**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

ПОГОДЖЕНО
Заступник Голови Державної служби спеціального зв'язку та захисту інформації України
_____ Петро ОПАЛЕНИК
«06» 02 2020 р.

ЗАТВЕРДЖУЮ
Ректор Державного університету телекомунікацій
_____ В.Б.Толубко
«__» _____ 2019р.

# ОСВІТНЯ ПРОГРАМА КУРСІВ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

## «Системи технічного захисту інформації»

**Галузь знань** **12 «Інформаційні технології»**
**Спеціальність** **125 «Кібербезпека»**

СХВАЛЕНО
На засіданні Вченої Ради
Державного університету
телекомунікацій
протокол №__10____
від «_02_»___грудня____ 2019р.

Київ - 2019

# ПЕРЕДМОВА

Розроблено проектною групою Навчально-наукового інституту захисту інформації Державного університету телекомунікацій (склад проектної групи затверджено наказом ректора університету № 525 від 19.11.2019 р.) у складі:

**Керівник – Савченко Віталій Анатолійович** – директор Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, доктор технічних наук з спеціальності 122 Комп'ютерні науки та інформаційні технології (05.13.06 - інформаційні технології), професор за кафедрою Систем інформаційного та кібернетичного захисту.

**Члени проектної групи:**

**Шуклін Герман Вікторович** – завідувач кафедри Систем інформаційного та кібернетичного захисту Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, кандидат технічних наук зі спеціальності 125 Кібербезпека (спеціальність 05.03.01 інформаційна безпека держави).

**Киричок Роман Васильович** – асистент кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету

# ПОЯСНЮВАЛЬНА ЗАПИСКА

Курсів підвищення кваліфікації "Системи технічного захисту інформації" призначені для підвищення кваліфікації фахівців у галузі інформаційної та кібербезпеки.

Освітня програма курсів підвищення кваліфікації "Системи технічного захисту інформації" (далі – Освітня програма) визначає зміст і об'єм знань, вмінь та навичок, що мають засвоюватися слухачами на курсах підвищення кваліфікації "Системи технічного захисту інформації".

Освітня програма ґрунтується на положеннях Законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про ліцензування видів господарської діяльності", Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 року № 1229, Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373, Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518.

Освітня програма відповідає Державному стандарту вищої освіти спеціальності 125 Кібербезпека, затвердженому наказом Міністерства освіти і науки України від 12.12.2018 № 1382, та забезпечує набуття слухачами курсів таких компетентностей:

Загальні компетентності:

**КЗ 1.** Здатність застосовувати знання у практичних ситуаціях.

**КЗ 2.** Знання та розуміння предметної області та розуміння професії.

Професійні компетентності за спеціальністю (ПК):

**КФ 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.

**КФ 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

**КФ 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та інш.).

**КФ 10.** Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

**КФ 12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.

Тривалість курсів підвищення кваліфікації "Системи технічного захисту інформації" за Освітньою програмою складає 120 годин (60 аудиторних та 60 самостійної роботи).

Освітньою програмою передбачено підвищення знань з питань:

вимог та порядку захисту інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності;

порядку оцінювання захищеності інформації;

вимог до кіберзахисту об'єктів критичної інфраструктури;

способів виявлення закладних пристроїв.

Освітньою програмою передбачено вдосконалення вмінь та навичок щодо:

захисту інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності;

оцінювання захищеності інформації;

виявлення закладних пристроїв;

кіберзахисту об'єктів критичної інфраструктури.

Освітня програма реалізується шляхом проведення лекційних і практичних занять з використанням засобів технічного захисту інформації, самостійного опрацювання запропонованої літератури. Більша частина навчального процесу відведена для вдосконалення практичних вмінь та навичок за темами, що вивчаються, та закріплення під час самостійної роботи слухачів.

Залежно від конкретних умов допускається зміна послідовності вивчення окремих тем та їх тривалості у межах тривалості курсів підвищення кваліфікації "Системи технічного захисту інформації".

На основі Освітньої програми розробляються робочі навчальні програми та навчально-тематичні плани для конкретних напрямів навчання, до яких входять окремі розділи Освітньої програми.

