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

Кафедра інженерії програмного забезпечення в енергетиці (ІПЗЕ)

Методи і засоби протидії злоякісному програмному забезпеченню

Робоча програма навчальної дисципліни

(Силабус)

Реквізитинавчальної дисципліни

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці*
Статус дисципліни	*вибіркова*
Форма навчання	*Очна(денна)*
Рік підготовки, семестр	*1 курс весняний семестр*
Обсяг дисципліни	4кредити, 120 годин, з яких 54 години аудиторних (36 год лекції, 18 год лабораторні), 66 години становить самостійна робота
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	http://rozklad.kpi.ua/
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: д.т.н., *професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85* Лабораторні заняття: д.т.н., *професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85*
Розміщення курсу	*Googleclassroom, Zoom, еКампус, Телеграмм*

Програманавчальної дисципліни

1. Описнавчальної дисципліни, її мета, предмет вивчання та результати навчання

Захист інформації та кібербезпека як такі й їх похідні, що формують окремі важливим напрями діяльності спеціалістів ІТ. Вивчення дисципліни «Методи і засоби протидії злоякісному програмному забезпеченню» присвячене різним підходам захисту комп'ютерних програм і інформації від несанкціонованого впливу, внесенню змін, зникненню, крадіжкам.

Метою навчальної дисципліни є формування у студентів здатностей до використання законодавства України, організаційних, технічних, алгоритмічних та інших методів і засобів захисту програм і даних, законодавства і стандартів у цій області, сучасних криптосистем;

здатність їх застосовувати у професійній діяльності для підтримки безпеки програм і даних об'єктів професійної діяльності.

Завдання. Основними завданнями вивчення дисципліни " є отримання магістром компетенцій для того, щоб приймати участь у проектуванні інформаційних систем, розглянуті загальні питання криптоаналізу, зокрема типи криптоаналізу з точки зору інформації, яку має криптоаналітик; надана класифікація шифросистем стосовно захищеності (стійкості до криптоаналізу). Наведені приклади зламування шифросистем. Значна увага приділяється електронному цифровому підпису, який підтверджує дійсність і цілісність документа та засвідчує авторство, реалізації дискретних структур різних типів, створення складних процедур обробки. В результаті вивчення дисципліни у студентів повинні сформуватися наступні компетентності:

В результаті вивчення дисципліни у студентів повинні сформуватися наступні компетентності:

загальні:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК1),
- Здатність спілкуватися іноземною мовою як усно, так і письмово (ЗК2),
- Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань/видів економічної діяльності) (ЗК4).

фахові:

- Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення (ФК5);
- Здатність проектувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів (ФК3);
- Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах (ФК7);

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні результати навчання:

- визначати вимоги політики безпеки та формувати свій профіль захисту відповідно до забезпечення послуг безпеки в інформаційній системі (ПРН1);
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в інформаційній системі (ПРН3);
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації (ПРН5);
- аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники інформаційних систем в цілому(ПРН7);
- проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту ПЗ, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів (ПРН7);
- забезпечувати захист програмного забезпечення від несанкціонованих дій (ПРН12).

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

Пререквізити дисципліни. Знання та вміння, отримані при вивченні дисциплін: «Комп'ютерна дискретна математика», «Алгоритмізація та програмування», «Операційні системи», «Об'єктно-орієнтований аналіз та конструювання програмних систем», «Захист комп'ютерних програм».

***Постреквізити дисципліни*.** Отримані знання при вивченні дисципліни «Комп'ютерне моделювання та оптимізація» формує базові знання для вивчення дисциплін, пов'язаних з моделюванням, чисельним розв'язком обчислювальних задач, оптимізації та розробки програмного забезпечення для систем захисту у бездротових, мобільних та хмарних системах накопичення, зберіганні і передавання інформації.

3. Зміст навчальної дисципліни

Зміст навчальної дисципліни

Розділ 1. Модель безпеки програмного забезпечення.

