Силабус *назва дисципліни* «Гібридні загрози та комплексна безпека»

№	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	*4*
7.	Структура дисципліни (розподіл за видами та годинами навчання)	*Лекції – 24 год.* *Практичні – 20 год.* *Самостійна робота – 76 год.*
8.	Форма підсумкового контролю	*Екзамен*
9.	Графік (терміни) вивчення дисципліни	*1 рік (1 курс), 1семестр*
10.	Цілі навчання за дисципліною	*Метою викладання навчальної дисципліни «Гібридні загрози та комплексна безпека» є формування системи знань та вмінь, необхідних для виконання організаційних, аналітичних та консультаційних функцій щодо ідентифікації та протидії гібридним загрозам і забезпечення комплексної безпеки на національному й міжнародному рівні.*
11.	Результати навчання	РН12. Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи та змінювати ризики. РН21. Розуміти комплексну природу, складність, логіку і закономірності гібридних загроз. РН22. Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.
12.	Анотація (зміст) дисципліни	Модуль 1. Асиметрія, гібридні загрози (HTs) та безпека Модуль 2. Концептуальна модель гібридних загроз Модуль 3. Домени (сфери) гібридних загроз Модуль 4. Інструменти гібридних загроз Модуль 5. Динаміка гібридних загроз Модуль 6. Основи захисту

<table>
<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>
<tr><td>15.</td><td>Сторінка курсу на платформі Moodle</td><td>-</td></tr>
<tr><td>16.</td><td>Література</td><td>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</td></tr>
</table>

		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 менеджменту, публічного управління та адміністрування, ауд. 608. Кафедра інформаційних технологій та дизайну, ауд. 601а.
19.	Викладач(і) – розробник(и) силабусу	Карпенко Оксана Олександрівна, доктор економічних наук, професор, професор кафедри менеджменту, публічного управління та адміністрування karpo_2004@ukr.net Завгородній Валерій Вікторович, кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та дизайну zavgorodnii@i.ua