МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою Національного
аерокосмічного університету
«Харківський авіаційний інститут»
«24» грудня 2025 р., протокол № 5

ОСВІТНЯ ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

ПРОВІДНИЙ ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

галузі знань: F «Інформаційні технології»
назва відповідно до ліцензії

спеціальність: F5 «Кібербезпека та захист інформації»
код і найменування спеціальності

категорія слухачів: фахівець з планування політики та стратегії кібербезпеки (7 рівень НРК), провідний фахівець з планування політики та стратегії кібербезпеки (7 рівень НРК)
назва категорії слухачів

Освітня програма підвищення
кваліфікації вводиться в дію
з «_25_» грудня 2025 р.

В. о. ректора Національного
аерокосмічного університету
«Харківський авіаційний інститут»

_____ Олексій ЛИТВИНОВ
наказ № 614 від 24» грудня 2025 р.

Харків 2025

Розробники програми:

- завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., професор, член-кореспондент НАН України В.С. Харченко;
- учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, д.т.н., професор О.К. Юдін;
- старша наукова співробітниця 3-го науково-дослідного відділу 2-го науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, к.т.н., доцентка Л.Г. Черниш;
- директорка Центру якості освіти, ліцензування та акредитації Національного аерокосмічного університету «ХАІ», к.т.н., доцентка Е.А. Дармофал;
- професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ», д.т.н., професор Г.В. Фесенко;
- завідувач кафедри права Національного аерокосмічного університету «ХАІ», д.ю.н., професор В.І. Павликівський;
- професор кафедри права Національного аерокосмічного університету «ХАІ», к.ю.н., доцент С.Ю. Лукашевич;
- професорка кафедри права Національного аерокосмічного університету «ХАІ», д.ю.н., професорка Н.Є. Філіпенко;
- завідувач кафедри загальної військової підготовки Національного аерокосмічного університету «ХАІ», к.пед.н., доцент В.В. Рютін
- асистент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ» Р.І. Демура;
- асистент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ» Р.С. Подгорний.

Рецензент:

головний науковий співробітник 3-го науково-дослідного відділу 2-го науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, доктор технічних наук, професор С. В. Толюпа.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Освітня програма підвищення кваліфікації «Провідний фахівець з планування політики та стратегії кібербезпеки» розроблена у відповідності до Типової програми підвищення кваліфікації «Провідний фахівець з планування політики та стратегії кібербезпеки», Розділу ІІІ професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки» та Національного класифікатора України ДК 003:2010 «Класифікатор професій» («Фахівець з планування політики та стратегії кібербезпеки» 2139.2), основних положень і вимог визначених законами України «Про освіту», «Про вищу освіту», інших законодавчих і нормативних документів.

Зміст Програми диференційовано за модулями відповідно до визначеної категорії слухачів і розраховано на розвиток їх професійних компетентностей.

Сьогодні інформаційні системи відіграють ключову роль у забезпеченні ефективності роботи державних установ, підприємств та організацій. Державні установи використовують різноманітні інформаційні системи для зберігання, обробки та передачі інформації. Фахівець з планування політики та стратегії кібербезпеки – це ключовий професіонал, який розробляє, впроваджує та керує комплексними заходами захисту інформаційних систем, мереж і даних від кіберзагроз, створюючи «цифрову фортецю», що включає політики безпеки, аудит, реагування на інциденти, навчання персоналу та постійне вдосконалення захисних механізмів для забезпечення безперебійної роботи бізнесу та збереження конфіденційної інформації. Фахівці з планування політики та стратегії кібербезпеки мають вільно та ґрунтовно забезпечувати комплексний захист, передбачаючи загрози, створюючи проактивні стратегії та «закриваючи» всі можливі канали для атак.

ОСНОВНІ ЗАВДАННЯ ПРОГРАМИ

– аналізувати, інтерпретувати, планувати та застосовувати вимоги нормативно-правової бази, кращих міжнародних практик, а також технології та документи забезпечення інформаційної та/або кібербезпеки;

– розробляти, впроваджувати та підтримувати процес формування організаційних заходів, технологій, документів, політик та стратегій інформаційної та/або кібербезпеки, узгоджених зі стратегічним планом організації;

– супроводжувати впровадження та дотримання нормативно-правових та організаційно-технічних заходів інформаційної та/або кібербезпеки;

– розробляти проєкти розвитку, здійснювати комунікацію (публікація політик, ознайомлення персоналу) та надавати консультації керівництву та персоналу з практичного застосування методологій інформаційної та/або кібербезпеки;

– моніторити виконання політик та принципів інформаційної безпеки та брати участь в аудитах для контролю їх ефективності;

– брати участь у формуванні політики та стратегії розвитку інформаційної безпеки на відомчому та корпоративному рівнях, оцінюючи потреби, співпрацюючи з зацікавленими сторонами та знаходячи консенсус щодо змін;

– розробляти, проводити та оцінювати ефективність навчально-методичних та консультативних заходів (навчання, тренінги, консультації) з питань інформаційної та/або кібербезпеки.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «Провідний фахівець з планування політики та стратегії кібербезпеки»

