СИЛАБУС
з навчальної дисципліни:
ОК 1.3.11. "Захист інформації в інформаційно-комунікаційних системах"

1. Загальна інформація про викладача	 **САМЧИШИН ОЛЕКСІЙ ВОЛОДИМИРОВИЧ** **Посада:** професор кафедри захисту інформації та кібербезпеки **Науковий ступінь:** кандидат технічних наук (20.02.14 – Озброєння і військова техніка) **Наукові профілі та ідентифікатори:** *Scopus*: 57203663374 *GoogleScholar*: Oleksyj Samchyshyn *ORCID*: 0000-0002-1542-1065 *Researchgate*: Samchyshyn, Oleksyj **Website:** https://www.zvir.zt.ua/ **Тел.:** (096)-870-60-03 **E-mail:** samyj123@ukr.net **Робоче місце:** 2/312
2. Код та статус **Назва навчальної дисципліни**	ОК 1.3.11 – обов'язкова навчальна дисципліна (*дисципліна вільного вибору студента*). Захист інформації в інформаційно-комунікаційних системах.
3. Кількість кредитів ESTS	12,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 375 42 20 8 14 333
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 1.3.8. Прикладна криптологія
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 із забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки 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 в інформаційно-комунікаційних системах, 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 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;* КЗ 5 – *здатність до пошуку, оброблення та аналізу інформації;* КФ 5 – *здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;* КФ 11 - *здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;* КФ 13 -*здатність до створення моделей кібербезпеки та проектування на їх основі систем кіберзахисту інформаційно-телекомунікаційних систем;* програмні результати навчання: РН 11 - *виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;* 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 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 28 - *аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;* РН 30 - *здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;* РН 47 - *вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;* РН 51 - *підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.* *10.2. Мета навчальної дисципліни* – сформувати та виробити на рівні автоматизму практичні навички з оцінювання рівня загроз інформації відкритих інформаційно-комунікаційних систем та мереж. *10.3. Завдання вивчення дисципліни* – навчити студентів визначати і усувати основні загрози інформаційної безпеки та розробляти політику інформаційної безпеки для відкритих інформаційно-комунікаційних систем та мереж.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Стандартизація і модельне представлення відкритих інформаційно-комунікаційних систем. 2. Інтранет як відкрита система. 3. Вразливість відкритих інформаційно-комунікаційних систем на прикладі Інтранету. 4. Атаки на інформаційно-комунікаційні системи. 2. Забезпечення інформаційної безпеки в інформаційно-комунікаційних системах. 3. Аутентифікація суб'єктів і об'єктів взаємодії в інформаційно-комунікаційних системах. Міжмережеві екрани. Протоколи захищених каналів. Системи виявлення вторгнень, системи попередження вторгнень. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Грайворонський М. В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича группа BHV, 2009. – 608 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. 3. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации // Київ : Юниор, 2003, 504 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	Курсова робота, екзамен у 8 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: samyj123@ukr.net або ауд. 2/312 Кафедра захисту інформації та кібербезпеки.

Лектор -
кандидат технічних наук,
професор кафедри захисту інформації та кібербезпеки
підполковник ***п/п*** Олексій САМЧИШИН
“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