

Український державний університет науки і технологій
Кафедра інформаційних технологій та систем

СИЛАБУС
навчальної дисципліни
«Методи та засоби кібербезпеки в галузі»

Назва дисципліни	Методи та засоби кібербезпеки в галузі
Шифр та назва спеціальності	122 – Комп'ютерні науки
Назва освітньої програми	Комп'ютерні науки і технології
Рівень вищої освіти	3-й (освітньо-науковий). Ступінь - Доктор філософії
Статус дисципліни	Дисципліна вільного вибору аспіранта
Обсяг дисципліни	5 кредити ЄКТС (150 академічних годин)
Терміни вивчення дисципліни	3 семестр (I – II чверті)
Назва кафедри, яка викладає дисципліну	Інформаційних технологій і систем (ІТС)
Провідний викладач (лектор)	Гнатушенко Вікторія Володимирівна, д. т. н, проф., завідувач кафедри ІТС E-mail: vvitagnat@gmail.com , кімн. 503
Мова викладання	Українська
Передумови вивчення дисципліни	Вивченню дисципліни має передувати вивчення дисциплін: - Вища математика; - Програмування
Мета навчальної дисципліни	Вивчення і освоєння студентами криптографічних методів, алгоритмів побудови процесів захисту інформації від несанкціонованого втручання та застосування протоколів організації технології захисту комп'ютерних систем
Компетентності, формування яких забезпечує навчальна дисципліна	Інтегральна компетентність. здатність продукувати нові ідеї, розв'язувати комплексні проблеми у сфері комп'ютерних наук, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення. СК01. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямках і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та

	<p>суміжних галузей.</p> <p>СК02. Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.</p> <p>СК03. Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень.</p> <p>СК04. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проєкти у галузі комп'ютерних наук та дотичні до неї міждисциплінарних проєктах, демонструвати лідерство під час їх реалізації.</p> <p>СК06. Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій</p> <p>СКд01 Здатність розвивати фундаментальні моделі інформаційних технологій, методики й техніки кібербезпеки, проектувати та створювати прототипи інформаційних систем та цифрових сервісів</p> <p>СКд03 Здатність управляти інформаційними ресурсами, інформаційними системами та цифровими сервісами</p>
<p>Програмні результати навчання</p>	<p>В результаті вивчення дисципліни студент повинен знати:</p> <ul style="list-style-type: none"> - типи і властивості методів криптографічного захисту інформації; - обмеження та можливості використання алгоритмів захисту інформації; - вимоги протоколів до організації технології захисту комп'ютерних систем для забезпечення крипостійкості. <p>вміти:</p> <ul style="list-style-type: none"> - проводити порівняльний аналіз властивостей криптографічних методів, алгоритмів захисту інформації від несанкціонованого втручання; - застосування протоколи організації технології захисту комп'ютерних систем. <p>Дисципліна забезпечує досягнення таких програмних результатів навчання:</p> <p>РН01. Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напрямку, отримання нових знань та/або здійснення інновацій.</p> <p>РН03. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.</p> <p>РН04. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямках.</p> <p>РН05. Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямків з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших</p>

	<p>дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.</p> <p>РН07. Розробляти та реалізовувати наукові та/або інноваційні інженерні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.</p> <p>РН08. Визначати актуальні наукові та практичні проблеми у сфері комп'ютерних наук, глибоко розуміти загальні принципи та методи комп'ютерних наук, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері комп'ютерних наук та у викладацькій практиці.</p> <p>РН10. Відшукувати, оцінювати та критично аналізувати інформацію щодо поточного стану та трендів розвитку, інструментів та методів досліджень, наукових та інноваційних проектів з комп'ютерних наук.</p> <p>РН11. Організовувати і здійснювати освітній процес у сфері комп'ютерних наук, його наукове, навчально-методичне та нормативне забезпечення, застосувати ефективні методики викладання навчальних дисциплін.</p> <p>РНс-2 Впроваджувати методи дослідження математичних моделей, розробляти та досліджувати алгоритми функціонування систем управління базами даних та знань, інформаційно-керуючих систем, розподілених та веб-базованих систем, систем хмарних обчислень та веб-сервісів, складних комп'ютерних мереж, інформаційно-пошукових систем, систем штучного інтелекту</p>
Зміст навчальної дисципліни	<p>Модуль 1. Криптографічний захист методами заміни та пістановок</p> <p>Модуль2. Метод гамірування.</p> <p>Модуль 3. Стандарти шифрування даних.</p> <p>Модуль 4. Методи захисту без обміну ключами - системи з відкритим ключем.</p> <p>Модуль 5. Прикладні пакети кібербезпеки</p>
Заходи та методи оцінювання	<p>Оцінювання модулів 1,2,3,4,5 здійснюється за результатами захисту лабораторних робіт за 12-бальною шкалою.</p> <p>Підсумкова оцінка навчальної дисципліни визначається як середнє арифметичне 5-х модульних оцінок (або іспит) за 12-бальною шкалою.</p>