Освітня програма навчання з курсу "Системи технічного захисту інформації" розрахована на слухачів з вищою інженерно-технічною освітою.

Заняття проводять висококваліфіковані викладачі Державного університету телекомунікацій за авторськими методиками навчання.

Після закінчення навчання слухачі складають екзамен.

Слухачі, які пройшли навчання і успішно склали екзамен, отримують свідоцтво про підвищення кваліфікації встановленого зразка.

**ТЕМАТИЧНИЙ ПЛАН**
**курсів підвищення кваліфікації**
**«Системи технічного захисту інформації»**

| № з/п | Найменування тем | Всього годин | Лекції | Практичні заняття | Примітка |
|---|---|---|---|---|---|
| 1 | **Цикл фахової підготовки** | | | | |
| 1.1 | Нормативно-правове забезпечення інформаційної та кібербезпеки | 6 | 2 | 4 | |
| 1.2 | Організація захисту інформації в ІТС | 2 | 2 | | |
| 1.3 | Захист інформації в ІТС від витоку технічними каналами | 6 | 2 | 4 | |
| 1.4 | Захист інформації в ІТС від несанкціонованих дій | 8 | 2 | 6 | |
| 1.5 | Створення комплексних систем захисту інформації в ІТС | 10 | 4 | 6 | |
| 1.6 | Захист інформації, що озвучується на ОІД. Виявлення закладних пристроїв | 6 | 2 | 4 | |
| 1.7 | Державна експертиза технічних і програмних засобів ТЗІ та ОТР на розгортання типової складової компоненти КСЗІ в ІТС | 2 | 2 | | |
| 1.8 | Захист інформації WEB сторінки від НСД | 2 | 2 | | |
| 1.9 | Міжмережеві екрани | 4 | 2 | 2 | |
| 1.10 | Система управління інформаційною безпекою підприємства | 4 | 2 | 2 | |
| 1.11 | Організація кіберзахисту об'єктів критичної інфраструктури | 4 | 2 | 2 | |
| | | | | | |
| 2 | Консультація | 2 | 2 | | |
| 3 | Екзамен | 4 | 4 | | |
| | | **60** | **30** | **30** | **-** |

# І. ЗМІСТ ПРОГРАМИ

## 1. Цикл фахової підготовки

### 1.1. Нормативно-правове забезпечення інформаційної та кібербезпеки

Поняття інформації. Інформація з обмеженим доступом. Порядок поводження з інформацією з обмеженим доступом та матеріальними носіями інформації з обмеженим доступом. Система управління діловодством в Україні. Документ. Електронний документ та електронний документообіг.

Законодавство України у сфері інформаційної та кібербезпеки (основні законодавчі та нормативно-правові акти, що регламентують захист інформації в інформаційно-телекомунікаційних системах (далі – ІТС) та на об'єктах інформаційної діяльності (далі – ОІД) та кіберзахист об'єктів критичної інфраструктури). Нормативні документи у сфері технічного захисту інформації (далі –НД ТЗІ). Вимоги законодавства України щодо захисту інформації в ІТС та на ОІД та кіберзахисту об'єктів критичної інфраструктури.

Охорона та захист об'єктів, де здійснюється обіг інформації з обмеженим доступом.

Ліцензування діяльності в галузі технічного захисту інформації ТЗІ.

Порядок здійснення контролю за дотриманням ліцензійних умов.

Міжнародні стандарти та стандарти розвинених країн світу з питань управління інформаційної безпекою (Європа, США, Великобританія). Основні положення стандартів серії ISO/IEC 27k, ISO/IEC 15408, NIST США, Cobit, ITIL.

### 1.2. Організація захисту інформації в ІТС

Класифікація автоматизованих систем (АС).

Інформація, що підлягає захисту в ІТС.

Організаційні засади забезпечення захисту інформації в ІТС. Комплексні системи захисту інформації (КСЗІ). Призначення та склад КСЗІ. Суб'єкти та об'єкти КСЗІ.

