Національний технічний університет Україна
«Київський політехнічний інститут імені Ігоря Сікорського»

ЗАТВЕРДЖУЮ:
Голова Предметної комісії
Гарант освітньої програми

Олексій НОВІКОВ

« ____ » « _____ » 2021 р.

ПОГОДЖЕНО:
Проректор з навчальної роботи
Мельниченко А.А. _____
м.п.

« ____ » « _____ » 2021 р.

ПРОГРАМА

ВСТУПНОГО ІСПИТУ

для здобуття наукового ступеня доктор філософії

за спеціальністю 125 Кібербезпека

Програму рекомендовано вченою радою фізико-технічного інституту

Київ – 2021

Зміст

I. ЗАГАЛЬНІ ВІДОМОСТІ.....3
II. ТЕМИ, ЩО ВИНОСЯТЬСЯ НА ВСТУПНЕ ВИПРОБОВУВАННЯ..4
III. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ.....8
IV. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ ВСТУПНОГО ВИПРОБУВАННЯ.....11
V. ПРИКЛАД ЕКЗАМЕНАЦІЙНОГО БІЛЕТУ.....12

І. ЗАГАЛЬНІ ВІДОМОСТІ

Вступний іспит на навчання для здобуття наукового ступеня доктор філософії спеціальності 125 «Кібербезпека» проводиться для тих вступників, які мають ступень магістра*.

Освітня програма «Кібербезпека» відповідає місії та стратегії КПІ ім. Ігоря Сікорського, за якою стратегічним пріоритетом університету є фундаменталізація підготовки фахівців. Особливості освітньої програми враховані шляхом обрання відповідних розділів програми вступного іспиту. Проведення вступного випробування має виявити рівень підготовки вступника з обраної для вступу спеціальності.

Теоретичні питання вступного іспиту можна поділити на чотири розділи:

1. Нормативно-правові та організаційні засади кібербезпеки.
2. Системи та технології кібербезпеки.
3. Математичні методи кібербезпеки.
4. Системи технічного захисту інформації.

Перші два розділи містять загальні питання, відповідь на які має знати кожен спеціаліст в галузі кібербезпеки. Останні два розділи є більш орієнтованими на поглиблену спеціальну підготовку вступника.

Завдання вступного випробування складається з трьох теоретичних питань. До екзаменаційного білету включаються відповідно: 1 питання з першого розділу, 2 та 3 питання — з другого, третього або четвертого розділів.

Вступне випробування зі спеціальності проводиться у формі усного екзамену.

Тривалість підготовки вступника до відповіді – 2 академічні години.

У наступному розділі програми наведені лише ті теми з зазначених розділів, які стосуються виконання завдань вступних випробувань.

Інформація про правила прийому на навчання та вимоги до вступників освітньої програми «Кібербезпека» наведено в розділі «Вступ до аспірантури» на веб-сторінці аспірантури та докторантури КПІ ім. Ігоря Сікорського за посиланням https://aspirantura.kpi.ua/

*Відповідно доп.2 Розділу XV закону Про вищу освіту вища освіта за освітньо-кваліфікаційним рівнем спеціаліста прирівнюється до вищої освіти ступеня магістра

ІІ. ТЕМИ, ЩО ВИНОСЯТЬСЯ НА ВСТУПНЕ ВИПРОБОВУВАННЯ

1. **Нормативно-правові та організаційні засади кібербезпеки**

1.1. **Нормативно-правове забезпечення** в сфері інформаційної і кібернетичної безпеки. Визначення, зміст та співпорядкованність понять «інформаційна безпека», «безпека інформації».

1.2. **Основи державної політики** України в сфері технічного захисту інформації. Захист інформації в інформаційно-телекомунікаційних системах.

1.3. **Організаціне забезпечення захисту інформації.** Склад і структура, основні завдання служби безпеки організації. Адміністративно-організаційні аспекти забезпечення режиму.

1.4. **Інформаційні аспекти безпеки підприємницької діяльності.** Інформаційна безпека в системі безпеки підприємницької діяльності. Комерційна таємниця Адміністративно-організаційні аспекти забезпечення режиму комерційної таємниці на підприємстві.

1.5. **Класифікація інформації** за режимом доступу та правовим режимом. Інформація з обмеженим доступом. Державна таємниця. Система захисту державних секретів в Україні.

1.6. **Загрози.** Визначення поняття «кібернетична загроза». Основні види кіберзагроз.

1.7. **Ризики.** Фактори та умови виникнення ризиків. Зміст та сутність оцінювання ризиків. Концепції та моделі ризику.

1.8. **Цінність інформації.** Методики визначення цінності інформації. Рекомендації міжнародних стандартів щодо визначення цінності інформаційних ресурсів.

