Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут
електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Проектування технічних систем захисту інформації

ЗАТВЕРДЖУЮ
Завідувачка кафедри
_____ __Ткач Ю.М._____
(підпис) (прізвище та ініціали)
26 серпня 2024р.

Розробник: Петренко Тарас Анатолійович, доцент кафедри кібербезпеки та математичного моделювання, к.т.н._____

Силабус обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від 26 серпня 2024р. №7

Узгоджено з гарантом освітньої програми: _____ __Ткач Ю.М._____

1. Загальна інформація про дисципліну

Тип дисципліни	Обов'язкова
Мова викладання	Українська
Рік навчання та семестр	Перший рік, другий семестр. 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Петренко Тарас Анатолійович, доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com.ua/citations?user=2bJE-4IAAAAJ&hl https://www.linkedin.com/in/taraspetrenko/ https://orcid.org/0000-0001-5571-3815 https://www.webofscience.com/wos/author/record/ABA-8146-2021 https://www.scopus.com/authid/detail.uri?authorId=57193026484
Контакти викладача	+380504650364, mail_taras@stu.cn.ua
Сторінка курсу в системі дистанційного навчання	https://eln.stu.cn.ua/course/view.php?id=3451

2. Анотація курсу.

Створення технічних систем захисту інформації залишається складною теоретичною й технічною проблемою. Необхідність у професійному проектуванні та впровадженні ТСЗІ виникає в самих різних областях – від військової справи й систем безпеки державних та приватних підприємств до повсякденного життя людини. Сьогодні забезпечення технічного захисту інформації є комплексною проблемою, вирішення якої потребує необхідної фахової підготовки, нормативного та методичного супроводження, технічного оснащення відповідних робіт. Безумовно, фахівець який не тільки в змозі організувати систему технічного захисту інформації за допомогою наявних технічних засобів, але і вміє проектувати та створювати нові технічні системи захисту інформації буде більш конкурентоспроможним на ринку праці.

На заняттях курсу «Проектування технічних систем захисту інформації» студенти отримують теоретичні знання та практичні вміння в сфері проектування, впровадження та професійної експлуатації технічних систем захисту інформації відповідно до поставлених задач. Знайомляться з теоретичними та прикладними аспектами проектування технічних систем захисту інформації. Розглядають методологічні підходи до проектування технічних систем захисту інформації. Проводять наукові дослідження в зазначених напрямках.

Успішне засвоєння дисципліни дозволяє магістру зі спеціальності 125 – Кібербезпека та захист інформації розширити коло застосування набутих раніше знань та практичних навичок для вирішення професійних задач організації захисту інформації, до якого традиційно включають і задачі технічного захисту інформації.

В результаті вивчення курсу студенти готують курсовий проект в якому проектують реальні технічні засоби та системи захисту інформації.

3. Мета та цілі курсу.

Метою викладання навчальної дисципліни “Проектування технічних систем захисту інформації” є формування науково-професійного світогляду магістра спеціальності 125 – Кібербезпека та захист інформації в області технічного захисту інформації та вивчення пов’язаних з ним основ проектування, створення та забезпечення функціонування технічних систем захисту інформації в інформаційно-телекомунікаційних системах підприємств, установ та організацій а також принципів організації охорони спеціальних об’єктів.

Об’єкт –технічні системи захисту інформації

Предмет – сучасні методи проектування ТСЗІ; основні теоретичних положення створення ТСЗІ; процеси проектування технічних систем захисту інформації, тобто виконання проектних робіт, що включає в себе розробку технічної документації ТСЗІ, її технічну підтримку та супровід, погодження у відповідних державних і відомчих органах, особливості проектування ТСЗІ відповідно до чинних вимог нормативних документів із дотриманням правил інформаційної безпеки.

Основними завданнями вивчення дисципліни “Проектування технічних систем захисту інформації” є:

- ознайомлення з сучасним станом та тенденціями розвитку проблеми проектування ТСЗІ;
- вивчення різновидів систем технічного захисту інформації;
- дослідження технічних каналів витоку інформації;
- практичне ознайомлення з особливостями та засвоєння основ робіт з проектування ТСЗІ.