### 1.3. Захист інформації в ІТС від витоку технічними каналами

Поняття та загальна характеристика технічних каналів витоку (ТКВ) інформації, що обробляється в ІТС. Причини виникнення ТКВ інформації, що обробляється в ІТС.

Побічні електромагнітні випромінювання та наведення (ПЕМВН) засобів обчислювальної техніки. Фізичні основи утворення ПЕМВН. Утворення каналів побічних електромагнітних випромінювань. Утворення каналів побічних електромагнітних наведень на лінії електроживлення, заземлення, передачі даних, зв'язку.

Витік інформації, що обробляється в ІТС, мережами живлення та колами заземлення. Причини витоку інформації мережею живлення. Причини витоку інформації колами заземлення.

Комплекси технічного захисту інформації, що обробляється в ІТС, від витоку каналами ПЕМВН.

Способи (методи) захисту інформації, що обробляється в ІТС, від витоку технічними каналами (пасивні, активні).

Засоби технічного захисту інформації. Вимоги до засобів ТЗІ.

Засоби виявлення ТКВ інформації (індикатори електромагнітних випромінювань, широкосмугові (панорамні) радіоприймальні пристрої, автоматизовані пошукові комплекси та інш.). Принципи роботи та характеристики засобів виявлення ТКВ. Заходи з виявлення ТКВ інформації.

### 1.4. Захист інформації в ІТС від несанкціонованих дій

Поняття та види несанкціонованих дій (НСД) з інформацією, що обробляється в ІТС. Об'єкти загроз інформації, що обробляється в ІТС, від НСД.

Поняття несанкціонованого доступу до інформації в ІТС.

Профілі захищеності інформації від несанкціонованого доступу до інформації в ІТС.

Програмні засоби (механізми) захисту інформації, що обробляється в ІТС, від НСД.

#### 1.4.1. Механізми авторизації (автентифікації) користувачів в ІТС

Загальна характеристика методів ідентифікації та автентифікації користувачів. Вимоги до ідентифікації та автентифікації користувачів. Парольні методи захисту. Принципи побудови протоколів посиленої автентифікації та вимоги до них. Протоколи автентифікації з використанням симетричних механізмів. Принципи використання несиметричних механізмів. Автентифікація повідомлень на основі цифрового підпису. Сертифікати відкритих ключів в несиметричних криптосистемах. Протоколи автентифікації з використанням несиметричних механізмів.

#### 1.4.2. Управління доступом користувачів до ресурсів ІТС

Вимоги до механізмів доступу. Довірче управління доступом. Адміністративне управління доступом. Загальні механізми та методи забезпечення цілісності інформації в системі. Методи забезпечення цілісності інформації при міжмережевій взаємодії. Методи забезпечення цілісності програмних засобів.

#### 1.4.3. Механізми та засоби захисту операційних систем

Механізми захисту операційних систем сімейства Windows та UNIX. Організація та методи захисту локальних робочих станцій (ЛРС) та локальних обчислювальних мереж (ЛОМ). Програмно-апаратні засоби захисту (ПАЗЗ) інформації, що обробляється в ІТС. Характеристики сучасних ПАЗЗ (Лоза-1, Лоза-2, Гриф, DLP). Організація захисту від програм з потенційно-небезпечними впливами (ППНВ). Класифікація та принципи дії ППНВ. Принципи роботи антивірусних засобів. Системи резервного копіювання інформації (повне, incremental та differential копіювання). Забезпечення безпеки інформації при резервному копіюванні.

### 1.5. Створення комплексних систем захисту інформації в ІТС

Етапи створення КСЗІ.

Категоріювання об'єктів електронно-обчислювальної техніки.

Обстеження середовищ функціонування ІТС. Порядок визначення загроз інформації, оформлення моделі загроз інформації та моделі порушника.

Розробка та оформлення політики безпеки інформації в ІТС. План захисту інформації. Розробка та оформлення технічного завдання (ТЗ) на створення КСЗІ, зміст розділів ТЗ на створення КСЗІ.

Ескізний, технічний, робочій (техно-робочій) проекти КСЗІ.

