СИЛАБУС
з навчальної дисципліни:
ОК 1.3.16. "Фізичні основи технічних каналів витоку інформації в інформаційно телекомунікаційних системах"

1. Загальна інформація про викладача	 **ГУМЕНЮК ІГОР ВОЛОДИМИРОВИЧ** **Посада:** доцент кафедри захисту інформації та кібербезпеки **Науковий ступінь:** кандидат технічних наук (20.02.14 – Озброєння і військова техніка) **Наукові профілі та ідентифікатори:** *GoogleScholar*: Ihor Humeniuk *ORCID*: 0000-0001-5853-3238 *Researchgate*: Ігор Володимирович Гуменюк **Website:** https://www.zvir.zt.ua/ **Тел.:** (096)-870-60-03 **E-mail:** ig_gum@ukr.net **Робоче місце:** 2/312
2. Код та статус **Назва навчальної дисципліни**	ОК 1.3.16 – обов'язкова навчальна дисципліна (*дисципліна вільного вибору студента*). Фізичні основи технічних каналів витоку інформації в інформаційно телекомунікаційних системах.
3. Кількість кредитів ESTS	3,0
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 90 10 4 4 2 80
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 1.2.2. Фізика; ОК 1.3.2. Основи теорії кіл, сигнали та процеси в електроніці; ОК 1.3.10. Системи технічного захисту інформації
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 оцінювання рівня загроз інформації можливих каналів витоку інформації, планування роботи щодо створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності органів військового управління, військових частин (підрозділів), установ Міністерства оборони України та Збройних Сил України, інших міністерств і відомств сектору безпеки та оборони держави. *Потреба вивчення цієї дисципліни обумовлена* необхідністю вирішення нагальних практичних завдань, які виникають в ході виконання службових обов'язків поза межами пунктів постійної дислокації в умовах жорстких часових та фінансових обмежень. *За результатами вивчення цієї дисципліни* студент зможе проводити оцінку рівня загроз інформації можливих каналів витоку інформації, вживати заходів щодо їх закриття, планувати роботи щодо створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. *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 5 - *здатність до пошуку, оброблення та аналізу інформації.* КФ 11 - *здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;* програмні результати навчання: РН 20 - *забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних 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.* *10.2. Мета навчальної дисципліни* – сформувати та виробити на рівні автоматизму практичні навички з оцінювання рівня загроз інформації можливих каналів витоку інформації, вживати заходів щодо їх закриття. *10.3. Завдання вивчення дисципліни* – навчити студентів фізичних принципів (основ) утворення технічних каналів витоку інформації та застосовувати сучасні методи (системи) захисту від несанкціонованого доступу.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Фізичні основи акустичних та оптичних каналів витоку інформації (Поняття та класифікація технічних каналів витоку інформації. Класифікація та фізичні основи акустичних каналів витоку інформації. Класифікація візуально-оптичних каналів витоку інформації. Системи прихованого відеонагляду. Основні характеристики, принципи дії та особливості застосування). 2. Дослідження акустичних та оптичних каналів інформації (Дослідження акустичних та оптичних каналів інформації в умовах відсутності засобів захисту від її витоку. Дослідження акустичних та оптичних каналів інформації в умовах захищеності від її витоку). 3. Фізичні основи каналів витоку інформації ПЕМВН (Загальні поняття та характеристики витоку інформації ПЕМВН. Класифікація каналів витоку інформації ПЕМВН. Основи утворення каналів витоку інформації ПЕМВН). 4. Канал побічних електромагнітних наведень (Канал ПЕМН на лінії електроживлення (заземлення) основних технічних засобів та систем. Канал ПЕМН на комунікації допоміжних технічних засобів та систем). 5. Дослідження каналів ПЕМН в умовах відсутності засобів захисту від її витоку (Дослідження каналів ПЕМН в умовах відсутності засобів захисту від її витоку. Дослідження каналів ПЕМН в умовах захищеності від її витоку). *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации // Київ : Юниор, 2003, 504 с. 2. Рибальський О. В., Смаглюк В. М., Хахановський В. Г. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України, Київ : Вид. Національної академії внутріш. справ, 2010, 255 с. *Житомирська обласна універсальна наукова бібліотека ім. Олега Ольжича:* http://www.lib.zt.ua. *Національна бібліотека України ім. В. І. Вернадського:* http://www.nbuv.gov.ua.
13. Підсумковий контроль, екзаменаційна методика	Екзамен 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;

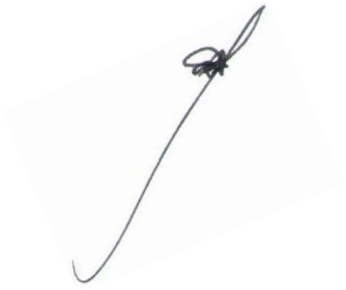
	1 - 34 балів – “неприйнятно” з обов’язковим повторним вивченням навчальної дисципліни.
15. Гнучкість та мобільність	У процесі вивчення дисципліни за ініціативою стейкхолдерів передбачається уточнення та коригування змісту навчальної дисципліни.
16. Політика курсу	1. До студентів напередодні вивчення 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: ig_gum@ukr.net або ауд. 2/312 Кафедра захисту інформації та кібербезпеки.

Лектор -
кандидат технічних наук
майор ***n/n*** Ігор ГУМЕНЮК
“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