НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ПРОГРАМА
ФАХОВОГО ІСПИТУ
З УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

для вступників на навчання для здобуття ступеня магістра
за освітньою програмою спеціальності 256 «Національна безпека»

Київ-2022

1. **Загальні положення**

Національна академія Служби безпеки України (далі – Академія) згідно з Порядку прийому на навчання для здобуття вищої освіти в 2022 році, затверджених наказом Міністерства освіти і науки України від 27 квітня 2022 року № 392 (зі змінами, внесеними наказом Міністерства освіти і науки України від 02 травня 2022 року № 400), зареєстрованих у Міністерстві юстиції України 03 травня 2022 року за № 487/37823, Правилами прийому до Національної академії Служби безпеки України у 2022 році проводить фахове вступне випробування з правових основ захисту інформації з обмеженим доступом для конкурсного відбору вступників на навчання на основі вищої освіти для здобуття освітнього ступеня магістра за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) з спеціалізації 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері).

Ця Програма розроблена фаховою атестаційною комісією з управління інформаційною безпекою Приймальної комісії Академії.

2. Вимоги до компетентності вступників з правових основ захисту інформації з обмеженим доступом визначено з урахуванням положень законодавства України у сфері захисту інформації та цілей і змісту навчання за освітньо-професійними програмами підготовки фахівців для професійної діяльності з організації захисту інформації з обмеженим доступом як суб'єктами владних повноважень, так і суб'єктами приватного права.

Відповідність рівня компетентності вступника визначається шляхом перевірки рівня володіння правовими знаннями у сфері захисту інформації та уміннями їх застосовувати для вирішення завдань захисту інформації з обмеженим доступом.

Навчальний матеріал, що виноситься на фахове вступне випробування, структурований за такими змістовними модулями: окремі тематичні положення нормативно-правової забезпечення у сфері інформаційної безпеки та кібербезпеки, законодавчої бази України , а саме: законів України «Про інформацію», «Про державну таємницю», «Про доступ до публічної інформації», «Про захист персональних даних», «Про банки і банківську діяльність», а також тематичних положень у сфері інформаційних технологій, інформаційної безпеки та кібербезпеки.

2.1. Тематичні положення нормативно-правової забезпечення у сфері інформаційної безпеки та кібербезпеки.

Зміст права на інформацію. Гарантії права на інформацію та механізми його реалізації. Поняття інформації з обмеженим доступом та її види. Суспільна значимість інформації. Перелік інформації, доступ до якої обмежувати заборонено. Поняття публічної інформації та суб'єкта владних

повноважень. Поняття державної таємниці та основні ознаки цього виду інформації з обмеженим доступом.

Класифікація інформації з обмеженим доступом та базові класифікаційні ознаки її видів. Критерії визначення суспільної значимості інформації та типові підстави її правомірного оприлюднення. Звід відомостей, що становлять державну таємницю, порядок його формування.

Ознаки таємної, конфіденційної та службової інформації. Загальні критерії обмеження доступу до інформації та зміст права суб'єктів інформаційної діяльності на обмеження доступу до інформації.

Закони України:

Про інформацію ; Про державну таємницю; Про захист інформації в інформаційно-телекомунікаційних системах; Про захист інформації в автоматизованих системах; Про Державну службу спеціального зв'язку та захисту інформації України; Про доступ до публічної інформації ; Про основні засади забезпечення кібербезпеки в Україні; Про електронні документи та електронний документообіг; Про захист персональних даних; Про ліцензування видів господарської діяльності; Про Національну систему конфіденційного зв'язку; Про національну безпеку України.

Укази Президента України:

Про Положення про технічний захист інформації в Україні; Про Положення про порядок здійснення криптографічного захисту інформації в Україні; Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»; Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» .

