХП»



Вікторія ШТЕФАН

Відповідальний секретар Центральної
приймальної комісії НТУ «ХП»



Сергій ПЕТРОВ

КРИТЕРІЇ ОЦІНКИ ВСТУПНОГО ВИПРОБУВАННЯ

Завдання вступного іспиту оцінюється за чотирьох бальною системою: «відмінно», «добре», «задовільно», «незадовільно».

При оцінці знань за основу слід брати повноту і правильність виконання завдань. Загальна оцінка визначається як середня виважена з оцінок відповідей на усі запитання.

Оцінка за 4 бальною системою	Характеристика відповіді
Відмінно (5)	Вступник: - досконало володіє теоретичним навчальним матеріалом для ґрунтовної відповіді на поставлені питання; - глибоко і повно оволодів понятійним апаратом, вільно та аргументовано висловлює власні думки; - демонструє культуру спеціальної мови і використовує сучасну технологічну термінологію, цілісно, системно, у логічній послідовності дає відповідь на поставлені запитання; - творчо використовує знання для розв'язання практичних завдань.
Добре (4)	Вступник: - володіє теоретичним навчальним матеріалом для відповіді на поставлені питання; - здатний застосовувати вивчений матеріал на рівні стандартних ситуацій; наводити окремі власні приклади на підтвердження певних тверджень; - грамотно викладає відповідь, але зміст і форма відповіді мають окремі неточності, припускає 2-3 неprincipові помилки, які вміє виправити, добираючи при цьому аргументи для підтвердження певних дій.
Задовільно (3)	Вступник: - частково володіє навчальним матеріалом, здатний логічно відтворити значну його частину; - виявляє знання і розуміння основних положень навчального матеріалу, але викладає його неповно, непослідовно, припускається неточностей у визначеннях понять, у застосуванні знань для вирішення практичних задач, не вміє доказово обґрунтувати свої думки; - завдання виконує, але припускає методологічні помилки.
Незадовільно (2)	Вступник: - має розрізнені безсистемні знання; - володіє матеріалом на елементарному рівні засвоєння, викладає його безладно, уривчастими реченнями; - припускає помилки у визначенні термінів, які приводять до викривлення їх змісту; - припускає принципові помилки при вирішенні практичних завдань; - не відповідає (або дає неповні, неправильні відповіді) на основні та додаткові питання.