МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра інформаційної безпеки

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

СЕРТИФІКАТНА ПРОГРАМА

для другого (магістерського) рівня вищої освіти
за освітніми програмами

«Системи, технології та математичні методи кібербезпеки»
«Системи технічного захисту інформації»

спеціальності

125 Кібербезпека та захист інформації

Ухвалено Методичною радою
КПІ ім. Ігоря Сікорського
від 7.12.2023 р., протокол № 9

Введено в дію наказом
*№ НОД.**2024 р., № ХХХ/ХХХ/20ХХ***

Київ – 2024

Розробники сертифікатної програми:

Ланде Дмитро Володимирович - завідувач кафедри інформаційної безпеки, д.т.н., професор

Стьопочкіна Ірина Валеріївна - доцент кафедри інформаційної безпеки, к.т.н., доцент

Смирнов Сергій Анатолійович - доцент кафедри інформаційної безпеки, к.ф.-м.н., доцент

Литвинова Тетяна Василівна - доцент кафедри інформаційної безпеки, к.т.н., доцент

ЗМІСТ

1. ОПИС СЕРТИФІКАТНОЇ ПРОГРАМИ

1. Загальна інформація	
Назва сертифікатної програми	**КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**
Рівень вищої освіти	Другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітні програми	Системи, технології та математичні методи кібербезпеки Системи технічного захисту інформації
Факультет / Інститут	Навчально-науковий фізико-технічний інститут
Кафедра	Інформаційної безпеки
Обсяг сертифікатної програми	19 кредитів ЄКТС
Мова викладання	Українська
Документ про опанування сертифікатної програми	Сертифікат встановленого зразка КПІ ім. Ігоря Сікорського
Термін дії сертифікатної програми	Безстроково
Інтернет- адреса постійного розміщення сертифікатної програми	

2. Мета сертифікатної програми

Поглиблення фундаментальних і формування спеціальних знань, умінь і навичок для вирішення наступних задач кібербезпеки (теоретичного та практичного характеру): захист інформації в спеціалізованих інформаційно-комунікаційних системах об'єктів критичної інфраструктури, аналіз кібернетичних загроз та інцидентів в таких системах, адміністрування та експлуатація захищених інформаційно-комунікаційних систем, у тому числі із урахуванням вимог захисту від атак соціальної інженерії, підготовка висококваліфікованих фахівців наукового і інженерно-технічного спрямування, які відповідають потребам ринку праці.

3. Особливості участі слухачів Сертифікатної програми

3.1. Сертифікатна програма (СП) - спеціалізований комплекс пов'язаних між собою дисциплін (освітніх компонентів) встановленого обсягу, який передбачає професійно спрямовану підготовку слухачів (студентів кафедри Інформаційної безпеки Фізико-технічного інституту) та споріднених спеціальностей інших факультетів/інститутів Національного технічного університету України КПІ ім. Ігоря Сікорського, а також зовнішніх слухачів). Якщо сертифікатна програма виконується за дуальною формою освіти, вступ за конкурсом партнерів-роботодавців.

3.2. Освітні компоненти СП, загальним обсягом 19 кредитів, складаються з вибіркових дисциплін другого (магістерського) рівня вищої освіти ОПП/ОНП спеціальності 125 Кібербезпека.

3.3. Запис здобувачів вищої освіти КПІ ім. Ігоря Сікорського на дисципліни СП проводиться у встановлені терміни індивідуального вибору на основі поданої заяви. Зарахування здійснюється на весь обсяг СП згідно Положенню про сертифікатні програми КПІ ім. Ігоря Сікорського.

3.8. За результатами опанування освітніх компонентів сертифікатної програми, набуттям програмних результатів навчання, здобувачу видається сертифікат КПІ ім. Ігоря Сікорського за підписом проректора. Інформація про опанування сертифікатної програми вноситься в додаток до диплому європейського зразка.

3.9 Передумовами опанування сертифікатної програми є знання основних відомостей щодо операційних систем і мереж, включаючи Linux, Windows (включаючи Active-Direktory) I MacOs, Web-застосунків і WEB-програмування, а також мова програмування Python.

3.10 Якщо сертифікатна програма виконується за дуальною формою освіти, відбір здобувачів на СП проводиться на основі співбесіди з представниками партнерів згідно Положенню про дуальну форму здобуття вищої освіти в КПІ ім. Ігоря Сікорського.

4. Компетентності та очікувані результати навчання

Сертифікатну програму запроваджено як профілізаційну складову освітньої програми, для задоволення освітніх потреб здобувачів – формування ними індивідуальної траєкторії здобуття вищої освіти.
Сертифікатна програма передбачає підвищення рівня сформованості спеціальних (фахових) компетентностей за спеціальністю, посилення професійної підготовки за освітньою програмою.
Сертифікатна програма спрямована на засвоєння слухачами особливостей організації кібернетичного захисту критичної інфраструктури.
Вона наповнена унікальним контентом та авторськими курсами, які характеризуються практичністю та актуальністю інформації, що дозволяє отримати додаткові знання та навички, розширити коло кар'єрних можливостей в сфері кібербезпеки та захисту інформації

Компетентності	**Загальні** Здатність застосовувати знання у практичних ситуаціях, здатність до абстрактного мислення, аналізу та синтезу. **Професійні** - Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки. - Здатність інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. - Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. - Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. - Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої

	стратегії і політики інформаційної безпеки та/або кібербезпеки організації. - Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
Очікувані результати навчання	- Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах - Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки - Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізикоматематичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення - Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення - Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури - Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки - Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. - Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки - Забезпечувати захист веб серверів і веб-застосунків від хакерських атак, - Забезпечувати дотримання повноважень на рівні політик захисту операційних систем і мереж - Проводити тестування на проникнення - Збирати інформацію про можливі вразливості і атаки

5. Перелік освітніх компонентів

Освітні компоненти сертифікатної програми	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр вивчення
1. Захист інформації в спеціалізованих інформаційно-	5	екзамен	2

телекомунікаційних системах			
2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	5	екзамен	2
3. Теорія і методи соціальної інженерії в кібербезпеці	5	екзамен	2
4. Аналіз кібернетичних загроз в інформаційно-телекомунікаційних системах із застосуванням методів машинного навчання	4	залік	2
5. Рішення в умовах невизначеності та ризику	4	залік	2
Загальний обсяг кредитів ЄКТС	**23**		

6. Викладання та оцінювання

Викладання та навчання	Лекції, практичні, семінарські, лабораторні заняття
Оцінювання	Види контролю результатів навчання: поточний, календарний, семестровий. Контроль проводиться згідно з Положенням про поточний, календарний та семестровий контроль результатів навчання в КПІ ім. Ігоря Сікорського Оцінювання результатів навчання здійснюється за рейтинговими системами, визначеними у силабусах навчальних дисциплін. Рейтингові системи оцінювання складені згідно з вимогами Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського

7. Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Лекції читають висококваліфіковані фахівці в галузі кібербезпеки та захисту інформації
Матеріально-технічне забезпечення	Освітні компоненти сертифікатної програми базуються на ресурсах НН ФТІ, кафедри інформаційної безпеки, партнерів – роботодавців за дуальною формою освіти.
Інформаційне та навчально-методичне забезпечення	Підручники, навчальні посібники, відеолекції, , курси Moodle, Google Classroom згідно силабусів

2. ОПИСИ ОСВІТНІХ КОМПОНЕНТІВ

1. Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах проф. Зубок	
Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	*Необхідно знати*: фізичну природу електромагнітних сигналів та середовища передачі даних, архітектуру комп'ютерних систем; операційні системи та їх безпеку; технології програмування; теорію інформації та кодування; нормативно правове забезпечення захисту інформації; методи та засоби забезпечення інформаційної безпеки; міжнародні та національні стандарти в сфері інформаційної безпеки. *Необхідно вміти*: виконувати класифікацію автоматизованих систем; виконувати класифікацію інформації; виконувати аналіз профілю захищеності; визначати межі контрольованої зони; виконувати проектування та знати процедури забезпечення КСЗІ; виконувати класифікацію об'єктів інформаційної діяльності; розробляти політику безпеки для ОІД (об'єкт інформаційної діяльності); оцінювати ефективність мір захисту інформації.
Що буде вивчатися	Навчальна дисципліна «Захист інформації в інформаційно-телекомуні-каційних системах спеціального призначення» присвячена окремим напрямкам та методам, які використовуються у напряму комплексного підходу до захисту інформаційних ресурсів на об'єктах інформаційної діяльності. Подається структурований матеріал, що відображає сучасні технології та моделі захисту інформації в телекомунікаційних системах та

	мережах. Докладно розглянуто основи захисту інформації та основні питання інформаційної безпеки національної мережі телекомунікацій, телекомунікаційних мереж загального користування та спеціального призначення, основні методи і засоби захисту телетрафіку, а також основи організації захисту інформації в галузі інформаційно-телекомунікаційних систем та їх мереж. Основні теми, які розглядаються у курсі: 1. Системи та мережі передачі. Класифікація; загальні моделі та характеристики систем передачі інформації. 2. Моделі канал зв'язку. Поняття динамічного діапазону каналу зв'язку, узгодження характеристик. 3. Сучасні інформаційно-телекомунікаційні мережі. Класифікація мереж та середовища передачі даних, типи протоколів передачі даних в аспекті захисту інформаційних ресурсів та їх властивостей. 4. Інформаційно-телекомунікаційні системи та технології як об'єкти інформаційної безпеки. 5. Нормативно-правове забезпечення захисту інформації в інформаційно-телекомунікаційних системах та мережах згідно вітчизняних та світових вимог і стандартів. 6. Вимоги та критерії безпеки інформаційно-телекомунікаційних систем. 7. Управління інформаційними активами інформаційно-телекомунікаційних систем загального та спеціального призначення. 8. Моделі загроз та моделі порушника в інформаційно-телекомунікаційних системах та мережах. 9. Ризик менеджмент в інформаційно-телекомунікаційних системах загального та спеціального призначення. 10. Профілі захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах та мережах. Технології та архітектура управління забезпеченням. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал.
Чому це цікаво/треба вивчати	Навчальна дисципліна розглядає законодавчі вимоги до кіберзахисту спеціалізованих систем, нормативне забезпечення, міжнародні стандарти на кращі світові практики цієї діяльності, перш за все, в аспекті кібербезпеки так званих Операційних технологій (ICS/SCADA систем). Безпека операційних технологій, "Промисловості 4.0", промислового Інтернету речей (IIoT) є одним з головних завдань кібербезпеки, особливо під час відновлення інфраструктури та промисловості України.
Чому можна навчитися	Сучасні технологічні тренди захисту інформації спеціалізованих ІКС. Загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих ІКС. Спеціалізовані ІКС в державному та банківському секторі, в промисловості. Міжнародні документи з кіберзахисту промислових ІКС. Ключові аспекти спеціалізованих комунікаційних технологій в промисловості. Кіберінциденти

	в промисловості. Огляд та архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту спеціалізованих ІКС в промисловості. Архітектури та топології промислових ІКС. Порівняння вимог до безпеки загальних ІТ систем та ІКС управління технологічними процесами (АСУТП). Архітектура кіберзахисту спеціалізованих промислових ІКС. Сегментація, сегрегація, засоби впровадження. Заходи з забезпечення кібербезпеки в промисловості. Реагування на інциденти. Побудова політики безпеки спеціалізованої ІТС з використанням «контролів безпеки».
Як можна користуватися набутими знаннями та вміннями	Вивчення дисципліни дозволяє поглибити розуміння технологій та моделей захисту інформації в інформаційно-телекомунікаційних системах та мережах, їх властивостей, внутрішніх зв'язків та інтерпретацій у термінах різних дисциплін.
Вид семестрового контролю	екзамен

2.Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення	Для успішного оволодіння матеріалом потрібно мати знання щодо методів захисту інформації в інформаційно- комунікаційних системах та підходів до захисту web-ресурсів.

