СИЛАБУС
з навчальної дисципліни:
ОК 1.3.18 "Основи кібербезпеки"

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 1.3.18.- обов'язкова навчальна дисципліна (*дисципліна вільного вибору студента*). Основи кібербезпеки.
3. Кількість кредитів ESTS	2
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 60 12 4 - 8 48
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.
9. Постреквізити	ОК 1.3.5. Архітектура комп`ютерних систем. ОК 1.3.9. Нормативно-правове забезпечення інформаційної безпеки
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок із безпечного використання кіберпростору. *Потреба вивчення цієї дисципліни обумовлена* необхідністю постійного використання в повсякденній діяльності кіберпростору із заданим гарантованим рівнем захищеності. *За результатами вивчення цієї дисципліни* студент зможе вільно проводити аналіз та розкриття особливостей видів кіберзагроз, проводити основні дії в кіберпросторі, а також здійснювати безпечне його використання. *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 2 - *знання та розуміння предметної області та розуміння професії;* КЗ 4 - *вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;* КЗ 6 - *здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;* 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 3 - *здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;* програмні результати навчання: 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 24 - *вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);* РН 32 - *вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;* РН 33 - *вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;* РН 45 - *застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;* РН 49 - *забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;* РН 52 -*використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах*. *10.2. Мета навчальної дисципліни* – формування теоретичних знань та практичних навичок з основ забезпечення кібербезпеки, засвоєння основних організаційних заходів забезпечення кібербезпеки в інформаційних системах різного класу та призначення, ва також формування компетенції втілення в життя державної політики в сфері забезпечення кібербезпеки.. *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати на практиці отримані знання та уміння щодо здійснення кіберзахисту ІТС.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Поняття кібербезпеки. Терміни та визначення. 2. Кібернетичні дії та їх особливість. 3. Шкідливе програмне забезпечення та мережеві кібератаки.. *Види занять:* лекції, практичні заняття. 4. Забезпечення кібербезпеки держави: концептуальні засади. *Методи навчання:* пояснювально-ілюстративні та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія /Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016 – 636 с. 2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 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	Залік в 2 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