СИЛАБУС
з навчальної дисципліни:
ОК 1.4.2. "Переддипломна практика"

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 1.4.2 - обов'язкова виробнича практика Переддипломна практика
3. Кількість кредитів ESTS	4,5
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції лабораторні диференційований залік самостійна робота	 135 4 2 - 2 131
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 1.2.6. Екологія та безпека життєдіяльності**;** ОК 1.3.5. Архітектура комп`ютерних систем ОК 1.3.6. Інформаційно-комунікаційні системи; ОК 1.3.8. Прикладна криптологія; ОК 1.3.9. Нормативно-правове забезпечення інформаційної безпеки; ОК 1.3.10. Системи технічного захисту інформації; ОК 1.3.11. Захист інформації в інформаційно-комунікаційних системах; ОК 1.3.12. Комплексні системи захисту інформації: проектування, впровадження, супровід; ОК 1.3.18. Основи кібербезпеки
9. Постреквізити	ОК 1.4.3. Дипломне проєктування
10. Характеристика навчальної дисципліни	*10.1. Переддипломна практика призначена* для здобуття практичних навиків роботи, ознайомлення студентів з функціонуванням 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, отримання аналітичних та статичних даних для виконання кваліфікаційної роботи, виявлення недоліків щодо захисту інформації та формування завдань на виконання кваліфікаційної роботи, здобуття практичних навиків щодо аналізу захищеності об'єктів та розробки організаційних, технічних заходів та засобів захисту від несанкціонованого доступу. Переддипломна практика направлена для здобуття практичних навиків роботи, ознайомлення студентів з функціонуванням систем захисту інформації, отримання аналітичних та статичних даних для виконання кваліфікаційної роботи, виявлення недоліків щодо захисту інформації на підприємствах та формування завдань на виконання кваліфікаційної роботи, здобуття практичних навиків щодо аналізу захищеності об'єктів та розробки організаційних, технічних заходів та засобів захисту від несанкціонованого доступу. ***Потреба вивчення цієї дисципліни обумовлена*** необхідністю вирішення начальних 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 аналіз програмних, технічних та організаційних складових систем захисту інформації; виявляти недоліки в роботі систем захисту інформації; працювати з типовим програмним забезпеченням систем захисту інформації та проводити відлагодження програмного забезпечення; складати техніко-економічні обґрунтування на розробку комплексних систем захисту інформації; розробляти організаційні заходи захисту інформації в інформаційно-комунікаційних системах та мережах; розробляти технічні засоби 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.

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

КФ 1 - Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки

КФ 2 - Здатність до використання інформаційно-комунікаційних технологій, сучасних методів та моделей інформаційної та/або кібербезпеки

КФ 3 - Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

КФ 5 - Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки

КФ 6 - Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження

КФ 7 - Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ 8 - Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

КФ 9 - Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою

КФ 10 - Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності

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 2 - організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 3 - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності

РН 5 - адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат

РН 6 - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності

10.2. Мета навчальної дисципліни є отримання аналітичних та статичних даних для виконання кваліфікаційної роботи; набуття практичних навиків виявлення недоліків щодо захисту інформації; поглиблення й закріплення теоретичних знань із забезпечення інформаційної та кібернетичної безпеки 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. *10.3. Завдання вивчення дисципліни* – набуття студентами необхідних практичних навичок самостійної роботи, формування у студентів навичок професійного використання засвоєних за час навчального процесу методів та засобів обробки інформації та її захисту, побудови сучасних систем захисту інформації для вирішення конкретних практичних задач, освоєння умов роботи в середовищі творчого колективу спеціалістів, виявлення недоліків щодо захисту інформації.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Аналіз захищеності об'єкта інформаційної діяльності: опис підрозділу, в якому студент проходив переддипломну практику, його функції та задачі; аналіз забезпечення функціонування 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. 2. Розробка організаційних заходів захисту інформації від несанкціонованого доступу: аналіз нормативно-правового та організаційного забезпечення 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. 3. Розроблення технічних заходів захисту від несанкціонованого доступу: аналіз систем технічного забезпечення 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; розроблення технічних засобів захисту інформації від несанкціонованого доступу 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. 4. Висновки в цілому по проходженню переддипломної практики на підставі проведеного аналізу, спостережень та виконання реальних практичних завдань. 5. Розроблення пропозиції щодо поліпшення загального стану 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 в цілому та їх техніко-економічне обґрунтування. 6. Оформлення звіту у відповідності до ДСТУ 3008-2015 та заповнення щоденнику переддипломної практики. ***Види занять:*** лекції, інструктажі та практичні заняття 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. ***Методи навчання:*** проблемно-пошукові та практичні методи навчання. ***Форма навчання:*** заочна.
12. Інформаційне забезпечення	***Бібліотека ЖВІ:*** 1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. - К.:Видавнича група BHV, 2009.– 608 с.: іл. 2. Домарев В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник / В.В. Домарев, В.А. Швець, В.В. Шестакова. - К.:НАУ, 2006. – 688 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. ***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	Диференційований залік у восьмому семестрі з захисту звіту за переддипломну практику та виконання індивідуальних завдань; усне опитування.
14. Система підсумкового оцінювання	Підсумкове оцінювання результатів навчання складається із суми балів, отриманих студентом під час звіту за переддипломну практику та виконання індивідуальних завдань 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. Переддипломна практика студентів повинна проводитись у відділах та службах безпеки 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. 3. Розподіл балів, які отримують студенти за навчальними елементами дисципліни доводиться до тих хто навчається на першому занятті 4. 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 у громадських місцях. 5. 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. 6. 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