Силабус *назва дисципліни* «Засоби захисту інформації»

№	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), 1 семестр*
10.	Цілі навчання за дисципліною	*Мета - закласти термінологічний фундамент, надання студентам теоретичних знань та практичних навичок в галузі захисту інформації від несанкціонованого доступу, криптографії та стеганографії, вивчення програмних продуктів в галузі захисту інформації; навчити студентів основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах з урахуванням негативного впливу гібридних загроз.*
11.	Результати навчання	РН01. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення. РН03. Будувати і досліджувати інформаційні процеси у прикладній області. РН17. Збирати, аналізувати, оцінювати необхідну для розв'язання наукових і прикладних задач інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела. 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	Тема 1. Поняття криптології. Криптографічні методи. Тема 2. Методи перевірки цілісності даних.

<table>
<tr><td></td><td></td><td>Тема 3. Введення в цифрову стеганографію.
Тема 4. Методи стеганографії.
Тема 5. Стегоалгоритми вбудовування інформації в зображення.
Тема 6. Загрози гібрідних війн.</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>
<tr><td>15.</td><td>Сторінка курсу на платформі Moodle</td><td>-</td></tr>
<tr><td>16.</td><td>Література</td><td>Niels Ferguson, Bruce Schneier Practical Cryptography ISBN: 978-0-471-22357-3 April 2003 432 Pages

Cachin C. An Information-Theoretic Model for Steganography // Proceeding of the Workshop on Information Hiding, 2016.

Simmons G.J. The prisoner`s problem and the subliminal channel, Proc. Workshop on CommunicationsSecurity (Crypto`83), 2014, 51-67.</td></tr>
</table>

Горбулін В.П. Проблеми захисту інформаційного простору України: монографія // Ін–т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.

Cachin C. An Information-Theoretic Model for Steganography // Proceeding of the Workshop on Information Hiding, 1998.

Simmons G.J. The prisoner`s problem and the subliminal channel, Proc. Workshop on CommunicationsSecurity (Crypto`83), 1984, 51-67.

Остапов С. Е. Євсеєв С. П. Король О. Г. Технології захисту інформації. Навчальний посібник [Електронний ресурс] – Режим доступа: http://www.repository.hneu.edu.ua/bitstream/.pdf.

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	Овчарук Ірина Вікторівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та дизайну ovch05@ukr.net Корнага Ярослав Ігорович, доктор технічних наук, доцент, професор кафедри інформаційних технологій та дизайну slovyan_k@ukr.net