Впровадження (інсталяція, актуалізація) комплексу засобів захисту від НСД.

Впровадження комплексу технічного захисту інформації, що обробляється в ІТС (у разі обробки інформації, що становить державну таємницю).

Порядок введення ІТС в експлуатацію. Попередні випробування. Дослідна експлуатація. Оцінювання захищеності інформації, що обробляється в ІТС: державна експертиза КСЗІ. Введення ІТС в експлуатацію.

Порядок організації та проведення державної експертизи КСЗІ. Особливості проведення державної експертизи КСЗІ шляхом експертних випробувань та шляхом аналізу декларацій.

Служба захисту інформації (СЗІ) в ІТС. Призначення та структура СЗІ. Завдання та функції СЗІ. Порядок організації робіт СЗІ.

### 1.6. Захист інформації, що озвучується на ОІД. Виявлення закладних пристроїв

Організація захисту інформації, що озвучується на ОІД: інформація, що підлягає захисту на ОІД, організаційні засади забезпечення захисту інформації, що озвучується на ОІД.

Поняття та загальна характеристика технічних каналів витоку інформації, що озвучується на ОІД.

Технічні канали витоку мовної інформації через закладні пристрої.

Засоби перехоплення акустичної інформації. Закладні пристрої (ЗП). Класифікація та основні технічні характеристики ЗП. Демаскуючі ознаки ЗП.

Способи (методи) захисту інформації, що озвучується на ОІД, від витоку технічними каналами (пасивні, активні).

Принципи роботи та характеристики засобів виявлення ТКВ інформації через закладні пристрої (індикатори поля, широкосмугові (панорамні) радіоприймальні пристрої, автоматизовані пошукові комплекси, локатори нелінійностей, та інш.).

Проведення пошукових дій щодо виявлення ТКВ інформації через закладні пристрої, оформлення акта проведення робіт з виявлення ЗП на ОІД.

Комплекси технічного захисту мовної інформації. Етапи створення комплексів ТЗІ: категоріювання ОІД, обстеження ОІД, визначення загроз інформації та розробка моделі загроз інформації від витоку технічними

каналами, розробка технічного завдання на створення комплексу ТЗІ, розробка технічного проєкту комплексу ТЗІ, впровадження комплексу ТЗІ.

Оцінювання захищеності інформації, що озвучується на ОІД: атестація комплексів ТЗІ.

### 1.7. Державна експертиза технічних і програмних засобів ТЗІ та ОТР

Організація та порядок проведення державної експертизи у сфері ТЗІ технічних та програмних засобів захисту інформації та організаційно-технічних рішень (ОТР) на розгортання типової складової компоненти КСЗІ в ІТС.

### 1.8. Захист інформації WEB сторінки від НСД

Вимоги нормативних документів щодо захисту інформації WEB-сторінки від несанкціонованого доступу. Послуги безпеки, що використовуються для захисту інформації WEB-сторінки. Створення системи захисту. Оцінювання якості системи захисту інформації WEB- сторінки.

### 1.9. Міжмережеві екрани

Міжмережеві екрани: призначення, класифікація, принципи дії, рекомендації щодо використання. Файерволи: види, особливості застосування в комп'ютерних мережах.

### 1.10. Система управління інформаційною безпекою підприємства

Система управління інформаційною безпекою (СУІБ): поняття, склад, призначення. Методика формування нормативних, розпорядчих та методичних документів в процесі впровадження та функціонування СУІБ. Організаційна структура служби інформаційної безпеки. Варіанти оброблення ризиків. Вибір методу оброблення ризиків. Програмна підтримка аналізу ризиків. Оцінка відповідності СУІБ своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.

### 1.11. Організація кіберзахисту об'єктів критичної інфраструктури

Поняття об'єктів критичної інфраструктури. Інформація, що підлягає захисту на об'єктах критичної інфраструктури.

Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки. Управління доступом користувачів до об'єктів захисту об'єкта критичної інфраструктури. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури. Реєстрація подій компонентами об'єкта критичної інфраструктури та їх періодичний аудит. Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інфраструктури. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інфраструктури. Визначення умов використання (та оновлення) програмного та апаратного забезпечення об'єкта критичної інфраструктури.