Види навчальної роботи та її обсяг в акад. годинах

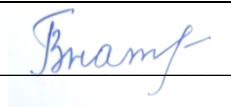
	Усього
Усього годин за навчальним планом	150
у тому числі:	48
Аудиторні заняття	
з них:	32
- лекції	
- лабораторні роботи	16
- практичні заняття	
- семінарські заняття	-

Самостійна робота	102
у тому числі при :	12
- підготовці до аудиторних занять	
- підготовці до заходів модульного контролю	8
- виконанні курсових проектів (робіт)	-
- виконанні індивідуальних завдань	-
- опрацюванні розділів програми, які не викладаються на лекціях	82
Семестровий контроль	середнє арифметичне 5-х модульних оцінок або іспит

Специфічні засоби навчання	Навчальний процес передбачає використання комп'ютерних робочих місць, програмного забезпечення: С.
Навчально-методичне забезпечення	<p><u>Основна література:</u></p> <ol style="list-style-type: none"> 1. Шнайдер Б. Прикладная криптография. – М.: Триумф., 2002. – 816 с. 2. Інформаційна та кібербезпека:соціалотехнічний аспект. [Підручник]/ В.Л. Бурячок, В.Б. Толодко, В.О. Хорошко, С.В. Толюпа/. – Львів: «Магнолія 2006», 2018 – 320с. ISBN 978-617-574-126-9 3. Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня 2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – 104 с. <p><u>Додаткова література:</u></p> <ol style="list-style-type: none"> 1. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл. ISBN 978-617-7609-22-2 2. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с. 3. Основи кіберпростору, кібербезпеки та кіберзахисту/Богуш В.М., Богуш В.В., Бровко В.Д., Настратін В.П., 2021. – 554с 4. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с. ISBN 978-617-582-069-8 5. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/ 6. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index. 7. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/ 8. Закон України “Про доступ до публічної інформації ”від 13.01.2011 № 2939-VI// Відомості Верховної Ради України. – 2011. – № 16. – с. 93. 9. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.

10. Закон України "Про державну таємницю" від 21.01.1994 // Відомості Верховної Ради України. – 1994. – № 16. – с. 93.
11. Закон України "Про основи національної безпеки України" // Урядовий кур'єр, 30 липня 2003 р.
12. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
13. Постанова Верховної Ради України від 16 січня 1997 року N 3/97-ВР "Про затвердження Концепції національної безпеки України"
14. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 р.
15. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
16. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
17. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
18. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
19. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)
20. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT).
21. ISO/IEC TR 27019:2013 Information technology — Security techniques — Information security management guide lines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (Інформаційні технології. Методи захисту. Настанова щодо менеджменту інформаційної безпеки на основі ISO/IEC 27002 для систем керування процесами в індустрії енергетичних сервісних програм).
22. ДСТУ IEC/TS 62351-1:2014 Керування енергетичними системами та пов'язаний з ним інформаційний обмін. Безпека даних та комунікацій. Частина 1. Безпека зв'язку мережі та системи. Загальні положення (IEC/TS 62351-1:2007, IDT).
23. Закон України "Про ліцензування господарської діяльності" // Відомості Верховної Ради (ВВР), 2015, № 23, ст.158. 13 Основи інформаційної та кібернетичної безпеки, 125 Кібербезпека
24. Указ Президента України "Про деякі заходи з дерегулювання підприємницької діяльності" від 23.07.1998 № 817.
25. Постанова Кабінету Міністрів України від 18.05.2011 року №517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.
26. Постанова Кабінету Міністрів України від 25.05.2011 року №543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню.
27. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ

Гарант освітньої програми, д.т.н., проф.



Вікторія ГНАТУШЕНКО