Державні стандарти України та норми:

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Основні положення (ДСТУ 3396.0 – 96);

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Порядок проведення робіт (ДСТУ 3396.1 – 96);

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Терміни та визначення (ДСТУ 3396.2 – 97);

ДСТУ ISO/IEC 27001 Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги.

Нормативні документи з технічного захисту інформації:

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

2.2. Тематичні положення з інформатики та комп'ютерної техніки.

Структура та системні ресурси персонального комп'ютера (ПК). Загальні поняття про ЕОМ. Структура ПК: системна плата, центральний процесор ПК, оперативна пам'ять ПК. Дискова підсистема ПК. Відеопідсистема та звукова (аудіо) підсистема. Корпус та блок живлення. Клавіатура та миша. Периферія. Використання комп'ютерної техніки для вирішення проблем автоматизації технологічних процесів.

Загальні поняття про ЕОМ: логічні та математичні основи побудови та функціонування ЕОМ. Поняття про системи числення. Принципи, методи і форми збереження інформації в пам'яті ПЕОМ. Принципи обробки даних на ПЕОМ.

Представлення даних у комп'ютері. Позиційні системи числення. Двійкові, вісімкові та шіснадцяткові числа. Переведення чисел між системами числення. Представлення чисел із знаком. Формати даних. Двійкова арифметика.

Структурна схема типового ПК. Системні та периферійні інтерфейси. Види та характеристики сучасних платформ ПК їх класифікація, основні характеристики системної плати, як базового елемента ПК. Призначення та алгоритм роботи процесора. Класифікація сучасних центральних процесорів ПК. Призначення оперативної пам'яті та принципи її роботи. Класифікація та основні характеристики оперативної пам'яті.

Призначення постійної пам'яті. Дискова підсистема. Класифікація та основні характеристики носіїв інформації. Призначення відеоадаптера. Класифікація сучасних графічних процесорів. Основні характеристики відеоадаптерів. Типи та основні характеристики моніторів. Призначення та функціонування звукової (аудіо) підсистеми. Акустика.

Формфактор корпуса системного блока та блока живлення. Розширений інтерфейс керування живленням ACPI. Призначення стандартних пристроїв введення. Взаємодія клавіатури з ПК. Кодування клавіш клавіатури. Типи та принцип дії комп'ютерних мишей. Принципи паралельної та послідовної передачі даних.

Системні ресурси ПК. Базова система введення- виведення. Поняття системних ресурсів ПК. Адреси пам'яті. Канали запитів переривань. Канали прямого доступу до пам'яті.

Основи BIOS. Апаратна і програмна частини BIOS. Процедура POST. Первинні настройки BIOS SETUP. Встановлення та структура ОС MS-DOS. Командна мова MS-DOS. ОС MS Windows. Основи операційних систем. Ядро операційної системи. Керування пам'яттю, процесами введення-виведення, файловою системою, організація взаємодії та диспетчеризація процесів, облік використання ресурсів, оброблення команд.

2.3. Тематичні положення з інформаційних технологій.

Основні визначення та їх зміст поняття інформаційних технологій (ІТ) Інформаційних технологій та систем (ІС). Базові інформаційні процеси їх реалізація. Інформаційні технології - основа інформаційної індустрії. Класифікація інформаційних технологій.

Інформація, її функції та властивості. Кількісні характеристики інформації. Види інформації та їх класифікація. Міри інформації. Продуктивність та надмірність джерела інформації. Поняття ентропії в інформаційних технологіях. Ефективність та надмірність джерел інформації.

Базові інформаційні процеси. Збирання, попередня обробка та аналіз даних. Зберігання та накопичення інформації та даних. Передавання, прийом та обробка інформації. Висвітлення (відображення інформації).

Сучасні інформаційні технології та системи. Технології розподіленої обробки даних. Класифікація та забезпечення інформаційних систем. Математичне та програмне забезпечення інформаційних систем.

