СИЛАБУС
з навчальної дисципліни:
ВК 2.1.7. "Організаційне забезпечення захисту інформації"

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 2.1.7 - вибіркова навчальна дисципліна Організаційне забезпечення захисту інформації
3. Кількість кредитів ESTS	**3**
4. Кількість годин: *загальний обсяг* **Аудиторних всього:** лекції семінари диф.залік самостійна робота	 90 10 4 4 2 80
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 1.3.18. Основи кібербезпеки, ОК 1.3.9. Нормативно-правове забезпечення інформаційної безпеки, ОК 1.3.10. Системи технічного захисту інформації, ВК 2.2.1. Правознавство
9. Постреквізити	ОК 1.4.3. Дипломне проектування
10. Характеристика навчальної дисципліни	*10.1. Навчальна дисципліна призначена* для набуття теоретичних знань, практичних вмінь та навичок, визначених освітньої програмою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань із 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 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 14 -** *Здатність розробляти та впроваджувати заходи із захисту інформації та/або кібербезпеки на об'єктах інформаційної діяльності;* **програмні результати навчання:** **РН 56** - *вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних (автоматизова-*

	них) системах; **РН 59** - *здійснювати експертизу, випробування комплексних систем захисту інформації ;* **РН 69** - *вирішувати задачі забезпечення безперервності функціонування інформаційно-телекомунікаційних систем у військовій частині (органі військового управління) на основі теорії ризиків та встановленої системи управління інформаційною безпекою з підтвердженою відповідністю згідно з вітчизняними та міжнародними (у разі потреби участі у міжнародних спільних військових навчаннях із залученням інформаційно-телекомунікаційних систем або їх складових) вимогами та стандартами.* *10.2. Мета навчальної дисципліни* полягає в ознайомленні студентів з організаційними основами забезпечення інформаційної безпеки об'єктів інформатизації, принципами системного підходу до вирішення цієї задачі, архітектурною побудовою та проектуванням систем захисту інформації, організаційно-правовим забезпеченням робіт з захисту інформації. *10.3. Завдання вивчення дисципліни* – надати студентам знання та основні поняття з основ організації забезпечення захисту інформації. Визначити основні методи та засоби забезпечення інформаційної безпеки, стратегії захисту інформації, моделювання систем та процесів захисту інформації. Розвивати у студентів прагнення творчого відношення до задач забезпечення захищеності інформації в інформаційних системах та мережах.
11. Навчальна логістика	*Зміст навчальної дисципліни:* 1. Основні положення щодо організації системи захисту інформації. Основи забезпечення інформаційної безпеки. Інформаційна безпека та її забезпечення. 2. Визначення інформаційних ресурсів, що підлягають захисту. Державна таємниця і конфіденційна інформація, що є власністю держави. Недержавна конфіденційна і відкрита інформація, що потребує захисту. 3. Концепція побудови системи безпеки підприємства. Загальна характеристика організаційних методів захисту інформації. Основні напрямки організаційного захисту інформації на підприємстві. 4. Дії по захисту інформації. Розголошення інформації, яка захищається. Способи запобігання розголошення інформації, яка захищається. Протидія несанкціонованому доступу до інформації. 5. Організаційне забезпечення безпеки інформації обмеженого доступу. Державна таємниця та порядок віднесення до неї інформації. Захист державної таємниці. Організація режиму секретності, його особливості та зміст. Комерційна таємниця та порядок її визначення. 6. Організація та функції служби безпеки підприємства. Організація внутрішньооб'єктного режиму на підприємстві. Організація та забезпечення за захисту комерційної таємниці на підприємстві. 7. Організація інформаційно-аналітичної роботи. Цілі та задачі інформаційно-аналітичної роботи. Направлення і методи аналітичної роботи. 8. Забезпечення безпеки інформації на найбільш вразливих напрямках діяльності підприємства. Захист інформації під час проведення засідань та переговорів, під час роботи з відвідувачами. 9. Організація роботи з персоналом підприємства. Підбір та підготовка кадрів. Перевірка персоналу на благонадійність. *Види занять:* лекції та семінарські заняття. *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. 4. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, В.Г. Конахович. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с. 5. Юдін О.К. Інформаційна безпека держави / О.К. Юдін, В.М. Богуш. – К.: «МК-Прес», 2005. – 432 с.: іл. *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; 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 ***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