СИЛАБУС
з навчальної дисципліни:
ВК 2.1.6. "Основи комп'ютерного проектування та моделювання систем захисту інформації"

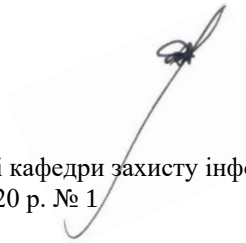
1. Загальна інформація про викладача	 **ГРИЩУК РУСЛАН ВАЛЕНТИНОВИЧ** **Посада:** начальник кафедри захисту інформації та кібербезпеки **Науковий ступінь:** доктор технічних наук (21.05.01 – Інформаційна безпека держави) **Вчене звання:** професор (125 – Кібербезпека) **Почесне звання:** заслужений діяч науки і техніки України **Наукові профілі та ідентифікатори:** *Scopus*: 57192962493 *Web of Science ID*: H-5679-2018 *GoogleScholar*: Ruslan Hryshchuk *ORCID*: 0000-0001-9985-8477 *Researchgate*: Ruslan Hryshchuk **Website:** https://www.zvir.zt.ua/ **Тел.:** (0412)-25-04-91 дод. 46-642 **E-mail:** Prof.Hry@gmail.com **Робоче місце:** 2/316
2. Код та статус **Назва навчальної дисципліни**	ВК 2.1.6 - вибіркова навчальна дисципліна (*дисципліна вільного вибору студента*). Основи комп'ютерного проектування та моделювання систем захисту інформації.
3. Кількість кредитів ESTS	3,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 105 50 24 - 26 55
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. Пререквізіти	ОК 1.2.1. Вища математика; ОК 1.2.2. Фізика; ОК 1.3.2. Основи теорії кіл, сигнали та процеси в електроніці; ОК 1.3.4. Електроніка; ОК 1.3.10. Системи технічного захисту інформації; ВК 2.1.4. Основи метрології.
9. Постреквізіти	ВК 2.1.8. Комп`ютерна стеганографія; ВК 2.1.7. Організаційне забезпечення захисту інформації.
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок з комп'ютерного проектування та моделювання систем захисту інформації об'єктів 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 спроектувати та змоделювати роботу тієї чи іншої системи захисту інформації на об'єкті інформаційної діяльності відповідно до існуючої моделі загроз. *У результаті вивчення дисципліни студент набуде:* програмні компетентності: КФ 13 - *здатність до створення моделей кібербезпеки та проектування на їх основі систем кіберзахисту інформаційно-телекомунікаційних систем;*

	програмні результати навчання: РН 12 - *розробляти моделі загроз та порушника*; РН-64 - *виконувати функціональну композицію програмних систем захисту інформації та проводити її об'єктно-орієнтований аналіз та візуальне проектування;* РН-64 - *проектувати бази даних систем захисту інформації та кібернетичної безпеки з використанням ER-моделі.* *10.2. Мета навчальної дисципліни* – сформувати та виробити на рівні автоматизму практичні навички з комп'ютерного проектування та моделювання систем захисту інформації. *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати САПР вільного поширення (Фонду вільного програмного забезпечення https://directory.fsf.org/wiki/Main_Page) для того щоб навчитися проектувати системи захисту інформації та моделювати їх роботу.
11. Навчальна логістика	*Зміст навчальної дисципліни:* *Модуль 1. Основи проектування систем захисту інформації.* Тема 1. Основні положення проектування систем захисту інформації. Вступ. Основні поняття та визначення, що використовуються при проектуванні систем захисту інформації. Нормативно-правове забезпечення робіт з проектування. Порядок проведення робіт із створення СЗІ в інформаційно-комунікаційних системах. Етапи побудови СЗІ. Тема 2. Життєвий цикл систем захисту інформації. Поняття проекту. Класифікація проектів. Основні фази проектування. Основні, допоміжні та організаційні процеси життєвого циклу СЗІ. Структура життєвого циклу СЗІ. Моделі життєвого циклу СЗІ. Тема 3. Розробка технічного завдання на створення системи захисту інформації в автоматизованій системі. Нормативне забезпечення. Основі складові, порядок розроблення, зміст, вимоги до змісту технічного завдання. Вимоги до системи захисту інформації та складу проектної та експлуатаційної документації. *Модуль 2. Концептуальні положення проектування та моделювання систем захисту інформації".* Тема 4. Основні концептуальні положення побудови систем захисту інформації Концептуальні підходи до проектування систем захисту інформації. Комплекс інженерно-технічного захисту інформації. Приклад багаторівневої інтегрованої автоматизованої системи охорони особливо важливих об'єктів. Особливості побудови систем захисту від несанкціонованого доступу. Тема 5. Загальні положення та визначення об'єктно-орієнтованого моделювання і проектування. Основи методології проектування систем захисту інформації. Методологія процедурно-орієнтованого програмування. Методологія об'єктно-орієнтованого аналізу і програмування. Методологія системного аналізу і системного моделювання. Розвиток методології об'єктно-орієнтованого аналізу і проектування систем. *Модуль 3. Методологія та технологія розробки систем захисту інформації.* Тема 6. Проектування та моделювання систем захисту інформації за допомогою UML. Призначення та загальна структура мови моделювання UML. Основні пакети та опис метамоделі UML. Відношення у мові моделювання UML та позначення цих відношень. Інтерфейс CASE засобу Rational Rose. Тема 7. Діаграми концептуального, логічного і фізичного моделювання UML Діаграми варіантів використання (use case diagram) системи: основні елементи діаграми; відношення на діаграмі елементів використання; текстові сценарії елементів використання; рекомендації для розроблення діаграм варіантів використання. Приклад побудови діаграми. Діаграми класів (class diagram) системи: класи та відношення між ними; розширення UML для побудови моделей програмного забезпечення; шаблони або параметризовані класи; моделювання та проектування класів. Приклад побудови діаграми. Діаграми кооперації (collaboration diagram) системи: основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми кооперації. Приклад побудови діаграми. Діаграми послідовності (sequence diagram) дій системи: основні елементи діаграми; відношення на діаграмі та зв'язки; примітки; рекомендації щодо побудови діаграми послідовності дій. Приклад побудови діаграми. Діаграми станів системи (statechart diagram): основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми станів. Приклад побудови діаграми.

	Діаграми діяльності (активності) (activity diagram) системи: основні елементи діаграми; відношення на діаграмі та зв'язки; рекомендації щодо побудови діаграми діяльності; переходи; доріжки; об'єкти. Приклад побудови діаграми. Діаграми компонентів (component diagram) та діаграми розгортання: компоненти; інтерфейси; залежності; вузли; з'єднання і залежності. Приклади побудови діаграм компонентів і діаграм розгортання. *Види занять:* лекції, практичні заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Хорошко В. О. Проектування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов. – К. : ВІТІ, ДУІКТ, 2011. – 245 с. 2. Томашевський В. М. Моделювання систем / В. М. Томашевський. – К. : Видавнича група BHV, 2005. – 352 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 5 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: Prof.Hry@gmail.com або ауд. 2/318 Кафедра захисту інформації та кібербезпеки.

Лектор -
заслужений діяч науки і техніки України,
доктор технічних наук, професор
полковник
“31”серпня 2020 року.



Руслан ГРИЩУК

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