ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
Луцького національного технічного університету

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КІБЕРБЕЗПЕКИ

Галузь знань: 12 Інформаційні технології
Освітньо-професійна програма: Комп'ютерна інженерія
Обслуговування комп'ютерних систем та мереж
Інформаційні системи та технології
Спеціальність: 123 Комп'ютерна інженерія
126 Інформаційні системи та технології

Рівень освіти	Фахова передвища освіта
Освітньо-професійний /освітній ступінь	Фаховий молодший бакалавр
Статус навчальної дисципліни	Вільного вибору студента (професійної підготовки)
Обсяг дисципліни (кредити ЄКТС/ загальна кількість годин)	5 кредитів ЄКТС/ 150 годин
Циклова комісія	Циклова комісія комп'ютерних систем та інформаційних технологій
Мова викладання	Українська
Мета навчальної дисципліни	**Метою вивчення** навчальної дисципліни «Основи кібербезпеки» є формування у студентів теоретичної та практичної бази знань з безпечної поведінки в мережі; умінь і навичок ефективно та безпечно налаштовувати свої облікові записи; розуміння принципів передачі даних через мережу та існуючих методів захисту.
Предмет і завдання дисципліни	**Предмет курсу** становлять основні засоби налаштувань політик безпеки системи, програмні додатки симуляції роботи мереж та налаштування їх безпеки, алгоритми шифрування для закодування інформації. **Основними завданнями курсу** є навчитися безпечно поводитися в Інтернеті, налаштовувати безпеку систем і мереж, своїх облікових записів. У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: знати: - типові загрози, атаки та області їх розповсюдження; - проблеми захисту даних; - засоби протидії злочинності; - основні поняття криптографії, алгоритми шифрування; - поняття ідентифікації, методів аутентифікації, авторизації; - основні типи засобів контролю цілісності даних; - технології реагування на інциденти; - основні кіберзакони, стандарти та відповідальність. вміти: - ідентифікувати можливі загрози чи атаки; - налаштовувати локальну та групову політики безпеки системи;

	- налаштовувати безпеку локальної мережі; - шифрувати конфіденційні дані стандартними алгоритмами шифрування; - налаштовувати безпеку веб-браузера; - користуватися цифровим підписом; - налаштовувати брандмауер; - відрізняти та розуміти який метод шифрування найкраще підійде для використання в певних умовах; - налаштовувати базову безпеку на маршрутизаторі; - застосовувати знання з кібербезпеки в практичній діяльності.
Форма підсумкового контролю	Диференційований залік

Зміст дисципліни	**ЗМІСТОВИЙ МОДУЛЬ 1.** **Тема 1. Потреба у кібербезпеці** 1.1. Правові та етичні проблеми кібербезпеки 1.2. Персональні дані 1.3. Корпоративні дані 1.4. Зловмисники та експерти з кібербезпеки 1.5. Кібервійни **Тема 2. Атаки, поняття та методи** 2.1. Аналіз кібератаки 2.2. Ландшафт кібербезпеки **Тема 3. Захист даних та конфіденційність** 3.1. Захист особистих даних 3.2. Захист конфіденційності в інтернеті **Тема 4. Захист організації** 4.1. Міжмережеві екрани 4.2. Підхід до кібербезпеки на основі поведінки 4.3. Підхід Cisco до кібербезпеки **ЗМІСТОВИЙ МОДУЛЬ 2.** **Тема 5. Кібербезпека – світ експертів і злочинців** 5.1. Світ кібербезпеки 5.2. Кіберзлочинці проти фахівців з безпеки 5.3. Типові загрози 5.4. Розповсюдження загроз кібербезпеки 5.5. Підготовка більшої кількості спеціалістів **Тема 6. Куб кібербезпеки.** 6.1. Три виміри куба кібербезпеки 6.2. Тріада КЦД 6.3. Стани даних 6.4. Засоби протидії кіберзлочинності 6.5. Структура керування ІТ безпекою **Тема 7. Загрози, вразливості та атаки** 7.1. Шкідливе програмне забезпечення та зловмисний код 7.2. Обман 7.3. Атаки **Тема 8. Мистецтво захисту таємниць** 8.1. Криптографія 8.2. Контроль доступу 8.3. Приховування даних **Тема 9. Мистецтво забезпечення цілісності** 9.1. Типи засобів контролю цілісності даних 9.2. Цифрові підписи 9.3. Сертифікати 9.4. Забезпечення цілісності баз даних

