

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**ЗАТВЕРДЖУЮ**  
Голова Вченої ради Фізико-  
технічного інституту

**О.М.Новіков**

«\_\_\_\_\_» \_\_\_\_\_ 2017 р.

**ПРОГРАМА ДОДАТКОВОГО ВСТУПНОГО  
ІСПИТУ**

**третього (освітньо-наукового) рівня вищої освіти  
для здобуття наукового ступеня доктор філософії**

**ГАЛУЗЬ ЗНАНЬ  
СПЕЦІАЛЬНІСТЬ**

**12 Інформаційні технології  
125 Кібербезпека**

Ухвалено Вченою радою Фізико-технічного інституту  
(протокол від «22» 03.2017р. № 3/2017)

Київ  
НТУУ «КПІ ім. Ігоря Сікорського»  
2017

## **Розробники програми:**

**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

---

## 1. Системи і технології кібербезпеки

- 1.1 **Нормативно-правове забезпечення** в сфері інформаційної безпеки і захисту інформації. Визначення, зміст та співпорядкованість понять «інформаційна безпека», «безпека інформації».
- 1.2. **Класифікація інформації** за режимом доступу та правовим режимом. Інформація з обмеженим доступом. Державна таємниця. Система захисту державних секретів в Україні.
- 1.3. **Основи державної політики** України в сфері технічного захисту інформації. Захист інформації в інформаційно-телекомунікаційних системах.
- 1.4. **Ризики.** Фактори та умови виникнення ризиків. Зміст та сутність оцінювання ризиків. Концепції та моделі ризику.
- 1.5. **Організаційне забезпечення захисту інформації.** Склад і структура, основні завдання служби безпеки організації. Адміністративно-організаційні аспекти забезпечення режиму.
- 1.6. **Інформаційні аспекти безпеки підприємницької діяльності.** Інформаційна безпека в системі безпеки підприємницької діяльності. Комерційна таємниця. Адміністративно-організаційні аспекти забезпечення режиму комерційної таємниці на підприємстві.
- 1.7. **Шкідливе програмне забезпечення** – класифікація, механізми функціонування, особливості застосування, заходи і технології протидії.
- 1.8. **Загрози безпеці інформації у комп'ютерних мережах,** віддалені атаки (класифікація, приклади).
- 1.9. **Засоби виявлення атак і протидії атакам** – класифікація, джерела інформації, принципи виявлення, обмеження.

## 2. Математичні методи кібербезпеки

- 2.1. **Основні поняття криптології.** Задачі, напрямки та методи захисту інформації. Криптографічний захист інформації. Основні поняття криптології. Моделі джерел відкритого тексту, ентропія на символ джерела. Етапи розвитку криптографії. Загальна класифікація класичних і сучасних шифрів.
- 2.2. **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.
- 2.3. **Випадкові та псевдовипадкові послідовності.** Різні підходи до визначення випадкової послідовності. Фізичні датчики випадкових послідовностей. Методи генерації випадкових та псевдовипадкових послідовностей. Покращення якості випадкових послідовностей.
- 2.4. **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.

- 2.5. **Складність алгоритмів та односторонні функції.** Односторонні функції, односторонні функції з секретом. Одностороння функція дискретного піднесення до степеня. Схема відкритого розподілу ключів Діффі і Хеллмана. Односторонні функції RSA, Рабіна. Оцінки складності обчислення та обернення функцій.
- 2.6. **Хеш-функції.** Криптографічні властивості. Загальні схеми побудови. Характеристики хеш-функцій, найбільш уживаних у системах захисту інформації. Колізії хеш-функцій. Математичні моделі оцінки ймовірностей колізій та трудомісткості їх побудови. Застосування хеш-функцій.
- 2.7. **Цифровий підпис.** Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з хеш-функцією в асиметричній криптографії. Цифровий підпис у схемі RSA з використанням хеш-функцій, цифрові підписи Эль-Гамала, Рабіна. Сліпий підпис. Атаки на цифровий підпис.
- 2.8. **Криптографічні протоколи.** Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Імовірнісне шифрування.
- 2.9. **Ідентифікація та аутентифікація.** Теорія імітостійкості Симмонса. Загальні принципи аутентифікації. Криптографічні алгоритми аутентифікації: парольна аутентифікація, аутентифікація з використанням симетричних и асиметричних криптосистем.
- 2.10. **Аналітичні методи криптоаналізу.** Метод розбиття простору ключів на декартовий добуток підпросторів і випробування ключа по частинам. Знаходження ключа з допомогою зведення до систем лінійних рівнянь. Розв'язання нелінійних систем булевих рівнянь приведенням їх до трапецеїдального виду. Розв'язання нелінійних систем булевих рівнянь методами лінеарізації.
- 2.11. **Статистичні методи криптоаналізу.** Частотний криптоаналіз класичних криптосистем. Побудова статистичних моделей криптосистем. Статистичний аналог. Математична модель шифру з використанням рівнянь зі спотвореними правими частинами. Методи розв'язання лінійних систем булевих рівнянь зі спотвореними правими частинами та їх застосування.

### **3. Системи технічного захисту інформації**

- 3.1. **Поняття перетворювача фізичних величин.** Фізична природа первинних перетворювачів.
- 3.2. **Небезпечні сигнали.** Об'єкти захисту інформації. Розгляд системи ТЗПІ при організації захисту інформації.
- 3.3. **Основні канали витоку інформації на ОІД.** Організаційні заходи та технічні засоби протидії витоку мовної інформації з виділених приміщень.
- 3.4. **Технічні заходи, спрямовані на захист інформації.** Перелік та опис.
- 3.5. **Локалізація випромінювань як пасивний метод технічних заходів ЗІ.** Перелік заходів та їх характеристики.
- 3.6. **Фільтрування інформаційних сигналів.** Види засобів фільтрування та їх характеристики.
- 3.7. **Заземлення технічних засобів.** Основні схеми заземлення та їх порівняльні характеристики. Переваги та недоліки різних схем заземлення.

- 3.8. **Звукове ізолювання приміщень.**
- 3.9. **Акустoeлектричні перетворювання та перетворювачі.** Метод ВЧ нав'язування, як спосіб інформаційної атаки.
- 3.10. **Методи та засоби активного захисту інформації,** поширюваної акустичними (мовними) каналами витоку в приміщеннях та каналах зв'язку.
- 3.11. **Пошук закладних пристроїв.** Детектування диктофонів, котрі працюють в режимі запису. Нелінійна локація. Принцип роботи нелінійних локаторів.

## Критерії оцінювання вступного випробування

Критерії оцінювання відповіді вступника враховують повноту та правильність відповіді, а також здатність вступника узагальнювати отримані знання, застосовувати загальні та специфічні наукові методи, принципи та закони на конкретних випадках; аналізувати, інтерпретувати та оцінювати отримані результати.

Відповідь вступника оцінюється за 100-бальною шкалою. Дана шкала складається з балів, які він отримує за відповіді на питання білету (кожен білет вступного випробування складається з трьох питань, максимально – 35 балів за перше та друге питання білету, 30 балів за третє питання білету).

Критерії оцінювання відповідей на перше та друге питання білету вступного випробування:

- 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.

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

Кількість балів	ECTS-оцінка	Національна оцінка
95-100	A	Зараховано
85-94	B	
75-84	C	
60-74	D	
60-64	E	
менше 60	Fx	Незараховано