## ПИТАННЯ ДО ЕКЗАМЕНУ

1. Дайте визначення правової основи захисту інформації?
2. Розкрийте поняття «інформаційна безпека»?
3. Що становить правову основу технічного захисту інформації в Україні та ким реалізується державна політика з технічного захисту інформації?
4. Які основні завдання покладаються на органи, щодо яких здійснюється ТЗІ?
5. Дайте визначення організаційних засобів захисту інформації?
6. Який порядок створення системи захисту від несанкціонованого доступу?
7. Що регулює Закон України «Про основні засади забезпечення кібербезпеки України»?
8. Що регулює Закон України «Про інформацію»
9. Що регулює Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»?
10. Що встановлює Закон України «Про електронні документи та електронний документообіг»?
11. Для чого необхідні стандарти інформаційної безпеки?
12. За якими чинниками класифікують інформацію з обмеженим доступом (приклади)?
13. Що повинні забезпечувати системи зберігання інформації та що є загальною вимогою для процесу поширення інформації?
14. Розкрийте поняття «інформація», «автоматизована система» та «інформаційна система»?
15. Які розрізняють правові режими, використання поширюваної інформації?
16. Розкрийте поняття «інформаційний ресурс», що відносять до інформаційних ресурсів, де вони можуть бути створені і чим регулюються?
17. Як поділяється інформація за режимом доступу? Класифікація та характеристика?
18. Розкрийте порядок визначення вищого ступеня обмеження доступу до інформації, яка циркулює на об'єктах інформаційної діяльності?
19. Яким чином (шляхом) здійснюється оцінювання захищеності інформації?
20. Роз'ясніть порядок отримання ліцензії на право провадження господарської діяльності у галузі ТЗІ?
21. Що таке служба захисту інформації і для чого вона створюється?
22. Яка структура, склад та основні завдання служби захисту інформації?
23. Які використовуються організаційно-технічні заходи захисту інформації від несанкціонованого доступу?
24. Що повинен містити план захисту інформації?
25. Що включає в себе перелік обов'язкових робіт під час проектування, впровадження та експлуатації систем і засобів захисту інформації на ОІД?
26. Які існують основні підходи до побудови моделі зловмисника?

27. З яких етапів складається ТЗІ та який зміст і послідовність робіт з протидії загрозам або їхньої нейтралізації?

28. З якою метою здійснюється обстеження підприємства та що є підставою для складання технічного завдання на розроблення системи захисту інформації?

29. Який порядок розроблення моделі загроз інформації при створенні комплексу технічного захисту інформації на ОІД?

30. Який порядок оформлення та побудова моделі загроз інформації при створенні комплексу технічного захисту інформації на ОІД?

31. Який порядок розроблення технічного завдання на створення комплексу ТЗІ?

32. Який порядок оформлення технічного завдання на створення комплексу ТЗІ?

33. Які використовуються технічні засоби захисту інформації від несанкціонованого доступу?

34. Провести аналіз методів та моделей (що для них є вхідними та вихідними параметрами, переваги і недоліки, основний принцип функціонування) оцінки рівня загроз інформації на ОІД.

35. Провести аналіз програмного забезпечення (що для нього є вхідними та вихідними параметрами, переваги і недоліки, основний принцип функціонування) призначеного для оцінки стану безпеки.

36. Які вимоги висуваються до оформлення протоколів, актів атестації та опишіть порядок їх складання?

37. З якою метою розробляється паспорт на комплекс ТЗІ, паспорти на приміщення, де озвучується та/або обробляється технічними засобами інформація з обмеженим доступом?

38. Який порядок заповнення паспорту на комплекс ТЗІ, паспортів на приміщення, де озвучується та/або обробляється технічними засобами інформація з обмеженим доступом?

39. Які існують правила розмежування доступу до інформації?

40. Яким чином здійснюється оцінка ризику як основної причини розмежування доступу до інформації?

41. Які дії повинні виконуватись службою безпеки при порушенні правил розмежування доступу до інформації?