В ході вивчення дисципліни магістр розгляне основні аспекти захисту програмного забезпечення (ПЗ) і даних, що циркулюють в інфокомунікаційних системах. На початку вивчення дисципліни будуть розглянуті основні історичні аспекти захисту ПЗ. Буде вивчена Базова модель безпеки інформації в програмах і даних. Основним аспектом стане вивчення і відпрацювання підходів забезпечення безпеки мережевої інфраструктури, безпекизберігання даних в ОС Microsoft, Linux. Також ми згадаємо порядок функціонування центру забезпечення безпеки Windows Security Center, центру забезпечення безпеки Windows Defender, Microsoft Baseline Security Analyzer і XSpider та сканеру безпеки XSpider. Коротко розглянемо мережеві антивірусні програмні засоби захисту ПЗ.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

Для забезпечення захисту програм і даних використовується широкий арсенал криптосистем. Буде вивчено Блокові шифри як основа сучасних криптосистем, Криптосистема DES(Data Encryption Standard), 3DES, AES, SHA128, SHA128 та сучасні симетричні криптосистеми, в тому числі і на інших принципах.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключем.

На основі вивчення Моделей асиметричної системи будуть розглянуті протоколи розподілення ключів на основі центрів довіри, протоколи асиметричного шифрування. Основою стане Криптосистема RSA та цифровий підпис. Програмна реалізація цифрового підпису засобами .NET та криптографічні дайджести та Геш-функції. Крім того будуть розглянуті підходи, програмні засоби блокчейн.

Заплановані види навчальної діяльності та методи навчання

Планується проведення навчальних занять у виді лекцій та лабораторних занять. Основний змістовний матеріал дисципліни викладається на лекціях. Лабораторні заняття проводяться з метою закріплення знань з основних тем дисципліни; формування у студентів навичок і вмінь з використання технологій захисту інформації Web-рисурсів.

4. Навчальні матеріали та ресурси

McNab C. NetworkSecurityAssessment : KnowYourNetwork, secondedition. – ISBN-10:0-596-51030-6.

HTML5 SecurityCheatsheet [Електронний ресурс]. – Режим доступу: https://html5sec.org.

AndrewHoffman .WebApplicationSecurity: ExploitationandountermeasuresforModernWebApplications, - :,2021.—336c.

Heiderich M., Nava E., Heyes G., Lindsay D. WebApplicationObfuscation. – ISBN-10: 1597496049.

OWASP Foundation. OWASP TestingGuide v4.0 [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Web_Application_Penetration_ Testing.

Ristic I. Bulletproof SSL and TLS: Understandinganddeploying SSL/TLS and PKI tosecureserversandWebapplications. – ISBN-10: 1907117040.

Stuttard D., Pinto M. TheWebApplicaionHackers'sHandbook: FindingandExploitingSecurityFlaws. – ISBN-10: 1118026470.

Zalewski M. TheTangledWeb: A GuidetoSecuringModernWebApplications. – ISBN-10: 1593273886.

Інформаційна стійкість комп’ютерних технологій і мереж : навч. посіб. / А. В. Луговой, О. Г. Славко, П. П. Костенко, М. І. Гученко, М. М. Гузій. – Кременчук : Вид-во ПП Щербатих О. В., 2015. – 350 с.

Лисиченко М. Л. Методичні рекомендації щодо механізму перевірки письмових робіт на плагіат / М. Л. Лисиченко, В. І. Жила, А. В.Левкін. – Х.: ХНТУСГ, 2017. – 28 с.

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

Зміст навчальної дисципліни

Розділ 1. Базова модель безпеки інформації.

Тема 1.1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Лекція 1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Вступ до курсу лекцій. Основні поняття та визначення. Правові аспекти захисту інформації. Властивості інформації з точки зору її захисту. Рівні формування режиму інформаційної безпеки.

Тема 1.2. Базова модель безпеки інформації.

Лекція 2. Базова модель безпеки інформації.

Шляхи витоку інформації і несанкціонованого доступу в інформаційних системах. Архітектура систем безпеки програм та даних.

Тема 1.3. Безпека мережевої інфраструктури.

Лекція 3. Безпека мережевої інфраструктури.

Основні механізми розгортання ОС, які застосовуються для ОС Microsoft: метод дублювання дисків з використанням утиліти Sysprep та метод віддаленої установки з використанням сервера віддаленої установки (RIS).

Тема 1.4. Безпека зберігання даних в ОС Microsoft.

Лекція 4. Безпека зберігання даних в ОС Microsoft.

Безпека зберігання даних в ОС Microsoft. Технологія тіньового копіювання даних. Архівація даних. Створення відмовостійких томів для зберігання даних. Робота з томами RAID.

Тема 1.5. Центр забезпечення безпеки Windows Security Center.