4. Результати навчання

Під час вивчення дисципліни здобувач вищої освіти має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 – Кібербезпека та захист інформації:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки

КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури

КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ 10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання, передбачені освітньою програмою:

ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

У підсумку ЗВО повинні знати :

– базові терміни та визначення в галузі технічного захисту інформації;
– українські та міжнародні стандарти систем технічного захисту інформації;
– основі технічні канали витоку інформації;
– способи несанкціонованого перехоплення інформації;
– особливості роботи з системами технічного захисту інформації;
– тенденції розвитку систем технічного захисту інформації;
– основні технічні системи, що використовуються для несанкціонованого перехоплення інформації;
– основні технічні системи, що використовуються для захисту інформації від несанкціонованого перехоплення;
– основи методів проектування ТСЗІ;
– порядок проектування ТСЗІ.
– основні положення політики безпеки об’єктів, принципи, за якими категоруються об’єкти, різновиди систем виявлення порушників та технічних каналів витоку інформації, а також організацію контролю доступу на об’єкт, та ін.

вміти :

– проектувати ТСЗІ та їх елементи з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію та технічне обслуговування;
– проектувати, встановлювати, налаштовувати та обслуговувати системи відеонагляду, протипожежні системи та сигналізації;

– експлуатувати прилади та системи виявлення закладних пристроїв негласного зйому інформації;

– забезпечувати надійний захист інформації за допомогою ТСЗІ від її витоку по технічним каналам;

– застосовувати отримані знання під час виконання курсового проекту з дисципліни, що вивчається, у дипломному проектуванні а також у майбутній професійній діяльності.

5. Пререквізити

Передумовою для вивчення дисципліни є успішне засвоєння дисциплін бакалаврату: «Фізика»; «Архітектура комп'ютерних систем»; «Схемотехніка»; «Системи технічного захисту інформації». Дисципліна є базовою для подальшої успішної професійної діяльності за спеціальністю, а також може використовуватися під час проходження переддипломної практики та підготовки випускної кваліфікаційної роботи магістра.

6. Обсяг курсу.

Вид заняття	Загальна кількість годин (очна/заочна форма навчання)
Лекції	24/10
Лабораторні заняття	24/8
Самостійна робота	132/162
Індивідуальне завдання –курсовий проект	
Всього кредитів – *вказати кількість кредитів*	6

Лекції – дистанційно в MS Teams.

Лабораторні заняття - очно в лабораторії кафедри та дистанційно в MS Teams.

Самостійна робота - з використанням системи дистанційного навчання університету, рекомендованих інформаційних джерел, презентацій, нормативно-правових актів тощо.

7. Тематика курсу

Змістовий модуль 1. Прикладні аспекти проектування технічних систем захисту інформації

Тема 1. Технічні канали витоку інформації

Основні терміни та визначення. Класифікація технічних каналів витоку інформації. Радіо- та електротехнічні канали витоку інформації. Акустичні та віброакустичні канали витоку інформації. Електричні канали витоку інформації. Візуально-оптичні та матеріально-предметні канали витоку інформації. Канали витоку інформації при експлуатації обчислювальних засобів.

Тема 2. Фізичні основи захисту інформації від витоку по технічним каналам

Захист від акустичних та віброакустичних каналів витоку інформації. Захист від електричних каналів витоку інформації. Захист від візуально-оптичних та матеріально-предметних каналів витоку інформації. Захист електромережі.

Тема 3. Технічні системи захисту від витоку інформації по технічним каналам

Нейтралізація радіо мікрофонів. Пасивні засоби захисту приміщень. Апаратні засоби активного захисту приміщень від витоку мовної інформації. Засоби віброакустичного захисту. Пригнічення диктофонів. Порядок проведення спеціальної перевірки технічних засобів. Спеціальні обстеження і дослідження під час виявлення технічних каналів витоку інформації.

Тема 4. Технічні системи пошуку та виявлення закладних пристроїв

Індикатори електромагнітного випромінювання. Радіочастотоміри. Радіоприймачі. Скануючі приймачі. Аналізатори спектру. Нелінійні локатори. Автоматизовані пошукові комплекси. Методологія пошуку та виявлення закладних пристроїв за допомогою пошукових комплексів.