42. Провести аналіз (вхідні та вихідні параметри, основний принцип функціонування, переваги і недоліки) сучасних засобів (методів, моделей, програмного забезпечення) виявлення атак на ресурси інформаційних систем.

43. Визначить і опишіть загрози АС класу 1 та сформуйте комплекс організаційних засобів для їх блокування.

44. Визначить і опишіть загрози АС класу 2 та сформуйте комплекс організаційних засобів для їх блокування.

45. Визначить і опишіть загрози АС класу 3 та сформуйте комплекс організаційних засобів для їх блокування.

46. Провести аналіз (вхідні та вихідні параметри, основний принцип функціонування, переваги і недоліки) сучасних засобів (методів, моделей, програмного забезпечення) реалізації атак на ресурси інформаційних систем.

47. Провести аналіз методів та моделей (що для них є вхідними та вихідними параметрами, переваги і недоліки, основний принцип функціонування) оцінки стану безпеки на ОІД.

48. Який порядок проведення атестації режимних територій (приміщень, зон)?

49. Які принципи охорони об'єктів та задачі захисту стаціонарних (мобільних) об'єктів?

50. Які використовуються засоби захисту стаціонарних (мобільних) об'єктів від несанкціонованого доступу, пожежі?

51. Яким чином організовується санкціонований доступ на ОІД?

52. Який порядок розбиття ОІД на зони безпеки?

53. Яким чином забезпечується фізичний захист стаціонарних (мобільних) об'єктів?

54. Яким чином здійснюється обладнання ОІД системами тривожної сигналізації, сповіщувачами системи охоронної та пожежної сигналізації?

55. Який склад та призначення систем телевізійного спостереження?

56. Яким чином здійснюється вибір засобів відбиття (нейтралізації) загроз?

57. Яким чином здійснюється вибір технічних засобів захисту периметра території об'єкта?

58. Яким чином здійснюється вибір технічних засобів захисту периметра будівлі?

59. Яким чином здійснюється вибір технічних засобів захисту для представницької зони будівлі?

60. Яким чином здійснюється вибір технічних засобів захисту для зони кабінетів і особливо важливих приміщень?

61. Яким чином здійснюється вибір технічних засобів захисту для зони сеймового приміщення, банку даних і зберігання цінностей?

62. Які існують засоби контролю доступу за пропускними документами?

63. Яким чином здійснюється контроль доступу за ідентифікаційними картами?

64. Які організаційні заходи із захисту інформації з обмеженим доступом вживаються в процесі виготовлення, обробки та передачі (транспортування) її носіїв?

65. Що означає у сучасній українській мові слово документ, електронний документ?

66. Яким вимогам відповідає система управління вітчизняного діловодства?

67. Вкажіть порядок обліку паперових і магнітних носіїв інформації з грифом "Для службового користування"?

68. Чим необхідно керуватися під час розробки картки автоматизованої реєстрації документів?

69. Які заходи включає контроль за виконанням документів?

70. Вкажіть перевірки, які виконуються щоденно, при прийманні та обробці документів з обмеженим доступом?

71. Що є базовим підходом до визначення підстав для віднесення відомостей до категорії конфіденційної інформації для фізичних осіб?

72. Що є базовим підходом до визначення підстав для віднесення відомостей до категорії конфіденційної інформації для юридичних осіб?

73. Які існують основні групи вимог до системи безпеки конфіденційного електронного документообігу?

74. Яким чином інформація з обмеженим доступом може бути отримана порушником?

75. Які існують штучні передбачені загрози інформаційної системи?

76. Які існують непередбачені штучні загрози інформаційної системи?

77. Вкажіть підходи виявлення загроз безпеки інформації (виявлені уразливих місць) в інформаційних системах з погляду еталонної моделі взаємозв'язку відкритих систем?

78. Як можливо класифікувати порушників інформаційних систем?

79. Провести аналіз законодавчого та нормативно-правового забезпечення, щодо наступних понять пов'язаних з інформацією обмеженого доступу: адвокатська таємниця, лікарська таємниця, таємниця голосування, таємниця наради суддів, таємниця телефонних розмов, комерційна таємниця, таємниця слідства.

