# ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

## Звіт про порівняння професійних компетенцій, знань та умінь у діючий освітньої програмі з професійними компетенціями, знаннями та уміннями, зазначеними в професійному стандарті «Фахівець сфери захисту інформації»

Оновлення освітньо-професійної програми «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти буде відбуватися через оновлення обов'язкових освітніх компонентів (дисциплін), з метою врахування у цих компонентах вибраних робочою групою професійних компетенцій, знань, умінь та навичок із професійного стандарту «Фахівець сфери захисту інформації». Для оновлення робочою групою вибрано 3 дисципліни діючої освітньої програми, також у навчальний план буде введено 2 нових дисципліни. Це рішення затверджено на засіданні випускової за спеціальністю 125 – Кібербезпека кафедри «Кібербезпеки та технічного захисту інформації».

У таблицях нижче показано порівняння професійних компетенцій, знань, умінь та навичок для трьох дисциплін, що будуть оновлюватись, та для професійного стандарту: у лівій частині таблиці – для поточної навчальної програми дисципліни, у правій – для нової навчальної програми дисципліни, показані елементи професійного стандарту, що будуть до неї включені.

Однаковим кольором показані **спільні, але не тотожні** професійні компетенції та/або знання, уміння й навички у діючій навчальній програмі дисципліни та у новій навчальній програмі. Незафарбовані елементи професійного стандарту (права частина таблиць) будуть введені до навчальних програм оновлювальних дисциплін. Для двох нових дисциплін у таблицях зазначені професійні компетенції, знання, уміння та навички зі стандарту, що будуть введені до навчальних програм.

1. Назва дисципліни: **Моніторинг та аудит інформаційно-комунікаційних систем (*оновлюється*)**

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| 1 | Здатність розробляти та впровадити комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам | Знання основи проведення аудиту безпеки інформаційних і комунікаційних систем | | **В5.** Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації | **В5.З1.** Методи та технології моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації<br>**В5.З2.** Методи, засоби та інформаційні технології виявлення несанкціонованого | **В5.У1.** Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації<br>**В5.У2.** Здійснювати моніторинг та аудит загроз для інформації, що озвучується<br>**В5.У3.**Використовувати інструменти та технології |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи<br>**В5.З4.** Інструментарій (прикладні програми) моніторингу (аудиту) загроз для інформації в інформаційних системах та мережах | безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах<br>**В5.У4.** Проводити аудити/огляди систем і комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем |
| 2 | Здатність розробляти та впровадити комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам | Знання методів створення систем моніторингу безпеки в інфокомунікаційних системах та мережах | | **В6.** Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки | **В6.З1.** Інструментарій сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах<br>**В6.З2.** Способи сканування розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах | **В6.У1.** Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки |

2. Назва дисципліни: **Спеціальні вимірювання в галузі технічного захисту інформації (*оновлюється*)**