2. **Системи та технології кібербезпеки**

2.1. **Класичні схеми шифрування.** Моноалфавітні підстановки. Методи криптоаналізу. Поліалфавітні підстановки. Шифр Віженера та його криптоаналіз. Інші шифри підстановки. Шифри перестановки: загальне визначення, шифри обходу, табличні перестановки, маршрути Гамільтона, грати Кардано, магічні квадрати, інші шифри перестановки. Комбіновані шифри.

2.2. **Основи стеганографії.** Предмет, термінологія, області застосування. Основні поняття та методи стеганографії. Математичні моделі стегосистем. Огляд стегоалгоритмів. Атаки на стегосистеми та протидії їм. Приклади стеганографічних систем.

2.3. **Цифровий підпис.** Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з геш-функцією в асиметричної криптографії.

Цифровий підпис у схемі RSA з використанням геш-функцій, цифрові підписи Эль-Гамаля, Рабіна. Сліпий підпис. Атаки на цифровий підпис.

2.4. **Криптографічні протоколи.** Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Імовірнісне шифрування.

2.5. **Безпека операційних систем.** Модель загроз для операційної системи, функціональні послуги безпеки і механізми, спрямовані на захист від кожної з загроз.

2.6. **Шкідливе програмне забезпечення** – класифікація, механізми функціонування, особливості застосування, заходи і технології протидії.

2.7. **Загрози безпеці інформації у комп'ютерних мережах.** Віддалені атаки (класифікація, приклади).

2.8. **Безпека веб-застосунків.** Атаки на сервери і клієнтів, заходи протидії.

2.9. **Архітектура безпеки взаємодії відкритих систем**. Стандарти, сервіси, механізми.

2.10. **Віртуальні приватні мережі.** Сервіси, технології, протоколи.

2.11. **Засоби виявлення атак і протидії атакам** – класифікація, джерела інформації, принципи виявлення, обмеження.

2.12. **Визначення ступеню захищеності інформації в системах зв'язку**. Перспективи криптозахисту. Способи скремблювання. Режими роботи скремблерів. Особливості витоку інформації від ЗОТ і ЛОМ та їх захисту.

2.13. **Комплексні системи захисту інформації (КСЗІ)**. Ефективність КСЗІ. Модель загроз інформації у захищених АС. Перелік загроз на різних рівнях моделі. Експертне оцінювання вразливості систем захисту.

2.14. **Системи управління інформаційною безпекою (СУІБ)**. Модель впровадження і функціювання, контрольні заходи, міжнародні стандарти і ДСТУ.

3. **Математичні методи кібербезпеки**

3.1. **Джерела загроз як основний чинник невизначеності.** Стохастична та лінгвістична невизначеність.

3.2. **Аналіз структури складних систем безпеки: Q-аналіз.** Симплеційний комплекс як модель системи складной структури. Алгоритми Q-аналізу: побудова структурного дерева та локальних карт, розрахунок ексцентриситетів.

3.3. **Ухвалення рішень в умовах ризику.** Дерево рішень. Основні елементи дерева рішень, алгоритм згортання дерева. Профіль ризику.

3.4. **Оцінка пріоритетів системою забезпечення безпеки.** Формування ієрархії задачі. Заповнення елементів матриці порівнянь. Оцінка значень змінних стану окремих сценаріїв.

3.5. **Стратегічне планування системою забезпечення кібербезпеки: SWOT - аналіз.** Правила здійснення SWOT - аналізу. Системна аналітика і SWOT – аналіз.

3.6. **Сучасні наукові концепції безпечного розвитку особи, суспільства та держави в кіберпросторі.** Концепція "суспільства ризику". Концепція "прийнятного ризику". Концепція "стратегічних ризиків".

3.7. **Марківський випадковий процес з дискретним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою однорідного марківського ланцюга.

3.8. **Марківський випадковий процес з дискретним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою неоднорідного марківського ланцюга.

3.9. **Марківський випадковий процес з неперервним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою однорідного марківського процесу з неперервним часом.

3.10. **Марківський випадковий процес з неперервним часом як модель зміни стану захищеності складних систем.** Правила побудови диференційних рівнянь Колмогорова для оцінки стану захищеності складних систем, що описуються марківськими процесами з неперервним часом.

3.11. **Розподіл Пуасона як математична модель реалізації загроз.** Кількісні показники реалізації загроз.

3.12. **Системи масового обслуговування як матемачні моделі оцінки діяльності системи забезпечення безпеки.** Системи обслуговування M/M/1 Д. Кендела: основні складові, критерії якості, рівняння Колмогорова для системи M/M/1.

3.13. **Практичні методи побудови нечітких функцій безпеки.** Методи побудови функцій належності, що характеризують безпеку складних систем.

3.14. **Оцінка стану захищеності складних систем.** Нечіткий метод аналізу ризику А. Недосекіна.