80. Провести аналіз законодавчого та нормативно-правового забезпечення, щодо наступних понять пов'язаних з інформацією обмеженого доступу: таємниця заповіту, таємниця про стан здоров'я, банківська таємниця, професійна таємниця, таємниця кореспонденції, військова таємниця,службова таємниця.

81. Провести аналіз законодавчого та нормативно-правового забезпечення, щодо наступних понять пов'язаних з інформацією обмеженого доступу: таємниця нотаріальних дій, таємниця усиновлення, таємниця слідства, таємниця псевдоніму, військова таємниця,адвокатська таємниця, професійна таємниця.

82. Провести аналіз законодавчого та нормативно-правового забезпечення, щодо наступних понять пов'язаних з інформацією обмеженого доступу: комерційна таємниця, службова таємниця, таємниця листування, таємниця страхування, таємниця внесків (рахунків), банківська таємниця, таємниця інформації у поштовому зв'язку.

83. Яким чином визначається факт порушення конфіденційності інформації?

84. Які організаційні заходи вживаються під час проведення навчання співробітників, що допускаються до інформації з обмеженим доступом?

85. Яким чином оформляються факти додержання чи порушення конфіденційності інформації?

86. Які існують системи захисту Web-ресурсів від НСД?

87. Програмні засоби ТЗІ. Призначення та технічні характеристики.

88. Портативний скануючий приймач AR 8200. Призначення та технічні характеристики.

89. Пошукова система DigiSkan EX. Призначення та технічні характеристики.

90. Скануючий приймач IC-R2500. Призначення та технічні характеристики.

91. Багатофункціональний пошуковий прилад ST-032. Призначення та технічні характеристики.

92. Портативний високочастотний цифровий детектор PROTECT-1206i. Призначення та технічні характеристики.

93. Персональний детектор поля PROTECT-1210. Призначення та технічні характеристики.

94. Локатор нелінійностей NR-900 EM. Призначення та технічні характеристики.

95. Портативний скануючий приймач IC-R20. Призначення та технічні характеристики.

96. Поняття об'єктів критичної інфраструктури.

97. Інформація, що підлягає захисту на об'єктах критичної інфраструктури.

98. Поняття системи інформаційної безпеки об'єкта критичної інфраструктури.

99. Поняття політики інформаційної безпеки об'єкта критичної інфраструктури.

100. Шляхи кіберзахисту об'єкта критичної інфраструктури.

101. Зміст та порядок формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

102. Управління доступом користувачів до об'єктів захисту об'єкта критичної інфраструктури.

103. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури.

104. Реєстрація подій компонентами об'єкта критичної інфраструктури та їх періодичний аудит.

105. Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інфраструктури.

106. Зміст та порядок визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інфраструктури.

107. Зміст та порядок визначення умов використання (та оновлення) програмного та апаратного забезпечення об'єкта критичної інфраструктури.

## КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ І ВМІНЬ СЛУХАЧІВ

В університеті розроблено критерії оцінювання знань і вмінь слухачів, які пройшли курси підвищення кваліфікації відповідного напряму підготовки. Використовується наступна шкала рейтингових показників та оцінок:

**Інтегральна шкала оцінювання**

| Рейтинговий показник | Оцінка у національній шкалі | Оцінка ECTS |
|---|---|---|
| 90-100 | 5 (відмінно) | A (відмінно) |
| 82-89 | 4 (добре) | B (добре) |
| 74-81 | | C (добре) |
| 64-73 | 3 (задовільно) | D (задовільно) |
| 60-63 | | E (задовільно) |
| 35-59 | 2 (незадовільно) | FX (незадовільно) з можливістю повторного складання |
| 1-34 | - | F (незадовільно) з обов'язковим повторним вивченням |