Загальна інформація	
Повна назва закладу розробника (ків)	Національний аерокосмічний університет «Харківський авіаційний інститут», Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Ступінь вищої освіти слухача	особи, які мають ступень вищої освіти бакалавр або вищий за нього
Форма підвищення кваліфікації	змішана (офлайн/онлайн)
Цільова група	фахівець з планування політики та стратегії кібербезпеки (7 рівень НРК), провідний фахівець з планування політики та стратегії кібербезпеки (7 рівень НРК)
Термін та обсяг програми	15 днів / 180 год. (6 кредитів ECTS)
Професійна кваліфікація	провідний фахівець з планування політики та стратегії кібербезпеки (трудові функції А, Б, В, Г, Д, Е)
Мета Програми	
Формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо планування, розробки, впровадження та супроводження, моніторингу політик, законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та кібербезпеки, а також надання освітніх, консультативних послуг та підтримання комунікації з зацікавленими сторонами в зазначеній сфері.	
Функціональна спрямованість	Розвиток стратегічних компетентностей, що охоплюють держполітику, правові засади, оцінку ризиків, реагування на інциденти та планування заходів кіберзахисту, з метою підготовки лідерів для ефективного управління кібербезпекою, забезпечення захисту критичної інфраструктури та адаптації до нових кіберзагроз
Фокус програми	Акцент на розвиток професійних компетентностей провідних фахівців з планування політики та стратегії кібербезпеки щодо поглибленого вивченні сучасних загроз, стратегічного планування захисту, управління ризиками, впровадження передових технологій (ШІ, Zero Trust), формуванні навичок розробки та реалізації політик кібербезпеки для захисту критичної інфраструктури та інформаційних ресурсів на державному та корпоративному рівнях, щоб відповідати динамічному кіберпростору
Орієнтація програми	Програма орієнтована на розвиток професійних компетентностей провідних фахівців з планування політики та стратегії кібербезпеки

Особливості програми	Програма підвищення кваліфікації провідних фахівців з планування політики та стратегії кібербезпеки адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки», на комплексному підході (люди, процеси, технології), стратегічному плануванні та управлінні ризиками, національному та міжнародному контексті, адаптивному навчанні до нових загроз та технологій, готуючи керівників, здатних формувати стійку кіберстійкість держави та організацій. Програма складається з 3 модулів / 4 змістовних модулів. Загальний обсяг програми – 180 акад. год. / 6 кредитів ECTS, з яких: *лекції – 40 год., практичні заняття – 10 год., самостійна робота – 120 год., консультації – 2 год., модульний контроль – 8 год.* Вид підсумкового контролю – комп'ютерне оцінювання знань на базі автоматизованої системи тестування
Професійні вимоги (компетентності) та продовження навчання	
Професійні вимоги (компетенції)	Визначаються посадовими інструкціями
Продовження навчання	Освітня Програма передбачає можливість подальшого розширення та поглиблення професійних знань, умінь, навичок у системі неформальної та інформальної освіти.
Програмні компетентності	
Загальні компетентності	1. Здатність мислити та розвіватися відповідно до змін зовнішнього середовища, безперервного навчання, постійного оновлення і поповнення знань, отримання нового або переосмслення старого досвіту, управління знаннями, самопізнання. 2. Здатність діяти активно, відповідально й ефективно реалізовувати громадянські права та обовязки з метою розвитку демократичного громадянського суспільства, усвідомлювати та сповідувати цінності громадянського суспільства. 3. Здатність виявляти повагу та цінувати українську національну культуру, багатоманітність і мультикультурність у суспільстві. 4. Здатність генерувати і втілювати нові ідеї у сферу інформаційної безпеки, що базується на креативності, творчості, відчутті нового, здатності до здорового ризику.
Фахові (предметно-орієнтовані)	Для провідних фахівців з планування політики та стратегії кібербезпеки потрібні фахові компетентності, що охоплюють: **1. Стратегічне планування та політика:** знання засад державної політики у сфері кібербезпеки, розробка політик та стратегій кіберзахисту на національному та

	організаційному рівнях, оцінка та управління кіберризиками на рівні організації, міжнародні стандарти та кращі практики кібербезпеки. **2. Технічні знання та технології:** глибоке розуміння сучасних кіберзагроз (APT, ransomware, фішинг тощо) та їхніх механізмів, ідентифікація, аналіз та протидія кіберінцидентам, захист критичної інформаційної інфраструктури, впровадження систем захисту інформації та забезпечення її властивостей (конфіденційності, цілісності, доступності). **3. Правові та управлінські аспекти:** знання нормативно-правової бази у сфері кібербезпеки та захисту інформації, механізми державного управління у сфері кібербезпеки, організаційно-технічні заходи захисту інформації. **4. Критичне мислення та прийняття рішень:** здатність аналізувати складні ситуації та приймати обґрунтовані рішення щодо реагування на загрози, прогнозування наслідків кіберінцидентів.
Програмні результати навчання	
Програма підвищення кваліфікації «Провідний фахівець з планування політики та стратегії кібербезпеки» спрямовано на досягнення програмних результатів навчання, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Збір та аналіз даних для планування законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.
ТФ Б РН 2	Розроблення, впровадження законодавчих, нормативно-правових, організаційно- технічних заходів інформаційної та/або кібербезпеки.
ТФ В РН 3	Супроводження процесів впровадження законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.
ТФ Г РН 4	Моніторинг впроваджених законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.
ТФ Д РН 5	Підтримання комунікації із зацікавленими сторонами для врахування їх пропозицій при плануванні законодавчих, нормативно-правових, організаційно- технічних заходів інформаційної та/або кібербезпеки.
ТФ Е РН 6	Надання освітніх та консультативних послуг щодо законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.

2. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ (А131, А132, А2.31 В1.31, В1.32, В1.34, Д3.32). Планування та розроблення СМІБ (А1.37, А2.32, А3.37, А3.38, А3.39, Д3.32). Реалізація та функціонування СМІБ (А1.37, А2.32, В4.31, Г1.32, Д3.32, Е2.33, Е2.34). Моніторинг, аналіз і вдосконалення СМІБ (В3.32, Г1.32, Г2.32, Г2.33).