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| 1 | Здатність вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки | | | **А1.** Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації | **А1.З1.** Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси<br>**А1.З2.** Поняття технічного та криптографічного захисту інформації<br>**А1.З5.** Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту<br>**А1.З6.** Політики та етичні норми приватності стосовно безпеки інформації та кібербезпеки<br>**А1.З7.** Принципи та способи захисту інформації, кібербезпеки та приватності<br>**А1.З10.** Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення<br>**А1.З11.** Моделі та симуляції інформаційних, електронних комунікаційних та | **А1.У1.** Визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників)<br>**А1.У2.** Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об’єктах інформаційної діяльності підприємства (організації)<br>**А1.У4.** Визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності підприємства (організації)<br>**А1.У5.** Здійснювати попередню оцінку достатності потреб і вимог користувачів |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації | (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту<br>**А1.У6.** Застосовувати політики безпеки для досягнення цілей безпеки системи<br>**А1.У7.** Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки<br>**А1.У8.** Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації |
| 2 | Здатність формулювати, аналізувати та синтезувати рішення наукових задач і проблем на абстрактному рівні шляхом декомпозиції їх на складові, які можна дослідити окремо в їх більш та менш важливих аспектах | | | **А2.** Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, | **А2.З1.** Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні | **А2.У2.** Виявляти загрози для інформації, що озвучується на об’єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз | впливи на засоби обробки інформації)<br>**А2.32.** Методи (способи) та методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз<br>**А2.33.** Форми та зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки<br>**А2.35.** Підходи, методи (способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки<br>**А2.37.** Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення), блокування інформації | каналів витоку інформації, що озвучується на конкретному об’єкті інформаційної діяльності)<br>**А2.У3.** Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп’ютерної системи (систем) для розробки профілю безпеки<br>**А2.У5.** Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації<br>**А2.У6.** Розробляти модель загроз для інформації від витоку технічними каналами<br>**А2.У7.** Розробляти модель загроз для інформації від спеціальних впливів на засоби обробки інформації |
| 3 | Здатність будувати та оцінювати на основі сучасних принципів, способів та методів теорії захищених систем моделі загроз, порушника, політики безпеки, досліджувати їх для отримання | | | **А3.** Здатність формувати стратегію і політики безпеки інформації в інформаційно- | **А3.34.** Зміст і порядок розробки політики безпеки інформації в інформаційних, електронних комунікаційних та | **А3.У4.** Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | нових висновків та поглибленого розуміння | | | комунікаційних системах | інформаційно-комунікаційних системах<br>**А3.35.** Поняття профілю безпеки інформації та функціональних послуг безпеки<br>**А3.36.** Поняття рівня гарантій реалізації функціональних послуг безпеки | автоматизованих системах різного класу |
| 4 | Здатність до пошуку, оброблення та аналізу інформації з різних джерел | | | **А5.** Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації | **А5.31.**Середовища функціонування автоматизованих систем<br>**А5.32.** Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації<br>**А5.33.** Порядок категоріювання об’єктів<br>**А5.34.** Порядок і методи (способи) обстеження середовищ функціонування автоматизованих систем та об’єктів інформаційної діяльності<br>**А5.35.** Порядок розробки моделей загроз для інформації<br>**А5.36.** Порядок розробки та зміст технічних завдань на створення комплексних систем | **А5.У1.** Здійснювати категоріювання об’єктів інформаційної діяльності (об’єктів електронно-обчислювальної техніки)<br>**А5.У2.** Здійснювати обстеження середовищ функціонування автоматизованих систем<br>**А5.У3.** Здійснювати обстеження об’єктів інформаційної діяльності<br>**А5.У4.** Розробляти моделі загроз для інформації<br>**А5.У5.** Розробляти технічні завдання на створення комплексних систем захисту інформації<br>**А5.У7.** Розробляти проекти комплексних |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | захисту інформації та комплексів технічного захисту інформації | систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності) |
| 5 | Здатність вчитися і бути сучасно навченим | | | **А6.** Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об’єктів інформаційної діяльності | **А6.31.** Поняття спеціальних досліджень засобів обробки інформації, технічних засобів<br>**А6.32.** Поняття спеціальних досліджень об’єктів інформаційної діяльності<br>**А6.34.** Поняття об’єкта інформаційної діяльності<br>**А6.35.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об’єкті інформаційної діяльності<br>**А6.37.** Методики спеціальних досліджень засобів обробки | **А6.У2.** Проводити спеціальні дослідження об’єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на об’єкті інформаційної діяльності та можливість (неможливість) створення на об’єкті інформаційної діяльності певних |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | інформації та об’єктів інформаційної діяльності | технічних каналів витоку інформації)<br>**А6.У3.** Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об’єкті інформаційної діяльності<br>**А6.У4.** Складати протоколи спеціальних досліджень<br>**А6.У5.** Складати приписи на експлуатацію засобів обробки інформації та об’єктів інформаційної діяльності |