дисципліни	
Що буде вивчатися	Метою навчальної дисципліни є отримання знань та навичок про архітектуру, налаштування та супровід технологій захисту сучасних інформаційно-комунікаційних систем.
Чому це цікаво/треба вивчати	Отримання знань та навичок щодо архітектури, налаштування та супроводу технологій захисту сучасних інформаційно-комунікаційних систем
Чому можна навчитися	В процесі вивчення дисципліни студенти засвоять такі теми: - Управління ідентифікаціями (Identity management) - Системи контролю привілеїв користувачів (Privileged access management) - Протоколи автентифікації та авторизації - Засоби побудови віртуальних захищених мереж (VPN) - Системи управління інформаційною безпекою та подіями безпеки (Security information and event management) - Використання засобів віртуалізації та хмарних технологій для побудови захищених інформаційно-комунікаційних систем
Як можна користуватися набутими знаннями та вміннями	В результаті вивчення навчальної дисципліни студенти зможуть застосувати отримані знання для аналізу захищеності інформаційно-комунікаційних систем, формування рекомендацій щодо підвищення ступеню їх захисту, а також роботи над обраними темами магістерських дисертацій
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1_zarwriqpQx7j4VWCVt4zzfXjp5j_cb1?usp=sharing
Вид семестрового контролю	екзамен
3. Теорія і методи соціальної інженерії в кібербезпеці	
Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг	5 кредитів ЄКТС

дисципліни та розподіл годин аудиторної та самостійної роботи	
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Бажане уміння програмувати на мовах Java, Python.
Що буде вивчатися	Соціальна інженерія є одним із найуспішніших напрямків здійснення атак на об'єкти різного типу. Слабкою ланкою кожної системи захисту є людина, саме з участю людського фактору соціальний інженер досягає своєї мети. Уміння та знання, набуті в цьому курсі, можуть бути використані там, де передбачається діяльність із кіберзахисту інформації, в тому числі із використанням наукоємних технологій, на стику із методиками HR-менеджмента. Навчальна дисципліна розглядає теоретичні основи відповідних атак. В тому числі, розглянуто моделі атак соціальної інженерії, моделі їх виявлення, сценарії різних видів атак соціальної інженерії, ПЗ, яке використовується при цьому та способи протидії цим атакам. Ці знання дають змогу зрозуміти фактори успіху відповідних атак, та попередити їх. Теоретичні матеріали курсу дають студенту знання про: - Моделі та сценарії атак та їх виявлення; - Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак; - Механізми здійснення різних атак соціальної інженерії; - Нові технології та засоби соціальної інженерії, засновані на ML та AI. - Рішення кіберзахисту та підходи до попередження атак соціальної інженерії. Також за дисципліною передбачено 5 комп'ютерних практикумів, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом.
Чому це цікаво/треба вивчати	Атаки на основі соціальної інженерії складно піддаються виявленню технічними засобами, і є дуже поширеним та багатогранним явищем. Великий відсоток таких атак є успішним.Відповідно, проходження даного курсу дозволяє розширити знання студентів щодо ефективній протидії таким атакам.
Чому можна	Технікам соціальної інженерії (для задач offensive security), опанувати засоби

навчитися	та методи протидії.
Як можна користуватися набутими знаннями та вміннями	В результаті виконання практикумів студенти набувають такі уміння: - Розробляти сценарії та моделі атак соціальної інженерії та здійснювати імітаційне моделювання; - Уміння розробляти програму тестування на проникнення із використанням різних підходів; - Використовувати наявні програмні засоби, за допомогою яких може діяти соціальний інженер, в цілях тестування на проникнення; - Уміння розробляти методики оцінки персоналу на чутливість до різних атак соціальної інженерії; - Уміння розробляти елементи засобів тестування на проникнення із використанням підходів соціальної інженерії.
Інформаційне забезпечення дисципліни	Платформа "Сікорський": курс «Теорія та методи соціальної інженерії в кібербезпеці» https://do.ipo.kpi.ua/course/view.php?id=1713
Вид семест-рового контролю	екзамен

4. Аналіз кібернетичних загроз в інформаційно-телекомунікаційних системах із застосуванням методів машинного навчання

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	- знання основ математичного аналізу; - знання основ спектрального аналізу сигналів; - знання пакетів для моделювання на мові програмування Python; - знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості).
Що буде вивчатися	Метою навчальної дисципліни є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації в інформаційно-комунікаційних системах в умовах

	опрацювання значних об’ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних.
Чому це цікаво/треба вивчати	Поглиблення розуміння принципів роботи, області застосування та обмежень сучасних статистичних моделей даних. Підвищення точності роботи статистичних моделей в умовах зашумленості та/або даних.
Чому можна навчитися	- Знання термінології в галузі аналізу та класифікації (кластеризації) даних; - Знання методів моделювання багатовимірних сигналів в умовах обмеженості або відсутності даних щодо їх статистичних характеристик; - Знання поширених методів класифікації (кластеризації) багатовимірних даних; - Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних. - Вміння вибору статистичних моделей багатовимірних сигналів з врахуванням наявної інформації щодо їх статистичних та кореляційних характеристик; - Вміння застосування методів класифікації (кластеризації) даних в умовах обробки реальних (зашумлених) сигналів; - Вміння проведення оцінювання якості роботи систем класифікації (кластеризації) даних
Як можна користуватися набутими знаннями та вміннями	Отримані знання та вміння можуть бути використаними для вирішення практичних завдань, пов’язаних із застосуванням методів теорії розпізнавання образів для обробки різнорідних типів даних.
Вид семестрового контролю	залік

5. Рішення в умовах невизначеності та ризику (доц. Смирнов С.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС

Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для успішного засвоєння курсу потрібні попередні знання з математичного аналізу, алгебри і геометрії, дискретного аналізу, математичного моделювання.
Що буде вивчатися	Метою курсу є вивчення теоретичних основ та практичних методів прийняття рішень в умовах невизначеностей різної природи: множинної, ймовірністної, конфліктної. Обговорюються також методи контролю та подолання різних форм складності, ризику та невизначеності, що містяться в практичних ситуаціях прийняття рішень.
Чому це цікаво/треба вивчати	Викладаються математичні засоби що дозволяють успішно долати шлях від неформалізованої постановки задачі з боку Замовника, через проактивне моделювання ситуації, до варіантів її точного розв'язання Виконавцем.
Чому можна навчитися	Розв'язувати задачі оцінювання та прийняття рішень в умовах невизначеності та ризику від початку до кінця
Як можна користуватися набутими знаннями та вміннями	Отримані знання та вміння щодо сучасних методів прийняття рішень в умовах невизначеності можуть бути використані для вирішення задач за темою магістерської дисертації.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/14Q8h3tj3SPojyXIVIZtb9SWGap_2_OIN?usp=sharing Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Рішення в умовах невизначеності та ризику " https://classroom.google.com/u/1/c/OTk3MTgyNzQzNDNa?hl=uk
Вид семестрового контролю	залік

4. СИЛАБУСИ ОСВІТНІХ КОМПОНЕНТІВ СЕРТИФІКАТНОЇ ПРОГРАМИ

Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

НН ФТІ

Кафедра інформаційної безпеки

Захист інформації в спеціалізованих інформаційно-комунікаційних системах
Робоча програма навчальної дисципліни
(Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	*Другий (освітньо-професійний)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*«Системи, технології та математичні методи кібербезпеки», «Системи технічного захисту інформації»*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*1 курс, 2 семестр*
Обсяг дисципліни	*5 кредитів ECTS (36 годин лекцій, 18 годин практ., 96 СРС)*
Семестровий контроль/ контрольні заходи	*Екзамен, МКР*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, старший дослідник Зубок Віталій Юрійович, telegram: @vit_zub, e-mail: vitaly.zubok@gmail.com* Практичні: *Зубок Віталій Юрійович*
Розміщення курсу	Посилання на дистанційний ресурс Платформа «Google Classroom», код hemn6u7

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Україна в даний час проходить етап стрімкої трансформації цифрового середовища. Попри широкомасштабну військову агресію з'являється все більше електронних послуг, які надають як державні структури, так і приватні компанії. В умовах продовження проти України гібридної війни значно зросли загрози інформаційно-телекомунікаційним системам (ІКС) різних галузей та призначень, зокрема і спеціалізованим ІКС, призначеним для обробки інформації в інформаційно-комунікаційних системах, у яких захист інформації забезпечується у тому числі з використанням засобів криптографічного захисту, а також ІКС, задіяних в функціонуванні промислових виробничих систем, зокрема, об’єктів критичної інфраструктури

(ОКІ). Для багатьох підприємств релокація та відновлення виробництва на новій більш безпечній локації надає можливість побудови кіберзахисту промислових ІКС (так хваних «Operation technologies») на новому, сучасному рівні.

Навчальна дисципліна «Захист інформації в спеціалізованих інформаційно-комунікаційних системах» розглядає законодавчі вимоги до кіберзахисту таких спеціалізованих систем, нормативне забезпечення, міжнародні стандарти на кращі світові практики цієї діяльності. Розглянуто загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих ІКС, ключові аспекти спеціалізованих комунікаційних технологій в промисловості, дослідження актуальних кіберзагроз, сценарії відомих кіберінцидентів, архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту. Ці знання дають змогу формулювати політики безпеки спеціалізованих ІКС, розуміти основні засоби реалізації цієї політики та контролювання її виконання з урахуванням законодавчих вимог.

Теоретичні матеріали курсу дають студенту знання про:

– класифікацію інформаційно-комунікаційних систем за вимогами інформаційної безпеки відповідно до призначення цих систем;

– нормативно-правове та законодавче регулювання питань кібербезпеки в спеціалізованих ІКС;

– міжнародні документи з питань кібербезпеки спеціалізованих ІКС, зокрема на об’єктах критичної інфраструктури та в промисловості;

– моделі та сценарії атак на промислові спеціалізовані ІКС та їх виявлення;

– механізми здійснення різних атак на промислові спеціалізовані ІКС;

– архітектуру кіберзахисту та сучасні комплексні засоби кіберзахисту спеціалізованих ІКС в промисловості;

– заходи з забезпечення кібербезпеки спеціалізованих ІТС в промисловості.

Також за дисципліною передбачено практичні заняття, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. Передбачається, що практикуми повинні бути здані вчасно, в разі перевищення дедлайну встановлений штраф: практикум захищається на мінімальну позитивну оцінку. Дати дедлайнів обговорюються зі студентами на першому занятті.

Предметом дисципліни є методи, засоби та нормативно-правове забезпечення захисту інформації в спеціалізованих інформаційно-комунікаційних системах.

В результаті опанування дисципліною студент отримує додаткові знання та навички, які розширюють коло кар’єрних можливостей в сфері кібербезпеки та захисту інформації, серед них такі ***фахові компетентності***:

– 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 з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;

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

– Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог;

– Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому;

– Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, критично оцінювати результати досліджень та інновацій, презентувати результати досліджень та формувати науково-технічну звітність;

та **програмні результати навчання**

– Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

– Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

– Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

– Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

– Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.

– Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

– 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.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна містить взаємозв’язки із такими попередніми дисциплінами: «Основи технологій захисту інформації», «Безпека комп’ютерних мереж», «Управління інцидентами кібербезпеки», «Теорія ризиків», «Аналіз та моніторинг кібернетичної безпеки».

Результати вивчення даної дисципліни можуть бути застосовані у професійній діяльності за фахом та для написання магістерської дипломної роботи.

3. Зміст навчальної дисципліни

– Спеціалізовані інформаційно-комунікаційні системи - сучасна семантика та термінологія предметної області. Основні відмінності загальних та спеціалізованих ІТ систем.

– Сучасні нормативні та технологічні тренди захисту інформації спеціалізованих ІКС. Загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих ІКС. Спеціалізовані ІКС в державному та банківському секторі.

– Спеціалізовані ІКС в промисловості. Міжнародні документи з кіберзахисту промислових ІКС. Ключові аспекти спеціалізованих комунікаційних технологій в промисловості. Кіберінциденти в промисловості.

– Дослідження актуальних кіберзагроз, аналіз та оцінювання ризиків кібератак на спеціалізовану ІКС.

– Огляд та архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту спеціалізованих ІКС в промисловості.

– Аналіз методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури та Cybersecurity Framework.