Лекція 5. Центр забезпечення безпеки Windows Security Center

Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows. Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки Internet Explorer. Створення виключення для програми. Створення виключення для порту.

Тема 1.6. Центр забезпечення безпеки Windows Defender.

Лекція 6. Центр забезпечення безпеки Windows Defender.

Windows Defender. Захист від шкідливого програмного забезпечення. Технологія безпеки, що захищає комп'ютер від програм-шпигунів і інших видів небажаних програм. Установка Windows Defender, вимоги до системи. Налаштування Windows Defender. Автоматична перевірка (Automatic scanning). Дії за умовчанням (Default actions). Параметри захисту в режимі реального часу (Real-time protection options). Виявлення підозрілих дій. Робота з карантином. Використання Провідника програмного забезпечення (Software Explorer).

Тема 1.7. Microsoft Baseline Security Analyzer і XSpider.

Лекція 7. Microsoft Baseline Security Analyzer і XSpider.

Системи аналізу захищеності корпоративної мережі (виявлення уразливостей). Принципи роботи систем аналізу захищеності. Вибір комп'ютера і опцій сканування в програмі MBSA. Опис перевірок, виконуваних MBSA.

Тема 1.8. Сканер безпеки XSpider.

Лекція 8. Сканер безпеки XSpider.

Можливості програми: повна ідентифікація сервісів на випадкових портах; евристичний метод визначення типів і імен серверів (HTTP, FTP, SMTP, POP3, DNS, SSH) незалежно від їх відповіді на стандартні запити; обробка RPC-сервисов з їх повною ідентифікацією; проведення перевірок на нестандартні DoS-атаки.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 2.1. Блокові шифри як основа сучасних криптосистем.

Лекція 9. Блокові шифри.

Блокові алгоритми і режими шифрування. Режим електронної кодової книги. Режим зціплення блоків по криптотексту.

Лекція 10. Блокові шифри.

Режим зціплення блоків по криптотексту. Режим з оберненим зв'язком по виходу. Режим з лічильником. Схема Фейстеля.

Тема 2.2. Криптосистема DES (Data Encryption Standard).

Лекція 10. Data Encryption Standard.

Загальна характеристика DES. Алгоритм шифрування/розшифрування DES. Структура функції шифрування. Криптографічна стійкість DES. Криптосистеми DESX, 3DES. DES і шифрована файлова система EFS. Програмна реалізація симетричних криптографічних алгоритмів DES і 3DES засобами .NET.

Тема 2.3. Сучасні симетричні криптосистеми.

Лекція 11. Сучасні симетричні криптосистеми

Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (Advanced Encryption Standard). Загальноєвропейський стандарт шифрування IDEA (International Data Encryption Algorithm). Програмна реалізація симетричних криптографічних алгоритмів AES засобами .NET.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключем

Тема 3.1. Модель асиметричної системи.

Лекція 12. Модель асиметричної системи.

Передумови виникнення асиметричних систем. Модель Діффі-Хеллмана криптосистеми з публічними ключами. Поняття односторонньої функції-пастки. Асиметрична криптосистема на основі використання «задачі рюкзака».

Тема 3.2. Протоколи розподілення ключів на основі центрів довіри.

Лекція 13. Протоколи розподілення ключів на основі центрів довіри.

Проблема розподілення ключів симетричної криптосистем. Протокол широкоротої жаби. Протокол Нідхейма-Шредера. Протокол Отвей-Ріса. Протокол Цербер. Протокол мережної аутентифікації Kerberos 5 і аутентифікація в Windows.

Тема 3.3. Протоколи асиметричного шифрування.

Лекція 14. Протоколи асиметричного шифрування.

Протокол Діффі-Хеллмана. Шифр Шаміра. Шифр Ель-Гамаля. Програмна реалізація алгоритму Діффі-Хеллмана засобами .NET.

Тема 3.4. Криптосистема RSA

Лекція 15. Криптосистема RSA

Принцип шифрування в RSA. Генерація пари ключів шифрування. Алгоритм шифрування/розшифрування RSA. Програмна реалізація алгоритму RSA засобами .NET.

Тема 3.5. Цифрові підписи.

Лекція 16. Цифрові підписи.

Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамаля. Алгоритм цифрового підпису DSA (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-94.

Тема 3.6. Програмна реалізація цифрового підпису засобами .NET.

Лекція 16. Програмна реалізація цифрового підпису засобами .NET.