Самостійна робота. Побудувати план розробки та впровадження СМІБ в організації. Сформувати політики інформаційної безпеки різних класів (1-3 рівнів), як складових СМІБ організації. Побудувати таблицю менеджменту інформаційних ресурсів організації. Скласти порядок розрахунку та аналізу ризиків за визначеним методом (кількісний або якісний). Вивчення нормативно-правової бази та передової практики щодо системи менеджменту інформаційної безпеки організації.

Модуль 2. ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ ТА МЕТОДИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Змістовний модуль 1. Концептуально-організаційні та проєктно-стратегічні засади інформаційної і кібербезпеки.

Концептуальні, технологічні та організаційні основи інформаційної та кібербезпеки (А1.31, А3.34, А2.33, А1.35, А1.36, А1.34, А1.38, А3.33, А2.35, А2.36). Планування та архітектура інформаційної і кібербезпеки в організації **(**А3.33, А3.35, А3.36, А3.38, А3.31, А3.32, А2.34, А3.37, А3.39**)**. Стратегії, політики та планування розвитку інформаційної і кібербезпеки **(**Б1.31, Б1.32, Б1.33, Б1.34, Б2.31, Б2.32, Б2.33, Б2.34, Б3.31, Б3.32, Б3.33, Б3.34, Б3.35**)**. Організаційні, проєктні та комунікаційні засади створення систем інформаційної та кібербезпеки **(**В1.35, В2.31, В2.32, В3.31, В3.32, В3.33, В3.34, В4.32**)**.

Самостійна робота. Ідентифікація активів, оцінювання ризиків та обґрунтування контрзаходів у сфері інформаційної та кібербезпеки. Вивчення нормативно-правової бази та передової практики з питань концептуально-організаційних та проєктно-стратегічних засад інформаційної і кібербезпеки.

Змістовний модуль 2. Управлінсько-методичні та освітньо-комунікаційні засади забезпечення інформаційної і кібербезпеки.

Методичні засади оцінювання, моніторингу та аудиту інформаційної та кібербезпеки (Г1.31, Г1.32, Г1.33, Г1.34, Г2.31, Г2.32, Г2.33). Управління бізнес-процесами та міжорганізаційна взаємодія у сфері інформаційної і кібербезпеки (Д1.31, Д1.32, Д1.33, Д2.31, Д2.32, Д2.33, Д2.34, Д2.35, Д3.31, Д3.32, Д3.33, Д3.34, Д3.35). Навчально-методичне та інформаційно-комунікаційне забезпечення підготовки у сфері інформаційної та кібербезпеки (Е1.31, Е1.32, Е1.33, Е1.34, Е1.35, Е1.36, Е1.37, Е1.38, Е1.39, Е1.310, Е1.311). Освітні технології, комунікація та оцінювання результатів навчання (Е2.31, Е2.32, Е2.33, Е2.34, Е2.35, Е2.36, Е2.37, Е2.38, Е3.31, Е3.32, Е3.33, Е3.34, Е3.35, Е3.36, Е3.37).

Самостійна робота. Оцінювання рівня інформаційної та кібербезпеки організації на основі методів аудиту та моніторингу. Аналіз бізнес-процесів та міжорганізаційної взаємодії у системі інформаційної і кібербезпеки. Вивчення нормативно-правової бази та передової практики щодо управлінсько-методичних та освітньо-комунікаційних засад забезпечення інформаційної і кібербезпеки.

Модуль 3. ПРАВОВІ ТА ПСИХОЛОГІЧНІ ЗАСАДИ ОБІГУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ

Змістовний модуль 1. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки інформаційних ресурсів.

Нормативно-правове забезпечення інформаційної безпеки, кібербезпеки, захисту інформації та забезпечення приватності даних (А2.З1, А2.З2, Б4.З2). Міжнародні нормативно-правові акти і стандарти, національне законодавство у сфері кібербезпеки та захисту інформаційних ресурсів організацій і підприємств різних форм власності (А1.З6, Б4.З1). Загальні засади юридичної відповідальності. Дисциплінарна, адміністративна та кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. Психологічні основи етичного хакінгу, забезпечення приватності даних, інформаційної безпеки та кібербезпеки (Б4.З2, Г1.З2).

Самостійна робота. Стандарти кібербезпеки та приватності, засад, політик, положень, законодавства, сертифікацій та найкращих світових практик (NIST, ENISA) (Б3.З2). Чинні вітчизняні закони, нормативні акти, директив, постанови у сфері кібербезпезпеки (Б4.З2). Закон України № 4336-IX від 27.03.25 року «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». Етичні вимоги організації кібербезпеки (NIST, ISACA, ENISA) (Г1.З2).