– Архітектури та топології промислових ІКС. Порівняння вимог до безпеки загальних ІТ систем та ІКС управління технологічними процесами (АСУТП). Архітектура кіберзахисту спеціалізованих промислових ІКС. Сегментація, сегрегація, засоби впровадження.

– Основні та додаткові заходи з забезпечення кібербезпеки спеціалізованих ІТС в промисловості. Реагування на інциденти. Побудова політики безпеки спеціалізованої ІТС з використанням «контролів безпеки».

4. Навчальні матеріали та ресурси

Базова література.

1. *Закон України «Про основні засади забезпечення кібербезпеки України». – К.: Відомості Верховної Ради. – 2017. – № 45. – с.403.*

2. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". – Введено в дію Указом Президента України №447/2021.

3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Наказ ДСТСЗІ СБУ від 28.04.99 № 22.

4. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Наказ ДСТСЗІ СБУ від 28.04.99 (зі змінами).

5. Положення про захист інформації та кіберзахист у платіжних системах. – Затверджено постановою Національного банку України від 19.05.2021 № 43.

6. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. – Затверджено Наказом Адміністрації ДССЗЗІ України від 06.10.2021 року № 601.

7. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. – National Institute of Standards and Technology. – April 16, 2018. DOI:10.6028/NIST.CSWP.04162018

8. NIST Special Publication 800-82 rev.2. Guide to Industrial Control Systems (ICS) Security, NIST, 2015 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. - Accessed : 07 February 2021.

9. Communication network dependencies for ICS/SCADA Systems. – ENISA. – December 2016. – DOI:10.2824/397676.

Додаткова література.

10. Система електронної взаємодії державних електронних інформаційних ресурсів. [Online] Доступно : https://trembita.gov.ua/ua . Дата доступу: 01 Вер 2021.

11. Державні послуги онлайн. [Online] Доступно : https://diia.gov.ua . Дата доступу: 12 Вер 2021.

12. Порядок прийняття рішень щодо визначення операторів інформаційно-телекомунікаційних систем (мереж) Національної системи конфіденційного зв'язку наказом Адміністрації Держспецзв'язку від 23 травня 2016 року № 346 (зі змінами).

13. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. - U.S. Department of Homeland Security. – October 2009. [Online]: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/ Defense_in_Depth_Oct09.pdf : Accessed 12 Jan 2022.

14. Concerning measures for a high common level of security of network and information systems across the Union. Directive (EU) 2016/1148 [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. - Accessed : 07 February 2021.

15. Communication network dependencies for ICS/SCADA Systems. December 2016 : ENISA : doi:10.2824/397676

16. NIST SP 800-53 Rev. 5 "Security and Privacy Controls for Federal Information Systems and Organizations"," 23 September 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final. - Accessed : 07 February 2021.

17. A.Ginter. "THE TOP 20 CYBERATTACKS on Industrial Control Systems" [Online] Available : https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf. – Accessed: 29 Oct 2021.

18. Зубок В.Ю. Факторний аналіз ризиків на прикладі інциденту з програмним забезпеченням реєстру глобальної маршрутизації. / В.Ю. Зубок // Реєстрація, зберігання і обробка даних. – ISSN: 1560-9189. – 2020. – Т.22. – №1. – С.49-55.

19. Зубок В.Ю. Особливості моделі порушника при аналізі атак на глобальну маршрутизацію в Інтернеті / В.Ю.Зубок // Реєстрація, зберігання і обробка даних. – ISSN: 1560-9189. – 2019 . – Т.41. – №5. – С. 59-70

20. IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models, IEC, 2009.

21. IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, IEC, 2016.

22. TCP/IP Illustrated, Volume 1: The Protocols. - Addison-Wesley Professional. - 1993. - ISBN: 9780201633467

23. D.E. Comer. Internetworking with TCP/IP Volume One: Principles, Protocols, and Architecture, 6th Edition. – «Pearson», 2013. – 744 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:

- лекції;
- практичні заняття;
- самостійна робота.

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити студентам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовано у відповідності із матеріалами лекцій і повністю узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Internet. На заняттях використовуються звичайна дошка, а також презентації лекцій з використанням мультимедіа-проектора. В дистанційному режимі використовуються засоби Google Meet та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

Теми та порядок освоєння дисципліни «Захист інформації в спеціалізованих інформаційно-комунікаційних системах» наведений нижче.

№ з/п	Назви тем і питань, що виноситься на заняття
	Розділ 1. Сучасний стан та розвиток кібербезпеки спеціалізованих інформаційно-комунікаційних систем
1	**Вступ.** РСО, предмет та об’єкт курсу. **Тема 1.** Спеціалізовані інформаційно-комунікаційні системи. Сучасна термінологія предметної області. Основна література: [1, 2]. Додаткова література: [3,4].
2	**Тема 2.** Основні відмінності загальних та спеціалізованих ІТ систем. Сучасні тренди кібербезпеки спеціалізованих ІТС. Основна література: [5]. Додаткова література: [10-12]
3	**Тема 3.** Загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих інформаційно-телекомунікаційних систем в промисловості. Основна література: [6,7]. Додаткова література: [13]
4	**Тема 4.** Міжнародні документи з кіберзахисту спеціалізованих інформаційно-телекомунікаційних систем в промисловості. Основна література: [7]. Додаткова література: [14]
5	**Тема 5.** Ключові аспекти кібербезпеки спеціалізованих комунікаційних технологій в промисловості. Кіберінциденти в промисловості. Основна література: [6,7]. Додаткова література: [15]
6	**Тема 6.** Дослідження актуальних кіберзагроз та аналіз ризиків. Аналіз відомих кіберінцидентів. Основна література: [7]. Додаткова література: [16]

7	**Тема 7.** Оцінювання ризику кібератак на спеціалізовану комунікаційну мережу. Основна література: [6]. Додаткова література: [17,18]
8	**Тема 8.** Архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту. Основна література: [8,9].
	Розділ 2. Методи та засоби кіберзахисту спеціалізованих інформаційно-комунікаційних систем
9	**Тема 9.** Аналіз методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури та Cybersecurity Framework. Основна література: [5].
10	**Тема 10.** Огляд спеціалізованих промислових ІКС. Архітектури та топології промислових ІКС Основна література: [7]. Додаткова література: [15]
11	**Тема 11.** Порівняння вимог до безпеки ІТ та АСУТП. Основна література: [7,8]. Додаткова література: [15]
12	**Тема 12.** Управління ризиками інформаційної безпеки промислових ІТ-систем. Основна література: [8]. Додаткова література: [15,20]
13	**Тема 13.** Архітектура кіберзахисту спеціалізованих промислових ІТ-систем. Сегментація, сегрегація, засоби впровадження. Основна література: [8]. Додаткова література: [20,21-23]
14	**Тема 14.** Архітектура кіберзахисту спеціалізованих промислових ІТ-систем. Безпека мережевих протоколів та технологій. Основна література: [8]. Додаткова література: [21-23]
15	**Тема 15.** Основні заходи з забезпечення кібербезпеки спеціалізованих ІТС в промисловості. Основна література: [7,8]. Додаткова література: [13]
16	**Тема 16.** Додаткові заходи з забезпечення кібербезпеки спеціалізованих ІТС в промисловості. Основна література: [7,8]. Додаткова література: [13]
17	**Тема 17.** Реагування на кіберінциденти в спеціалізованих ІТС. Основна література: [6-8]. Додаткова література: [16,18]
18	**Тема 18.** Побудова політики безпеки спеціалізованої ІТС з використанням «контролів безпеки». Основна література: [6-8]. Додаткова література: [20]

Теми практичних занять

№ КП	Теми практичних занять	Кількість ауд. годин
1. .	Дослідження сучасних трендів захисту інформації в спеціалізованих ІКС	2
2. .	Аналіз вимог національних галузевих органів стандартизації щодо кіберзахисту спеціалізованих ІКС (NERC, AGA, DOE, CISA)	2
3. .	Аналіз загроз та моделювання кібератак на інформаційну інфраструктуру промислового об’єкта	2

4. .	Дослідження та порівняння відомих платформ та систем кіберзахисту для промислових ІКС	2
5. .	Дослідження архітектури та топології спеціалізованих ІКС в промисловості (ICS, SCADA та DCS) з точки зору побудови системи кіберзахисту.	2
6.	Особливості реалізації фреймворку оцінювання ризиків в ICS.	2
7.	Вирішення задач мережевої безпеки в ICS	2
8.	Вирішення задач мережевої безпеки в ICS (продовження)	2
9.	Проектування та планування заходів з реагування на кіберінциденти та відновлення в ICS	2
Всього		18

6. Самостійна робота здобувача

Самостійна робота здобувача складається із опанування та засвоєння відповідних лекційних матеріалів, підготовки до МКР та екзамену. Також здобувачі самостійно доопрацьовують результати практичних занять та оформлюють їх у вигляді звітів, допоміжні контрольні питання надано в [2].

Самостійна робота студента

№ з/п	**Вид самостійної роботи**	**Кількість годин СРС**
1.	Підготовка до практичних робіт	30
2.	Підготовка до лекцій	16
3.	Підготовка до МКР	20
4.	Підготовка до екзамену	30
	Всього	**96**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Контроль відвідування проводиться викладачем вибірково. Завдання практичних занять виконуються та захищаються у відповідності до встановлених дедлайнів протягом семестру. Під час виконання практичних робіт а також під час контрольних заходів здобувачами повинна дотримуватись політика академічної доброчесності, згідно Кодексу Честі НТУУ “КПІ”.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: робота на практичних заняттях та захист звітів, МКР.

Критерії оцінювання МКР (макс.бал - 15):

- вичерпна відповідь – 13-15 балів;
- неповна відповідь – 9-12 бали;
- частково правильна відповідь, наведено основні базові поняття для розв'язку, є помилки – 6-8 балів;
- грубі помилки – 3-5 балів;
- незадовільна відповідь – 0 балів.

Календарний контроль: *проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.*

Екзамен та робота в семестрі

Екзамен є обов'язковим контрольним заходом. Рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 60 балів).

Заохочувальні та штрафні бали (не більше 6 балів) :

Заохочувальні бали		Штрафні бали	
Критерій	Ваговий бал	Критерій	Ваговий бал
Активність на практичному занятті	+2 бали	Невчасне здання звіту з практичного заняття	-2 бали

Умови допуску до семестрового контролю: мінімальна позитивна оцінка за комп'ютерні практикуми / семестровий рейтинг більше 30 балів.

Максимальна кількість балів за семестр – 60.

Семестровий контроль: екзамен. На екзамені здобувач одержує білет, відповідь на який оцінюється по 40-бальній шкалі.

Оцінювання відповідей на екзамені:

- вичерпна відповідь – 35-40 балів;
- вичерпна відповідь з незначними помилками – 30-34 балів;
- неповна відповідь та помилки – 20 – 29 балів;
- грубі помилки – 8-19
- незадовільна відповідь – 0 балів.

№ з/п	Контрольний захід	Макс. бал	Кіл-ть	Всього
1.	Практичні заняття	5	9	45
2.	Модульна контрольна робота	15	1	15
2.	Екзамен	40	1	40
	Всього			100

Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
95 ≤ RD ≤ 100	Відмінно	-
85 ≤ RD ≤ 94	Дуже добре	-
75 ≤ RD ≤ 84	Добре	-
65 ≤ RD ≤ 74	Задовільно	-
60 ≤ RD ≤ 64	Достатньо	-
RD < 60	Незадовільно	-
Невиконання умов допуску	Не допущено	-

9. Додаткова інформація

Питання, що виносяться на екзамен, повністю відповідають змісту дисципліни.
Необхідною умовою роботи здобувача є його реєстрація на курсі "Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах" на платформі Сікорський https://do.ipo.kpi.ua/course/view.php?id=5543

Робочу програму навчальної дисципліни (силабус):

Склав: професор кафедри Інформаційної безпеки, докт.техн.наук, ст. досл. Зубок Віталій Юрійович

Ухвалено кафедрою інформаційної безпеки (протокол №6/2023 від 08.06.2023).

Погоджено Методичною комісією НН ФТІ (протокол № 6/2023 від 29.06.2023).

Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

НН ФТІ

Кафедра інформаційної безпеки

Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем
Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***другий (освітньо-науковий, освітньо-професійний)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*«Системи, технології та математичні методи кібербезпеки», «Системи технічного захисту інформації»*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна(денна)*
Рік підготовки, семестр	*1 курс, осінній*
Обсяг дисципліни	*150 год (5 кред ECTS) (36 годин лекцій, 18 годин комп'ютерних практикумів, 96 годин самостійна робота студентів)*
Семестровий контроль/ контрольні заходи	*Екзамен / модульна контрольна робота*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: кандидат технічних наук, *доцент, Барановський Олексій Миколайович, контактні дані e-mail: o.baranovskyi@kpi.ua* Практичні: кандидат технічних наук, *доцент, Барановський Олексій Миколайович, контактні дані e-mail: o.baranovskyi@kpi.ua*
Розміщення курсу	

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Дисципліна "Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем" призначена для навчання студентів сучасним підходам та методам управління та обслуговуванням інформаційних та комунікаційних систем з підвищеним акцентом на їхню безпеку та захист від потенційних загроз інформаційної безпеки. Ця дисципліна важлива в сучасному інформаційному суспільстві, де даними, інформацією та

комунікаційними системами оперують на всіх рівнях бізнесу, державного управління і особистого життя.

Теоретичні матеріали курсу дають студенту знання надають студентам підготовку для ефективного адміністрування, експлуатації та захисту інформаційних та комунікаційних систем в сучасному інформаційному середовищі. Вони також допомагають студентам розробляти стратегії та плани дій для забезпечення безпеки даних та мереж у різних сферах діяльності.

За студентами передбачено низку практичних занять, що поглиблюють загальний курс. Передбачається їх вчасне виконання, а в разі перевищення зазначеного часу встановлений штраф: практичні роботи захищаються на мінімально позитивну оцінку. Внаслідок виконання практичних занять за допомогою статистичних методів студент набуває такі уміння:

- Інтеграцію та керування системами автентифікації, авторизації та управління доступом;
- Інтеграцію та керування системами виявлення та протидії вторгненням;
- Інтеграцію та керування системами збереження та доступу до сертифікатів, секретів та атрибутів доступу;
- Інтеграцію та керування системами типу «honeypot»;

Мета дисципліни: Ознайомити студентів з основними принципами, технологіями та інструментами адміністрування і експлуатації інформаційно-комунікаційних систем.

Навчити студентів впроваджувати та підтримувати заходи зі збереження та забезпечення конфіденційності, цілісності та доступності інформації у комп'ютерних мережах та системах.

Розвинути вміння аналізувати та оцінювати ризики інформаційної безпеки та визначати відповідні заходи їх запобігання та виявлення.

Об'єкт дисципліни: Об'єктом дисципліни є захищені інформаційно-комунікаційні системи (ІКС). Це включає в себе різноманітні комп'ютерні мережі, сервери, бази даних, програмне забезпечення та обладнання, які використовуються для зберігання, обробки та передачі інформації.

Предмет дисципліни:

Предметом дисципліни є технології, методи та процедури адміністрування і експлуатації інформаційно-комунікаційних систем з фокусом на забезпеченні їхньої безпеки. Це включає в себе такі аспекти, як:

- Планування та розгортання захищених ІКС.
- Конфігурування та управління застосунками та інфраструктурою.
- Виявлення та відповідь на інциденти інформаційної безпеки.
- Захист від хакерських атак, вірусів, інших загроз.
- Розробка та впровадження політик і процедур забезпечення інформаційної безпеки на технічному рівні.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем» частково використовує знання та уміння, набуті під час вивчення курсів «Управління інцидентами інформаційної безпеки», «Основи технологій захисту інформації», «Безпека систем та мереж» (вони викладалися на бакалавраті спеціальності «Кібербезпека») тощо та поглиблює їх у напрямку розуміння технічних аспектів керування система забезпечення кібербезпеки.

3. Зміст навчальної дисципліни

Розділ 1. Архітектура Zero Trust

1. Огляд та принципи архітектури «нульової довіри»
2. Можливості та виклики
3. Еталонна архітектура нульової довіри
4. Багаторівнева сегментація
5. Розробка успішного плану сегментації

Розділ 2. Системи Identity Management

1. Identity та атрибути доступу
2. Встановлення довіри до identity
3. Identity в інфраструктурі: SPN, ролі, маркери, керовані ідентифікатори тощо.
4. Довгоживучі та ефемерні Identity
5. Identity-Native інфраструктура

Розділ 3. Системи автентифікації

1. Оцінка методів автентифікації
2. Системи багатофакторної автентифікації
3. Single Sign-On: federation, OpenID, SAML.
4. Identity-Native автентифікація

Розділ 4. Системи авторизації та керування доступом

1. Типи авторизації та моделі авторизації
   - Моделі RBAC, MAC, DAC
   - Прив'язка груп до ролей
   - SAML assertion
2. Системи управління привілеями
   - Системи privilege access management
   - Умовний доступ
   - Zero Standing Privilege
   - Just-in-Time Access
   - Подвійна авторизація
3. Ідентичність і нульова довіра
   - Контекстно-керований доступ
   - Identity-Aware Proxy

Розділ 5. Системи керування секретами

1. Різні типи секретів
2. Ім'я користувача та паролі
   - Токени

- Ключі API/SSH
- Сертифікати
- Ключі шифрування
- Специфічні секрети хмари
- Власні секрети
- Токени RSA/MFA
- Секрети, які не є секретами

3. Сховища секретів
   - Секрети програми
   - Секрети, пов'язані з платформою
   - Секрети в коді
   - Автоматично створені секрети
   - Vault сховища
   - Короткочасні облікові дані
4. Управління секретами
   - Різні секрети для різних середовищ
   - Управління секретами в хмарі
   - Управління таємницею локально
   - Керування секретами в конвеєрах CI/CD
5. Ін’єкції секретів
   - Секрети змінних середовища
   - Секрети з файлу
   - Впровадження секретів із конвеєра CI/CD
   - Використання Vault

Розділ 6. Технології високої продуктивності та доступності

1. Архітектури високопродуктивних програм: балансувальники навантаження, розподілення навантаження
2. Високопродуктивна архітектура даних
3. Гарантія доступності: хмари (регіони, зони)
4. Підходи до аварійного відновлення: розподіл ресурсів і доступ до них, системи резервного копіювання

4. Навчальні матеріали та ресурси

Базова література

1. Zero Trust Architecture. Cindy Green-Ortiz, Brandon Fowler, David Houck, Hank Hensel, Patrick Lloyd, Andrew McDonald, Jason Frazier. 2023. ISBN-13: 978-0-13-789973-9, ISBN-10: 0-13-789973-4
2. Solving Identity Management in Modern Applications. Yvonne Wilson, Abhishek Hingnikar. 2023. ISBN 978-1-4842-8260-1
3. Identity-Native Infrastructure Access Management. Ev Kontsevoy, Sakshyam Shah, Peter Conrad. 2023. ISBN 978-1-098-13190-6
4. High-Performance Data Architectures. Joe McKendrick, Ed Huang. O'Reilly Media, Inc. August 2023

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем» заплановані наступні види навчальних занять:

- лекційні заняття;
- практичні заняття;
- самостійна робота студентів.

На лекціях розкриваються найбільш суттєві теоретичні питання, що дозволяють забезпечити студентам можливість самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовані в логічній послідовності і цілком узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Інтернет. На заняттях використовуються звичайна дошка, а також презентації лекцій з використання мультімедіа-проектора. В дистанційному режимі використовуються засоби Zom та відповідні слайди лекцій.

Теми та порядок освоєння дисципліни «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем» наведений нижче.

№ з/п	Тема		Кількість аудиторних годин, лекції	Кількість аудиторних годин, комп'ютерний практикум	Кількість годин, СРС
1.	Архітектура Zero Trust [1]	14	4	2	8
2.	Системи Identity Management [2]	18	6	2	8
3.	Системи автентифікації [3]	20	6	4	10
4.	Системи авторизації та керування доступом [4]	36	10	6	20
5.	Системи керування секретами [5]	10	4	4	4
6.	Технології високої продуктивності та доступності [6]	14	4		10
7.	Разом	112	34	18	60
8.	Модульна контрольна робота	8	2		6

9.	Екзамен	30			30
	Всього	**150**	**36**	**18**	**96**

Теми комп'ютерного практикуму

№ з/п	**Теми практичних занять**	**Кількість аудиторних годин**
1.	Архітектура Zero Trust	2
2.	Системи Identity Management	2
3.	Системи автентифікації	4
4.	Системи авторизації та керування доступом	6
5.	Системи керування секретами	4

Політика та контроль

6. Самостійна робота здобувача

Самостійна робота здобувача складається з опанування питань лекційного матеріалу, підготовки до практичних занять, модульної контрольної роботи і екзамену.

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Контроль відвідування здійснюється викладачем систематично.

Завдання практичних занять виконуються та захищаються у відповідності до встановлених дедлайнів впродовж семестру.

Під час виконання практичних занять, а також під час контрольних заходів здобувачами повинна виконуватися політика академічної доброчесності, згідно Кодексу Честі НТУУ «КПІ».

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: виконання та захист практичних занять, МКР.

Критерії оцінювання практичних занять (макс. бал - 9):

- повне виконання вимог – 8-9 балів;
- повне виконання завдань, але є невеликі недоліки – 5-7 балів;
- часткове виконання завдань, або суттєві недоліки – 3-4 балів;
- незадовільне виконання – 0 балів.

Критерії оцінювання МКР (макс.бал - 15):

- вичерпна відповідь – 13-15 балів;
- неповна відповідь – 9-12 бали;

- частково правильна відповідь, наведено основні базові поняття для розв'язку, є помилки – 5-8 балів;
- грубі помилки – 3-4 балів;
- незадовільна відповідь – 0 балів.

Заохочувальні та штрафні бали (не більше 6 балів)

Заохочувальні бали		**Штрафні бали**	
Критерій	**Додається до семестрового рейтигу**	**Критерій**	**Віднімається від базового балу**
Активність на більшості занять	+ 5 балів	Невчасна здача практичних завдань	- 2 бали

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Контрольний захід	**Макс. бал**	**Кількість**	**Всього**
МКР	15	1	15
Практичні заняття	9	5	45
Екзамен			40
			100

Семестровий контроль: екзамен.

Екзамен є обов'язковим контрольним заходом. Рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD), менших 60 балів. На екзамені студент отримує білет, відповідь на який оцінюється по 40-бальній шкалі.

Екзамен. Умовою допуску до семестрового контролю студента є виконання усіх поточних контрольних заходів: практичних робіт, модульної контрольної роботи, а також якщо він має поточний рейтинг більший 35 балів (RD ≥ 35). Максимальна кількість балів за семестр – 60 балів. Оцінювання відповідей на екзамені:

- вичерпна відповідь - 35-40 балів;
- неповна відповідь – 11-34 бали;
- грубі помилки – 8-10 балів;
- незадовільна відповідь – 0 балів.

Таблиця переведення рейтингових балів до оцінок за університетською шкалою

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
95 ≤ RD ≤ 100	Відмінно	-
85 ≤ RD ≤ 94	Дуже добре	-
75 ≤ RD ≤ 84	Добре	-
65 ≤ RD ≤ 74	Задовільно	-
60 ≤ RD ≤ 64	Достатньо	-
RD < 60	Незадовільно	-
Невиконання умов допуску	Не допущено	-

9. Додаткова інформація з дисципліни (освітнього компонента)

Питання, що виносяться на екзамен цілком відповідають тим, що були зазначені в змісті дисципліни.

Для практичної реалізації знань і умінь, отриманих під вивчення курсу «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем», було би бажано познайомитися з програмним середовищем R як важливим інструментом статистичного моделювання.

Робочу програму навчальної дисципліни (силабус):

Склав: доцент кафедри інформаційної безпеки, к.т.н., Барановський Олексій Миколайович

Ухвалено кафедрою інформаційної безпеки (протокол № 6 від 08.06.2023 р.)

Погоджено Методичною комісією ННФТІ (протокол № 6 від 29.06.2023 р.)

Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

НН ФТІ
Кафедра інформаційної безпеки

Теорія та методи соціальної інженерії в кібербезпеці
Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Другий (освітньо-професійний)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*«Системи, технології та математичні методи кібербезпеки», «Системи технічного захисту інформації»*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*1 курс, 2 семестр*
Обсяг дисципліни	*5 кредитів ECTS , 150 год. (36 - год. лек., 18- год. лаб., СРС- 96 год.)*
Семестровий контроль/ контрольні заходи	*Екзамен, МКР*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *кандидат технічних наук, Стьопочкіна Ірина Валеріївна, telegram: @ivst1113, e-mail: irst-ipt@lll.kpi.ua* Практичні: *Ільїн Костянтин Іванович, @KosAtTin*
Розміщення курсу	Посилання на дистанційний ресурс (Платформа “Сікорський”: курс Теорія та методи соціальної інженерії в кібербезпеці https://do.ipo.kpi.ua/course/view.php?id=1713 ,

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Соціальна інженерія є одним із найуспішніших напрямків здійснення атак на об’єкти різного типу. Слабкою ланкою кожної системи захисту є людина, саме з участю людського фактору соціальний інженер досягає своєї мети. Уміння та знання, набуті в цьому курсі, можуть бути використані там, де передбачається діяльність із кіберзахисту інформації, в тому числі із використанням наукоємних технологій, на стику із методиками HR-менеджмента.

Навчальна дисципліна «Теорія та методи соціальної інженерії в кібербезпеці» розглядає теоретичні основи відповідних атак. В тому числі, розглянуто моделі атак соціальної інженерії, моделі їх виявлення, сценарії різних видів атак соціальної інженерії, ПЗ, яке використовується при цьому та способи протидії цим атакам. Ці знання дають змогу зрозуміти фактори успіху відповідних атак, та попередити їх.

Мета дисципліни – надання студенту знання щодо:

- Моделі та сценарії атак та їх виявлення;
- Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак;
- Механізми здійснення різних атак соціальної інженерії;
- Нові технології та засоби соціальної інженерії, засновані на ML та AI, в тому числі DeepFake та інші.
- Рішення кіберзахисту та підходи до попередження атак соціальної інженерії.

Також за дисципліною передбачено 5 комп'ютерних практикумів, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. Передбачається, що практикуми повинні бути здані вчасно, в разі перевищення дедлайну встановлений штраф: практикум захищається на мінімальну позитивну оцінку. Дати дедлайнів обговорюються зі студентами на першому занятті.

В результаті опанування дисципліною студент отримує додаткові знання та навички, які розширюють коло кар'єрних можливостей в сфері кібербезпеки та захисту інформації, серед них такі ***компетентності***:

- Розробляти сценарії та моделі атак соціальної інженерії та здійснювати імітаційне моделювання;
- Уміння розробляти програму тестування на проникнення із використанням різних підходів;
- Використовувати наявні програмні засоби, за допомогою яких може діяти соціальний інженер, в цілях тестування на проникнення;
- Уміння розробляти методики оцінки персоналу на чутливість до різних атак соціальної інженерії;
- Уміння розробляти елементи засобів тестування на проникнення із використанням підходів соціальної інженерії.

За курсом передбачено модульну контрольну роботу для контролю засвоєння практичного та теоретичного матеріалу.

Предметом дисципліни є моделі та методи соціальної інженерії в кібербезпеці.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

В результаті опанування дисципліною студент отримує додаткові знання та навички, які розширюють коло кар'єрних можливостей в сфері кібербезпеки та захисту інформації, серед них такі ***компетентності та програмні результати навчанняі***:

Загальні компетентності

– Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми

Фахові компетентності

– Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог

– Здатність формалізувати, будувати та використовувати у практичній діяльності моделі та методи інтелектуального аналізу даних.

Програмні результати навчання:

- Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
- Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
- Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- Після вивчення дисципліни студент володітиме знаннями щодо теоретичних моделей та методів соціальної інженерії, уміннями: застосовувати відповідні методи до виявлення атак соціальної інженерії, складати програми та методики тестування на проникнення із використанням відповідних методів.

Дисципліна не містить суттєвих взаємозв'язків із попередніми та наступними дисциплінами. Для виконання завдань необхідне володіння інформаційними технологіями загального характеру.

Результати вивчення даної дисципліни можуть бути застосовані у професійній діяльності за фахом та для написання магістерської дипломної роботи.

Зміст навчальної дисципліни

1. Поняття соціальної інженерії, приклади. Основні вихідні припущення, які гарантують успіх атаки.

2. Життєвий цикл атак соціальної інженерії різного типу. Контрзаходи.

3. Основні вектори атак соціальної інженерії. Способи протидії соціальній інженерії у організаціях та підприємствах.

4. Моделі соціальної інженерії. Моделі виявлення атак соціальної інженерії. SEADM, психологічні тригери. Суб'єктивна теорія корисності та здатність приймати раціональні рішення. Приклади.

5. Особистісні фактори, які впливають на успішність атак соціальної інженерії. Психологічний портрет жертви соціального інженера. Модель виявлення емоційного стану потенційної жертви соціального інженера.

6. Побудова сценаріїв атак та розпізнавання атак на основі автоматизованих засобів. Модель виявлення атаки

7. Автоматизовані засоби соціальної інженерії: можливості та призначення. Збір інформації про жертву та її використання. Тестування на проникнення із використанням деяких автоматизованих засобів.

8. Обхід двохфакторної автентифікації як популярний засіб соціальної інженерії. Шляхи заволодіння факторами. Підходи до автентифікації. Схеми та приклади атак. Типи зворотніх проксі та атаки з їх використанням.

9. Спам-листи як носій запитів соціальної інженерії. Архітектура поштового сервісу. Способи автоматизованої генерації спам-листів на основі машинного навчання. Обхід спам-фільтрів.

10. Налаштування спам-фільтрів. Генерація повідомлень для автоматизованого пентесту.

11. Техніки роботи спам-фільтрів. Методи підвищення роботи класифікатора спаму, виділення суттєвих ознак. Поведінкові шаблони, контентні та неконтентні ознаки.

12. Порівняльний аналіз існуючих спам-фільтрів та принципів їх роботи. Спам у вигляді посилань. Зловмисні інфраструктури переспрямувань.

13. Розпізнавання фішингових сайтів. Визначення фішингу та його сучасні різновиди. Життєвий цикл виявлення та протидії атакам фішингу. Фішинг із використанням сайтів. Виділення класифікаційних ознак фішингових сайтів. Алгоритм виявлення фішингового сайту: датасети, підготовка даних, обробка результатів. Приклад

14. Засоби генерації фейкових зображень, голосу та відео на основі технології DeepFake. Алгоритмічні, програмні основи технологій підробки. Види атак соціальної інженерії де використовується підробка голосу. Технологія клонування голосу. Проблеми розпізнавання діпфейків. Візуальні ознаки діпфейку. Споріднені задачі по виявленню фейків, зокрема виявлення фейкових профілів.

Навчальні матеріали та ресурси

Базова література.

1. *Стьопочкіна І.В. Теорія та методи соціальної інеженерії. Матеріали дистанційного курсу [Режим доступу]:* https://do.ipo.kpi.ua/course/view.php?id=1713
2. *Теорія та методи соціальної інженерії в кібербезпеці. Методичні вказівки до комп'ютерного практикуму /Стьопочкіна І.В. [Режим доступу]:* https://do.ipo.kpi.ua/course/view.php?id=1713
3. *C. Hadnagy, Social engineering: The art of human hacking. – [Режим доступу: https://www.oreilly.com/library/view/social-engineering-the/9780470639535/]*
4. *K.Mitnick, The art of deception. - [Режим доступу: https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf]*

Додаткова література.

1. *Maltego. [Електронний ресурс]. – Режим доступу: https://www.maltego.com/maltego-community/ (1)*
2. *Recon-ng. [Електронний ресурс]. – Режим доступу: https://github.com/lanmaster53/recon-ng (1)*
3. *How to use Burp-suite for penetration testing. [Електронний ресурс]. – Режим доступу: https://portswigger.net/ burp/documentation/ desktop/penetration- testing*
4. *Shodan. [Електронний ресурс]. – Режим доступу:https://developer.shodan.io/*
5. *ISO/IEC 27032 . - Режим доступу: https://www.iso.org/standard/44375.html*
6. *ISO/IEC 27004 . – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en (3)*
7. *K. Krombholz, Social Engineering Attackson the Knowledge Worker. – Режим доступу: https://www.researchgate.net/publication/262393147_Social_engineering_attacks_on_the_knowledge_worker (4)*
8. *M. Turner, J. Banas et al. The Effects of Altercasting and Counterattitudinal Behavior on Compliance: A Lost Letter Technique Investigation. – Режим доступу: https://www.researchgate.net/publication/233074668_The_Effects_of_Altercasting_and_Counterattitudinal_Behavior_on_Compliance_A_Lost_Letter_Technique_Investigation*

9. *Social Engineering Toolkit. [Електронний ресурс]. – Режим доступу: https://github.com/trustedsec/social-engineer-toolkit*
10. *Google IP address ranges for outbound mail servers.- Режим доступу: https://support.google.com/a/answer/60764*
11. *About DMARC. – Режим доступу: https://support.google.com/a/answer/2466580*
12. *Eleuther. [Електронний ресурс]. – Режим доступу: https://www.wired.com/story/ai-generate-convincing-text-anyone-use-it/*
13. *W. Fan et al. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. – Режим доступу: https://www.researchgate.net/publication/312020665_Social_Engineering_I-E_based_Model_of_Human_Weakness_for_Attack_and_Defense_Investigations*
14. *A. Bhowmick, S. Hazarika. E-Mail Spam Filtering: A Review of Techniques and Trends. – Режим доступу: https://www.researchgate.net/publication/320703241_E-Mail_Spam_Filtering_A_Review_of_Techniques_and_Trends*
15. *J.-H. Hoepman, J. Van Nieuwenhuizen, F. D. Garcia. Spam filter analysis. – Режим досmупу: https://www.researchgate.net/publication/46298891_Spam_Filter_Analysis.*
16. *Deep Insights of Deepfake Technology : A Review. – Режим доступу: https://www.researchgate.net/publication/351300442_Deep_Insights_of_Deepfake_Technology_A_Review*

Навчальний контент

2. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:

- лекції;
- комп'ютерні практикуми;
- самостійна робота.

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити аспірантам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовано у відповідності із матеріалами лекцій і повністю узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Internet. На заняттях використовуються звичайна дошка, а також презентації лекцій з використанням мультимедіа-проектора. В дистанційному режимі використовуються засоби Google Meet та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

Теми та порядок освоєння дисципліни «Теорія та методи соціальної інженерії в кібербезпеці» наведений нижче.

Для виконання комп'ютерних практикумів використовуються загальнодоступні можливості соціальних мереж, методи, надані середовищем Google.

Лекційні заняття

№ з/п	Назви тем і питань, що виноситься на заняття
1	**Вступ.** РСО, предмет та об'єкт курсу. **Тема 1.** Поняття соціальної інженерії, приклади. Основні вихідні припущення, які гарантують успіх атаки. Основна література: [1, 3]. Додаткова література: [1,2].

