СИЛАБУС
з навчальної дисципліни:
ОК 1.3.9 "Нормативно-правове забезпечення інформаційної безпеки"

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 1.3.9.- обов'язкова навчальна дисципліна (*дисципліна вільного вибору студента*). Нормативно-правове забезпечення інформаційної безпеки.
3. Кількість кредитів ESTS	2
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні семінари самостійна робота	 60 10 4 - 6 50
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 1.3.18. Основи кібербезпеки.
9. Постреквізити	ОК 1.3.8. Прикладна криптологія.
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок із застосування нормативно-правових актів України та міжнародного законодавства при вирішенні питань забезпечення технічного захисту інформації, інформаційної та кібернетичної безпеки. *Потреба вивчення цієї дисципліни обумовлена* необхідністю неухильно дотримуватись значної кількості нормативно-правових актів як України так і міжнародних з питань забезпечення інформаційної та кібернетичної безпеки при вирішення нагальних практичних завдань, які виникають в ході виконання службових обов'язків як у пункті постійної дислокації так і за її межами. *За результатами вивчення цієї дисципліни* студент зможе вільно використовувати законодавчу бузу України за професійним спрямуванням для аналізу та розкриття особливостей правового статусу видів інформації з обмеженим доступом, застосовувати на практиці здобуті знання, розуміти і застосовувати у повсякденній діяльності нормативно-правові основи інформаційної та кібернетичної безпеки, використовувати основні правові джерела щодо планування та реалізації заходів захисту інформації в інформаційно – телекомунікаційних системах відомств, установ, організацій України. *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 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 2 - *здатність до використання інформаційно-комунікаційних технологій, сучасних методів та моделей 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.);* програмні результати навчання: РН 8 - *готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;* РН 23 - *реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;* РН 33 - *вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;* 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 43 - *застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;* РН 44 - *вирішувати задачі безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;* *10.2. Мета навчальної дисципліни* – вивчення основних понять нормативно-правового забезпечення технічного захисту інформації та кібербезпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство, опанування основними термінами та категоріями нормативно-правового забезпечення інформаційної безпеки на рівні їх тлумачення та відтворення, для практичного застосування та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки.. *10.3. Завдання вивчення дисципліни* – сформувати у студентів уявлення про правові передумови захисту інформації, інформаційної та кібернетичної безпеки в Україні, цілісні знання про правові норми, що регламентують суспільні відносини з приводу у інформаційній галузі в Україні.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Нормативно-правові акти, які закріплюють концептуальні положення інформаційної безпеки України. Види таємниць особистого життя з урахуванням чинного законодавства 2. Розвиток стандартів управління інформаційною безпекою. Стандарти ISO/IEC управління інформаційною безпекою. 3. Нормативно-правові акти з охорони державної таємниці. 4. Нормативно-правові акти щодо захисту інформації в телекомунікаційних системах. 5. Нормативно-правові акти з технічного захисту інформації. 6. Закони про електронний документообіг та цифровий підпис. 7. Підзаконні акти щодо електронного документообігу та цифрового підпису. 8. Нормативно-правові акти з ліцензування діяльності у сферах інформаційної безпеки. 9. Нормативно-правові акти з державної експертизи у сферах інформаційної безпеки *Види занять:* лекції, семінарські заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Нормативні основи забезпечення технічного захисту інформації в інформаційно-телекомунікаційних системах: Збірник документів – Житомир: ЖВІ, 2018. – 191 с. 2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативних документів/О.Г. Корченко, Ю.О. Дрейс. – Житомир: ЖВІ, 2010. – 280 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 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