Силабус курсу

«Програмні та апаратні методи захисту інформації»

Рівень вищої освіти: доктор філософії
Кваліфікація: доктор філософії , комп'ютерні науки
Заняття: 4 семестр
лекції: 46 год.
Практичні заняття: 62 год.

Кількість кредитів: 4
Мова викладання: українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=4963

Сафаров Олександр Олександрович 	Кандидат технічних наук **https://bit.nmu.org.ua/ua/pro_kaf/prepods/saforov.php** **E-mail:** safarov.o.o@nmu.one

1. Анотація до курсу

Програмні та апаратні методи захисту інформації - це дисципліна для вивчення системних та прикладних методів, які призначені для захисту інформації, що передається по телекомунікаційним каналам. Найчастіше програмні засоби захисту інформації застосовують для виконання таких процесів як ідентифікація й автентифікація користувачів, розмежування доступу користувачів до інформаційної мережі, парольний захист і перевірка повноважень, шифрування інформації, а також її захист від несанкціонованих змін, зчитування, копіювання.

2. Мета та завдання курсу

Мета дисципліни – закласти термінологічний фундамент, навчити здобувачів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам та засобам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу:
У результаті вивчення курсу аспіранти повинні вивчити: методи забезпечення функціонування спеціального програмного забезпечення щодо захисту даних від руйнуючих програмних засобів та проводити аналіз ефективності систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів.

3. Результати навчання:

Отримання знань та навичок у використанні сучасних методів розроблення програмних засобів захисту інформації та синтезу комплексів засобів захисту інформації.

У результаті навчання аспіранти навчаться: застосовувати методи математичного та комп'ютерного моделювання для вирішення широкого спектру задач інформаційної та кібербезпеки, вибирати засоби інформаційних комп'ютерних технологій для захисту програмного забезпечення.

4. Структура курсу.

Види та тематика навчальних занять	**Обсяг складових,** *години*
ЛЕКЦІЇ	**46**
Тема 1. Базові поняття інформаційної безпеки Основні поняття. Захист інформації та його основні завдання. Класифікація загроз для інформації та їх джерел. Поняття про інформацію з обмеженим доступом. Структура політики безпеки та її основні частини.	4
Тема 2. Механізми і політики розмежування прав доступу TCSEC - перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria - європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Вимоги довіри. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу"	4
Тема 3. Шифрування даних. Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах". Симетричні, асиметричні та комбіновані криптосистеми. Їх переваги та недоліки.	5
Тема 4. Системи захисту програмного забезпечення. Мета і доцільність використання систем захисту. Класифікація системи захисту інформації. Пакувальники/шифратори. Системи захисту від несанкціонованого копіювання. Системи захисту від несанкціонованого доступу. Основні алгоритми захисту програмного забезпечення.	5
Тема 5. Розповсюджені типи захистів та їх недоліки. Основні вимоги до розробки систем захисту. Розповсюджені типи захистів та їх недоліки	5
Тема 6. Засоби подолання систем захисту. Проблема існування засобів зламу захистів програмного забезпечення. Класифікація засобів подолання систем захисту програмного забезпечення. Програми розпакування, дешифрування та криптоаналізу.	5
Тема 7. Основні поняття ОС, необхідні для створення систем захисту. Склад операційної системи. BIOS. CMOS. Переривання, їх роль і процедура звертання в програмах. Робота з дисками на фізичному рівні.	5
Тема 8. Загальні принципи захисту програм від несанкціонованого дослідження. Принципи побудови систем захисту та їх функції. Основні	5

Види та тематика навчальних занять	Обсяг складових, *години*
методи та засоби дослідження програм. Способи вбудовування захисних механізмів в програмне забезпечення. Структура програм, захищених від дослідження.	
Тема 9. Захист від дизасемблювання. Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Поняття обфускації та його види.	4
Тема 10. Захист від несанкціонованого налагоджування Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми антиналагоджувального програмування.	4
ПРАКТИЧНІ ЗАНЯТТЯ	**62**
Практична робота №1 **Тема: Розмежування повноважень користувачів на основі парольної аутентифікації.** Мета роботи: Розробка програми розмежування повноважень користувачів на основі парольної аутентифікації. Завдання: Розробити програму розмежування повноважень користувачів на основі парольної аутентифікації.	22
Практична робота №2 **Тема: Логування дій користувачів у програмних системах.** Мета роботи: Засвоїти методику та отримати практичні навики розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонапрямленими хеш-функціями. Завдання: Удосконалити розроблену в лабораторній роботі № 1 програмну систему з метою покращення функції ідентифікації та аутентифікації користувачів.	20
Практична робота №3 **Тема: Методи захисту програмного забезпечення.** Мета роботи: Одержати практичні навики реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження. Завдання: 1. Розробити програмний продукт (або удосконалити ПЗ розроблене в попередніх лабораторних роботах), що виконує мінімум 10 функцій (для прикладу - відкриття файлу, збереження файлу, довідка, друк, перегляд параметрів файлу, пошук та інші).	20
КОНСУЛЬТАЦІЇ/ЗАЛІК	**12**
Разом	**120**

5. Система оцінювання та вимоги

5.1. Навчальні досягнення аспірантів за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Сума балів за навчальні досягнення аспіранта	Оцінка за національною шкалою
90 – 100	відмінно
75-89	добре
60-74	задовільно
0-59	незадовільно

5.2. Аспіранти можуть отримати підсумкову оцінку з дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Лабораторна частина		Бонус	Разом
	При своєчасному складанні	При несвоєчасному складанні		
65	30	20	5	**100**

Підсумковий контроль відбувається у формі письмової роботи.

Білет містить 23 запитання, з яких 20 – тестів, 3 задачі.

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи.

5.3. Критерії оцінювання підсумкової роботи:

18 тестових завдань з чотирма варіантами відповідей, 1 правильна відповідь оцінюється у 3 бали.
Задача – 1 правильна відповідь оцінюється в 5 балів, причому
5 балів – відповідність еталону, з одиницями виміру;
4 бали – відповідність еталону, без одиниць виміру або помилками в розрахунках.
3 бали – незначні помилки у формулах, без одиниць виміру.
2 бали – присутні суттєві помилки у рішенні
1 бал – наведені формули повністю не відповідають еталону.
0 балів – рішення не наведене.

5.4. Критерії оцінювання лабораторної роботи:

5 балів – Достатня зрозумілість відповіді
4 бали – Добра зрозумілість відповіді
3 бали – Задовільна зрозумілість відповіді
0 балів – Незадовільна зрозумілість відповіді

6. Політика курсу

6.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

6.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

6.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

6.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

6.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов’язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об’єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

6.6. Бонуси

За активність та правильні відповіді на лекційних та практичних заняттях студент може отримати до +2 балів до семестрової оцінки на кожному занятті.

7. Рекомендовані джерела інформації

1. Дудатьєв А.В. Захист програмного забезпечення. Частина 1 : навчальний посібник / А.В. Дудатьєв, В.А. Каплун, В.П. Семеренко. – Вінниця : ВНТУ, 2005. – 140 с.

2. Захист програмного забезпечення. Частина 2 : навчальний посібник / В.А. Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця : ВНТУ, 2014 . – 105 с.

3. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

4. Нестеров С.А. Основы информационной безопасности. Учебное пособие. — СПб.: Изд-во Политехн. ун-та, 2014. — 322 с. — ISBN 978-5-7422-4331-1

8. Технічне обладнання та/або програмне забезпечення.

Спеціалізовані середовища розробки (MS Visual Studio, JetBrains PyCharm).