Реалізація цифрового підпису на основі RSA. Використання криптопровайдера цифрового підпису на основі DSA.

Тема 3.7. Криптографічні геш-функції.

Лекція 18. Криптографічні геш-функції.

Геш-функції і їх призначення. Ключові геш-функції. Безключові геш-функції. Програмна реалізація алгоритмів геширування в .NET.

Виконання лабораторних робіт

	Завдання	Час
1	Розділ 2. Розробити технологію віддаленого виклику типу GRPC.процедур .	6
2	Роздлі 3. Робота з брокерами повідомлень.	6
3	Розділ 4 На основі створеної **GRPC** розробити децентралізовану систему.	6

Самостійна робота студента

1. Розділ 1. Історія захисту ПЗ
2. Розділ 2. Безпека мережевої інфраструктури.
3. Розділ 3. Microsoft Baseline Security Analyzer і XSpider.
4. Розділ 4. Сканер безпеки XSpider.

Політика та контроль

6. Політика навчальної дисципліни (освітнього компонента)

Для успішного проходження курсу та складання контрольних заходів необхідним є вивчення навчального матеріалу за кожною темою. Специфіка курсу передбачає акцент на розумінні підходів і принципів, отримання практичних навичок, а не просто запам'ятовування визначень. Кожен студент повинен ознайомитися і слідувати Положенню про академічну доброчесність, Статуту і розпорядку дня університету. Для успішного засвоєння програмного матеріалу студент зобов'язаний:

– не запізнюватися на заняття;

– не пропускати заняття, а в разі пропуску відновити за допомогою консультування з викладачем та з використанням конспекту на платформі дистанційного навчання «Сікорський», самостійно вивчити матеріал пропущеного заняття та скласти відповідні контрольні заходи в індивідуальному порядку;

– конструктивно підтримувати зворотній зв'язок на всіх заняттях;

– брати активну участь у освітньому процесі;

– своєчасно і старанно виконувати завдання для самостійної роботи;

– бути доброзичливим до однокурсників та викладачів;

– брати участь у контрольних заходах;

– за об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній online формі за погодженням із деканом факультету);

– будь-яке копіювання або відтворення результатів чужої праці (у тому числі списування), якщо тільки робота не має груповий формат, використання чужих завантажених з Інтернету матеріалів кваліфікується як порушення норм і правил

академічної доброчесності та передбачає притягнення винного до відповідальності, у порядку, визначеному чинним законодавством та Положенням про академічну доброчесність університету. Результатом невиконання та/або недотримання правил може бути оцінка «не зараховано» за курс.

Система вимог, які викладач ставить перед студентом:

- Кодекс честі: http://kpi.ua/code;

- Правила внутрішнього розпорядку: http://kpi.ua/admin-rule;

- Положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського: https://kpi.ua/regulations.

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

***Поточний контроль**: тестування або експрес опитування, МКР, виконання завдань до практичних занять.*

***Календарний контроль**: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.*

Семестровий контроль: *залік.*

***Умови допуску до семестрового контролю**: семестровий рейтинг більше 40 балів.*

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше 60	Незадовільно
Менше 30	Не допущено

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

- *тестування або експрес опитування полекційним заняттям;*
- *виконання завдань до практичних занять;*
- *виконання модульної контрольної роботи (МКР);*
- *виконання і захист індивідуального домашнього завдання;*
- *виконання додатковий завдань.*

Тестування (або експрес опитування)по лекціям	Практичні заняття	МКР	Захист індивідуального домашнього завдання	Додаткові бали
18	27	15	40	10

Тестування (або експрес опитування) по матеріалам лекційних занять

***Ваговий бал - 1.** Максимальна кількість балів за тестування – 1 бал * 18 лекцій = 18 балів.*

Тестування може проводиться за допомогою систем дистанційного навчання, наприклад Moodle, яке доступне протягом 2 робочих днів після завершення поточної лекції. У деяких випадках термін проходження тестування може бути продовжений лектором. Тривалість проходження одного тестування – 10 хвилин. Кількість спроб – одна. У деяких випадках, що пов'язані з технічними проблемами студентів, може надатися повторна спроба на окремі тестування.

Кожне тестування містить 10 запитань різного формату (вибір правильного варіанту з переліку; вірно/невірно; визначити відповідність; чисельна відповідь; вибір пропущених слів; перетаскування на зображення тощо).