| 6 | Здатність формулювати (роблячи презентації або представляючи звіти) нові гіпотези та наукові задачі в області інформаційної безпеки. Вибирати належні напрями і відповідні методи для їх розв’язання, беручи до уваги наявні ресурси | | | **А7.** Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об’єктах | **А7.З6.** Порядок розробки та зміст технічних проєктів комплексних систем захисту інформації та комплексів технічного захисту інформації | **А7.У10.** Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об’єктах інформаційної діяльності<br>**А7.У11.** Оцінювати якість виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах і на об’єктах |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| 7 | Здатність розробляти та впровадити комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо) | | | **А9.** Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації | **А9.З1.** Систему технічних документів щодо систем і комплексів захисту інформації<br>**А9.З2.** Вимоги до структури та змісту технічних документів щодо систем і комплексів захисту інформації<br>**А9.З3.** Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем і комплексів захисту інформації<br>**А9.З4.** Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності | **А9.У3.** Розроблювати (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем і комплексів захисту інформації<br>**А9.У5.** Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах |
| 8 | Здатність сприймати ново здобуті знання в області технологій та засобів кібербезпеки та інтегрувати їх із уже наявними. Здатність зорієнтуватися на рівні спеціаліста в певній вузькій області знань кібербезпеки, яка лежить поза межами обраної спеціалізації. | | | **А10.** Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності | **А10.З1.** Поняття закладних пристроїв для зняття інформації, що озвучується та/або обробляється на об’єкті інформаційної діяльності<br>**А10.З2.** Класифікація закладних пристроїв | **А10.У1.** Розробляти методику виявлення закладних пристроїв на об’єктах інформаційної діяльності<br>**А10.У2.** Здійснювати виявлення (брати участь у виявленні) закладних пристроїв на об’єктах |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | **А10.33.** Принцип дії закладних пристроїв основних класів<br>**А10.34.** Методи (способи) виявлення закладних пристроїв на об’єктах інформаційної діяльності | інформаційної діяльності<br>**А10.У3.** Оформлювати акти за результатами виявлення закладних пристроїв на об’єктах інформаційної діяльності |
| 9 | | Базові знання діючих державних та міжнародних стандартів, що пред'являються до інформаційної безпеки інформаційно-комунікаційних систем | | **Б2.** Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації | **Б2.31.** Поняття та шляхи проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації<br>**Б2.32.** Порядок, умови та організація проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації<br>**Б2.33.** Поняття та загальний зміст програми та методики проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації<br>**Б2.34.** Методи тестування та оцінки захищеності систем | **Б2.У1.** Складати програму та методику проведення державної експертизи комплексних систем захисту інформації<br>**Б2.У2.** Проводити попереднє ознайомлення з об’єктом експертизи та поглиблене обстеження об’єкта експертизи<br>**Б2.У4.** Оформлювати протоколи експертних випробувань та атестати відповідності комплексних систем захисту інформації<br>**Б2.У5.** Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності комплексних систем захисту інформації та організовувати їх |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | **Б2.З7.** Документи, що оформлюються за результатами державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації | затвердження та реєстрацію |
| 10 | | | Вміння готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки інформаційно-комунікаційних систем | **Д2.** Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації | **Д2.З1.** Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації<br>**Д2.З2.** Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації | **Д2.У1.** Розробляти (брати участь у розробці) нормативні документи системи технічного та криптографічного захисту інформації<br>**Д2.У2.** Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали<br>**Д2.У3.** Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації<br>**Д2.У4.** Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації<br>**Д2.У5.** Використовувати результати аналізу кращих світових практик, стандартів при |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | | розробці нормативних документів системи технічного та криптографічного захисту інформації |
| 11 | | | | **Е1.** Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки | **Е1.З1.** Керівництва (настанови, інструкції), нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/ організації<br>**Е1.З2.** Посадові інструкції фахівців структурних підрозділів підприємства/організації, до функцій яких входять питання захисту інформації та кібербезпеки<br>**Е1.З3.** Основи управління персоналом | **Е1.У1.** Здійснювати методичне та технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки<br>**Е1.У2.** Координувати роботи (брати участь у координації робіт) із захисту інформації та кібербезпеки в структурних підрозділах підприємства/організації<br>**Е1.У5.** Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань |
| 12 | | | Здійснювати перевірку об’єктів інформаційної | **Б1.** Здатність проводити оцінку відповідності | | **Б1.У2.** Здійснювати перевірку повноти і відповідності |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | діяльності (ОІД) і технічних засобів | (атестацію) комплексів технічного захисту інформації | | реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ |
| 13 | | | Здійснювати оцінку захищеності ОІД по технічних каналах витоку інформації, виявляти закладні пристрої та засоби схованого відеоспостереження | **Б1.** Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації | **Б1.З5. З**асоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації | **Б1.У1.** Складати програму та методику атестації комплексу технічного захисту інформації (далі – ТЗІ) **Б1.У2.** Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | | актів та нормативних документів системи ТЗІ<br>**Б1.У6.** Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію |
| 14 | | | Здійснювати документальне оформлення протоколів спецдослідження або перевірки захищеності виділеного приміщення різної категорії | **А6.** Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності | **А6.35.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті інформаційної діяльності<br>**А6.37.** Методики спеціальних досліджень засобів обробки інформації та об'єктів інформаційної діяльності | **А6.У2.** Проводити спеціальні дослідження об'єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на об'єкті інформаційної діяльності певних технічних каналів витоку інформації)<br>**А6.У4.** Складати протоколи спеціальних досліджень |

