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

ЗАТВЕРДЖУЮ:
Гарант освітньої програми

Ланде Д.В.

«22 » лютого 2022 р.

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

«22» лютого 2022 р.

# ПРОГРАМА

## ДОДАТКОВОГО ВСТУПНОГО ІСПИТУ

## для здобуття наукового ступеня доктор філософії

***за спеціальністю 125 Кібербезпека***

***(для випускників магістратури інших спеціальностей)***

***Програму рекомендовано вченою радою науково-навчального фізико-технічного інституту***

**Київ – 2022**

**Зміст**

# І. ЗАГАЛЬНІ ВІДОМОСТІ

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

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 додаткового вступного випробування має виявити спроможність вступника брати участь в основному вступному випробуванні для вступу на обрану спеціальність.

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.

Перший розділ містить загальні питання. Останні три розділи є орієнтованими на окремі спеціалізації в рамках спеціальності «Кібербезпека».

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

Додаткове вступне випробування зі спеціальності проводиться у формі усного екзамену.

Тривалість підготовки вступника до відповіді – 60 хвилин.

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.

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

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

### 2. Системи та технології кібербезпеки

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

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

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

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

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

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

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

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

3. **Математичні методи кібербезпеки**

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

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

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

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

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

3.6. **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.

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

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

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

## 4. Системи технічного захисту інформації

4.1. **Поняття перетворювача фізичних величин.** Фізична природа первинних перетворювачів.

4.2. **Небезпечні сигнали**. Об’єкти захисту інформації. Розгляд системи ТЗПІ при організації захисту інформації.

4.3. **Технічні заходи, спрямовані на захист інформації**. Перелік та опис.

4.4. **Основні канали витоку інформації на ОІД**. Організаційні заходи та технічні засоби протидії витоку мовної інформації з виділених приміщень.

4.5. **Локалізація випромінювань як пасивний метод технічних заходів ЗІ**. Перелік заходів та їх характеристики.

4.6. **Фільтрування інформаційних сигналів**. Види засобів фільтрування та їх характеристики.

4.7. **Заземлення технічних засобів**. Основні схеми заземлення та їх порівняльні характеристики. Переваги та недоліки різних схем заземлення.

4.8. **Звукове ізолювання приміщень.**

4.9. **Методи та засоби активного захисту інформації**, поширюваної акустичними (мовними) каналами витоку в приміщеннях та каналах зв’язку.

4.10. **Пошук закладних пристроїв**. Детектування диктофонів, котрі працюють в режимі запису. Нелінійна локація. Принцип роботи нелінійних локаторів.

## 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
7. 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.
8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах — Затверджено постановою Кабінету Міністрів України від 29.03.2006 р. № 373


### Література до 2-го розділу


9. Грайворонський М.В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ / Грайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.
10. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посіб. – К: Видавничий дім «КМ Академія», 2003. – 243 с.
11. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
12. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
13. Казарин О.В. Теория и практика защиты программ. – М.: 2004. – 450 с.

14. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М. Изд. центр “Академия”, 2005 – 144 с.
15. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. – Екатеринбург: 2008. – 212 с.
16. Алферов А.П. Основы криптографии / Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. – М.: Гелиос АРВ, 2001.
17. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. - М.: Издательство ТРИУМФ, 2003. - 816 с.
18. 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.
19. Хогланд Г. Взлом программного обеспечения: анализ и использование кода / Хогланд Г., Мак-Гроу Г. – М: «Вильямс», 2005. – 384 с.
20. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. – СПб.: БХВ-Петербург, 2005. – 432 с.
21. Симмонс Г.Дж. Обзор методов аутентификации информации. ТИИЭР. – 1988. – Т.76, №5.

**Література до 3-го розділу**

22. Качинський А.Б. Безпека складних систем: математичне моделювання небезпечних процесів і системний аналіз її забезпечення – К.: «Азимут-Україна», 2016. 498 с.
23. Зайченко Ю.П. Теорія прийняття рішень: підручник .- НТУУ «КПІ», - 2014. -412 с.
24. Томашевський В.М. Моделювання систем. -К.: Видавнича група BHV. - 2005. -352 с.
25. Волошин О.Ф., Мащенко С.О. Моделі та методи прийняття рішень. - Київ.; Університет. -2010. -336 с.
26. 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**

27. 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.
28. Вінницький И.П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В.П.Вінницький, В.Г.Поліщук. – К.: ІВЦ “Видавництво «Політехніка»”, 2004. – 436 с.

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

30. 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.

## IV. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ ВСТУПНОГО ВИПРОБУВАННЯ

На екзамені вступники готуються до усної відповіді на завдання екзаменаційного білету. Кожне завдання додаткового вступного випробування містить два теоретичні питання.

Рейтинг вступника за додаткове вступне випробування розраховується виходячи із 100-бальної шкали. Кожне з двох питань оцінюється у 50 балів за такими критеріями:

- 48…50 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 43…47 – повна відповідь (містить не менше 85% потрібної інформації);
- 38…42 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 33…37 – достатня відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 30…32 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації або окремі помилки);
- менше 30 – незадовільна відповідь.

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 |
|---|---|
| 60-100 | Зараховано |
| менше 60 | Не зараховано |

## 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*

Затверджено

Гарант освітньої програми _____ Дмитро ЛАНДЕ

Київ 2022

## 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 Навчально-наукового фізико-технічного інституту

Голова ради _____ протокол № 2 від «1» лютого 2022 р.

(підпис)

.