Силабус *назва дисципліни* «Інформаційна безпека та гібридні загрози»

№	Назва поля	Контент, коментарі
1.	Рівень вищої освіти	*Другий (магістерський)*
2.	Спеціальність	121 «Інженерія програмного забезпечення»
3.	Тип і назва освітньої програми	Освітньо-професійна програма Інженерія програмного забезпечення
4.	Статус дисципліни	*Основна*
5.	Мова викладання	*Українська*
6.	Кількість ЄКТС кредитів	*3*
7.	Структура дисципліни (розподіл за видами та годинами навчання)	*Лекції – 20 год.* *Практичні – 10 год.* *Самостійна робота – 60 год.*
8.	Форма підсумкового контролю	*Екзамен*
9.	Графік (терміни) вивчення дисципліни	*1 рік (1 курс), 2семестр*
10.	Цілі навчання за дисципліною	*Метою викладання навчальної дисципліни «Інформаційна безпека та гібридні загрози» є набуття необхідних практичних навичок розробки та дослідження макетних зразків підсистем інформаційної безпеки в умовах впливу гідридних загроз, які являють собою втілення ефективних підходів та алгоритмів створення комплексної системи захисту інформації від несанкціонованого доступу.*
11.	Результати навчання	РН12. Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи та змінювати ризики. РН19. Знати, аналізувати, вибирати, застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних задач та створюваних програмних систем. РН22. Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.
12.	Анотація (зміст) дисципліни	**Модуль 1: Зв’язок гібридних загроз та предметної області** Тема 1. Проблеми інформаційної безпеки в комп’ютерних системах і мережах. Тема 2. Комплексний підхід до створення систем захисту інформації в умовах впливу гібридних загроз. **Модуль 2: Предметна область як об'єкт та інструмент гібридних впливів**

<table>
<tr><td></td><td></td><td>Тема 3. Ідентифікація суб’єктів та управління доступом на основі парольної системи.
Тема 4. Дискретне розмежування доступу суб’єктів до інформації в обмеженій матричній моделі інформаційної безпеки системи.
Тема 5. Базові алгоритмічні підходи до криптографічного захисту інформації з обмеженим доступом в умовах впливу гібридних загроз.
Тема 6. Симетричне шифрування в системах зв’язку з відкритими комунікаціями в умовах впливу гібридних загроз.
Тема 7. Асиметричні системи шифрування на основі відкритих та таємних ключів в умовах впливу гібридних загроз.
Модуль 3. Основи захисту предметної області
Тема 8. Підвищення крипостійкості в асиметричних системах шифрування в умовах впливу гібридних загроз.
Тема 9. Автентифікація суб’єктів та встановлення «довірчого» зв’язку в розподілених системах та мережах.
Тема 10. Засоби підвищення «довіри» віртуальних відносин в умовах впливу гібридних загроз.</td></tr>
<tr><td>13.</td><td>Система оцінювання</td><td><table><tr><td>Вид заняття</td><td>1 зміст. модуль (максимум балів)</td></tr><tr><td>Поточний контроль</td><td>max 40</td></tr><tr><td>Модульний контроль (МК)</td><td>max 20</td></tr><tr><td>Екзамен</td><td>max 40</td></tr></table>Максимальна кількість балів – 100 (60 та більше – зараховано, 59 та менше – не зараховано)</td></tr>
<tr><td>14.</td><td>Якість освітнього процесу</td><td>Дотримання принципів академічної доброчесності здійснюється відповідно до Кодексу академічної доброчесності Державного університету інфраструктури та технологій, Положення про систему забезпечення академічної доброчесності у Державному університеті інфраструктури та технологій та принципам академічної доброчесності, викладеним в Положенні про організацію освітнього процесу в Державному університеті інфраструктури та технологій, п.4.9.

Інструментом контрольних заходів є рейтингове оцінювання студентів. Кожен бал надається за конкретне досягнення, перелік яких оприлюднюється на початку курсу. Протягом семестру студенти «набирають» певну кількість балів за результати своєї роботи.

Всі практичні роботи мають груповий характер та виконуються на занятті.

По завершенню курсу проводиться анонімне опитування студентів для отримання зворотного зв'язку щодо корисності запропонованого матеріалу та складності виконання роботи.</td></tr>
</table>

15.	Сторінка курсу на платформі Moodle	-
16.	Література	Андриевский Т. Гибридная война: сущность и базовые стратегии / Т. Андриевский. – Desecuritate. – 2017. – No 1(3). – С. 158–166. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В. Л. Бурячок // Сучас. спеціал. техніка. – 2011. – No 3 (26). – С. 104–114. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ : Інтертехнологія, 2009. – 164 с. Курбан О. В. Основи сучасної національної інформаційної безпеки України / О. В. Курбан // Вісн. ХДАК. – 2017. – Вип. 50. – С. 55–62. Лалак О. А. Ризики і виклики кібербезпеки: досвід України та Польщі / О. А. Лалак, L. Klich // Міжнародні відносини. Серія “Політичні науки”. – 2017. – No 13. – URL: journals.iir. kiev.ua/index.php/pol_n/article/view/3001. – Назва з екрана. Сопілко І. М. Становлення мережевого суспільства та питання кібербезпеки / І. М. Сопілко // Юрид. вісн. – 2016. – No 1 (38). – С. 79–85. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві / І. В. Феськов // Актуал. пробл. політики. – 2016. – Вип. 58. – С. 66–76. Четверик Г. Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки / Г. Г. Четверик // Вісн. Дніпропетр. ун-ту. Політологія. – 2012. – No 9/2. – Вип. 22. – С. 241–246. Шорошев В. Базова модель експертної системи оцінки безпеки інформації в комп’ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. с. 86-90. Електронний ресурс: Європейський центр з протидії гібридним загрозам Hybrid CoE https://www.hybridcoe.fi/ Глосарій гібридних загроз https://warn-erasmus.eu/ua/glossary/ Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. - Swedish Defence University.

		ISBN 978-91-86137-73-1. URL: https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf EU Security Union Strategy: connecting the dots in a new security ecosystem. ULR: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1379/IP_20_1379_EN.pdf JOINT STAFF WORKING DOCUMENT. Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 24.7.2020.SWD(2020) 153 final. URL: https://ec.europa.eu/transparency/regdoc/rep/10102/2020/EN/SWD-2020-153-F1-EN-MAIN-PART-1.PDF Business community and hybrid threats: Report of Pasi Eronen Foundation for Defense of Democracies. Helsinki, 2018. URL: https://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c#/page=1 Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city. – Helsinki, Finland: Hybrid CoE. URL:https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf
17.	Матеріально-технічне, лабораторне, програмне забезпечення дисципліни	Спеціалізована навчальна лабораторія є складовою факультету управління і технологій Державного університету інфраструктури та технологій, учасником міжгалузевого середовища з протидії гібридним загрозам WARN. В 2021 році лабораторія отримала потужне комп'ютерне обладнання на загальну суму більш ніж 736 тис. грн., профінансоване грантом проєкту Еразмус+ «Академічна протидія гібридним загрозам – WARN» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
18.	Кафедра	Кафедра інформаційних технологій та дизайну, ауд. 601а.
19.	Викладач(і) – розробник(и) силабусу	Мухін Вадим Євгенійович, доктор технічних наук, професор, професор кафедри інформаційних технологій та дизайну v_mukhin@i.ua Завгородній Валерій Вікторович, кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та дизайну zavgorodnii@i.ua