СИЛАБУС
з навчальної дисципліни:
ОК 1.3.15. "Прикладні системи оцінювання ризиків в кібербезпеці"

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**	ОК 1.3.15 – обов'язкова навчальна дисципліна (*Дисципліни загально-професійної підготовки*). Прикладні системи оцінювання ризиків в кібербезпеці.
3. Кількість кредитів ESTS	3
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 90 14 6 - 8 76
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; ОК 1.3.18. Основи кібербезпеки; ОК 1.3.5. Архітектура комп'ютерних систем; ОК 1.3.3. Операційні системи.
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 студентами теоретичних та практичних знань з питань оцінювання ризиків кібербезпеці інформаційно-телекомунікаційних систем військового та (або) подвійного призначення. *Потреба вивчення цієї дисципліни обумовлена* необхідністю вирішення нагальних практичних завдань, які виникають в ході виконання службових обов'язків в умовах імплементації та динамічного переходу Україною на кращі світові безпекові практики відповідно до стандартів ISO/IEC серії 2700х, 290хх, 13335, 15408, 18044, 18028, 15947, 15443 тощо. *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 8: *здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;* КФ 11: *здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;*

	КФ 12: *здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;* програмні результати навчання: РН 9: *впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;* РН 18: *використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;* РН 19: *застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;* РН 30: *здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;* РН 42: *впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;* РН 46: *здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;* РН 49: *забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;* РН 50: *забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);* РН 52: *використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.* *10.2. Мета навчальної дисципліни – надати основні теоретичні знання та привити ключові практичні навички з питань застосування прикладних систем оцінювання ризиків в кібербезпеці.* *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати прикладні системи оцінювання ризиків.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Базові поняття та міжнародні стандарти в галузі аналізу та оцінювання ризиків кібербезпеки: оцінювання ризику кібербезпеки інформаційно-телекомунікаційних систем; аналіз ризиків кібербезпеці; управління ризиком кібербезпеці; міжнародні стандарти в галузі аналізу та оцінювання ризиків кібербезпеки (NIST 800-30; BSI-Standard 100-3; РС БР ИББС-2.2-2009; ISO/IEC 27005:2008; AS/NZS 4360:2004; ISO/FDIS 31000). 2. Методологічний інструментарій та прикладні системи оцінювання ризиків кібербезпеці: методи – CRAMM; баєсовські мережі; VAR; Coras; EBIOS; ISAMM; – методики: COBRA; TRA; FRAP; Risk Matrix; Mehari; MAGERIT; Information Security RA; – методологія: IRAM2; – інструментарій: RA2 Art of Risk; PTA; Callio Secura 17799. Прикладні системи оцінювання ризиків кібербезпеці: система RiskWatch; система КЕС управління інформаційною безпекою «АванГард»; система Enterprise Risk Assessor; система vsRisk, система Risk Assessment Tool; система OCTAVE; система Гриф 2006; система RiskPAC; система Microsoft Security Assessment Tool. Бази даних уразливостей кібербезпеки. 3. Бази даних уразливостей кібербезпеки: національна база даних уразливостей (National Vulnerability Database); банк даних загроз безпеці інформації; база даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database); база даних уразливостей IBM X-Force; база даних записів уразливостей US-CERT; база даних уразливостей SecurityFocus. *Види занять:* лекції, практичні заняття. *Методи навчання:* словесні (лекція, бесіда, розповідь), наочні (демонстрація, ілюстрація), практичні (вправи). *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* *1. Грищук Р. В. Основи кібернетичної безпеки : Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.* *2. Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems / Hryshchuk R., Yevseiev, S. Shmatko A. – Vienna.: Premier Publishing s. r. o., 2018. – 284 p.* *3. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: моно-графія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 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. *Інтернет:* *1. О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с.* *2. Information technology – Security techniques – Information security risk management: ISO/IEC 27005:2008. – [Чинний від 15-06-2008]. — Женева: [б.в.], 2008. – 64 с. – (Міжнародні стандарти ISO/IEC).* *1. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О.Г. Пузиренко, С.О. Івко, О.О. Лаврут // Системи обробки інформації .- Х.: ХУПС,; 2014. – Вип. 8 (124). – С. 128-134.* *2. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Архипов, А. Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366–375.* *3. Бучик С. Методика оцінювання інформаційних ризиків в автоматизованій системі / С. Бучик, С. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – 2015. – Вип. 11. – С. 33–43.* *4. Віннікова І. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними / І. Віннікова, С. Марчук // Східна Європа: економіка, бізнес та управління. – 2018. – № 5. – С. 110–114.*
13. Підсумковий контроль, екзаменаційна методика	Залік в 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: 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 ***n/n*** Руслан ГРИЩУК
“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