3. НАВЧАЛЬНИЙ ПЛАН ЗА МОДУЛЯМИ ОРІЄНТОВАНИЙ РОЗПОДІЛ ГОДИН ЗА ВИДАМИ НАВЧАННЯ

3.1. Система менеджменту інформаційної безпеки

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Система менеджменту інформаційної безпеки організації						
1.1 Основи і принципи побудови СМІБ (А1З1, А1З2, А2.З1 В1.З1, В1.З2, В1.З4, Д3.З2). Поняття та значення СМІБ. Цілі, завдання та функції СМІБ. Принципи побудови СМІБ (системний, процесний, ризик-орієнтований підхід). Цикл PDCA (Plan-Do-Check-Act). Взаємозв'язок підходів побудови СМІБ з циклом PDCA. Взаємозв'язок СМІБ із іншими системами менеджменту.	**8**	**2**				**6**
1.2 Планування та розроблення СМІБ (А1.З7, А2.З2, А3.З7, А3.З8, А3.З9, Д3.З2). Визначення контексту організації. Формування політики	**12**	**2**		**2**		**8**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
інформаційної безпеки. Ідентифікація та класифікація інформаційних активів. Оцінювання ризиків інформаційної безпеки. Планування оброблення ризиків. Розроблення структури та документації СМІБ. План розробки та впровадження СМІБ.						
1.3 Реалізація та функціонування СМІБ (А1.3.7, А2.3.2, В4.3.1, Г1.3.2, Д3.3.2, Е2.3.3, Е2.3.4). Впровадження політики інформаційної безпеки. Управління доступом і користувачами. Управління технічними та організаційними контролями. Управління ризиками інформаційної безпеки. Моніторинг безпеки та контроль ефективності. Документування та управління записами СМІБ. Навчання, підготовка та підвищення компетентності персоналу. Засоби реалізації та підтримки функціонування СМІБ.	**10**	**4**		**2**		**4**
1.4 Моніторинг, аналіз і вдосконалення СМІБ (В3.3.2, Г1.3.2, Г2.3.2, Г2.3.3). Система моніторингу інформаційної безпеки. Оцінювання результативності та ефективності СМІБ. Внутрішній аудит СМІБ. Управлінський огляд СМІБ. Аналіз невідповідностей і коригувальні дії. Управління змінами та розвиток СМІБ. Постійне вдосконалення СМІБ.	**8**	**2**				**6**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Побудувати план розробки та впровадження СМІБ в організації.	**1**					**1**
Самостійна робота 1.2. Сформувати політики інформаційної безпеки різних класів (1-3 рівнів), як складових СМІБ організації.	**1**					**1**
Самостійна робота 1.3. Побудувати таблицю менеджменту інформаційних ресурсів організації.	**1**					**1**
Самостійна робота 1.4. Скласти порядок розрахунку та аналізу ризиків за визначеним методом (кількісний або якісний).	**1**					**1**
Самостійна робота / теоретична складова						
Самостійна робота 1.5. Вивчення нормативно-правової бази та передової практики щодо системи менеджменту інформаційної безпеки організації.	**6**					**6**
Всього годин за модуль 1	**48**	**10**	**0**	**4**		**34**
Модульна контрольна робота за Частиною 1	**2**				**2**	
Всього годин за Частиною 1	**50**	**10**	**0**	**4**	**2**	**34**

3.2. Організаційно-управлінські та методичні засади забезпечення інформаційної та кібербезпеки