**«A» (90-100)** – Слухач виявляє особисті творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування й нахили.

**«B» (82-89)** – Слухач вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.

**«C» (74-81)** – Слухач вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.

**«D» (64-73)** – Слухач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих

**«E» (60-63)** – Слухач володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.

**«FX» (35-59)** – Слухач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

**«F» (1-34)** – Слухач володіє матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів,елементів, обєктів.

При оцінюванні знань і вмінь слухачів увага звертається передусім на:

уміння слухача визначати найсуттєвіші проблемні питання, що потребують концептуального вирішення;

наявність нестандартних елементів аналізу та діагностики;

різноманітність використаних способів зіставлення інформації;

здатність слухача до комбінування та рекомбінування вихідної інформації;

глибину опрацювання проблеми;

адекватність запропонованих заходів виявленим проблемам;

наявність чітко визначеної позиції автора;

аргументованість, переконливість обґрунтування запропонованих рішень;

уміння слухача стисло, послідовно і чітко викласти сутність і результати своїх пропозицій;

розвиненість мови, оригінальність стилю;

наявність посилань на джерела, з яких запозичено будь-яку інформацію, та дотримання етики цитування;

логічність, конкретність і переконливість та повноту відповідей на запитання;

здатність аргументовано захищати свої пропозиції, думки, погляди;

вільне володіння економічною та управлінською термінологією;

загальний рівень підготовки слухача та рівень практичної підготовки . слухача відповідно до кваліфікаційних вимог програми підвищення кваліфікації.

## ІІ. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

*а) основна література:*


1. Закон України "Про інформацію". https://zakon.rada.gov.ua/laws/main/2657-12
2. Закон України "Про доступ до публічної інформації".
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. Закон України "Про основні засади забезпечення кібербезпеки України". https://zakon.rada.gov.ua/laws/main/2163-19
5. Закон України "Про електронні документи та електронний документообіг". https://zakon.rada.gov.ua/laws/show/851-15
6. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF
7. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12.04.2002 р. № 522.
8. Постанова Кабінету Міністрів України "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних" від 04.02.1998 № 121. https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF
9. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.
10. Постанова Кабінету Міністрів України "Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію" від 19 жовтня 2016 р. № 736.
11. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення.
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
12. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
13. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. https://zakon.rada.gov.ua/rada/show/v0215519-13
14. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920

15. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=89740&cat_id=89734&ctime=1547204009788

16. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

17. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

18. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

19. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342

20. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1). http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

21. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2". http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343

22. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344

23. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. http://www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid=103253

24. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46075

25. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

26. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101924&cat_id=89734&ctime=1344501363205

27. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id=89734&ctime=1344500065981

28. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=120206&cat_id=89769&ctime=1421836194327

29. ДСТУ ISO/IEC 27001: 2015 Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001: 2013, IDT).

30. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).

31. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).

32. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27.09.1999 № 1229.

33. Бурячок В.Л., Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Посібник. – К. : ДУТ. – КНУ, 2016. – 178 с.

34. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник. – К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

35. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підручник. К. ДУІКТ, 2010. – 316 с.

36. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков — «Издательские решения», 2018. – 249 с.

37. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

38. Хорошко В.О., Азаров О.Д., Максименко Г.О., Яремчук Ю.Є. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник. – Вінниця: ВНТУ, 2007. – 333 с.

39. Технічний захист інформації в інформаційних та телекомунікаційних системах: навч. посібн. / Г.І. Ластівка, П.М. Шпатар // – Чернівці, ЧНУ, 2018. – 252 с.

*б) додаткова література:*

1. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.

2. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.

4. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

5. Кукаркін О.Б. Електронний документообіг та захист інформації: навч. посіб. // – К.: НАДУ, 2015. – 84 с.

6. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с.

7. Захист інформаційних ресурсів: навчально-методичний посібник до курсу "Захист інформаційних ресурсів" / укл. С. О. Троян. – Умань : [б.в.], 2012.-120 с.

8. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации – Москва: Горячая Линия, 2010. – 48 с.

9. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие для вузов. – Москва: Горячая Линия, 2016. – 166 с.

**Керівник проектної групи**
Директор Навчально-наукового інституту захисту інформації
Державного університету телекомунікацій

В.А. Савченко