Критерії оцінювання

- запитання типу «вибір правильного варіанту з переліку», «вірно/невірно», «чисельна відповідь» оцінюються однозначно: вірна відповідь – 0,1 бал, невірна відповідь – 0 балів;

- запитання, на які немає однієї конкретної відповіді, типу «визначити відповідність», «вибір пропущених слів», «перетаскування на зображення» оцінюються у відповідності до кількості елементів у тесті (наприклад, якщо треба вставити 4 слова у текст, то студент отримає по 0,025 балів за одне правильне вставлене слово, а за всі 4 правильно вставлені слова отримає відповідно 0,1 бал) – невірна відповідь – 0 балів, частково вірна відповідь – 0,01-0,09 балів, вірна відповідь 0,1 бал.

Практичні заняття

***Ваговий бал –3**. Максимальна кількість балів за всі практичні заняття – 3 бали * 9 занять= 27балів.*

На практичних занять студенти разом із викладачем розв'язують завдання за тематикою практичного заняття. Після кожного практичного заняття студенти отримують домашнє завдання, яке необхідно вирішити та надати на перевірку викладачу до початку наступного заняття (зазвичай це 2 тижні, однак іноді цей час може бути змінений викладачем у деяких конкретних випадках).

Перше практичне заняття, зазвичай, поводиться коли лекційний матеріал ще не начитаний, тому його тематика не пов'язана з конкретними темами дисципліни, а направлена на перевірку логічного мислення студентів та можливості інтуїтивно, без знать методів синтезу, складати схеми для простих логічних задач.

Критерії оцінювання

- домашнє завдання вирішено вірно та здано протягом 2-х тижнів після практичного заняття – 3 бали;

- домашнє завдання вирішено вірно, але здано протягом більш ніж 2-х тижнів після практичного заняття – 2,5 бал;

- домашнє завдання вирішено із незначними помилками та здано протягом 2-х тижнів після практичного заняття – 2 бали;

- домашнє завдання вирішено із незначними помилками та здано протягом більш ніж 2-х тижнів після практичного заняття – 1,5 балів;

- домашнє завдання вирішено із значними помилками – повертається на доопрацювання.

Модульна контрольна робота

***Ваговий бал МКР – 15**. Максимальний бал за МКР складає 15 балів.*

На модульній контрольній роботі студент має виконати 3 завдання. Завдання оцінюються від 0 до 5 балів в залежності від правильності вирішення.

Критерії оцінювання

- завдання вирішено вірно та здано протягом 2-х тижнів після практичного заняття – 5 бали;

- завдання вирішено вірно, але здано протягом більш ніж 2-х тижнів після практичного заняття – 4 бал;

- завдання вирішено із незначними помилками та здано протягом 2-х тижнів після практичного заняття – 3 бали;

- завдання вирішено із незначними помилками та здано протягом більш ніж 2-х тижнів після практичного заняття – 2 балів;

- домашнє завдання вирішено із значними помилками – повертається на доопрацювання.

Захист індивідуального домашнього завдання (презентація).

Ваговий бал – 40*. Максимальний бал за захист індивідуального домашнього завдання (презентація) складає 40 балів.*

Студент представляє презентацію проєкту політики системи управління якістю по своїй магістерській дисертації.

Критерії оцінювання

1. Рейтинг захисту Rз = 35 - 40 балів – повністю виконані всі завдання, своєчасно оформлено та представлено супровідну пояснювальну записку. При захисті грамотно та логічно послідовно викладено основні положення роботи у вигляді доповіді, в процесі відповідей на питання продемонстрував наявність глибоких вичерпних знань, або твердих та достатньо повних знань.

2. Рейтинг захисту Rз = 30 - 35 балів – відповідаючи на питання під час презентаціївласної роботи, здобувач припускається окремих помилок, але може їх виправити за допомогою викладача, знає визначення основних понять і величин, впевнено орієнтується в своїй роботі.

3. Рейтинг захисту Rз = 25 - 30 балів – здобувач відповідає майже на всі питання під час презентаціївласної роботи. Відповіді іноді непослідовні та нечіткі. Своєчасно оформив та представив презентацію власного проєкту.

4. Рейтинг захисту Rз = 20 - 25 балів – здобувач частково відповідає на всі питання під час презентаціївласної роботи, показує знання, але не впевнено орієнтується в своїй роботі. Відповіді непослідовні та нечіткі. Не своєчасно оформив та представив презентацію власного проєкту.