2	**Тема 2.** Життєвий цикл атак соціальної інженерії різного типу. Контрзаходи. Основна література: [1-4]. Додаткова література: [3-6]
3	**Тема 3.** Основні вектори атак соціальної інженерії. Способи протидії соціальній інженерії у організаціях та підприємствах. Основна література: [1-3]. Додаткова література: [7]
4	**Тема 4.** Моделі соціальної інженерії. Моделі виявлення атак соціальної інженерії. SEADM, психологічні тригери. Суб'єктивна теорія корисності та здатність приймати раціональні рішення. Приклади. Основна література: [1-3]. Додаткова література: [8]
5	**Тема 5.** Особистісні фактори, які впливають на успішність атак соціальної інженерії. Психологічний портрет жертви соціального інженера. Модель виявлення емоційного стану потенційної жертви соціального інженера. Основна література: [1,3-5]. Додаткова література: [8]
6	**Тема 6.** Побудова сценаріїв атак та розпізнавання атак на основі автоматизованих засобів. Модель виявлення атаки. Основна література: [1,2]. Додаткова література: [4-7,9]
7	**Тема 7.** Автоматизовані засоби соціальної інженерії: можливості та призначення. Збір інформації про жертву та її використання. Тестування на проникнення із використанням деяких автоматизованих засобів. Основна література: [1,2]. Додаткова література: [1-4]
8	**Тема 8.** Обхід двохфакторної автентифікації як популярний засіб соціальної інженерії. Шляхи заволодіння факторами. Підходи до автентифікації. Схеми та приклади атак. Типи зворотніх проксі та атаки з їх використанням. Основна література [1-3].
9	**Тема 9.** Спам-листи як носій запитів соціальної інженерії. Архітектура поштового сервісу. Способи автоматизованої генерації спам-листів на основі машинного навчання. Обхід спам-фільтрів. Основна література: [1,2]. Додаткова література: [10,11,15]
10	**Тема 10.** Налаштування спам-фільтрів. Генерація повідомлень для автоматизованого пентесту. Основна література: [1,2]. Додаткова література: [10,11,15]
11	**Тема 11.** Техніки роботи спам-фільтрів. Методи підвищення роботи класифікатора спаму, виділення суттєвих ознак. Поведінкові шаблони, контентні та неконтентні ознаки. Основна література: [1]. Додаткова література: [14]
12	**Тема 12.** Порівняльний аналіз існуючих спам-фільтрів та принципів їх роботи. Спам у вигляді посилань. Зловмисні інфраструктури переспрямувань. Основна література: [1]. Додаткова література: [14,15]
13	**Тема 13.** Розпізнавання фішингових сайтів. Визначення фішингу та його сучасні різновиди. Життєвий цикл виявлення та протидії атакам фішингу. Фішинг із використанням сайтів. Виділення класифікаційних ознак фішингових сайтів. Алгоритм виявлення фішингового сайту: датасети, підготовка даних, обробка результатів. Приклад. Основна література: [1,2]. Додаткова література: [5,6]
14	**Тема 14.** Засоби генерації фейкових зображень, голосу та відео на основі технології DeepFake. Алгоритмічні, програмні основи технологій підробки. Види атак соціальної інженерії де використовується підробка голосу. Технологія клонування голосу. Проблеми розпізнавання діпфейків. Візуальні ознаки діпфейку. Споріднені задачі по виявленню фейків, зокрема виявлення фейкових профілів. Основна література: [1,3]. Додаткова література: [16]

	Всього
	Модульна контрольна робота
	Екзамен
	Разом годин: 150

Теми комп'ютерних практикумів (зміст наведено у [2]).

№ КП	Теми	Кількість ауд. годин
1.	Пошук електронної адреси як основного контакту для дій соціального інженера. Одержання інформації облікових записів в Facebook	2
2.	Використання можливостей Google Dorking для пошуку інформації у відкритому доступі	4
3.	Налаштування роботи веб-ресурсу для упередження індексації деяких розділів сайту пошуковими сервісами	4
4.	Виявлення фішингових сайтів методами машинного навчання	4
5.	Сценарії пошуку інформації по цільовому об'єкту засобами відкритої розвідки	4
Всього		18

Самостійна робота студента

Самостійна робота здобувача складається із опанування та засвоєння відповідних лекційних матеріалів, підготовки до МКР та екзамену. Також здобувачі самостійно доопрацьовують результати комп'ютерних практикумів та готуються до їх захисту, допоміжні контрольні питання надано в [2].

Самостійна робота студента

№ з/п	**Вид самостійної роботи**	**Кількість годин СРС**
1.	Засвоєння теоретичних матеріалів та підготовка до комп'ютерних практикумів	56
3.	Підготовка до МКР	10
4.	Підготовка до екзамену	30
	Загалом	**96**

Політика та контроль

3. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Завдання комп'ютерних практикумів виконуються та захищаються у відповідності до встановлених дедлайнів протягом семестру.

Під час виконання комп'ютерних практикумів а також під час контрольних заходів здобувачами повинна дотримуватись політика академічної доброчесності, згідно Кодексу Честі НТУУ "КПІ".

Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: виконання та захист комп'ютерних практикумів.

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Комп'ютерні практикуми сформовані таким чином, що їх завдання сприяють одержанню практичних навичок та засвоєнню матеріалу за темами дисципліни. Комп'ютерні практикуми передбачають їх виконання та захист.

Критерії оцінювання комп.практ. (макс. бал - 8):

- повне виконання вимог – 7-8 балів;
- повне виконання завдань, але є невеликі недоліки – 5-6 балів;
- часткове виконання завдань, або суттєві недоліки – 3-4 балів;
- незадовільне виконання – 0 балів.

Критерії оцінювання МКР (макс.бал - 20):

вичерпна відповідь – 18-20 балів;

- неповна відповідь – 15-17 балів;
- частково правильна відповідь, наведено основні базові поняття, є помилки – 10-14 балів;
- грубі помилки – 8-9 балів;
- незадовільна відповідь – 0 балів.

Заохочувальні бали*:*

Заохочувальні бали	
Критерій	Ваговий бал
Активність на більшості занять	+5 балів

Семестровий контроль: екзамен. Екзамен є обов'язковим контрольним заходом. Рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 60 балів). На екзамені здобувач одержує білет, відповідь на який оцінюється по 40-бальній шкалі.

Умови допуску до семестрового контролю: мінімальна позитивна оцінка за комп.практ / семестровий рейтинг більше 35 балів.

Оцінювання відповідей на екзамені:

- вичерпна відповідь – 35-40 балів;
- вичерпна відповідь з незначними помилками – 30-34 бали;
- неповна відповідь та помилки – 20 – 29 балів;
- грубі помилки – 8-19
- незадовільна відповідь – 0 балів.

РСО

№ з/п	Контрольний захід	Макс. бал	Кіл-ть	Всього
1.	Комп.практ	8	5	40
2.	Модульна контрольна робота	20	1	20
3.	Екзамен	40	1	40
	Всього			100

Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
95 ≤ RD ≤ 100	Відмінно	-
85 ≤ RD ≤ 94	Дуже добре	-
75 ≤ RD ≤ 84	Добре	-
65 ≤ RD ≤ 74	Задовільно	-
60 ≤ RD ≤ 64	Достатньо	-
RD < 60	Незадовільно	-
Невиконання умов допуску	Не допущено	-

Додаткова інформація

Питання, що виносяться на екзамен, повністю відповідають змісту дисципліни. Необхідною умовою роботи здобувача є його реєстрація на курсі "Теорія та методи соціальної інженерії в кібербезпеці" на платформі Сікорський
https://do.ipo.kpi.ua/course/view.php?id=1713

Робочу програму навчальної дисципліни (силабус):

Склав: доц. каф. Інформаційної безпеки Стьопочкіна Ірина Валеріївна

Ухвалено кафедрою інформаційної безпеки (протокол №6/2023 від 08.06.2023).

Погоджено Методичною комісією НН ФТІ (протокол № 6/2023 від 29.06.2023).

Національний технічний університет України «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»		НН ФТІ Кафедра інформаційної безпеки

Аналіз кібернетичних загроз в інформаційно-телекомунікаційних системах із застосуванням методів машинного навчання

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*«Системи, технології та математичні методи кібербезпеки», «Системи технічного захисту інформації»*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 курс, весняний семестр*
Обсяг дисципліни	*5 кредитів ЄКТС / 150 год.:* *(36 год. – лекції, 18 год. – практичні заняття, 96 год. – СРС)*
Семестровий контроль/ контрольні заходи	*Залік, МКР, поточний контроль*
Розклад занять	*http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *к.т.н. доцент, Прогонов Дмитро Олександрович (progonov.dmytro@lll.kpi.ua)* Практичні: *к.т.н. доцент, Прогонов Дмитро Олександрович (progonov.dmytro@lll.kpi.ua)*
Розміщення курсу	Google classroom: https://classroom.google.com/c/NjE4ODkxMDE1MTUz?cjc=ccbtwcx

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Особлива увага при розробці сучасних комплексних систем захисту інформації приділяється виявленню несанкціонованої передачі інформації. Це може відбуватися за рахунок використання як технічних каналів витоку (наприклад, акустичних, електромагнітних тощо), так і шляхом модифікації даних, які циркулюють в інформаційно-комунікаційних системах. Виявлення даних сигналів ускладнюється за рахунок суттєвого зменшення їх енергії та маскування на фоні сильних завад, що обмежує використання класичних методів спектрального аналізу. Вирішення даної задачі потребує використання новітніх методів статистичного аналізу сигналів різної фізичної природи, а також розробки автоматизованих систем обробки даних для виявлення та класифікації сигналів.

Метою навчальної дисципліни є розширення у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації в інформаційно-комунікаційних системах в умовах опрацювання значних об’ємів даних.

Предметом навчальної дисципліни є методи статистичного аналізу та статистичного моделювання числових даних.

В результаті опанування дисципліною студент отримує додаткові знання та навички, які розширюють коло кар'єрних можливостей в сфері кібербезпеки та захисту інформації, серед них такі ***компетентності та програмні результати навчанняі***:

Загальні компетентності

Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми;

- Здатність застосовувати знання у практичних ситуаціях;
- Здатність до абстрактного мислення, аналізу та синтезу

Фахові компетентності:

- Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки.

Програмні результати навчання:

- Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах
- Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки
- Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки
- Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки

Пререквізити та постреквізити дисципліни

- Для успішного засвоєння дисципліни необхідні знання: основ математичного аналізу; основ теорії імовірності та математичної статистики; основ комп'ютерного моделювання систем та процесів; методів обробки багатовимірних сигналів.
- Засвоєні теоретичні знання та отримані практичні навички під час вивчення навчальної дисципліни «Захист конфіденційної інформації з використанням методів машинного навчання» можна використовувати в подальшому під час вивчення спеціальних навчальних дисциплін з інтелектуальної обробки даних та для написання магістерської дипломної роботи.

Зміст навчальної дисципліни

Розділ 1. Основи інтелектуального аналізу даних.

Тема 1.1. Термінологія та основні визначення в галузі інтелектуального аналізу даних.

Тема 1.2. Сучасні автоматизовані системи аналізу та обробки інформації.

Розділ 2. Методи статистичного моделювання сигналів.

Тема 2.1. Методологія побудови статистичних моделей сигналів.

Тема 2.2. Огляд поширених імовірнісних моделей сигналів.

Тема 2.3. Побудова статистичних моделей сигналів в умовах обмеженості або відсутності даних щодо їх статистичних характеристик.

Тема 2.4. Визначення параметрів статистичних моделей сигналів при обробці зашумлених даних

Розділ 3. Методи класифікації та кластеризації сигналів.

Тема 3.1. Основні підходи до класифікації сигналів.

Тема 3.2. Методи кластеризації сигналів.

Тема 3.3. Методи підвищення точності класифікації сигналів в умовах обробки зашумлених даних.

Тема 3.4. Методи класифікації об’єктів та систем в умовах обмеженості або відсутності апріорних даних щодо їх особливостей.

Навчальні матеріали та ресурси

Базова рекомендована література

1. Статистичні методи в інженерних дослідженнях. Навчальний посібник для здобувачів вищої освіти з інженерних спеціальностей. / *В.А. Пашинський*: – Кропивницький: ЦНТУ, 2020. – 106 с.
2. *Murphy Kevin P.* Probabilistic Machine Learning: An Introduction. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2022. – 864 p. – ISBN 978-0262046824.
3. *Murphy Kevin P.* Probabilistic Machine Learning: Advanced Topics. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2023. – 1360 p. – ISBN 978-0262048439.
4. *Charu C. Aggarwal.* Neural Networks and Deep Learning: A Textbook. – 1st edition. – Springer, 2018. – 520 p. – ISBN 978-3319944623.

