Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

Технічний захист інформації

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020)
Форма навчання	Денна
Розробник (викладач)	Глинчук Людмила Ярославівна, кандидат фізико-математичних наук
Контактна інформація	Електронна адреса викладача: Hlynchuk.Ludmila@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	6 семестр, III курс
Обсяг дисципліни	Загальний обсяг: 4,5 кредити / 135 годин. Аудиторних годин: 64; з них: лекцій – 30 год., лабораторних – 34 год. Самостійної роботи: 63 год. Консультації: 8 год.
Форма контролю	Екзамен
Час занять	Тижневих годин – 4 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна «Технічний захист інформації» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Спрямована на підвищення рівня обізнаності щодо нормативно-правової бази у сфері ТЗІ та технічних засобів захисту інформації. У курсі викладені основні положення та нормативні акти для ТЗІ, класифікація каналів витоку інформації, методи та засоби захисту від витоку; фізичні та апаратні засоби захисту інформації.
Предреквізити дисципліни	Для вивчення даної дисципліни, будуть корисні знання та вміння отримані з предметів «Нормативно-правова база кібербезпеки», «Архітектура комп'ютерних систем та схемотехніка», «Проектування мікроконтролерних систем та основи мехатроніки» та ін.
Постреквізити дисципліни	Знання та вміння, отримані в результаті вивчення дисципліни, можуть бути використані для вивчення предмету: «Комплексні системи захисту інформації» та написання курсової роботи з навчальних дисциплін циклу професійної підготовки, а також у професійному

	розвитку та роботі.
Мета вивчення дисципліни	Мета дисципліни полягає в освоєнні принципів побудови ТЗІ в комп'ютерних системах, а також формування умінь використовувати на практиці набуті знання для аналізу захищеності сучасного обладнання та програмного забезпечення, проектування та експлуатації ефективної системи захисту інформації від несанкціонованого доступу. Формування професійних навиків від користування необхідною нормативно-правовою базою до вибору та експлуатації технічних пристроїв для захисту інформації на відповідних ОІД.
Що буде вивчатись	1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням. Положення про державну експертизу в сфері технічного захисту інформації. 2. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. 3. Порядок проведення перед проектних досліджень на об'єкті інформаційної діяльності. 4. Рекомендації щодо розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності та інші документи у сфері ТЗІ. 5. Перехоплення даних. Класифікація каналів витоку інформації. Технічні канали витоку інформації. 6. Методи за засоби захисту від витоку інформації. 7. Поняття інженерно-технічного захисту. Фізичні засоби захисту: охоронні системи, охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації. 8. Апаратні засоби захисту. Ключові елементи, персональні кодові карти, персональний ідентифікатор, пристрої розпізнавання голосу користувача чи форми його пальців. 9. Класифікація закладних пристроїв, їх основні характеристики та застосування. Способи та засоби боротьби. 10. ТЗІ на мережевому рівні. 11. Система технічного захисту інформації в Україні: стан та напрями розвитку. 12. Огляд засобів для технічного захисту на ринку України та дозвіл користування ними.
Результати навчання	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному

	простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. РН 36. Виявляти небезпечні сигнали технічних засобів. РН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

Оцінювання

Оцінювання навчальних досягнень з дисципліни “Технічний захист інформації” здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та модульний контроль (оцінюються модульні контрольні роботи у вигляді тестів або письмово або у вигляді індивідуальних завдань). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 60 балів.

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 75 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів. Оцінка за семестр, у випадку складання екзамену, є сумою балів поточного контролю та балів, отриманих під час екзамену.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми.

Під час модульного та підсумкового контролю (заліку) студентам заборонено користуються такими засобами як мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання мають бути виконані у встановлений термін. Несвоєчасно виконані завдання оцінюються на нижчу оцінку. Виключенням можуть бути завдання, які не вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, то він (вона) вивчає матеріал самостійно, використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу, у випадку розміщення його на платформі дистанційного навчання Moodle, виконує всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс, прикріпивши виконанні завдання у відповідні комірки та попередити викладача про здане завдання, або під час консультацій або надіслати виконане завдання на корпоративну пошту викладача. Зворотній зв'язок з викладачем для з’ясування всіх питань: використання форуму, чату дистанційного курсу, корпоративної пошти університету або відповідної бесіди у певному месенджері.

Перескладання модульного контролю (письмового чи тестування) заборонено.

Рекомендована література

1. Нормативно-правова база у сфері ТЗІ. [Електронний ресурс]. – Режим доступу до ресурсу: http://altersign.com.ua/korysna-informacija/normatyvna-baza-u-sferi-tzi
2. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. [Електронний ресурс]. – Режим доступу до ресурсу: https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11
3. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с
4. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.
5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.