Інформаційні системи передачі та прийому даних. Основні поняття каналу передачі даних. Структура систем передачі інформації. Основні характеристики каналу передачі даних. Основні види передачі даних по каналу зв’язку. Частотний діапазон передавання та прийому даних. Завади та спотворення в каналах передачі даних.

Основи мультимедіа технологій. Історія розвитку мультимедіа технологій. Складові мультимедіа. Особливості опрацювання та зберігання мультимедіа даних.

Геінформаційні технології (ГІС). Поняття та класифікація ГІС. Структури та моделі даних в ГІС. Введення даних та створення баз даних ГІС. Методи та засоби візуалізації Геоінформації.

Інтелектуальні інформаційні технології та системи: основні поняття. Моделі представлення знань в інтелектуальних технологіях. Технології автоматичного розпізнавання образів. Інтелектуальні технології обробки текстової інформації. Інтелектуальні технології пошуку інформації. Інтелектуальні технології управління знаннями.

2.4. Тематичні положення з комп’ютерних систем та мереж.

Основи мережних технологій. Історія розвитку комп’ютерних мереж. Стандартизація комп’ютерних мереж. Рівнева архітектура та еталонна модель взаємодії відкритих систем OSI.

Середовища передавання сигналів. Класифікація. Носії передачі сигналу: (вита пара, коаксіальний кабель, оптоволокно). Безпровідний зв’язок: електромагнітний спектр, радіозв’язок, зв’язок у мікрохвильовому діапазоні, інфрачервоні і міліметрові хвилі, зв’язок у видимому діапазоні, супутниковий зв’язок, мобільний телефонний зв’язок, кабельне телебачення. Характеристика та порівняння носіїв передачі інформації.

Базові мережні технології. Безпровідні мережі. Топології комп’ютерних мереж. Канали, комутація, селекція. Стандарти серії IEEE 802.xx

Архітектури комп’ютерних мереж. Локальні мережі Ethernet. Комп’ютерні мережі та їх топологія. Кабелі Ethernet. Структура сегмента мережі різних стандартів Ethernet.

Пристрої та обладнання локальних мереж (повторювач, міст, концентратори). Комутатори (MAC-адреси, моніторинг, фільтрація, функції безпеки, прив'язка портів). Маршуритазатор та шлюз. Точка доступу. Протоколи та засоби керування в комп’ютерних мережах.

Програмне забезпечення комп’ютерних мереж. Стек протоколів TCP/IP як основа мережі Інтернет TCP/IP. Мережевий рівень в Інтернет. Система IP-адресації. Технології розподілу мережного простору. Транспортна служба. Типи мережевих з'єднань і класи транспортних протоколів. Логічна модель транспортного рівня. Транспортні протоколи Інтернету.

Маршрутизація у комп'ютерних мережах. Методи маршрутизації. Алгоритми вибору найкоротшого шляху. Алгоритм Дейкстри. Алгоритм Форда–Фалкерсона. Керування мережевим трафіком. Рівні керування трафіком.

Протоколи маршрутизації. Дистанційно-векторні протоколи IGP. Протоколи глобальних мереж EGP. Протокол RIP: алгоритм векторів, розповсюдження таблиць маршрутизації. Граничні зонні маршрутизатори.

Протокол автономних систем. Сучасні маршрутизатори та їх основні характеристики. Пристрої Cisco. Пристрої Juniper. Пристрої D-link.

Адміністрування комп’ютерних мереж. Пристрої віртуальних приватних мереж. Принципи VPN. Програмні VPN. Апаратні VPN.

Безпека комп’ютерних мереж. Проблеми і категорії безпеки мереж. Методи несанкціонованого доступу до інформації та мереж. Захист від атак. Криптографічні засоби захисту. Основні засоби та стратегії захисту комп'ютерних мереж. Фільтрація пакетів і протоків. Міжмережний екран. Асиметричний трафік. Детектування атак.

2.5 Тематичні положення з управління інформаційною безпекою.