Допоміжна рекомендована література

1. *Goodfellow I., Bengio Y. and Courville A.* Deep Learning. – Adaptive Computation and Machine Learning series. – The MIT Press, 2016. – 800 p. – ISBN 978-0262035613.
2. *Mallat S.* A Wavelet Tour of Signal Processing, Third Edition: The Sparse Way. – 3rd edition. – Academic Press, 2008. – 832 p. – ISBN 978-0123743701.
3. *Bishop Christopher M.* Pattern Recognition and Machine Learning. – Information Science and Statistics series. – Springer, 2016. – 758 p. – ISBN 978-1493938438.
4. *Bishop Christopher M.* Neural Networks for Pattern Recognition. – Advanced Texts in Econometrics series. – 1st edition. – Clarendon Press, 1996. – 504 p. – ISBN 978-0198538646.
5. *Raschka S.* Python Machine Learning. – Packt Publishing, 2015. – 454 p. – ISBN 978-1783555130.

Навчальний контент

2. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студента для засвоєння студентами матеріалу та розвитку у них практичних навичок. Для проведення занять застосовується практичний метод. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання. Для проведення практичних робіт використовується частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами типові задачі в галузі статистичного аналізу та теорії розпізнавання образів та пропонує рекомендовані шляхи вирішення даних задач.

Рекомендоване інформаційно-програмне забезпечення для виконання практичних робіт за курсом:

JetBrain Pycharm 2023.1.4 Community Edition (Free Educational License), Python 3.8 (відкрита мова програмування)

Дистанційна форма навчання: Google Classroom, платформа для проведення онлайн-зустрічей Zoom / Google Meet, електронна пошта, канали Telegram.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1.	Тема 1.1. Термінологія та основні визначення в галузі інтелектуального аналізу даних Основні питання: - поняття класифікації та кластеризації даних - основні підходи до побудови статистичних моделей - основи узагальненого спектрального аналізу даних - основи теорії імовірності та математичної статистики
2.	Тема 1.2. Сучасні автоматизовані системи аналізу та обробки інформації Основні питання: - інтелектуальні системи аналізу даних (Google, Bing) - системи підтримки прийняття рішень - великі лінгвістичні моделі (ChatGPT, Bard, HuggingChat)
	Тема 2.1. Методологія побудови статистичних моделей сигналів - байесовий підхід до побудови статистичних моделей - частотний підхід до побудови моделей
	Тема 2.2. Огляд поширених імовірнісних моделей сигналів - моделі гаусової суміші - узагальнені лінійні моделі
	Тема 2.3. Побудова статистичних моделей сигналів в умовах обмеженості або відсутності даних щодо їх статистичних характеристик - моделі на основі графів - приховані лінійні моделі - марківські моделі
	Тема 2.4. Визначення параметрів статистичних моделей сигналів при обробці зашумлених даних - моделі суміші сигналів - розріджені лінійні моделі
	Тема 3.1. Основні підходи до класифікації сигналів - лінійна та робастна регресія

№ з/п	Назва теми лекції та перелік основних питань
	- логістична регресія - метод опорних векторів
	Тема 3.2. Методи кластеризації сигналів - метод k-середніх - методи ієрархічної кластеризації - штучна нейронна мережа Кохонена - метод DBSCAN
	Тема 3.3. Методи підвищення точності класифікації сигналів в умовах обробки зашумлених даних - ансамблеві моделі - класифікація даних з використанням штучних нейронних мереж
	Тема 3.4. Методи класифікації об’єктів та систем в умовах обмеженості або відсутності апріорних даних щодо їх особливостей - спеціальні типи штучних нейронних мереж (автоенкодери, трансформери тощо) - поняття та принципи побудови фільтрів Калмана

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1.	Моделювання багатовимірних сигналів з використанням поширених статистичних моделей
2.	Методи класифікації багатовимірних сигналів
3.	Методи кластеризації багатовимірних сигналів

Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Самостійна робота студента (відповідно до робочого плану)

№ з/п	**Вид самостійної роботи**	**Кількість годин СРС**
1.	Підготовка до практичних занять	46
2.	Підготовка до МКР	20
3.	Підготовка до екзамену	30
	Загалом	**96**

Політика та контроль

3. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, що розвивають практичні уміння та навички.

Правила захисту практичних завдань

Виконання практичних робіт за курсом є обов'язковим. Захист практичної роботи проводиться в два етапи:

- Опитування за теоретичними питаннями, що розглядаються в практичній роботі;
- Представлення та пояснення отриманих результатів практичної роботи.

Правила призначення заохочувальних балів

- Публікація студентом матеріалів за темою курсу у матеріалах всеукраїнських та міжнародних конференцій (при представлені бібліографічного опису публікації) – 5 балів;
- Публікація студентом матеріалів за темою курсу у фахових рецензованих періодичних виданнях (при представлені бібліографічного опису публікації) – 10 балів.

Пропущені контрольні заходи

Результат самостійної або модульної контрольної роботи для студента, який не з'явився на контрольний захід без поважної причини, є нульовим. Студент має можливість написати контрольний захід, але максимальний бал за нього буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

Пропущений екзамен не зараховується; у такому випадку студент отримує запис у відомості «не з'явився» та повинен складати екзамен на додатковій сесії.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: на початку кожного лекційного заняття проводиться експрес-опитування студентів за темою попередньої лекції (окрім першої лекції за курсом). У випадку повної та розгорнутої відповіді ставиться 2 бали, у випадку часткової (неповної) відповіді ставиться 1 бал, у всіх інших випадках ставиться 0 балів (макс.6 балів)
Критерії оцінювання МКР (макс.бал - 24):

- вичерпна відповідь – 22-24 балів;
- неповна відповідь – 18-21 бал;
- частково правильна відповідь, наведено основні базові поняття для розв'язку, є помилки – 12-17 балів;
- грубі помилки – 8-11 балів;
- незадовільна відповідь – 0 балів.

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Додаткові (бонусні) бали

Рейтинговою системою оцінювання передбачені додаткові бали за виконання додаткових завдань. Один студент не може отримати більше ніж 10 бонусних балів у семестрі. В якості додаткових завдань студентам пропонується підготовка реферату за запропонованим викладачем переліком тем.

Семестровий контроль: екзамен

Семестрова атестація (екзамен) проводиться зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску є:

- семестровий рейтинг RD ≥ 36;
- виконання та захист 3 практичних робіт.

На екзамені здобувач одержує білет з питаннями, відповіді на які оцінюється по 40-бальній шкалі за такими критеріями:

- повна відповідь (не менше 90% потрібної інформації), 35 - 40 балів;
- достатньо повна відповідь (не менше 75% потрібної інформації), 30 -34 балів;
- неповна відповідь (не менше 60% потрібної інформації), 20 – 29 балів;
- незадовільна відповідь – до 20 балів.

Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:

№ з/п	Контрольний захід	Макс бал	Кіл-ть	Всього
1.	Виконання та захист пакету з 3 практичних робіт	12	3	36
2.	Написання модульної контрольної роботи	24	1	24
3.	Екзамен	40	1	40
	Всього			100

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено доцент кафедри ІБ, к.т.н., доцент Прогонов Дмитро Олександрович

Ухвалено кафедрою інформаційної безпеки НН ФТІ (протокол № 6/2023 від 08.06.2023р.)

Погоджено Методичною комісією НН ФТІ (протокол № 6/2023 від 29.06.2023р.)

Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

НН ФТІ
Кафедра інформаційної безпеки

Рішення в умовах невизначеності та ризику

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*«Системи, технології та математичні методи кібербезпеки»*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 курс, весняний семестр*
Обсяг дисципліни	*120 год, 4 кред ECTS (36 лекцій, 18 лаб., 66 годин самостійна робота студентів)*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
Розклад занять	*http://roz.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доцент кафедри інформаційної безпеки, кандидат фізико-математичних наук, с.н.с. Смирнов Сергій Анатолійович, контактні дані e-mail: s.smirnov@kpi.ua* Практичні: *проводить лектор*
Розміщення курсу	*https://classroom.google.com/c/OTk3MTgyNzQzNDNa*

2. Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Навчальна дисципліна «Рішення в умовах невизначеності та ризику» є вибірковою дисципліною і присвячена формуванню у студентів здатності розуміти та застосовувати спеціальні поняття, означення, постановки задач та методи їх розв’язання, що необхідні для успішної професійної діяльності за фахом, засвоєння найважливіших професійно корисних результатів теорій та практики прийняття рішень.

Завдання навчальної дисципліни — навчити студентів використовувати методи і прийоми моделювання проблемних ситуацій, аналізувати отримані моделі, передбачати загрози та вразливості, пов'язані з структурою та наповненням моделей, а також з наявними варіантами доступності інформації про них. Вибір стратегій захисту інформації, стратегій убезпечення систем керування тісно пов’язані з прийняттям рішень. Моделі ситуацій прийняття рішень, з урахуванням найрізноманітніших ускладнень, моделі вибору критеріїв та методи вибору найкращих альтернатив, в сучасних умовах є найбільш цінною частиною засобів підтримки прийняття рішень на основі (в тому числі) великих даних.

Мета дисципліни: навчити студентів моделюванню, аналізу та плануванню процедур прийняття ефективних рішень з врахуванням умов невизначеності та факторов ризику.

Об'єкт дисципліни: підтримка прийняття рішень у складних ситуаціях.

Предмет дисципліни: моделі та процедури прийняття рішень при невизначеності та ризиках.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

Загальні компетентності

ЗК 2 – Здатність проводити дослідження на відповідному рівні.

ЗК 3 - Здатність до абстрактного мислення, аналізу та синтезу.

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

Фахові компетентності

ФК 1 – Здатність обґрунтовано застосовувати, інтегрувати, розробляти та вдосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки.

ФК 5 – Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

ПРН 2 – Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН 4 – Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки

ПРН 5 - Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН 16 - 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.

ПРН 21 - Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН 22 - Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна «Рішення в умовах невизначеності та ризику» спирається на знання з обов'язкових дисциплін 1 семестру «Математичне моделювання систем і процесів» і «Аналіз

кіберінцидентів методами машинного навчання», частково використовує знання та вміння, набуті під час навчання по бакалаврських програмах спеціальності 125 «Кібербезпека», а саме: з алгоритмів та структур даних, математичного аналізу, дискретної математики, теорії ймовірностей, математичної статистики та випадкових процесів, поглиблює їх у напрямку аналізу та математичного моделювання ситуацій прийняття рішень.

Результати вивчення даної дисципліни можуть бути корисними для підготовки студентів другого (магістерського) рівня вищої освіти при вивченні курсів «Моделювання складних систем», «Стохастичне моделювання систем забезпечення безпеки», «Технології створення систем захисту інформаційно-комунікаційних систем», написання ними магістерських дисертацій та у професійній діяльності за фахом.

3. Зміст навчальної дисципліни

Розділ 1. Постановки задач прийняття рішень, критерії, фактори невизначеності та ризику.

Тема 1.1. Задачі прийняття рішень (ПР) в кібербезпеці. Формальна структура ПР в умовах невизначеності. Моделювання ризику. Геометрична інтерпретація ПР. Класичні критерії ПР: MM, BL, S, GMM, умови застосовності.

Тема 1.2. Узагальнення допустимих альтернатив: змішані стратегії в теорії рішень та ковзні режими в оптимальному управлінні.

Тема 1.3. Похідні критерії ПР: HW, HL, G; складові критерії Мушика BL(MM), BL(S); умови застосовності. Графічне дослідження критеріїв ПР, зв'язок між критеріями, геометрична оптимізація.

Розділ 2. Аналіз ситуації ПР, уточнення та спрощення моделей ситуацій ПР.

Тема 2.1. Кількісні характеристики ситуації ПР, змінні, види завдання параметрів. Дані спостережень і повторні реалізації рішення.

Тема 2.2. Абсолютна і відносна релевантність, ентропія і значимость незалежного параметра. Диференціальна ентропія. Апроксимація ентропії розбиття. Принцип максимальної ентропії.

Тема 2.3. Ранжування незалежних параметрів за значимостью, вибір інтервалів дискретизації. Дискретизація параметру по функції розподілу.

Тема 2.4. Спрощення моделі СПР: метод Ханселя та його модифікації. Призначення рівнів факторів при плануванні експерименту.

Розділ 3. Емпірико-прогностичні ситуації прийняття рішень.

Тема 3.1. Ситуації та завдання ПР: помилка оцінювання, розмір емпіричної і апостеріорної вибірок, міра ризику, критерії. Інтервальні оцінки. Схема Бернуллі і розподіл Бернуллі. Бернулізація.

