СИЛАБУС
з навчальної дисципліни:
ВК 2.1.8. "Комп'ютерна стеганографія"

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**	ВК 2.3.8 - вибіркова навчальна дисципліна Комп'ютерна стеганографія.
3. Кількість кредитів ESTS	3,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні практичні самостійна робота	 105 14 6 8 - 91
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 1.2.1. Вища математика; ОК 1.2.3. Теорія ймовірності і математична статистика; ОК 1.2.4 Дискретна математика; ОК 1.2.5. Інформаційні технології; ОК 1.3.1. Технології програмування; ОК 1.3.7. Теорія інформації та кодування; ОК 1.3.8. Прикладна криптологія; ВК 2.1.2. Програмування
9. Постреквізити	ОК 1.3.11. Захист інформації в інформаційно-комунікаційних системах; ОК 1.4.3. Дипломне проектування; 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 стеганографічного 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 стеганографічного 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:** **КФ 17** - *здатність до безпечної експлуатації систем передачі інформації в інформаційно-телекомунікаційних системах***;** **програмні результати навчання:** **РН 27** - *вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах***;** **РН-60** - *розробляти алгоритми розв'язку типових прикладних задач забезпечення інформаційної та кібернетичної безпеки***.**

	10.2. Мета навчальної дисципліни – сформувати та виробити на рівні автоматизму практичні навички з стеганографічного захисту інформації в інформаційно-телекомунікаційних системах та мережах. *10.3. Завдання вивчення дисципліни* – навчити студентів застосовувати відомі вітчизняні та зарубіжні стеганографічні алгоритми захисту інформації в інформаційно-телекомунікаційних системах та мережах.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Загальні відомості про стеганографічні системи. Загальні відомості про комп'ютерну стеганографію. Структурна схема типової комп'ютерної стеганографічної системи. Принципи побудови комп'ютерних стеганографічних системи та напрями їх застосування. 2. Приховування даних з використанням комп'ютерних стеганографічних методів шляхом вбудовування їх в нерухомих зображеннях: Характеристика, моделі та режими графічних файлів; Приховування даних в просторової області нерухомих зображень заміни найменш значущого біта, методом псевдовипадкового інтервалу та перестановки, блоковим методом, методом заміни палітри, методом квантування зображення та методом Куттера-Джордана-Боссена. 3. Приховування даних з використанням комп'ютерних стеганографічних методів шляхом вбудовування їх в частотної області нерухомих зображень: Приховування даних в частотної області методом відносної заміни величин коефіцієнтів ДКП; Приховування даних в частотної області методом розширення спектру. 4. Приховування даних з використанням комп'ютерних стеганографічних методів шляхом вбудовування їх в аудіосигналах та текстових файлах: Приховування даних у часової області аудіосигналів методом кодування найменш значущих бітів; Приховування даних у частотній області аудіосигналів методом розширення їх спектру; Приховування даних у частотній області аудіосигналів методом фазового кодування. 5. Приховування даних з використанням комп'ютерних стеганографічних методів шляхом вбудовування їх в текстових файлах: за допомогою методу зміни інтервалу між реченнями; методу додавання пробелів в кінець кожного текстового рядку; методу зміни кількості пропусків між словами вирівняного по ширині тексту. *Види занять:* лекції, лабораторні та практичні заняття. *Методи навчання:* проблемно-пошукові та практичні методи навчання. *Форма навчання:* заочна.
12. Інформаційне забезпечення	*Бібліотека ЖВІ:* 1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. - К.: "МК-Пресс", 2006. – 288 с.: ил. 2. Смирнов А.А. Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: монография / А.А. Смирнов. – Кировоград: "Код", 2012. – 352 с.: ил. 3. Шенон К. Работы по теории информации и кибернетики / Пер. с англ.; К. Шенон. – М.: Иностранная литература, 1963. – 829 с.: ил. 4. Быков С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии//Защита информации. Конфидент, 2000. № 3. *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 сьомому семестрі; усне опитування або 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 наступного 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 ***n/n*** 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 ***n/n*** Володимир ОХРІМЧУК

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:
Заслужений діяч науки і техніки України,
доктор технічних наук, професор
полковник

Руслан ГРИЩУК