Система управління інформаційною безпекою (СУІБ) в Україні. Основні положення СУІБ. Діяльність міжнародних організацій в сфері інформаційної безпеки. Робота міжнародних професіональних об’єднань в сфері стандартизації СУІБ. Визначення поняття інформаційної безпеки та кібербезпеки.

Основні напрями розвитку менеджменту в сфері інформаційної безпеки. Норми та стандарти інформаційної та кібербезпеки. Вимоги щодо стандартів СУІБ та їх класифікація. Загальний огляд стандартів системи СУІБ. Роль стандартів серії ISO 270xx у сфері СУІБ. Визначення атрибутів та властивостей інформаційної безпеки. Модель інформаційної безпеки: КЦД.

Інформаційні ресурси підприємства. Загальна класифікація. Загрози інформаційним ресурсам та їх класифікація. Загальна процедура реалізації

загроз. Уразливість інформації та критичність послуг. Поняття моделі загроз. Атака на інформаційні ресурси та її наслідки. Модель PDCA СУІБ. Загальні поняття щодо політики інформаційної безпеки. Інформаційна та кібербезпека інформаційно-комунікаційних систем та бізнес процесів підприємства.

Ризики та їх класифікація. Поняття управління ризиками в сфері інформаційної безпеки. Дії з ризиками у сфері інформаційної безпеки. Поняття моделі порушника. Способи порушення інформаційної безпеки.

Класифікація забезпечення інформаційної безпеки підприємства. Нормативно-правове забезпечення інформаційної безпеки. Організаційне забезпечення інформаційної безпеки. Технічне забезпечення інформаційної безпеки. Методи та засоби захисту інформаційних ресурсів. Система аудиту СУІБ. Контроль та моніторинг стану СУІБ. Введення в дію СУІБ на підприємстві.

2.6. Тематичні положення з розробки та впровадження комплексних систем захисту інформації.

Галузь використання КСЗІ згідно чинного законодавства України. Нормативно-правове забезпечення створення, введення та експлуатації ЗЗІ та КСЗІ. Визначення та термінологія в сфері КСЗІ. Мета та задачі розробки КСЗІ. Загальні положення створення та експлуатації КСЗІ. Дозвільна діяльність в сфері ТЗІ та КЗІ в Україні.

Етапи створення КСЗІ. Складові, порядок, задачі, функції. Формування загальних вимог до КСЗІ в ІТС. Обґрунтування необхідності створення КСЗІ. Перелік інформації, що підлягає автоматизованому обробленню в ІТС та потребує захисту. Опис інформаційних ресурсів ІТС. Вибір варіанту КСЗІ. Функціональні та структурно-логічні схеми побудови КСЗІ.

Послуги інформаційної системи та КСЗІ. Види, функції , задачі. Положення про службу захисту інформації в ІТС. Опис політики безпеки інформації в ІТС. Опис моделі порушника безпеки інформації в ІТС. Опис моделі загроз для інформації, оброблюваної в ІТС.

Структура звіту за результатами аудита безпеки ІС й аналізу ризиків. Формування цілей та завдання на створення КСЗ. Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ. Загальні положення. План захисту інформації в ІТС. Складові та завдання.

Проектна документація КСЗІ. Робочий проект КСЗІ. Складові та задачі. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС. Навчання персоналу та користувачів. Комплектування КСЗІ.

Державна експертиза КСЗІ. Аудит безпеки інформаційних систем. Порядок проведення робіт з експертизи комплексних систем захисту інформації.

Експлуатаційна документація компонентів (складових частин) КЗЗ КСЗІ. Інструкції щодо забезпечення правил оброблення ІзОД в ІТС. Інструкції про порядок використання засобів КЗІ.

Рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи комплексної системи захисту інформації.

3. Специфікація фахового випробування з управління інформаційною безпекою.

3.1. Академія проводить фахове вступного випробування з управління інформаційною безпекою у письмовій формі із використанням технологій тестування.