	ЗМІСТОВИЙ МОДУЛЬ 3. **Тема 10. Концепція п'яти дев'яток** 10.1. Висока доступність 10.2. Заходи для поліпшення доступності 10.3. Реагування на інциденти 10.4. Відновлення після катастроф **Тема 11. Захист домену кібербезпеки** 11.1. Захист систем та пристроїв 11.2. Укріплення захисту серверів 11.3. Укріплення захисту мережі 11.4. Фізична безпека **Тема 12. Спеціаліст з кібербезпеки** 12.1. Домени кібербезпеки 12.2. Розуміння етики роботи у кібербезпеці 12.3. Дослідження професії кібербезпеки
Рекомендована література	**Основна** 1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ – Київ : Видавництво НА СБ України, 2020. 256 с. 2. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с. 3. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, - К.; ПВП «Задруга», 2014. - 222 с 4. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с. 5. Навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с. 6. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p. 7. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p. 8. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p. **Додаткова** 1. Лабораторний практикум з навчальної дисципліни "Інформаційна безпека". Навчально- практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 256 с. (Укр. мов.) 2. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб./ За заг. ред. Проф. Я.Ю. Кондратьєва. – К., 2004. 3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006. 4. Методичні рекомендації для виконання лабораторних робіт з дисципліни АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ / [Ю. Є. Добришин, І.О.Чернозубкін]; Університет економіки та права «КРОК» – Київ - 2019. – 49 с. 5. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного

	забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с. 6. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений. М., 2005. 7. Білоус Л. Ф. Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с. 8. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с 9. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем — К. : Видавнича група BHV, 2009. — 608 с. 10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22 https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf 11. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12. 12. 2007 р. № 232. https://tzi.com.ua/downloads/3.1-001-07.pdf **Інтернет-ресурси** 1. https://www.netacad.com/ 2. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text 3. https://zakon.rada.gov.ua/laws/show/2297-17#Text 4. https://zakon.rada.gov.ua/laws/show/3855-12#Text 5. https://zakon.rada.gov.ua/laws/show/2657-12#Text
Види занять, методи і форми навчання	Форми організації освітнього процесу: лекції, практичні заняття, дослідницькі роботи, самостійна робота, консультації зі викладачами, участь у наукових конференціях, екскурсії, дистанційне навчання. Освітні технології: традиційні, інтерактивні, інформаційно-комунікативні, проектного навчання.
Пререквізити	Дисципліна «Основи кібербезпеки» може вивчатись одночасно або після вивчення предмету «Інформатика», що підвищує ефективність засвоєння курсу. Під час вивчення дисципліни «Основи кібербезпеки» студенту рекомендується пройти курси «Introduction to Cybersecurity» та «Cybersecurity Essentials» на сайті https://www.netacad.com.
Постреквізити	Дисципліни «Захист інформації». Здійснення професійної діяльності
Критерії оцінювання	**Критерії оцінювання:** Оцінка «**відмінно**» виставляється, якщо здобувач освіти у повному обсязі володіє навчальним матеріалом, вільно, самостійно й аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує задачі стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки.

	Оцінка «**добре**» виставляється, якщо здобувач освіти достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією, але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. Оцінка «**задовільно**» виставляється, якщо здобувач освіти відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони, однак нездатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Оцінка «**незадовільно**» виставляється, якщо здобувач освіти достатньо не володіє навчальним матеріалом, однак фрагментарно, поверхово (без аргументації й обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань.
Політика курсу	Курс передбачає індивідуальну та групову роботу. Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. Якщо здобувач освіти відсутній з поважної причини, він/вона презентує виконані завдання під час консультації викладача. Під час роботи над індивідуальними завданнями та проектами не допустимо порушення академічної доброчесності.

Базою навчання є матеріали освітньої платформи CISCO NETWORKING ACADEMY

QR-код	Веб-посилання	Опис
	https://www.netacad.com/ru/courses/security/introduction-cybersecurity/	Мережева академія Cisco Networking Academy — це програма професійного і кар'єрного розвитку в сфері IT, яка доступна для навчальних закладів і студентів по всьому світу.