Тема 3.2. Емпірична ситуація ПР, прогностична ситуація ПР, загальна емпірико-прогностична ситуація ПР. Гарантований підхід: редукція до спеціальної задачі лінійного програмування.

Тема 3.3. Розв'язання допоміжної задачі ЛП, геометрична інтерпретація і процедура.

Розділ 4. Загальні ситуації ПР з невизначеностями та ризиками: моделі та рішення.

Тема 4.1. Довірчі фактори в емпірико-прогностичних ситуаціях — критерії та процедури.
Тема 4.2. Гнучкий критерій ПР: постановка задачи та побудова критерію.
Тема 4.3. Багатокритеріальна оптимізація з інтервальними оцінками вагових коефіцієнтів.

1. 4. Навчальні матеріали та ресурси

Базова література

*1. **Смирнов С.А.** Матеріали лекцій дистанційного курсу "Рішення в умовах невизначеності та ризику" (Платформа дистанційного навчання "Сікорський": https://classroom.google.com/c/OTk3MTgyNzQzNDNa).*

2. Файнзільберг Л.С., Жуковська О.А., Якимчук В.С. Теорія прийняття рішень. Підручник. Нац. Техн. ун-т України «Київ. політехнічний інститут ім. Ігоря Сікорського». – Київ: Освіта України, 2018. - 246 с. https://ela.kpi.ua/handle/123456789/22849

3. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. – К. : Нац. акад. СБУ, 2015. – 248 с. https://drive.google.com/file/d/1YyY2JE6SmFPpEEdWBB9MZZR4sPFqXNqn/view

4. Волошин О.Ф., Мащенко С.О. Теорія прийняття рішень. –К.: Київ. Університет. –2010. - 336 с. http://www.csc.univ.kiev.ua/uk/library/books/voloshyn-20.pdf

*5. **S. A. Smirnov**, O. O. Glushchenko, K. A. Ilchuk, I. L. Makeenko. Assignments of factors levels for design of experiments with resource constraints // Continious and Distributed Systems. Theory and Applications. Ser. Solid Mechanics and Its Applications. Vol. 211. Springer. 2014. P. 81-86. https://doi.org/10.1007/978-3-319-03146-0_6*

Додаткова література

6. Muschick E., Muller P. Metody prinyatiya tehnicheskih resheniy. - Mir, 1990. 208 p. ISBN 5030012842. https://drive.google.com/file/d/1lCCi6ktB1jlxHIILoxBClOqCRW0iWqpz/view?usp=drive_link

7. Качинський А. Б. Безпека складних систем. – К. : Видавництво "Юстон", 2017. – 498 с.

(НТБ КПІ імені Ігоря Сікорського, Книгосховище, В чит. залі, примірник 519.876 К30) https://drive.google.com/file/d/12TZphJAYs8n_2lchjBvNrvIszt-LhOa3/view?usp=sharing

8. M. Rausand, S. Haugen. Risk Assessment: Theory, Methods, and Applications, 2nd Edition. - John Wiley & Sons, Inc., 2020. - 771 p. ISBN: 978-1-119-37722-1. https://drive.google.com/file/d/14OYUk7ekxpl4Z7G65chYV8yzEFyMVrLq/view?usp=drive_link

3. Навчальний контент

- **5. Методика опанування навчальної дисципліни (освітнього компонента)**

В рамках дисципліни «Рішення в умовах невизначеності та ризику» заплановані наступні види навчальних занять: *лекційні заняття; лабораторні заняття; самостійна робота студентів*.

Навчання здійснюється на основі гуманного підходу та стратегії активної взаємодії викладача та здобувача для засвоєння студентами матеріалу та розвитку у них практичних навичок. Для лекційних занять використовуються пояснювально-ілюстративний метод та підхід проблемного навчання, для проведення практичних занять використовується інтуїтивно-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами задачу, і вони розв'язують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, знаходячи для цього необхідні дані, методи, підходи тощо.

На лекціях розкриваються найбільш суттєві теоретичні питання, що дозволяють забезпечити студентам можливість самостійного вивчення всього матеріалу курсу. Показуються методи розв'язання типових задач за курсом (в тому числі тих, що входять до складу МКР). Теми та порядок самостійної роботи сформовані в логічній послідовності і цілком узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та матеріалах з глобальної мережі Інтернет. На заняттях використовуються звичайна дошка, а також презентації лекцій з використання мультимедіа-проектора. В дистанційному режимі використовуються засоби *Google Classroom* та платформа для проведення онлайн-зустрічей *Zoom*, електронна пошта, канали *Telegram,* забезпечується доступ до лекційних занять онлайн та до відеозаписів лекцій.

Лекційні заняття

№ з/п	Тема
1.	Прийняття рішень в задачах кібербезпеки. Системна постановка задачі прийняття рішень (ЗПР). Види невизначеності і класифікація ЗПР. Матриця рішень, оціночна функція, ризик. Оптимістична, нейтральна, песимістична позиція. Відносний песимізм. [1, 2, 3, 4]
2.	Геометрична інтерпретація ПР. УТ і АУТ, поле корисності рішення. Конус переваги і антиконус, області невизначеності. Лінія рівня і функції переваги. Опуклість і увігнутість. Їх зв'язок з характеристикою позиції. [1, 2, 4]
3.	Класичні критерії ПР: MM, BL, S, GMM, умови застосовності. Матричні ігри, змішані стратегії, ідея поповнення [1, 2, 4]
4.	Ковзні режими в оптимальному управлінні, приклад. Мінімізуючи послідовності, «слабка» межа. Замикання, опукле замикання. Реалізація ковзання, апроксимація. [1, 4]
5.	Похідні критерії ПР: HW, HL, G, умови застосовності. Моделі ризику. Складові критерії Мушика: BL (MM), BL (S), умови застосовності. [1, 2, 3, 4]
6.	Графічне дослідження критеріїв ПР. Зв'язок між критеріями ПР. Геометрична оптимізація для MM, G, BL, S. Напрямні та лінії рівня, конуси. Геометрична оптимізація для G, BL, HL, HW, BL (MM). [1, 4]
7.	Кількісні характеристики ситуації ПР. Незалежні і обрані змінні. Невідомі параметри. Релевантність, ентропія та значимость незалежного параметра. [1, 3]
8.	Диференціальна ентропія. Апроксимація ентропії розбиття. Принцип максимальної ентропії. Дискретизація рівномірна та за ймовірністю. [1, 4, 5]
9.	Дискретизація задачи ПР, її спрощення: метод Ханселя та його модифікації. Призначення рівнів факторів при плануванні експерименту. [1, 4, 5].
10.	Опис ситуації ПР, постановка завдання ПР: допустима помилка оцінювання, розмір емпіричної і прогностичної вибірок, критерії. [1, 6]
11.	Інтервальні оцінки невідомих параметрів. Схема Бернуллі і розподіл Бернуллі. Бернулізація задачи. [1, 6]

12.	Емпірична та прогностична ситуації ПР, гарантований підхід, редукція до задачі лінійного програмування. [1, 6]
13.	Емпірико-прогностична ситуація ПР, гарантований підхід, редукція до задачі лінійного програмування. [1, 6]
14.	Геометрія та рішення допоміжної задачі лінійного програмування. [1, 6]
15.	Довірчі фактори в емпірико-прогностичних ситуаціях ПР. [1, 4, 6]
16.	Гнучкий критерій ПР: постановка задачи та побудова критерію. [1, 4, 6]
17.	Багатокритеріальна оптимізація з інтервальними оцінками вагових коефіцієнтів. Когнітивна карта курсу. [1, 5]

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1.	Матриця рішень, класичні критерії в умовах невизначеності, геометрична інтерпретація
2.	Похідні критерії, геометрична оптимізація критеріїв.
3.	Оцінки ризику, складові критерії Мушика
4.	Оцінки релевантності, ентропії та значимості незалежних параметрів ситуації ПР.
5.	Дискретизація задачі: розподіл ресурсу по параметрах відповідно їх значимості
6.	Бернулізація, побудова інтервальнихі оцінок параметрів за допустимою похибкою
7.	Спеціальні задачі лінійного програмування
8.	Емпірико-прогностичні задачі ПР
9.	Довірчі фактори та задачи ПР з гнучким критерієм

4. Політика та контроль

1. 6. Самостійна робота студента

5. Самостійна робота здобувача складається з опанування питань лекційного матеріалу, підготовки до практичних занять, подготовка до МКР. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал, провести розрахунки за завданнями, отриманими на попередньому занятті, розв’язати та оформити відповідні задачі. Також в СРС міститься підготовка до модульної контрольної роботи (розбір типових задач). Розподіл часу по видах СРС:

№ з/п	Вид самостійної роботи	Кількість годин СРС
1.	Підготовка до лекційних занять	30
2.	Підготовка до лабор. занять	18
3.	Підготовка до МКР	12
4.	Підготовка до заліку	6
	Загалом	66

2. 7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Контроль відвідування здійснюється викладачем на кожному занятті. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно. У будь-якому випадку студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання практичних завдань та контрольних робіт.

Результат модульної контрольної роботи для студента, який не з'явився на контрольний захід, є нульовим. Студент має можливість написати контрольний захід пізніше, але максимальний бал за нього буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: *https://kpi.ua/code*.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: *https://kpi.ua/code*.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

3. 8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль виконання завдань та відповіді на практичних заняттях, тестові питання на кожному лекційному занятті (реалізовано в Гуглкласі курсу), МКР.

Практичні заняття розроблені таким чином, що їх завдання сприяють засвоєнню матеріалу за темами дисципліни «Рішення в умовах невизначеності та ризику» та формуванню практичних знань і навичок.

Студенти можуть отримати додаткові бали за виконання додаткових завдань. Один студент не може отримати більше ніж 10 бонусних балів. Штрафні бали не застосовуються.

Критерії оцінювання для МКР:

Робота складається з теста (відкритого) по теоретичних питаннях (10 питань по 3 бали за кожне) та задач. Студентам для розв'язання пропонується шість задач, кожна оцінюється з п'яти балів на основі наступної шкали:

- 5 балів – повний правильний розв'язок, >95% інформації наведено;
- 4 бали за кожну задачу – правильний розв'язок, 80% інформації наведено;
- 3 бали – завдання виконано на 60% або правильний розв'язок з арифметичними помилками;
- 2 бали – наведено 40% розв'язку, розв'язок неповний, помилки змістовні;
- 1 бал - наведено 20% розв'язку, розв'язок фрагментарний;

- 0 балів - наведено менше 20% розв’язку, або розв’язок відсутній;
- списані (ідентичні) розв’язки не зараховуються.

Календарний контроль (атестація)
проводиться двічі на семестр як моніторинг поточного плану виконання вимог силлабусу, базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Семестровий контроль: залік.
Залік є обов’язковим контрольним заходом, його оцінка формується як рейтингова оцінка роботи за семестр і складається з результатів роботи в семестрі (RD) (в рамках 100 балів).
Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:

№ з/п	Контрольний захід	Макс бал	Кіл-ть	Всього
1.	ЛР	5	8	40
2.	Модульна контрольна робота	60	1	60
	Всього			100

Для здобувачів, набравших у семестрі менше 60 балів допускається підвищення семестрового балу у спосіб проведення додаткової співбесіди по матеріалах курсу, але не більше ніж на 20 балів.

Таблиця переведення рейтингових балів до оцінок за університетською шкалою

Рейтингові бали, RD	**Оцінка за університетською шкалою**
95 ≤ RD ≤ 100	Відмінно
85 ≤ RD ≤ 94	Дуже добре
75 ≤ RD ≤ 84	Добре
65 ≤ RD ≤ 74	Задовільно
60 ≤ RD ≤ 64	Достатньо
RD < 60	Незадовільно
Невиконання умов допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено доцент кафедри інформаційної безпеки, к.ф.-м.н.,

с.н.с., Смирнов Сергій Анатолійович

Ухвалено кафедрою ІБ (протокол № 6/2023 від 08.06.2023р.)

Погоджено Методичною комісією НН ФТІ (протокол № 6/2023 від 29.06.2023р.)