СИЛАБУС
з навчальної дисципліни:
ОК 1.3.12. "Комплексні системи захисту інформації: проектування, впровадження, супровід"

1. Загальна інформація про викладача	 **ГРИЩУК РУСЛАН ВАЛЕНТИНОВИЧ** **Посада:** начальник кафедри захисту інформації та кібербезпеки **Науковий ступінь:** доктор технічних наук (21.05.01 – Інформаційна безпека держави) **Вчене звання:** професор (125 – Кібербезпека) **Почесне звання:** заслужений діяч науки і техніки України **Наукові профілі та ідентифікатори:** *Scopus*: 57192962493 *Web of Science ID*: H-5679-2018 *GoogleScholar*: Ruslan Hryshchuk *ORCID*: 0000-0001-9985-8477 *Researchgate*: Ruslan Hryshchuk **Website:** https://www.zvir.zt.ua/ **Тел.:** (0412)-25-04-91 дод. 46-642 **E-mail:** Prof.Hry@gmail.com **Робоче місце:** 2/316
2. Код та статус **Назва навчальної дисципліни**	ОК 1.3.12 – обов'язкова навчальна дисципліна (*Дисципліни загально-професійної підготовки*). Комплексні системи захисту інформації: проектування, впровадження, супровід.
3. Кількість кредитів ESTS	11
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 330 36 16 8 12 294
5. Консультації	Згідно з графіком консультацій.
6. Час і навчальні локації	Визначається відповідно до затвердженого начальником військового інституту *Розкладу навчальних занять*.
7. Самостійна робота	Позааудиторні заняття.
8. Пререквізити	ОК 1.2.5. Інформаційні технології; ОК 1.3.3. Операційні системи; ОК 1.3.5. Архітектура комп'ютерних систем; 1.3.6. Інформаційно-комунікаційні системи; ОК 1.3.8. Прикладна криптологія; ОК 1.3.18. Основи кібербезпеки
9. Постреквізити	ОК 1.4.2. Переддипломна практика; ОК 1.4.3. Дипломне проєктування.
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційно-телекомунікаційних системах різного цільового призначення. *Потреба вивчення цієї дисципліни обумовлена* необхідністю вирішення практичних завдань, які виникають в процесі проектування, впровадження та супроводу комплексних систем захисту інформації. *За результатами вивчення цієї дисципліни* студент зможе самостійно або у складі служби захисту інформації спроектувати, впроваджувати та супроводжувати комплексні системи захисту інформації в інформаційно-телекомунікаційних системах різного цільового призначення. *У результаті вивчення дисципліни студент набуде:* програмні компетентності: КФ 1*: здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;* КФ 7: *здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);* КФ 9: *здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;*

	КФ 11: *здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;* КФ 13: *здатність до створення моделей кібербезпеки та проектування на їх основі систем кіберзахисту інформаційно-телекомунікаційних систем;* програмні результати навчання: РН 16: *реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;* РН 29: *здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;* РН 30: *здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;* РН 35: *вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;* РН 57: *вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;* РН 58: *вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.* *10.2. Мета навчальної дисципліни* – набуття навчаємими практичних навичок з проектування, впровадження та супроводу комплексних систем захисту інформації різного призначення. *10.3. Завдання вивчення дисципліни* – навчити студентів на основі діючих нормативно-правових документів впевнено проектувати, створювати та супроводжувати комплекси системи захисту інформації.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Порядок проведення робіт зі створення КСЗІ (1.1. Загальні положення; 1.2. Етапи створення КСЗІ). 2. Технічне завдання на створення КСЗІ в ІТС (2.1. Загальні вимоги до розроблення технічного завдання; 2.2. Вимоги до змісту розділів технічного завдання). 3. Оцінка захищеності інформації в ІТС від НСД (3.1. Побудова і структура критеріїв захищеності інформації; 3.2. Критерії конфіденційності, цілісності, доступності, спостереженості; 3.3. Оцінка коректності реалізації послуг безпеки (критерії гарантій)). 4. Особливості проектування КСЗІ для ІТС різних класів (4.1. Класифікація інформаційно-телекомунікаційних (автоматизованих) систем; 4.2. Функціональні профілі захищеності ІТС; 4.3. Особливості стандартних функціональних профілів захищеності ІТС. 5. Особливості захисту службової інформації від НСД в ІТС класу 2 (5.1. Загальні вимоги із захисту службової інформації; 5.2. Характеристика типових умов функціонування та вимог із захисту інформації в ІТС класу 2; 5.3 Політика реалізації послуг безпеки інформації в ІТС класу 2). 6. Планування захисту інформації в ІТС (6.1. Призначення та структура Плану захисту інформації в ІТС; 6.2. Зміст Плану захисту інформації в ІТС; 6.3. Календарний план робіт з захисту інформації в ІТС. 7. Випробування комплексу технічного захисту інформації та його атестація (7.1. Випробування комплексу технічного захисту інформації; 7.2. Атестація комплексів захисту інформації; 7.3. Порядок розроблення та оформлення паспорта на комплекс ТЗІ). 8. Управління комплексною системою захисту інформації в ІТС (8.1. Призначення, структура і зміст управління КСЗІ; 8.2.Служба захисту інформації в ІТС: призначення, завдання, функції, повноваження та відповідальність). 9. Введення КСЗІ в дію (9.1. Введення КСЗІ в дію; 9.2. Застосування КСЗІ за призначенням; 9.3. Технічна експлуатація КСЗІ). *Види занять:* лекції, практичні заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	1. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с. 2. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / Гайворонський М.В., Новиков О.М. – К.: вид. група BHV, 2009. – 608 с.