5. Рейтинг захисту Rз = 15 – 20 балів – здобуваччастково відповідає на деякі питання під час презентаціївласної роботи, показує незадовільні знання. Відповіді непослідовні та нечіткі. Не своєчасно оформив та представив презентацію власного проєкту.

6. Рейтинг захисту Rз< 20 балів – у відповіді здобувач припускається суттєвих помилок, не може виправити помилки за допомогою викладача. Відповіді некоректні, а в деяких випадках не відповідають суті поставленого питання. Не своєчасно оформив та представив презентацію власного проєкту.

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. При отриманні більш ніж 10 балів, вони обмежуються на рівні 10. Бонусні бали можуть бути отримані за такі види робіт: «Івенти», «Додаткові лекції» та «Завдання до лекцій».

Івенти. *Івенти - це спеціальні події для студентів, які хочуть отримати додаткові бали за вирішення ускладнених завдань. Івенти активуються у визначений час і активні обмежений час. Додаткові бали отримують тільки ті студенти, які надали правильну відповідь вчасно її завантажили. Кількість балів за додаткові завдання визначає кожен івент окремо. Один студент не може отримати більш ніж 10 балів за івенти.*

Додаткові лекції*. Самостійна робота студентів передбачає до 10 додаткових лекцій, які студенти повинні опрацювати та законспектувати. За опрацювання однієї лекції вигляді у конспекту нараховується 1 бал. Максимальна кількість балів, що можна отримати за опрацювання додаткових лекції складає 5 балів.*

Завдання до лекцій. *Студенти, за бажанням, можуть виконувати додаткові завдання за матеріалами лекцій (розв'язати приклад, зробити доповідь тощо). За одне*

додаткове завдання нараховується 0,5 бали. Максимальна кількість балів, що можна отримати за завдання до лекцій складає 5 балів.

Форма семестрового контролю – залік

Максимальна сума балів складає 100. Необхідною умовою допуску до заліку є зарахування всіх домашніх робіт та робота на практичних заняттях.Для отримання заліку з кредитного модулю «автоматом» потрібно мати рейтинг не менше 60 балів, а також виконані умови допуску до заліку.

Здобувачі, які наприкінці семестру мають рейтинг менше 60 балів, а також ті, хто хоче підвищити свою оцінку в системі ECTS, виконують залікову контрольну роботу. При цьому набрані бали студентом анулюються, а оцінка за залікову контрольну роботу є остаточною.

Залікова робота. *Залікова робота проводиться на останньому лекційному занятті. Здобувач проходить тестування очного або у середовищі дистанційного навчання, наприклад Moodle. На тестування пропонується 100 тестових, кожне з яких оцінюється в 1 бал. Для отримання позитивної оцінки необхідно набрати 60 балів і вище. Час тестування зазвичай складає 100 хвилин, але може бути скоригований лектором та (або) викладачам, що приймає залік.*

9. Додаткова інформація з дисципліни (освітнього компонента)

Вимоги до спеціального матеріально-технічного та/або інформаційного забезпечення:

Наявність діючих облікових записів: Користувача на Платформі дистанційного навчання "Сікорський" та Сервісів Google;

Вимоги до мережевої інфраструктури: достатні для отримання доступу до https:// google.com/ та https://do.ipo.kpi.ua.

Операційна система: не специфікується;

Інтернет браузер: не специфікується;

Текстовий редактор: не специфікується.

Перелік питань, які виносяться на семестровий контроль

1. *Істрія появи проблематики і необхідності захисту ПЗ.*
2. *Інфокомункаційні мережі та протоколи..*
3. *Асиметричні і семеричні шифри: особливості, подібності і відмінності.*
4. *Оцінка вразливості архітектури ПЗ.*
5. *Підходи проведення порівняння сучасних та ранніх версій додатків Windows Security Center..*
6. *Що має на озброєнні Windows DefenderBaseline Security Analyzer і XSpider*
7. *Механізми сканеру безпеки XSpider.*

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри інженерії програмного забезпечення в енергетиці НН ІАТЕ, д.т.н., проф., Гаврилком Євгеном Володимировичем

Ухвалено кафедрою інженерії програмного забезпечення в енергетиці НН ІАТЕ(протокол № 28 від 15.05.2023 р.)

Погоджено Методичною комісією НН ІАТЕ (протокол № 9 від 26.05.2023 р.)