3. Назва дисципліни: **Комплексні системи безпеки (*оновлюється*)**

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| 1 | | Знання основ проектних процедури та принципів проектування складних технічних систем, принципів побудови систем автоматизованого проектування | | **А1.** Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації | **А1.З10.** Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення **А1.З11.** Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації | **А1.У2.** Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об’єктах інформаційної діяльності підприємства (організації) **А1.У5.** Здійснювати попередню оцінку достатності потреб і вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту |
| 2 | Здатність формулювати, аналізувати та синтезувати рішення наукових задач і проблем на абстрактному рівні шляхом декомпозиції їх на складові, які можна дослідити окремо в їх більш та менш важливих аспектах. | | | **А2.** Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз | **А2.З1.** Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації) | **А2.У1.** Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А2.У3.** Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | **А2.33.** Форми та зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки | комп'ютерної системи (систем) для розробки профілю безпеки<br>**А2.У5.** Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації |
| 3 | Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. | | | **А7.** Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах | **А7.32.** Методології забезпечення мережевої безпеки<br>**А7.33.** Способи та апаратні засоби захисту інформації, методи автентифікації, авторизації та контролю доступу<br>**А7.37.** Методи техніко-економічного аналізу та обґрунтування проєктних рішень<br>**А7.311.** Способи провадження апаратних засобів захисту інформації | **А7.У1.** Використовувати методи комп'ютерного проєктування та моделювання систем для розробки технічних проєктів комплексних систем захисту інформації та комплексів технічного захисту інформації<br>**А7.У2.** Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи, або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності |

| Чч | Поточна навчальна програма / силабус | | | Оновлена навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|---|---|---|
| | Професійні (фахові) компетенції | Знання | Уміння | Професійні компетенції | Знання | Уміння та навички |
| | | | | | | **А7.У3.** Аналізувати проєктні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації)<br>**А7.У10.** Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об'єктах інформаційної діяльності |

4. Назва дисципліни: **Кіберфізична безпека об'єктів критичної інфраструктури (*нова*)**

| Чч | Нова навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|
| | Професійні компетенції | Знання | Уміння та навички |
| 1 | **А1.** Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації | **А1.33.** Концепції і протоколи комп'ютерних мереж, методики забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних)системах і на об'єктах інформаційної діяльності<br>**А1.311.** Моделі та симуляції інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації | **А1.У4.** Визначити (формулювати) вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності підприємства (організації)<br>**А1.У8.** Використовувати моделі та симуляції інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації |
| 2 | **А2.** Здатність виявляти, досліджувати (оцінювати) системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та | **А2.32.** Методи (способи) та методики виявлення. Дослідження та системного аналізу загроз для інформації та кіберзагроз<br>**А2.36.** Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки. | **А2.У1.** Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах<br>**А2.У3**. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості |

| | | | |
|---|---|---|---|
| | кібербезпеки інформації у разі реалізації загроз | | комп'ютерної системи (систем) для розробки профілю безпеки |
| 3 | **А3.** Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах | **А3.31.** Поняття стратегії і політики безпеки інформації в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах<br>**А3.32.** Концепції архітектури безпеки мережі, включаючи технологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту)<br>**А3.35.** Поняття профілю безпеки інформації та функціональних послуг безпеки | **А3.У1.** Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах<br>**А3.У4.** Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в автоматизованих системах різного класу<br>**А3.У6.** Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи |
| 4 | **А4.** Здатність аналізувати, розробляти та супроводжувати систему управління інформаційною безпекою підприємства/організації | **А4.33.** Принципи створення систем інформаційної безпеки (NIST SP 800-160) | **А4.У6.** Створення системи (брати участь у створенні систем) інформаційної безпеки<br>**А4.У7.** Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації |
| 5 | **А5.** Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації | **А5.31.** Середовища функціонування автоматизованих систем | **А5.У7.** Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності) |
| 6 | | **А6.318**. Концепції та протоколи комп'ютерних мереж | |
| 7 | **А7.** Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах | **А7.32.** Методології забезпечення мережевої безпеки<br>**А7.35.** Методи програмування мікроконтролерів і контролерів відповідно до норм IEC 61131-3<br>**А7.39.** Процедури підключення до локальної мережі підприємства (організації) та до глобальних мереж, процедури активізації | **А7.У2.** Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес функцій з метою відновлення або поновлення після відмови системи, або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності |

| | | | |
|---|---|---|---|
| | | (настроювання) програмних мережевих механізмів захисту інформації<br>**А7.З10.** Концепції управління послугами для мереж і відповідних стандартів (бібліотека інфраструктури інформаційних технологій ( ITIL) | **А7.У3.** Аналізувати проектні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації)<br>**А7.У8.** Впроваджувати (налаштовувати) програмно-апаратні засоби захисту мережних комунікацій. |
| 8 | **А9.** Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації | **А9.З4.** Сучасні підходи по формуванню вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності | **А9.У1.** Формулювати (брати участь у форму ванні) вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності<br>**А9.У5.** Розроблювати плани аварійного відновлення та безперервності операцій інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах |
| 9 | **В2.** Здатність проводити періодичне обслуговування інформаційних систем та мереж , комплексних систем захисту інформації та комплексів технічного захисту інформації | **В2.З1.** Типи та періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення. | **В2.З5.** Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмово стійкі кластери, дублювання/»зеркалювання»<br>**В2.У6.** Здійснювати оновлення баз даних, антивірусних програм, програмних механізмів захисту інформації |
| 10 | **В6**. Здатність проводити процедуру сканування вразливостей і розпізнавання вразливостей в системах безпеки | **В6.З2.** Способи сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах | **В5.У6.** Використовувати відповідні інструменти для відновлення програмного та апаратного периферійного обладнання системи<br>**В5.У8.** Співпрацювати із системними аналітиками ,інженерами, програмістами, з метою отримання інформації про обмеження та можливості системи, вимог до продуктивності та інтерфейсів, шляхів модернізації системи і комплексів технічного захисту інформації |
| | | | **Д1.У3.** Проводити системний аналіз світових практик, стандартів із захисту інформації |
| | | | **Д2.У2.** Писати та публікувати методики та настанови з кібербезпеки та інструктивні матеріали |
| 11 | **Е2.** Здатність взаємодіяти з керівництвом і фахівцями технологічних та інших | **Е2.З2.** Положення про структурні підрозділи підприємства (організації), що задіяні в | **Е2.У**1. Взаємодіяти з керівництвом та працівниками технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, |

| | | | |
|---|---|---|---|
| | підрозділів підприємства/ організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту | спільному виконанні технологічних та функціональних завдань | пов'язаних із забезпеченням захисту інформації та кіберзахисту (організовувати та отримувати від технологічних та інших підрозділів інформацію, необхідну для організації захисту інформації та кіберзахисту, узгоджувати та погоджувати технічну документацію на системи та комплекси захисту інформації, доводити до керівництва підрозділів недоліки у захисті інформації та пропозицій до їх усунення, пропозицій про удосконалення систем та комплексів захисту інформації. |
| 12 | **Е3.** Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень. | **Е3.З4.** Порядок розроблення та виконання договірних робіт для зовнішніх партнерів | Е3.У1. Співпрацювати із зовнішніми партнерами доступними засобами комунікації стосовно питань захисту інформації та кіберзахисту |

5. Назва дисципліни: **Управління доступом до інформаційних ресурсів (*нова*)**

| Чч | Нова навчальна програма / силабус – з професійного стандарту | | |
|---|---|---|---|
| | Професійні компетенції | Знання | Уміння та навички |
| 1 | **А3.** Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах | **А3.З2.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту) | **А3.У1.** Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах |
| 2 | **А6.** Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності | **А6.З5.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті інформаційної діяльності<br>**А6.З15.** Статистична радіотехніка (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів) | **А6.У3.** Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності |