СИЛАБУС
з навчальної дисципліни:
ОК 1.3.8. "Прикладна криптологія"

1. Загальна інформація про викладача	 **СІДЕНКО ВОЛОДИМИР ПАВЛОВИЧ** **Посада:** доцент кафедри захисту інформації та кібербезпеки **Науковий ступінь:** **Вчене звання:** **Почесне звання:** **Наукові профілі та ідентифікатори:** **Website:** https://www.zvir.zt.ua/ **Тел.:** (0412)-25-04-91 дод. 46-641 **E-mail:** sidvkadpavl@gmail.com svhzt1952@gmail.com **Робоче місце:** 2/314
2. Код та статус Назва навчальної дисципліни	ОК 1.3.8 - обов'язкова навчальна дисципліна Прикладна криптологія.
3. Кількість кредитів ESTS	9
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні курсовий проект самостійна робота	 300 28 16 12 - 30 272
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 1.2.3. Теорія ймовірності і математична статистика; ОК 1.2.4 Дискретна математика; ОК 1.2.5. Інформаційні технології; ОК 1.3.4. Електроніка; ОК 1.3.7. Теорія інформації та кодування; ОК 1.3.9. Нормативно-правове забезпечення інформаційної безпеки
9. Постреквізіти	ОК 1.3.11. Захист інформації в інформаційно-комунікаційних системах; ОК 1.4.3. Дипломне проєктування; ВК 2.1.8. Комп`ютерна стеганографія
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок з криптографічного 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 використати методи та засоби криптографічного захисту інформації та забезпечити 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: 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 2 - Знання та розуміння предметної області та розуміння професії КЗ 4 - Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

	КФ 10 - Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності програмні результати навчання: РН 17 - забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент РН 23 - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах РН 31 - застосовувати теорії та методи захисту для забезпечення безпеки 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 48 - виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах *10.2. Мета навчальної дисципліни* – сформувати та виробити на рівні автоматизму практичні навички з криптографічного захисту інформації в інформаційно-телекомунікаційних системах та мережах. *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати відомі вітчизняні та зарубіжні криптографічні алгоритми та пристрої захисту інформації в інформаційно-телекомунікаційних системах та мережах.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Основи інформаційної безпеки. Загрози безпеки інформаційних систем. Загальні відомості про криптологію, криптографію та криптоаналіз. Класифікація й загальна характеристика криптографічних систем. 2. Класичні криптографічні системи з шифрами заміни (підстановки), з шифрами перестановки та гамування. 3. Принципи побудови стійких криптографічних алгоритмів шифрування даних. Загальні відомості про криптографічні системи симетричного шифрування даних. Потокове шифрування даних. 4. Шифрування даних за допомогою блокових симетричних криптографічних алгоритмів. Побудова криптографічного алгоритму блокового симетричного шифрування даних AES. Побудова криптографічного алгоритму блокового симетричного шифрування даних "Калина". 5. Перетворення даних за допомогою криптографічних алгоритмів з відкритими ключами та хешування. Криптографічні алгоритми шифрування даних з відкритими ключами. Криптографічні алгоритми шифрування даних з відкритими ключами RSA та Ель-Гамаля. 6. Криптографічні алгоритми гешування даних. Криптографічні алгоритми гешування SHA-1, SHA-512, Купина-п. 7. Криптографічні алгоритми цифрових підписів, стійкість яких засновується на використанні дискретних логарифмів RSA, Ель-Гамаля, Шнора та DSA. 8. Криптографічні алгоритми цифрових підписів, стійкість яких засновується на використанні еліптичних кривих ECDSS, ГОСТ Р 34.10-2018 та ДСТУ 4145-2002. 9. Управління та розподіл ключів шифрування даних (повідомлень). *Види занять:* лекції, лабораторні та практичні заняття, курсове проектування. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво "Форт", 2012. – 880 с.: іл. 2. Корченко О.Г. Прикладна криптологія: системи шифрування: підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУТ - ТОВ "Наш формат", 2014. – 448 с.: іл. 3. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник / В.В. Поповский, А.В. Персиков: В 2-х т. Том 1. – Харьков: ООО "Компания СМИТ", 2006. – 238 с.: ил. 4. ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення". – К.: Держстандарт України, 2015. – 235 с.

	5. ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”. – К.: Держстандарт України, 2015. – 43 с. 6. ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”. – К.: Держстандарт України, 2003. – 44 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:* 2. http://www.uran.net.ua/~ukr/uran-members.htm.
13. Підсумковий контроль, екзаменаційна методика	Екзамен у шостому та сьомому семестрах; диференційований залік у сьомому семестрі з захисту курсового проєкту; усне опитування та комп’ютерне тестування по тестах.
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 тих хто навчається 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 початку 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: sidvkadpavl@gmail.com; svpzt1952@gmail.com або ауд. 2/314 Кафедра захисту інформації та кібербезпеки.

Лектор –
доцент кафедри захисту інформації та кібербезпеки
працівник ЗСУ ***п/п*** Володимир СІДЕНКО
“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