СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	Вибіркова компонента освітніх програм першого (бакалаврський) рівня вищої освіти
Рекомендовано для спеціальностей	Для всіх ОПП запроваджених ДУІТЗ
Форма навчання	Денна, заочна

Викладачі

Корчинський Володимир Вікторович
vladkorchin@ukr.net

Професор кафедри кібербезпеки та технічного захисту інформації, доктор технічних наук, професор

Загальна інформація про дисципліну

Анотація до дисципліни

Дисципліна «Забезпечення кібербезпеки у Збройних Силах України» має міждисциплінарний характер. Вона інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: фізика», програмування, іноземна фахова мова, комп'ютерні технології, комп'ютерні мережі, теорія інформації та кодування, законодавство в області інформаційної безпеки, методи та засоби захисту інформації.

Предметом навчання дисципліни є формування у здобувачів системи знань щодо становлення та розвиток кібербезпеки у ЗСУ, механізмів управління безпекою процесів взаємодії користувачів з системами і ресурсами у

	ЗСУ, особливістю застосування завадозахищених систем радіозв'язку, які забезпечують захист інформації на різних рівнях моделі OSI в умовах радіоелектронного конфлікту. Основними завданнями вивчення дисципліни є набуття теоретичних та практичних знань, необхідних майбутнім фахівцям в галузі військової кібербезпеки, щодо механізмів управління безпекою процесів взаємодії користувачів з системами і ресурсами та застосування завадозахищених систем радіозв'язку у ЗСУ.
Мета дисципліни	формування у студентів теоретичних та практичних знань, необхідних майбутнім фахівцям в галузі військової кібербезпеки, щодо механізмів управління безпекою процесів взаємодії користувачів з системами і ресурсами та застосування завадозахищених систем радіозв'язку у ЗСУ.
Компетентності, формуванню яких сприяє дисципліна	Здатність застосовувати знання у практичних ситуаціях. Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
Результати навчання	реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
Обсяг дисципліни	Загальний обсяг дисципліни 6 кредитів ЄКТС (180 академічних годин)
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркових компонент освітньої програми

Програма дисципліни

Тема 1.	***Кібербезпека як важлива складова всієї системи захисту держави*** Огляд проблеми, основні поняття та терміни: кіберзбезка, кіберзброя та інше. Роль кібербезпеки в системі захисту держави. Кібернетичні операції в умовах введення гібридної війни. Аналіз наслідки кібератак. Заходи щодо реалізації Концепції кібербезпеки.
Тема 2.	***Правила інформаційної та кібернетичної безпеки в зоні проведення ООС*** Рекомендації з кібернетичної безпеки. Рекомендації щодо використання мобільних телефонів та радіостанцій. Правила поведінки в соціальних мережах.
Тема 3.	***Кіберзагрози та рекомендації щодо захисту даних*** Інформаційно-телекомунікаційні системи у ЗСУ. Захист персональних даних. Фішинг. Безпека доступу до мережі Інтернет. Супутниковий зв'язок. Бездротовий доступ.
Тема 4.	***Аспекти кіберзагроз*** Соціальні мережі. Мобільні телефони. Електронна пошта. Комп'ютерні віруси. Носії інформації.
Тема 5.	***Кібератаки російської федерації*** Важливість кібернетичної безпеки для незалежної держави. Направленість кібератак з боку російської федерації. Указ Президента України «Про

	Стратегію кібербезпеки України».
Тема 6.	***Мобільні віруси. Виявлення та протидія*** Загрози використання та безпека мобільних пристроїв. Типові шляхи розповсюдження вірусів. Як відрізнити віруси від звичайних програм. Захист смартфонів від вірусів.
Тема 7.	***Захист інформації в системах обміну даними*** Електронні засоби обміну даними у ЗСУ. Використання захищених систем обміну у ЗСУ. Використання захищених систем обміну у ЗСУ. Основні методи захисту інформації.
Тема 8.	***Аналіз можливостей радіотехнічної розвідки і радіоелектронного придушення*** Аналіз розвідзахищеності мереж пакетного радіозв'язку. Аналіз засобів радіотехнічної розвідки. Аналіз засобів радіопридушення. Аналіз технічного оснащення складу та тактико-технічних можливостей підрозділів радіорозвідки та РЕБ (США та військами НАТО).
Тема 9.	***Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності*** Основні поняття. Теоретичні основи дослідження соціального інжинірингу. Методика дослідження. Результати дослідження. Перспективи подальших досліджень.
Тема 10.	***Перехоплення радіосигналів малогабаритними засобами радіотехнічної розвідки.*** Різновиди SDR приймачів, їх переваги та недоліки. Тактико-технічні характеристики SDR приймачів. Інтерфейс програмного забезпечення SDR приймачів та принцип пошуку радіосигналів.

Список рекомендованих джерел

1. Shon Harris, F., & Maymi, F. (2021). CISSP All-in-One Exam Guide. McGraw Hill.
2. Корчинский В.В.Методичний посібник до лекційних занять з дисципліни «Забезпечення кібербезпеки у Збройних Силах України» – Одеса: ОНАЗ ім. О.С. Попова, 2020.
3. Практикум до практичних робіт з дисципліни «Забезпечення кібербезпеки у Збройних Силах України». Корчинський В.В. ДУІТЗ, 2022 р.
4. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.
5. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина 1: лаб. практ. – Одеса: ОНАЗ ім. О.С. Попова, 2011.
6. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.

Інформація про консультації

Індивідуальні та колективні консультації проводяться в час, визначений за попередньою домовленістю з викладачем через засоби зв'язку.

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну до 60 балів, за результати індивідуального завдання – до 40 балів.
При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов'язковим повторним вивченням дисципліни</td><td>Не зараховано з обов'язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування:
Відвідування та відпрацювання пропущених занять є обов'язковим. Допускаються пропуски занять з поважних причин, які підтверджується документально. За такої умови навчання може відбуватися в режимі он-лайн за погодженням із деканатом.
Дотримання принципів академічної доброчесності:
Політика щодо академічної доброчесності побудована на основі «Положення про академічну доброчесність» в університеті. Списування під час виконання письмових контрольних видів робіт заборонено. Користуватися мобільними пристроями, під час проведення різних видів контролю успішності, дозволяється лише з дозволу викладача.
Умови зарахування пропущених занять:
Відпрацювання пропущених занять проходять в дні згідно графіку консультацій викладачів кафедри.