Тема 5. Технічні системи контролю доступу до приміщень

Приймальні пристрої доступу — ідентифікатори особистості, зчитувачі, кодонаборні пристрої, пульти, панелі і консолі управління. Ввиконавчі пристрої доступу — електромеханічні, електромагнітні і механічні кодові замки, автоматичні турнікети та шлагбауми. Засоби виявлення - металодетектори, виявителі вибухових речовин і радіаційних матеріалів. Засоби збору, обробки та відображення інформації — контрольні панелі, концентратори, світлові та звукові сповіщувачі, тощо. Проектування технічних засобів контролю доступу до приміщень

Тема 6. Технічні системи протипожежних систем

Характеристика технічних систем протипожежних систем. Призначення. Основні проектні рішення. Склад і розміщення обладнання. Принцип роботи автоматичної пожежної сигналізації. Діючі нормативно-технічні документи. Системи виявлення — пожежні сповіщувачі (теплові, димові, світлові, газові, температурні. Проектування технічних систем протипожежних систем.

Тема 7. Технічні системи спостереження

Обладнання для IP систем відеоспостереження. Обладнання для HD систем відеоспостереження. Обладнання для аналогових систем відеоспостереження. Камери відеоспостереження. Відеореєстратори. Пульти управління. Пристрої обробки і збереження відеоінформації. Приймачі/передавачі відеосигналу. IP камери відеоспостереження. IP відеореєстратори. Мобільні реєстратори. Тепловізори. Проектування технічних систем спостереження.

Тема 8. Технічні системи сигналізацій та охорони периметру

Дослідження характеристик датчиків охоронної сигналізації. Системи оповіщення — сирени, гучномовці, світлові табло і покажчики. Системи контролю і управління зонами оповіщення та аварійної автоматикою — підсилювачі, комутатори, магнітофони, мікрофони.

Змістовий модуль 2. Методологічні підходи до проектування технічних систем захисту інформації

Тема 9. Аналіз інформаційного процесу як середовища захисту інформації

Модель інформаційного системи що ґрунтується на знаковій чутливості. Поняття знакової чутливості інформаційної системи. Побудова геометричної моделі інформаційної системи. Модель інформаційних потоків, що ґрунтується на принципах функціонування нервової системи людини.

Тема 10. Моделювання систем і засобів захисту інформації

Методи моделювання систем і засобів захисту інформації. Аналіз моделей захисту інформації. Класифікація моделей захисту інформації. Приклади побудови моделей захисту інформації. Аналіз якості захищеності системи захисту інформації з повним перекриттям загроз технічними засобами захисту. Визначення математичної моделі конфлікті загроз з системою захисту інформації. Визначення показників якості захищеності моделі захисту інформації.

Тема 10. Методи проектування технічних систем захисту інформації

Методи захисту інформації від витоку по технічних каналах. Основні положення "Критеріїв оцінки захищеності інформації в комп'ютерних системах від НСД". Засоби виявлення каналів витоку інформації. Класифікація і аналіз постановок задач проектування технічних засобів захисту інформації. Методологія формування вимог щодо захисту інформації. Принципи та методи визначення значень параметрів інформації. Послідовність і загальний зміст проектування технічних засобів захисту інформації.

Тема 11. Розробка проекту технічної системи захисту інформації

Модель простору заходів і систем захисту. Критерій і особливості проектування оптимальної системи захисту інформації. Технічне завдання на розробку технічної системи захисту інформації і план захисту інформації. Технологія планування захисту інформації.

Тема 12. Впровадження, визначення якості і управління технічними системами захисту інформації

Реалізація проекту (плану) захисту інформації. Визначення якості реалізованої системи захисту. Контроль функціонування і управління технічними засобами захисту інформації в системі захисту.

Неформальний підхід в методиці оцінки ефективності проектування технічних систем захисту інформації.

8. Система оцінювання та вимоги

З дисципліни студент може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на екзамені.

Умовою допуску до екзамену є виконання всіх видів навчальної роботи передбачених даною робочою програмою – захист усіх лабораторних робіт, які виконувались у поточному семестрі, оформлення звіту по лабораторним роботам відповідно до стандартів, оформлення відповідно до стандартів курсового проекту та його захист.

Для захисту лабораторної роботи студент повинен відповісти на всі контрольні питання з методичних вказівок та на питання, за вибором викладача, з лекційного курсу по темі лабораторної роботи. За кожну лабораторну роботу студент отримує певну кількість балів з урахуванням максимальної кількості балів. При цьому враховується якість оформлення звіту та повнота відповідей на питання при захисті лабораторної роботи.

