СИЛАБУС
з навчальної дисципліни:
ОК 1.3.13. "Управління кібербезпекою"

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 1.3.13 – обов'язкова навчальна дисципліна (*Дисципліни загально-професійної підготовки*). Управління кібербезпекою.
3. Кількість кредитів ESTS	3,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 105 14 8 - 6 91
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 1.3.18. 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 управління кібербезпекою в інформаційно-телекомунікаційних системах. *Потреба вивчення цієї дисципліни обумовлена* необхідністю вирішення практичних завдань, які виникають в процесі управління кібербезпекою в інформаційно-телекомунікаційних системах. *За результатами вивчення цієї дисципліни* студент зможе самостійно або у складі служби захисту інформації управляти на основі міжнародних стандартів кібербезпекою інформаційно-телекомунікаційних систем. *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 2: *здатність до використання інформаційно-комунікаційних технологій, сучасних методів та моделей інформаційної та/або кібербезпеки;* *КФ 3: здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;* КФ 6: *здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;*

	КФ 8: *здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;* КФ 9: *здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;* КФ 10: *здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;* КФ 12: *здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;* програмні результати навчання: РН 12: *розробляти моделі загроз та порушника;* РН 14: *вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;* РН 19: *застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;* РН 22: *вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;* РН 41: *забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;* РН 43: *застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;* РН 46: *здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;* РН 49: *забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.* *10.2. Мета навчальної дисципліни* – набуття практичних навичок з розроблення політики та побудови моделей інформаційної безпеки для управління кібербезпекою інформаційно-телекомунікаційних систем. *10.3. Завдання вивчення дисципліни* – навчити студентів на основі діючих міжнародних стандартів створювати систему управління інформаційною безпекою та управляти за її допомогою кібербезпекою інформаційно-телекомунікаційних систем.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Аналіз інформаційно-телекомунікаційної системи, як об'єкта захисту (Постановка задачі. Аналіз структури ІТС. Аналіз інформаційних потоків в ІТС). 2. Моделі загроз і моделі порушника (Поняття загроз та їх джерела. Канали витоку інформації та методи оцінки їх інформативності. Методика оцінювання загроз. Неформальні моделі порушника. 3. Оцінювання ризиків порушення кібербезпеки ІТС (Поняття ризику кібербезпеки. Методи оцінювання ризиків. Оцінювання ймовірності реалізації загроз. Методи оцінки вартості активів).4. Система управління інформаційною безпекою (Поняття проблеми управління інформаційною безпекою. Цикл PDSA. Модель СУІБ. Приватний менеджмент СУІБ. сертифікація СУІБ). 5. Політика інформаційної безпеки (Поняття політики інформаційної безпеки організації. Принципи розроблення політики інформаційної безпеки. Роль керівництва організації і служби забезпечення інформаційної безпеки). 6. Управління інцидентами інформаційної безпеки (Поняття інциденту інформаційної безпеки. Класифікація інцидентів інформаційної безпеки. Оцінка наслідків інцидентів інформаційної безпеки). 7. Стандарти управління інформаційною безпекою (Міжнародні стандарти інформаційної безпеки. Група стандартів з інформаційної безпеки ISO 27000. Оброблення інцидентів інформаційної безпеки. Аудит інформаційної безпеки. Рекомендації щодо захисту. Кращі практики забезпечення інформаційної безпеки). *Види занять:* лекції, практичні заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	1. Васильев Р. А. Управление информационной безопасностью: Курс лекций, 2012 – 169 с. 2. ISO/IEC 27001:2013 «Системи управління інформаційною безпекою». 3. Грищук Р. В. Основи кібернетичної безпеки: монографія / Р. Грищук, Ю. Даник. – Житомир, 2016, 630 с. 4. Pérez González, D., Trigueros Preciado, S., & Solana-González, P. (2019). Organizational practices as antecedents of the information security management performance. https://doi.org/10.1108/ITP-06-2018-0261
13. Підсумковий контроль,	Залік в 7 семестрі, усне опитування.

екзаменаційна методика	
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 ***п/п*** 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