3.15. **Прогнозування небезпечних явищ і процесів.** Нечіткий метод Делфі.

3.16. **Вибір альтернатив у безпековому середовищі.** Методи нечіткого виводу.

3.17. **Нечіткі когнітивні карти небезпечних явищ і процесів.** Алгоритм побудови.

4. Системи технічного захисту інформації

4.1. **Варіанти утворення** небезпечних сигналів.
4.2. **Поняття перетворювача фізичних величин.** Фізична природа первинних перетворювачів.
4.3. **Небезпечні сигнали**. Об’єкти захисту інформації. Розгляд системи ТЗПІ при організації захисту інформації.
4.4. **Акустоелектричні перетворювання та перетворювачі**. Метод ВЧ нав’язування, як спосіб інформаційної атаки.
4.5. **Технічні заходи, спрямовані на захист інформації**. Перелік та опис.
4.6. **Основні канали витоку інформації на ОІД**. Організаційні заходи та технічні засоби протидії витоку мовної інформації з виділених приміщень.
4.7. **Методи та засоби активного захисту інформації**, поширюваної акустичними (мовними) каналами витоку в приміщеннях та каналах зв’язку.
4.8. **Межі ослаблення електромагнітних хвиль** для різних типів електромагнітних екранів. Конструкції екранів.
4.9. **Типи екранів**. Вимоги до безпомилкового монтажу електростатичного та електромагнітного екранів.
4.10. **Пошук закладних пристроїв**. Детектування диктофонів, котрі працюють в режимі запису. Нелінійна локація. Принцип роботи нелінійних локаторів.
4.11. **Локалізація випромінювань як пасивний метод технічних заходів ЗІ**. Перелік заходів та їх характеристики.
4.12. **Межі досяжності ослаблення електромагнітних хвиль** для різних типів екранувальних засобів.
4.13. **Звукове ізолювання приміщень**.
4.14. **Фільтрування інформаційних сигналів**. Види засобів фільтрування та їх характеристики.
4.15. **Заземлення технічних засобів**. Основні схеми заземлення та їх порівняльні характеристики. Переваги та недоліки різних схем заземлення.
4.16. **Питання електромагнітної сумісності (ЕС) технічних засобів**.
4.17. **Основні параметри закладних пристроїв**.

ІІІ. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ

Література до 1-го розділу

1. Богуш В.М. Інформаційна безпека від А до Я / Богуш В.М., Кудін А.М. - К.: МОУ, 1999. - 456 с.
2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В.В. - К.: ООО "ТИД ДС", 2001. - 688 с.
3. Закон України «Про основні засади забезпечення кібербезпеки України» - Відомості Верховної Ради України (ВВР), 2017, № 45, ст.403, зі змінами.
4. Закон України «Про інформацію» - Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650, зі змінами.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» - Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286, зі змінами.
6. Проект Стратегії кібербезпеки України (2021–2025 роки) — РНБО [Електронний ресурс], URL: https://www.rnbo.gov.ua/files/2021/ STRATEGIYA KYBERBEZPEKI/proekt strategii_kyberbezpeki_Ukr.pdf

Література до 2-го розділу

7. Грайворонський М.В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ / Грайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.
8. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посіб. – К: Видавничий дім «КМ Академія», 2003. – 243 с.
9. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
10. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
11. Казарин О.В. Теория и практика защиты программ. – М.: 2004. – 450 с.
12. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М. Изд. центр “Академия”, 2005 – 144 с.
13. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. – Екатеринбург: 2008. – 212 с.
14. Алферов А.П. Основы криптографии / Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. – М.: Гелиос АРВ, 2001.
15. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. - М.: Издательство ТРИУМФ, 2003. - 816 с.

16. Menezes A. Handbook of Applied Cryptography / Menezes A., P. van Oorschot, S.Vanstone. – CRC Press, 1997. – 780 p.
17. Гроувер Д. Защита программного обеспечения. Пер с англ. / Д. Гроувер, Р. Сатер, Дж. Фипс и др. Под редакцией Д. Гроувера – М.:, Мир, 1992. – 285 с.
18. Хогланд Г. Взлом программного обеспечения: анализ и использование кода / Хогланд Г., Мак-Гроу Г. – М: «Вильямс», 2005. – 384 с.
19. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. – СПб.: БХВ-Петербург, 2005. – 432 с.
20. Девянин П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин и др. – М.: Радио и связь, 2000. – 192 с.
21. Кузьмин Н.В. Основы теории информации и кодирования / Кузьмин Н.В., Кедрус В.А. – К.: “Вища школа”, 1977.
22. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. – М. “Связь”, 1979.
23. Диффи У. Защищенность и имитостойкость. / Диффи У., Хеллман М. – ТИИЭР. – 1979. – Т.67, №3.
24. Месси Дж.Л. Введение в современную криптологию. / ТИИЭР. – 1988. – Т.76, №5.
25. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003.
26. Симмонс Г.Дж. Обзор методов аутентификации информации. ТИИЭР. – 1988. – Т.76, №5.
27. 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.
28. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах — Затверджено постановою Кабінету Міністрів України від 29.03.2006 р. № 373