Для складання письмової компоненти модульного контролю існує перелік питань до модульного контролю. В залежності від повноти відповіді студент отримує певну кількість балів з урахуванням максимальної кількості балів. Студент, який не здає вчасно роботу, одержує оцінку нуль балів. Повторне складання студентом письмової компоненти модульного контролю не допускається.

Курсовий проект з дисципліни виконується у другому семестрі, відповідно до методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та практичних вмінь, набутих студентом у процесі засвоєння навчального матеріалу дисципліни в області проектування технічних систем захисту інформації. Для захисту курсового проекту студент повинен відповісти на декілька питань за вибором викладача по розрахункових частинах роботи. В тому випадку, коли студент відповідає на всі питання без помилок (або з несуттєвими помилками), курсовий проект вважається захищеним. Якщо при відповіді студент допускає грубі помилки, або питання виконані менш ніж на половину, то курсовий проект вважається незахищеним.

Складання екзамену є обов'язковим елементом підсумкового контролю знань для студентів, які претендують на оцінку «добре» або «відмінно». Якщо студент виконав всі види робіт протягом семестру та набрав 60% підсумкової оцінки (тобто «задовільно»), то він, за бажанням, може залишити набрану кількість балів як підсумкову оцінку і не складати екзамен.

З тими ЗВО, які до проведення підсумкового семестрового контролю не встигли виконати всі обов'язкові види робіт та мають підсумкову оцінку від 0 до 19 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни. У випадку якщо студент не має необхідних знань, він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань студентів НУ «Чернігівська політехніка».

Для складання екзамену існують білети. Якщо відповідь повна і зміст відповіді студента повністю відповідає сутності поставленого запитання, він може отримати від 33 до 40 балів. В тому випадку, коли студент виконує всі завдання без грубих помилок, він може отримати від 24 до 32 балів. Якщо при виконанні білету студент допускає грубі помилки і всі питання виконані менш ніж на половину, то він може отримати від 17 до 24 балів. При невиконанні хоча б одного завдання білету, студент не може отримати більше 16 балів.

Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється.

Дисципліну можна вважати такою, що засвоєна, якщо студент:

- знає базові терміни та визначення в галузі технічного захисту інформації;
- орієнтується в стандартах систем технічного захисту інформації;
- може охарактеризувати основі технічні канали витоку інформації;
- знає способи несанкціонованого перехоплення інформації;
- вміє працювати з системами технічного захисту інформації;
- вміє проектувати ТСЗІ та їх елементи з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію та технічне обслуговування;
- вміє проектувати, встановлювати, налаштовувати та обслуговувати системи відеонагляду, протипожежні системи та сигналізації;
- може забезпечити захист інформації за допомогою ТСЗІ від її витоку по технічним каналам;

В цьому випадку студент може отримати підсумкову оцінку «задовільно» - 60 балів – Е (в т.ч. й під час ліквідації академічної заборгованості з дисципліни).

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є поточний та семестровий контроль. Поточний контроль складається з опитувань, які проводяться під час лекцій, а також – захисту лабораторних робіт та курсового проекту. Запитання для поточного контролю знаходяться у відповідних методичних рекомендаціях. Семестровий контроль проводиться у вигляді екзамену, запитання до якого на початку семестру розміщується у системі дистанційного навчання. Екзаменаційні білети знаходяться в пакеті документації на дисципліну.

Оцінювання знань ЗВО здійснюється відповідно до «про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»», затвердженого Вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 та введено в дію наказом ректора від 31 серпня 2020 р. № 26.

Для визначення рівня засвоєння студентами навчального матеріалу використовуються такі методи оцінювання знань:

- поточний контроль на лабораторних заняттях (усне та письмове опитування, тестування, оцінка правильності та своєчасності виконання лабораторних робіт);
- оцінка за різні види самостійної роботи (наукові дослідження, реферати, домашні контрольні роботи, презентації, курсовий проект);
- проміжний модульний контроль;
- підсумковий контроль (2-й семестр - екзамен).