Кожному вступникові надається екзаменаційний білет, що містить п’ять тестових питань, що передбачають вибір правильної відповіді із трьох запропонованих та одне питання для самостійного письмового викладу його змісту. Питання надаються відповідно до обсягу навчального матеріалу, визначеного в пункті 2 цієї Програми. Зміст відповіді вступник фіксує на виданих йому аркушах встановленого зразка, які після закінчення випробування передає секретарю комісії.

3.2. Результати фахового випробування оцінюються за 200-бальною шкалою шляхом додавання результатів відповідей на тестові запитання (по 20 балів за кожну правильну відповідь) та оцінки комісією рівня відповіді на питання для самостійного письмового викладу за шкалою від 1 до 100 балів. Мінімальний бал із фахового випробування з правових основ захисту інформації з обмеженим доступом, з яким вступник допускається до подальшої участі в конкурсному відборі для зарахування на навчання, складає 100 (сто) балів.

Відповідь вступників на питання для самостійного письмового викладу оцінюються комісією на підставі таких критеріїв:

Бали	Критерії оцінювання
1-10	Вступник може на рівні «так-ні» відтворити кілька термінів з обсягу питання, обрати правильний варіант відповіді з двох запропонованих.
11-20	Вступник може двома-трьома простими реченнями передати основний зміст питання, має про нього загальне уявлення.
21-30	Вступник може, відтворити більшу частину основного змісту питання, дати визначення поняття.
31-40	Вступник може: відтворити основний зміст питання, визначити поняття й охарактеризувати його окремі ознаки
41-50	Вступник може: самостійно викласти матеріал основного змісту питання, застосовуючи необхідну термінологію; дати визначення понять; підтвердити одним, двома аргументами висловлене ним оцінювальне судження.
51-60	Вступник володіє матеріалом змісту питання і використовує знання за аналогією, може порівнювати, узагальнювати, систематизувати інформацію.
61-70	Вступник вільно оперує матеріалом змісту питання, узагальнює та аналізує окремі визначення та принципи, формулює висновки та обґрунтовує їх конкретними аргументами.
71-80	Вступник вільно викладає зміст питання, застосовуючи необхідну термінологію та нормативно-правову базу, робить аргументовані висновки.
81-90	Вступник може вільно викладати власні судження й переконливо їх аргументувати, самостійно аналізує положення чинного законодавства, які стосуються питання.
91-100	Вступник володіє глибокими й міцними знаннями, дає ґрунтовну відповідь на поставлене питання, викладає власну позицію і переконливо її аргументує, критично оцінює зміст нормативних актів, що стосуються питання, вміє узагальнити поданий матеріал.

3.3.Оцінка відповіді вступника проводиться згідно із зазначеними у п. 3.2 цієї Програми критеріями оцінювання не менше ніж двома членами комісії, які виносять результати оцінки відповіді на загальне обговорення. Оцінки за результатами фахового випробування виставляються за результатами їх загального обговорення на засіданні фахової атестаційної комісії, що скликається після перевірки усіх письмових робіт.

Результати фахового випробування фіксуються у відомості складання вступного випробування та оголошуються вступникам не пізніше наступного дня після проведення вступного випробування.

3.4. Вступникам під час випробування забороняється користуватись електронними засобами, підручниками, навчальними посібниками та іншими матеріалами, якщо це не передбачено рішенням Приймальної комісії.

У разі використання вступником під час фахового випробування сторонніх джерел інформації він відсторонюється від подальшого складання випробування та участі в конкурсному відборі, про що складається акт.

Перескладання фахового випробування не дозволяється.

Апеляції на результати випробування розглядає апеляційна комісія Академії у порядку, визначеному Правилами прийому.

4. Акти законодавства України, що зазначені в Програмі, слід вивчати за їх текстами в останній редакції, що міститься на сайті Верховної Ради України (www.rada.gov.ua)