Література до 3-го розділу

29. Качинський А.Б. Безпека складних систем: математичне моделювання небезпечних процесів і системний аналіз її забезпечення – К.: «Азимут-Україна», 2016. 498 с.
30. Зайченко Ю.П. Теорія прийняття рішень: підручник .- НТУУ «КПІ», - 2014. -412 с.
31. Томашевський В.М. Моделювання систем. -К.: Видавнича група BHV. - 2005. -352 с.

32. Волошин О.Ф., Мащенко С.О. Моделі та методи прийняття рішень. - Київ.; Університет. -2010. -336 с.

33. Полуциганова В.І., Смирнов С.А. Методологія побудови основних метрик Q-аналізу та їх застосування // Системний аналіз та інформаційні технології, 2019, №3, с. 76-88.

Література до 4-го розділу

34. 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.

35. Вінницький И.П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В.П.Вінницький, В.Г.Поліщук. – К.: ІВЦ “Видавництво «Політехніка»”, 2004. – 436 с.

36. Хорев А.А. Способы и средства защиты информации. М.: МО РФ, 1999, 316 с. утверждено в качестве учебного пособия.

37. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. 2-е изд., исправл. и доп. – М.: Энергоатомиздат, 1997. – 304 с.: ил.

38. Магуенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. Учебное пособие / Магуенов Р.Г. - М.: Горячая линия - Телеком, 2004. - 367 с.

39. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. - К.: Издательство Юниор, 2003. - 504 с.

40. Гарсиа М.Л. Проектирование и оценка систем физической защиты / Гарсиа М.Л. - Пер. с англ. - М.: Мир-ООО АСТ, 2002. - 386 с.

41. Иванов И.В. Охрана периметров / Иванов И.В. - М.: «Паритет Граф», 2000. - 196 с., ил.

IV. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ ВСТУПНОГО ВИПРОБУВАННЯ

1. Початковий рейтинг вступника за вступне випробування розраховується виходячи із 100-бальної шкали. При визначенні загального рейтингу вступника початковий рейтинг за екзамен перераховується у 200-бальну шкалу за відповідною таблицею (п.4) .

2. Під час вступного випробування вступники готуються до усної відповіді на завдання екзаменаційного білету. Кожне завдання вступного випробування містить три теоретичні питання.

Кожне з перших двох питань оцінюється у 35 балів за такими критеріями:

- 33…35 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 30…32 – повна відповідь (містить не менше 85% потрібної інформації);
- 27…29 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 24…26 – достатня відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 21…23 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації або окремі помилки);
- менше 20 – незадовільна відповідь.

Критерії оцінювання відповідей на третє питання білету вступного випробування:

- 29…30 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 27…28 – повна відповідь (містить не менше 85% потрібної інформації);
- 24…26 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 21…23 – достатня відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 18…20 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації або окремі помилки);
- менше 20 – незадовільна відповідь.

3. Загальна кількість балів за відповідь вступника визначається шляхом підсумовування балів за відповіді на питання білету вступного випробування. Перерахування отриманих балів в оцінку проводиться згідно з таблицею.

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
менше 60	Незадовільно

4. Сума балів за відповіді переводиться до 200-бальної шкали згідно з таблицею:

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

V. ПРИКЛАД ЕКЗАМЕНАЦІЙНОГО БІЛЕТУ

Форма № Н-5.05

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

(повне найменування вищого навчального закладу)

Освітній ступінь *доктор філософії*

Спеціальність *125 Кібербезпека*

(назва)

Навчальна дисципліна *Вступний іспит*

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № ____

1. Питання 1

2. Питання 2

3. Питання 3

Затверджено

Гарант освітньої програми _____ Олексій НОВІКОВ

Київ 2021

РОЗРОБНИКИ:

Мачуський Євгеній Андрійович	доктор технічних наук, професор, в.о.завідувача кафедри фізико-технічних засобів захисту інформації
Грайворонський Микола Владленович	кандидат фізико-математичних наук, доцент, в.о.завідувача кафедри інформаційної безпеки
Савчук Михайло Миколайович	доктор фізико-математичних наук, доцент, в.о.завідувача кафедри математичних методів захисту інформації
Качинський Анатолій Броніславович	доктор технічних наук, професор, професор кафедри інформаційної безпеки

Програму рекомендовано:

Вченою радою фізико-технічного інституту

Голова вченої ради _____

_____

протокол № ____

від « ____ » « _____ » 2021 р.