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Концептуально-організаційні та проєктно-стратегічні засади інформаційної і кібербезпеки						
1.1 Концептуальні, технологічні та організаційні основи інформаційної та кібербезпеки (А1.3.1, А3.3.4, А2.3.3, А1.3.5, А1.3.6, А1.3.4, А1.3.8, А3.3.3, А2.3.5, А2.3.6).	**8**	**4**				**4**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Фундаментальні кіберконцепції, термінологія, принципи, обмеження та ефекти кібероперацій у сфері інформаційної та кібербезпеки. Принципи забезпечення інформаційної та кібербезпеки і захисту персональних даних, включно з питаннями безперервності діяльності та відновлення після інцидентів. Сучасні, нові та перспективні технології інформаційної та кібербезпеки, а також галузеві показники та тенденції їх розвитку. Критерії стійкості та надійності організацій у контексті захисту кіберресурсів, суспільної та персональної безпеки. Зміст і порядок адаптивного та кризового планування в умовах обмеженого часу при реагуванні на інциденти інформаційної та кібербезпеки. Методи аналізу кризових ситуацій у сфері інформаційної та кібербезпеки з метою забезпечення стійкості та надійності організацій.						
1.2 Планування та архітектура інформаційної і кібербезпеки в організації (А3.З3, А3.З5, А3.З6, А3.З8, А3.З1, А3.З2, А2.З4, А3.З7, А3.З9). Концепції та протоколи комп'ютерних мереж і методологія забезпечення безпеки мереж у системах інформаційної та кібербезпеки. Сервісорієнтовані принципи побудови архітектури інформаційної та/або кібербезпеки та зміст і функції відповідної інформаційної структури. Аналіз потреб і вимог користувачів для планування архітектури інформаційної та/або кібербезпеки в організації. Аналіз потреб безпеки та вимог до програмного забезпечення для забезпечення інформаційної та/або кібербезпеки в організації. Політики, конфігурації, процедури, програмне забезпечення, обладнання та прикладні технології, що застосовуються для планування заходів інформаційної та/або кібербезпеки. Концепції та організація діяльності щодо планування інформаційної та/або кібербезпеки в організації.	**10**	**2**				**8**
1.3 Стратегії, політики та планування розвитку інформаційної і кібербезпеки (Б1.З1, Б1.З2, Б1.З3, Б1.З4, Б2.З1, Б2.З2, Б2.З3, Б2.З4, Б3.З1, Б3.З2, Б3.З3, Б3.З4, Б3.З5). Теоретичні засади стратегічного управління та їх застосування у сфері інформаційної та кібербезпеки організації. Класифікація кіберспроможностей (захисних, наступальних, експлуатаційних) та їх урахування під час формування стратегій і політик кібербезпеки. Порядок розроблення, структура та зміст стратегій, політик, програм і планів розвитку інформаційної та кібербезпеки. Перспективні технології забезпечення інформаційної та кібербезпеки та їх вплив на стратегічне і оперативне планування. Планування безперервності операцій та аварійного відновлення, тестування систем інформаційної та кібербезпеки перед введенням в експлуатацію. Управління програмами і проєктами з інформаційної та кібербезпеки, оцінювання стану кібербезпеки організації,	**10**	**2**				**8**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
оперативне планування, класифікація інформації та функції внутрішнього консультанта.						
1.4 Організаційні, проєктні та комунікаційні засади створення систем інформаційної та кібербезпеки (В1.З5, В2.З1, В2.З2, В3.З1, В3.З2, В3.З3, В3.З4, В4.З2). Сучасні та перспективні технології комунікації, що застосовуються в системах інформаційної та кібербезпеки. Корпоративні цілі та завдання організації, пов'язані з використанням інформаційних технологій і побудовою систем інформаційної та кібербезпеки. Структура і зміст планів, настанов, повноважень та інших організаційно-розпорядчих документів у сфері інформаційної та кібербезпеки. Інструменти, методи та методики проєктування систем, включаючи автоматизовані системи аналізу та засоби проєктування систем безпеки. Порядок оцінювання проєктів систем інформаційної та/або кібербезпеки та критерії їх ефективності. Порядок розроблення технічної документації, а також положення програм класифікації інформації і процедур її розкриття в організації.	**10**	**2**		**2**		**6**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Ідентифікація активів, оцінювання ризиків та обґрунтування контрзаходів у сфері інформаційної та кібербезпеки.	**2**					**2**
Самостійна робота / теоретична складова						
Самостійна робота 1.2. Вивчення нормативно-правової бази та передової практики з питань концептуально-організаційних та проєктно-стратегічних засад інформаційної і кібербезпеки.	**8**					**8**
Всього годин за модулем 1	**48**	**10**	**0**	**2**	**0**	**36**
Змістовний модуль 2. Управлінсько-методичні та освітньо-комунікаційні засади забезпечення інформаційної і кібербезпеки						
2.1 Методичні засади оцінювання, моніторингу та аудиту інформаційної та кібербезпеки (Г1.З1, Г1.З2, Г1.З3, Г1.З4, Г2.З1, Г2.З2, Г2.З3). Методи соціальної інженерії та їх вплив на стан інформаційної і кібербезпеки. Класифікація методів оцінювання безпеки інформаційних технологій та порядок їх практичного застосування. Галузеві стандартизовані методи оцінки, впровадження та розповсюдження інструментів і процедур оцінювання безпеки ІТ, моніторингу, виявлення та усунення несправностей. Процедури аудиту та логування інформаційних систем, у тому числі серверного логування, у системах кіберзахисту. Підходи до розроблення, верифікації та застосування критеріїв оцінювання персоналу щодо реалізації стратегій, політик і програм розвитку кіберзахисту. Методи та процеси тестування і оцінювання персоналу з метою забезпечення ефективності заходів інформаційної та кібербезпеки.	**8**	**4**				**4**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
2.2 Управління бізнес-процесами та міжорганізаційна взаємодія у сфері інформаційної і кібербезпеки (Д1.З1, Д1.З2, Д1.З3, Д2.З1, Д2.З2, Д2.З3, Д2.З4, Д2.З5, Д3.З1, Д3.З2, Д3.З3, Д3.З4, Д3.З5). Місія організації, основні бізнес-процеси та їх роль у забезпеченні інформаційної та кібербезпеки. Технологічні завдання управління та лідерства в організації, механізми прийняття управлінських рішень і вирішення проблем у сфері кіберзахисту. Види та способи доведення інформації в організаційних процесах (асимілятивні, слухові, кінестетичні) та їх вплив на ефективність управління. Методи та процедури прогнозування потреб у послугах інформаційної та/або кібербезпеки, включно з моделюванням загроз і спроможностей. Політика організації та практика планування співпраці з внутрішніми і зовнішніми організаціями-партнерами, їх можливості, обмеження, повноваження та відповідальність. Нормативне, технологічне та інформаційне забезпечення діяльності організації і партнерів у сфері кіберзахисту, включно з аналізом звітів та використанням новітніх технологій і інструментів.	**8**	**2**				**6**
2.3 Навчально-методичне та інформаційно-комунікаційне забезпечення підготовки у сфері інформаційної та кібербезпеки (Е1.З1, Е1.З2, Е1.З3, Е1.З4, Е1.З5, Е1.З6, Е1.З7, Е1.З8, Е1.З9, Е1.З10, Е1.З11). Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування з використанням текстових, мовних і візуальних засобів. Концепції, процедури, програмне забезпечення, обладнання та прикладні технології, що застосовуються для організації навчання і підготовки персоналу. Вимоги до структури та змісту навчально-методичних і консультативних матеріалів та сучасні підходи до їх розроблення. Принципи, методи та форми навчання і консультування, включно з розробленням навчальних програм, інструктажів і тренінгів на робочому місці. Інструктивні матеріали, технічна документація та стандартні операційні процедури як складові забезпечення діяльності персоналу. Методи перегляду та вдосконалення навчальних планів і програм, вимоги до системи забезпечення якості, а також урахування основних небезпек, ризиків і вразливостей.	**10**	**4**		**2**		**4**
2.4 Освітні технології, комунікація та оцінювання результатів навчання (Е2.З1, Е2.З2, Е2.З3, Е2.З4, Е2.З5, Е2.З6, Е2.З7, Е2.З8, Е3.З1, Е3.З2, Е3.З3, Е3.З4, Е3.З5, Е3.З6, Е3.З7). Зміст навчальної програми та особливості організації освітнього процесу для різних форм набуття компетентностей. Форми організації освітнього процесу та сучасні методи, засоби і технології викладання. Методи і способи організації індивідуальної та групової роботи здобувачів освіти, включно з підготовкою доповідей і	**10**	**2**		**2**		**6**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
презентацій. Освітні комп'ютерні послуги, технології дистанційної освіти та методи ефективної комунікації в освітньому процесі. Методики, порядок та критерії оцінювання результатів навчання, включно з тестуванням і верифікацією критеріїв оцінювання. Академічна доброчесність, захист авторських прав та методи збору, узагальнення і систематизації інформації в освітній діяльності.						
Самостійна робота / практичне завдання						
Самостійна робота 2.1. Оцінювання рівня інформаційної та кібербезпеки організації на основі методів аудиту та моніторингу.	**2**					**2**
Самостійна робота 2.2. Аналіз бізнес-процесів та міжорганізаційної взаємодії у системі інформаційної і кібербезпеки.	**2**					**2**
Самостійна робота/ теоретична складова						
Самостійна робота 2.3. Вивчення нормативно-правової бази та передової практики щодо управлінсько-методичних та освітньо-комунікаційних засад забезпечення інформаційної і кібербезпеки.	**8**					**8**
Всього годин за модулем 2	**48**	**12**	**0**	**4**	**0**	**32**
Модульна контрольна робота за Частиною 2	**2**	**0**	**0**	**0**	**2**	**0**
Всього годин за Частиною 2	**98**	**22**	**0**	**6**	**2**	**68**

