СИЛАБУС
з навчальної дисципліни:
ОК 1.3.10 "Системи технічного захисту інформації"

1. Загальна інформація про викладача	 **ОХРІМЧУК ВОЛОДИМИР ВАСИЛЬОВИЧ** **Посада:** старший викладач кафедри захисту інформації та кібербезпеки **Науковий ступінь:** **Вчене звання:** **Почесне звання:** **Наукові профілі та ідентифікатори:** *Scopus*: 57195468928 *GoogleScholar*: Володимир Васильович Охрімчук *ORCID*: 0000-0001-7518-9993 **Website:** https://www.zvir.zt.ua/ **Тел.:** (0412)-25-04-91 дод. 46-642 **E-mail:** okhrimchuk84@ukr.net **Робоче місце:** 2/318
2. Код та статус **Назва навчальної дисципліни**	ОК 1.3.10.- обов'язкова навчальна дисципліна (*дисципліна вільного вибору студента*). Системи технічного захисту інформації.
3. Кількість кредитів ESTS	4,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 135 16 10 - 6 119
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 1.3.5. Архітектура комп`ютерних систем.
9. Постреквізити	ОК 1.3.16. Фізичні основи технічних каналів витоку інформації в інформаційно телекомунікаційних системах.
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок із застосування систем технічного захисту інформації для виявлення та перекриття технічних каналів витоку інформаційні . *Потреба вивчення цієї дисципліни обумовлена* необхідністю здійснювати в процесі виконання професійних задач заходів із забезпечення захисту інформації від витоку її технічними каналами. *За результатами вивчення цієї дисципліни* студент зможе вільно проводити аналіз можливих причин і джерел утворення технічних каналів просочування інформації, аналіз технічних можливостей несанкціонованого отримання інформації, застосовувати методики пошуку технічних каналів витоку інформації, а також застосовувати технічні засоби пошуку та нейтралізації каналів несанкціонованого витоку інформації.. *У результаті вивчення дисципліни студент набуде:* програмні компетентності: КЗ 0 - *здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов;* КЗ 1 - *здатність застосовувати знання у практичних ситуаціях;* КЗ 2 - *знання та розуміння предметної області та розуміння професії;* КЗ 4- *вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;*

	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 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;* програмні результати навчання: РН 18 - *використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;* РН 21 - *вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;* РН 23 - *реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;* РН 36 - *виявляти небезпечні сигнали технічних засобів;* РН 37 - *вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;* РН 38 - *інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;* РН 39 - *проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документа;* РН 40 - *інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;* РН 52 -*використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах*. *10.2. Мета навчальної дисципліни* – формування теоретичних знань та практичних навичок дослідження технологій передачі та обробки інформації в інформаційно-комунікаційних системах з метою виявлення можливих каналів несанкціонованого отримання інформації, вивчення причин і джерел виникнення технічних каналів просочування інформації, методів і способів несанкціонованого до-ступу до інформації і її руйнування, методів і технічних засобів захисту інформації, принципів побудови і експлуатації технічних засобів виявлення і захисту каналів передачі інформації. *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати на практиці отримані знання та уміння щодо захисту інформації, що циркулює на об'єктах інформаційної діяльності від витоку технічними каналами з використанням технічних засобів захисту.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Організаційно-правові засади технічного захисту інформації. Технічні канали витоку інформації. 2. Методи і засоби несанкціонованого доступу до інформації. 3. Методи і засоби технічного захисту інформації. *Види занять:* лекції, практичні заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. В.О.Хорошко, О.Д. Азаров, Г.О.Максименко, Ю.Є.Яремчук. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник.-Вінниця: ВНТУ, 2007.-333 с. 2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. *Електронна бібліотека ЖВІ:* 1. https://zvir.zt.ua/home/pro-instytut з доступом до електронних баз даних у локальній комп'ютерній мережі в усіх навчальних корпусах військового інституту. *Українська науково-освітня телекомунікаційна мережа УРАН:* 1. http://www.uran.net.ua/~ukr/uran-members.htm.

13. Підсумковий контроль, екзаменаційна методика	Екзамен в 4 семестрі, письмові відповіді на запитання білетів.
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: okhroimchuk84@ukr.net або ауд. 2/318 Кафедра захисту інформації та кібербезпеки.

Лектор –
старший викладач кафедри захисту інформації та кібербезпеки
підполковник ***n/n*** Володимир ОХРІМЧУК
“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 ***n/n*** Володимир ОХРІМЧУК

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