	3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / НД ТЗІ 2.5 – 004 – 99. – К.: 1999. – 51 с. 4. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] / НД ТЗІ 3.7 –003 – 05. – Київ.: 2005. – 35 с. 5. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу./ НД ТЗІ 1.1 – 003 – 99. – К.: 1999. – 47 с.
13. Підсумковий контроль, екзаменаційна методика	Екзамен в 6, 8 семестрах, залік в 7 семестрі, усне опитування.
14. Система підсумкового оцінювання	Підсумкове оцінювання результатів навчання складається із суми балів, отриманих студентом за виконання індивідуальних завдань та контрольних заходів, передбачених робочою програмою навчальної дисципліни за 100-бальною шкалою та національною шкалою, і становить: 90 - 100 балів, за національною шкалою – "відмінно"; 80 - 89 балів – "дуже добре"; 65 - 79 балів – "добре"; 55 - 64 балів – "задовільно"; 50 - 54 балів – "достатньо"; 35 - 49 балів – "незадовільно" з можливістю повторного складання; 1 - 34 балів – "неприйнятно" з обов'язковим повторним вивченням навчальної дисципліни.
15. Гнучкість та мобільність	У процесі вивчення дисципліни за ініціативою стейкхолдерів передбачається уточнення та коригування змісту навчальної дисципліни.
16. Політика курсу	1. До студентів напередодні вивчення дисципліни доводиться система організації навчального процесу на кафедрі захисту інформації та правила поведінки на заняттях. 2. Розподіл балів, які отримують студенти за навчальними елементами дисципліни доводиться до навчаємих на першому занятті 3. Під час навчання студенти зобов'язані дотримуватися академічної доброчесності: самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю; дотримуватися норм законодавства про авторське право; приймати активну участь у навчальному процесі; не запізнюватися на заняття, не пропускати заняття без поважних причин; самостійно і своєчасно опановувати матеріали пропущених з поважних причин занять; дотримуватися правил військової дисципліни та правил поведінки військовослужбовців громадських місцях. 4. Студенти, які мають навчальну заборгованість з даної дисципліни, повинні ліквідувати її у строк, установлений начальником військового інституту, але не пізніше чергового навчального збору. У разі документально підтверджених поважних причин повторне складання екзаменів дозволяється в період поточного збору у строк, установлений начальником військового інституту. 5. Студенти, які без поважних причин не виконали навчальний план (не ліквідували академічну заборгованість у встановлений строк, систематично не виконують індивідуальні завдання або не склали в період навчального збору звітність та в інших випадках, передбачених законодавством, відраховуються з військового інституту.
17. Адреса для зауважень та пропозицій	E-mail: Prof.Hry@gmail.com або ауд. 2/318 Кафедра захисту інформації та кібербезпеки.

Лектор -
заслужений діяч науки і техніки України,
доктор технічних наук, професор
полковник Руслан ГРИЩУК
"31"серпня 2020 року.

Розглянуто та ухвалено на засіданні кафедри захисту інформації та кібербезпеки.
Витяг з протоколу від 31 серпня 2020 р. № 1
Секретар кафедри -
старший викладач
підполковник ***п/п*** Володимир ОХРІМЧУК

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:
Заслужений діяч науки і техніки України,
доктор технічних наук, професор
полковник Руслан ГРИЩУК