3.3. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки інформаційних ресурсів						
1.1 Нормативно-правове забезпечення інформаційної безпеки, кібербезпеки, захисту інформації та забезпечення приватності даних (А2.З1, А2.З2, Б4.З2).	**5**	**2**				**3**
1.2 Міжнародні нормативно-правові акти і стандарти, національне законодавство у сфері кібербезпеки та захисту інформаційних ресурсів організацій і підприємств різних форм власності (А1.З6, Б4.З1).	**5**	**2**				**3**
1.3 Загальні засади юридичної відповідальності. Дисциплінарна, адміністративна та кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки.	**4**	**2**				**2**
1.4 Психологічні основи етичного хакінгу, забезпечення приватності даних, інформаційної безпеки та кібербезпеки (Б4.З2, Г1.З2)	**4**	**2**				**2**
Самостійна робота / практичне завдання						

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Самостійна робота 1.1. Стандарти кібербезпеки та приватності, засад, політик, положень, законодавства, сертифікацій та найкращих світових практик (NIST, ENISA) (**Б3.32**).	**2**					**2**
Самостійна робота 1.2. Чинні вітчизняні закони, нормативні акти, директив, постанови у сфері кібербезпезпеки (**Б4.32**).	**2**					**2**
Самостійна робота / теоретична складова						
Самостійна робота 1.3. Закон України № 4336-IX від 27.03.25 року «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури».	**2**					**2**
Самостійна робота 1.4. Етичні вимоги організації кібербезпеки (NIST, ISACA, ENISA) (**Г1.32**)	**2**					**2**
Модульна контрольна робота за Частиною 3	**2**				**2**	
Всього годин за Частиною 3	**28**	**8**	**0**	**0**	**2**	**18**
Консультація з комп’ютерного оцінювання на базі автоматизованої системи тестування	**2**				**2**	
Підсумковий контроль – комп’ютерне оцінювання на базі автоматизованої системи тестування	**2**				**2**	
Всього годин за програмою	**180**	**40**	**0**	**10**	**10**	**120**

4. ОСНОВНІ МЕТОДИ НАВЧАННЯ

Під час викладання передбачено застосування наступних форм.

Лекція – логічно довершений, науково обґрунтований та систематизований виклад певного наукового або науково-педагогічного питання, ілюстрований засобами наочності та демонстрацією результатів досліджень.

Лекція є одним із основних видів і, водночас, методів проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Вона закладає основи наукових знань, визначаючи напрям, основний зміст та характер усіх видів навчальних занять, а також, головним чином, самостійної роботи здобувачів вищої освіти.

Практичне заняття – форма навчального заняття, на якому у здобувача вищої освіти під керівництвом викладача формуються вміння та навички практичного застосування теоретичних положень навчальної дисципліни шляхом виконання здобувачем вищої освіти відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторії, оснащеною комп’ютерною технікою та технічними засобами навчання.

Практичне заняття включає в себе: проведення викладачем контролю знань, вмінь та навичок здобувачів вищої освіти, постановку загальної проблеми (завдання) та її обговорення за участю здобувачів вищої освіти, розв’язування завдань та їх обговорення, виконання контрольних завдань, їх перевірку та оцінювання викладачем.

Консультація – форма навчального заняття, на якому здобувач вищої освіти отримує від викладача відповіді на конкретні запитання або пояснення окремих теоретичних положень та їх використання на практиці.

Самостійна робота забезпечується навчально-методичними засобами, передбаченими для вивчення навчальної дисципліни: підручниками, навчально-методичними посібниками, конспектами лекцій, практикумами, електронно-обчислювальною технікою тощо.

Самостійна робота над засвоєнням навчального матеріалу може виконуватися в бібліотеці, комп'ютерному класі.

Форми самостійної роботи здобувачів вищої освіти:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, передбачених для самостійного опрацювання;
- виконання різних за формою і змістом завдань;
- підготовка до практичних занять;
- підготовка до поточного, модульного та підсумкового контролю знань;
- пошук та огляд літературних джерел за проблематикою навчальної дисципліни;
- виконання індивідуальних завдань (написання курсової роботи);
- аналітичний розгляд наукової публікації тощо.

Методи навчання:

– під час проведення лекційних занять – лекція-діалог, бесіда, а також наочних методів навчання, зокрема використання мультимедійних презентацій. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії;

– під час проведення практичних занять – використання роздаткового матеріалу, нормативно-правові акти.

5. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання можуть оцінюватись за формами:

- стандартною формою;
- комп'ютерне оцінювання знань на базі автоматизованої системи тестування.

5.1 Форма 1. Стандартна форма

Результати навчання слухача з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	**0,6**
Підсумковий контроль (ПК)	**0,4**

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю є:

Види навчальної діяльності	Мах кількість балів
Частина №1	
Виконання та захист одного практичного заняття *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 18 балів**)*	15
Усього за частиною №1	30
Частина №2	
Виконання та захист одного практичного заняття *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 22 бали**)*	12
Усього за частиною №2	36
Частина №3	
Виконання та захист практичного завдання самостійної роботи *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 8 балів**)*	14
Усього за частиною №3	14
Усього за частинами №1, №2, №3	**80**
Комп'ютерне оцінювання на базі автоматизованої системи тестування	**20**
Усього за дисципліною	**100**

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач виявляє особливі 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 і нахили.
B	84-89	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач 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	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач 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	65-74	*Задовільно – непогано, але зі значною кількістю недоліків.* Здобувач 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.

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
E	60-64	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

5.4 Форма 2. Комп'ютерного оцінювання (далі - КО): форма – очна на базі автоматизованої системи тестування (далі – АСТ) мережі Кваліфікаційного центру, формат – електронний.

Для проведення КО побудовано Банк запитань/тестів довжиною 120 запитань у відповідності до узагальненої програми процедури оцінювання з професійної кваліфікації «Провідний фахівець з планування політики та стратегії кібербезпеки (трудові функції А, Б, В, Г, Д, Е)» професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки».

До одного варіанту тесту входить 40 тестових запитань.

Розподіл запитань між змістовними блоками та перекриття усіх трудових функцій професійної кваліфікації представлено у Таблиці 1. У Таблиці 1 параметр «Питома вага розділу» вказує відсоток, який слугує орієнтиром для обрання кількості тестових запитань відповідного розділу. Параметр «Кількість запитань у варіанті тесту» вказує, скільки запитань повинно бути включено до варіанту тесту за відповідною трудовою функцією. Параметр «Кількість запитань у Банку запитань» вказує, скільки запитань з загальної кількості відносяться до певної трудової функції.

При формуванні контрольно-вимірювальних матеріалів відповідно до Порядку присвоєння\підтвердження та цього Регламенту повинно бути забезпечено включення відповідної кількості тестів, які відносяться до кожної трудової функції. Таким чином, забезпечується покриття всіх 100% включених до професійної кваліфікації відповідного стандарту трудових функцій.

Усі завдання з загального Банку завдань мають різний рівень складності (від 1 до 3). На відповідь рівня складності 1 відводиться 1 хвилина, рівня 2 – 3 хвилини, рівня 3 – 5 хвилин.

Варіант тесту складається з 40 запитань. Розподіл запитань за трудовими функціями/змістовними розділами представлено у Таблиці 1. З 40 запитань 23 запитання мають рівень складності 1, 14 запитання рівень складності 2, 3 запитань – рівень складності 3.

На проходження варіанту тесту здобувачеві виділяється 1 година 20 хвилин:

$$23*1+14*3+3*5 = 80 \text{ хв.}$$

Таблиця 1

Відповідність Банку завдань та варіанту тесту професійної кваліфікації

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	Теоретичний модуль тестування знань	**60%**	**24**	**72**
А	Збір та аналіз даних для планування законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	12%	5	15
Б	Розроблення, впровадження законодавчих, нормативно-правових, організаційно- технічних заходів інформаційної та/або кібербезпеки.	12%	5	15
В	Супроводження процесів впровадження законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
Г	Моніторинг впроваджених законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	12%	5	15
Д	Підтримання комунікації із зацікавленими сторонами для врахування їх пропозицій при плануванні законодавчих, нормативно- правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
Е	Надання освітніх та консультативних послуг щодо законодавчих, нормативно- правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Збір та аналіз даних для планування законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
Б	Розроблення, впровадження законодавчих, нормативно- правових, організаційно- технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
В	Супроводження процесів впровадження законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
Г	Моніторинг впроваджених законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	8%	3	9
Д	Підтримання комунікації із зацікавленими сторонами для врахування їх пропозицій при плануванні законодавчих, нормативно- правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	4%	2	6
Е	Надання освітніх та консультативних послуг щодо законодавчих, нормативно- правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	4%	2	6
			40	**120**

Система оцінювання. Оцінювання складається з двох частин: Теоретичний модуль (60%) та Практичний модуль (40%). Теоретична частина та практична частина оцінюється одночасно.

Кожне з 40 завдань одного варіанту тесту вважається зарахованим, якщо відповідь вірна та повна, або не зарахованим, якщо відповідь не вірна або неповна.

Оцінювання вважається зараховано за умови не менше 75% правильних відповідей.

За результатами проведених процедур оцінювання комісія ухвалює одне з таких рішень, що відображається у протоколі та подається для затвердження Кваліфікаційним центром інформаційних технологій та кібербезпеки Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації:

- визнати результати навчання, присвоїти/підтвердити повну професійну кваліфікації. Теоретичні знання та практичні навички відповідають критерію не менше 75%;
- відмовити у присвоєнні/підтвердженні повної/часткової професійної кваліфікації. Теоретичні та практичні знання не відповідають критерію - не менше 75%.

6. РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Рекомендовані джерела інформації

Основна література:

1. Богуш В. М., Бровко В. Д., Настрадін В. П. Кіберпростір: основи кібербезпеки та кіберзахисту : навч. посіб. У 3 ч. Ч.3. Основи кіберзахисту. Київ : Нац. акад. СБУ, 2020. 72 с.

2. Левченко О. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Євро-Волинь, 2021. 172 с.

3. Когут Ю. І. Кібервійна та безпека об’єктів критичної інфраструктури : Практ. посібник. Київ : Консалтингова компанія "СІДКОН", 2021. 332 с.

4. Організаційно-правові основи забезпечення кібербезпеки : підруч. / М. В. Гуцалюк, А. І. Марущак, Д. С. Мельник [та ін.]; За заг. ред. М. М. Присяжнюка Київ : Наук.-вид. відділ НА СБ України, 2023. 320 с.

Допоміжна література:

5. Бурячок В. Л., Аносов А. О., Семко В. В., Соколов В. Ю., Складанний П. М. Технології забезпечення безпеки мережевої інфраструктури : підруч. Київ : КУБГ, 2019. 218 с.

6. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп’ютерних системах : підруч. Ніжин: ФОП Лук’яненко В. В., ТПК «Орхідея», 2020. 236 с.

7. Козачок В. А., Гайдур Г. І., Гахов С. О., Хмелевський Р. М., Чумак Н. С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів Київ: ДУТ ННІЗІ, 2020. 167 с.

Базові Стандарти:

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT).
2. ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT).
3. ДСТУ ISO/IEC 27035-1:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (ISO/IEC 27035-1:2023, IDT).
4. ДСТУ ISO/IEC 27035-2:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2023, IDT).
5. ДСТУ ISO/IEC 27035-3:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 3. Настанова щодо реагування на інциденти у сфері ІКТ (ISO/IEC 27035-3:2020, IDT).
6. ДСТУ EN ISO/IEC 27000:2022 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (EN ISO/IEC 27000:2020, IDT; ISO/IEC 27000:2018, IDT).
7. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).
8. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).
9. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT).
10. ДСТУ EN ISO/IEC 27006:2022 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (EN ISO/IEC 27006:2020, IDT; ISO/IEC 27006:2015, including Amd 1:2020, IDT).
11. ДСТУ EN ISO/IEC 27007:2022 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою (EN ISO/IEC 27007:2022, IDT; ISO/IEC 27007:2020, IDT).
12. ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (ISO/IEC TS 27008:2019, IDT).
13. ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT).
14. ДСТУ ISO/IEC TR 15446:2024 Інформаційна технологія. Методи безпеки. Настанови щодо створення профілів захисту та цілей безпеки (ISO/IEC TR 15446:2017, IDT).

15. ДСТУ ISO/IEC TS 27022:2024 Інформаційні технології. Настанова щодо процесів системи керування інформаційною безпекою (ISO/IEC TS 27022:2021, IDT).

16. ДСТУ EN ISO/IEC 17021-1:2017 Оцінка відповідності. Вимоги до органів, які здійснюють аудит і сертифікацію систем управління. Частина 1. Вимоги (EN ISO/IEC 17021-1:2015, IDT; ISO/IEC 17021-1:2015, IDT).

17. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2023, IDT).

18. ДСТУ ISO/IEC 15408-1:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT).

19. ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT).

20. ДСТУ ISO/IEC 15408-3:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення (ISO/IEC 15408-3:2022, IDT).

21. ДСТУ ISO/IEC 15408-4:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності (ISO/IEC 15408-4:2022, IDT).

22. ДСТУ ISO/IEC 15408-5:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки (ISO/IEC 15408-5:2022, IDT).

23. ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT).

24. ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проєктування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT).

25. ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проєктування та проблеми керування (ISO/IEC 27033-3:2010, IDT)

26. ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT).

27. ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT)

28. ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі (ISO/IEC 27033-6:2016, IDT).

29. ДСТУ ISO/IEC TR 20004:2017 Інформаційні технології. Методи захисту. Уточнений аналіз вразливості програмного забезпечення згідно з ISO/IEC 15408 та ISO/IEC 18045 (ISO/IEC TR 20004:2015, IDT).

30. NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View.

31. NIST SP 800-12 Rev.1 An Introduction to Information Security.

32. NIST SP 800-18 Rev.1 Guide for Developing Security Plans for Federal Information Systems.
33. NIST SP 800-100 Information Security Handbook: A Guide for Managers.
34. NIST SP 800-55 Rev.1 Performance Measurement Guide for Information Security.
35. NIST SP 800-137 Information Security Continuous Monitoring (ISCM).
36. NIST SP 800-50 Building an Information Technology Security Awareness and Training Program
37. NIST SP 800-53 — Security and Privacy Controls for Information Systems and Organizations.
38. NIST SP 800-160 (Vol. 1) Systems Security Engineering.
39. NIST SP 800-41 Guidelines on Firewalls and Firewall Policy.
40. NIST SP 800-175B Guideline for Using Cryptographic Standards.
41. NIST SP 800-57 (Parts 1–3) Key Management.
42. NIST SP 800-38 Series Modes of Operation for Block Ciphers.
43. NIST SP 800-30 Guide for Conducting Risk Assessments.
44. NIST IR 8183 Cybersecurity Framework Manufacturing Profile.
45. NIST SP 800-82 Guide to ICS Security.
46. NIST SP 800-37 Risk Management Framework (RMF).
47. NIST SP 800-53A Assessing Security and Privacy Controls.
48. NIST SP 800-115 Technical Guide to Information Security Testing.
49. NIST SP 800-63 (A, B, C) Digital Identity Guidelines.
50. NIST SP 800-162 Attribute-Based Access Control (ABAC).
51. NIST SP 800-34 Contingency Planning Guide.
52. NIST SP 800-184 Cyber Incident Recovery Guide.
53. NIST SP 800-61 Rev.2 Computer Security Incident Handling Guide.
54. NIST SP 800-92 Guide to Computer Security Log Management.
55. NIST Cybersecurity Framework (CSF 2.0).
56. COBIT 5/SACA. Control Objectives for Information and Related Technology / Контрольні об’єкти інформаційних та суміжних технологій).
57. ITAF. Information Technology Assurance Framework ISACA. Основні положення професійної практики аудиту та підтвердження довіри до ІС. Стандарт ITAF.
58. ITIL. IT Infrastructure Library. Бібліотека інфраструктури інформаційних технологій.
59. Prince2 v.3. Проєкти в контрольованому середовищі.

Інформаційні ресурси:

1. https://www.mathcad.com/en/education
2. www.zakon.rada.gov.ua
3. http://cert.gov.ua/