Поточний контроль проводиться шляхом спілкування із студентами під час лабораторних занять та консультацій, налагодження систем технічного захисту інформації, комп'ютерної техніки та програмного забезпечення, під час оцінювання виконання самостійної роботи. Бали, які набрані студентом під час поточного контролю, дораховуються до модульних оцінок.

Підсумковий контроль включає модульний та семестровий контроль. Модульний контроль проводиться у вигляді письмової відповіді на теоретичне запитання та вирішення практичної задачі.

Семестровий контроль за результатами вивчення дисципліни проводиться в останній атестаційний тиждень семестру (сесію) шляхом зваженого додавання результатів модульного контролю та постановки підсумкової оцінки до залікової відомості.

Для діагностики знань використовується модульно-рейтингова система зі 100-бальною шкалою оцінювання.

Поточний контроль за модулями			
Модуль за тематичним планом дисципліни та форма контролю		Кількість балів	
Змістовий модуль 1. Прикладні аспекти проектування технічних систем захисту інформації		0	45
1	Конспект за темами лекційних занять .	0	8
2	Оцінка виконання лабораторних робіт (підготовленість, самостійність, своєчасність)	0	24
5	Самостійна робота	0	8
6	Модульний контроль	0…	5
Змістовий модуль 2. Методологічні підходи до проектування технічних систем захисту інформації		0	15
1	Конспект за темами лекційних занять .	0	5
2	Самостійна робота	0	5
3	Модульний контроль	0	5
Підсумкова оцінка		0	60
Екзамен		0	40
Всього		0	100

Шкала оцінювання результатів навчання

Оцінка в балах	Оцінка ECTS	Оцінка за національною шкалою (диференційований залік)	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення

Особливістю виконання лабораторних робіт є застосування спеціальних технічних засобі захисту інформації: Аналізатор спектру С4-77, Аналізатор спектру Я40-0830, відеокамера LBA-A700/922, Веб-камера Logitech ConferenceCan BCC950, вимірювальні прилади NLMZ-4/50, SVT 401, УИП-88, генератори радіотехнічного шуму Ріас 1 ГМ, Ріас 1ГС, Ріас 1АЖ, генератор акустичного шуму Ріас 1ГМ, Генератор шуму для силової мережі Базальт 2ГС та ін.

10. Політики курсу.

Академічна доброчесність – самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності – академічний плагіат, корупція, несанкціонована співпраця, обман, списування, фабрикація, фальсифікація, хабарництво, шахрайство. Відповідно до Кодекс академічної доброчесності Національного університету «Чернігівська політехніка» введеного в дію наказом ректора № 100 від 31 травня 2021 року за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження підсумкового чи поточного оцінювання; повторне вивчення відповідного освітнього компонента освітньої програми; відрахування з Університету; позбавлення академічної стипендії

Політика дедлайнів – своєчасність здачі лабораторної роботи оцінюється в 0,5 бала за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 2 бали. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

Політика перезарахування кредитів у випадку мобільності – перезарахування відбувається якщо назви навчальних дисциплін ідентичні або мають незначну стилістичну відмінність, але обсяги та змістова частина навчальних програм не відрізняються; кількість кредитів, відведена на вивчення навчальної дисципліни відрізняється менше, ніж на 25 %; форми підсумкового контролю з дисциплін однакові. При перезарахуванні дисципліни зберігається раніше здобута позитивна оцінка. Перескладання іспиту з дисципліни з метою підвищення оцінки, визначеної в документах виданих здобувачу вищої освіти за попереднім місцем навчання, не дозволяється. Перезарахування кредитів проводиться відповідно Порядком визначення академічної різниці та визнання результатів попереднього навчання в Національному університеті «Чернігівська політехніка»

Політика щодо відвідування – відвідування занять є обов’язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

Політика щодо правил поведінки на заняттях – активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв тільки для навчання.

Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

11. Рекомендована література та інформаційні джерела

1. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.
2. Гупал Д. — “Технічні засоби захисту інформації від витоку технічними каналами з об’єктів інформаційної діяльності Національної поліції України” (2020)
3. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
7. Система дистанційного навчання НУ «Чернігівська політехніка».– [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=3451
8. Державна служба спеціального зв’язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua
9. Офіційний портал Верховної Ради України [Електронний ресурс]. – Режим доступу: www.rada.gov.ua/