


СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Програмні методи захисту інформації»

	Ступінь освіти	магістр
	Освітня програма	Кібербезпека
	Тривалість викладання	3,4 чверті
	Заняття:	весняний семестр
	лекції:	2 години
	практичні заняття:	2 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача:

Саксонов Генадій Михайлович	ст.викладач
Персональна сторінка	http://bit.nmu.org.ua/ua/pro_kaf/prepods/saksonov.php
Е-пошта:	Saksonov.h.m@nmu.one

1. Анотація до курсу

Програмні засоби захисту інформації — системні та прикладні, 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. Найбільшу увагу розробники й користувачі сьогодні приділяють програмним засобам захисту від несанкціонованого доступу до інформаційних ресурсів і особливо до мережі Інтернет. Організаційні, технологічні й апаратні методи захисту, як правило, не можуть бути здійснені без програмної складової. При цьому слід мати на увазі, що вартість здійснення багатьох програмних системних рішень із захисту інформації суттєво перевищує за затратами апаратні, технологічні й організаційні рішення. Іншими недоліками програмних засобів захисту інформації є використання ресурсів системи, що призводить до зниження її ефективності, принципова можливість обходу такого захисту або його злочинної зміни в процесі експлуатації.

Найпоширенішими прикладами програмних засобів захисту інформації є такі:

- система контролю і управління доступом;
- антивірусні програми;
- шифрувальне програмне забезпечення;
- система управління інформаційною безпекою

2. Мета та завдання курсу

Мета: закласти термінологічний фундамент, навчити правильно проводити аналіз прогроз інформаційної безпеки, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку в комп'ютерних системах здійснення погруз зі сторони потенційних порушників.

Завдання: забезпечити 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

Використовувати на практиці сучасні технології розроблення програмних засобів захисту інформації та синтезу комплексів засобів захисту інформації.

Застосувувати методи математичного та комп'ютерного моделювання для вирішення широкого спектру задач інформаційної та кібербезпеки

4. Структура курсу

ЛЕКЦІЇ.

1. Програма Debug.

1.1 Знайомство з програмою розробки та відладки програм Debug.

1.2 Пам'ять та процесор.

1.3 Дезасемблювання.

2. Антивірусні програми.

2.1 Знайомство з програми. розробки та відкладки програм.

2.2 Налагодження.

2.3 Пам'ять і процесор.

2.4 Діасемблювання

3 Крекінг за допомогою OllyDbg

3.1. Регистри та флаги. Призначення.

3.2. Математичні та логічні конструкції.

3.3. Робота з секціями, боротьба з антидампом.

4. Обфускація даних

4.1. Методи обфускації.

4.2. Захист від дослідження програмного забезпечення за допомогою технології .NET.

ПРАКТИЧНІ ЗАНЯТТЯ

1.Розробка програми з реалізацією загрози «переповнення» буфера

2.Проведення крекінгу програми за допомогою системи OllyDbg.Визначення пароля входу до програми

3.Розробка обфусцированої програми на мові програмування C++

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активованій акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

Технічне обладнання до практичних робіт:

№ роботи	Назва роботи	Інструменти, обладнання та програмне забезпечення, що застосовуються при проведенні роботи
1	Розробка програми з реалізацією загрози «переповнення» буфера	Компілятор C\C++
2	Розробка обфусцированої програми	Компілятор C\C++
3	Проведення крекінгу програми Визначення пароля входу до програми	Система OllyDbg.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6.2. Оцінка виставляється на основі двох теоретичних модулів та шести практичних робіт. Максимальний бал за кожний теоретичний модуль складає 20 балів (2 теоретичні питання по 10 балів). Кожна з практичних робіт «важить» 10 балів.

Критерії оцінювання

Реальні результати навчання студента ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерія використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$O_i = 100 a/m,$$

де a – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення; m – загальна кількість запитань або суттєвих операцій еталону.

Зміст критеріїв спирається на компетентнісні характеристики, визначені НРК для магістерського рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання Для 7-го кваліфікаційного рівня за НРК

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
Знання		
– спеціалізовані концептуальні	Відповідь відмінна – правильна, обґрунтована, осмислена.	95-100

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	Характеризує наявність: <ol style="list-style-type: none"> спеціалізованих концептуальних знань на рівні новітніх досягнень; критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей 	
	Відповідь містить не грубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73
	Відповідь демонструє нечіткі уявлення студента про об'єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64
Рівень знань незадовільний	<60	
Уміння/навички		
<p>– спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур;</p> <p>– здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах;</p> <p>– здатність розв'язувати проблеми у нових або незнайомих середовищах за</p>	Відповідь характеризує уміння: <ol style="list-style-type: none"> виявляти проблеми; формулювати гіпотези; розв'язувати проблеми; оновлювати знання; інтегрувати знання; провадити інноваційну діяльність; провадити наукову діяльність 	95-100
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності з не грубими помилками	90-94
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	Відповідь характеризує уміння/навички застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь/навичок незадовільний	<60
Комунікація		
– зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	Зрозумілість відповіді (доповіді). <i>Мова:</i> 10. правильна; 11. чиста; 12. ясна; 13. точна; 14. логічна; 15. виразна; 16. лаконічна. <i>Комунікаційна стратегія:</i> 17. послідовний і несуперечливий розвиток думки; 18. наявність логічних власних суджень; 19. доречна аргументації та її відповідність відстоюваним положенням; 20. правильна структура відповіді (доповіді); 21. правильність відповідей на запитання; 22. доречна техніка відповідей на запитання; 23. здатність робити висновки та формулювати пропозиції; 24. використання іноземних мов у професійній діяльності	95-100
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільна зрозумілість відповіді (доповіді) та	70-73

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
	доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
<i>Відповідальність і автономія</i>		
<p>– управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів;</p> <p>– відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів;</p> <p>– здатність продовжувати навчання з високим ступенем автономії</p>	Відмінне володіння компетенціями: 25. використання принципів та методів організації діяльності команди; 26. ефективний розподіл повноважень в структурі команди; 27. підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); 28. стресовитривалість; 29. саморегуляція; 30. трудова активність в екстремальних ситуаціях; 31. високий рівень особистого ставлення до справи; 32. володіння всіма видами навчальної діяльності; 33. належний рівень фундаментальних знань; 34. належний рівень сформованості загальнонавчальних умінь і навичок	95-100
	Упевнене володіння компетенціями відповідальності і автономії з незначними хибами	90-94
	Добре володіння компетенціями відповідальності і автономії (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями відповідальності і автономії (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями відповідальності і автономії (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано п'ять вимог)	70-73
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями	60-64

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
	відповідальності і автономії (рівень фрагментарний)	
	Рівень відповідальності і автономії незадовільний	<60

7. Політика курсу

7.1. 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.

7.2. Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

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

7.3. 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).

7.4 Політика щодо оскарження оцінювання

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

7.5. 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.

7.6. Бонуси

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

8 Рекомендовані джерела інформації

1. Дмитрий Скляров "Искусство защиты и взлома информации" © "БХВ-ПЕТЕРБУРГ", 2004
2. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях.
3. Чернов А. В. Анализ запутывающих преобразований программ / Библиотека аналитической информации [Электронный ресурс]
4. А. В. Анисимов. Подходы к защите программного обеспечения от атак злонамеренного хоста. УДК 681.3:004.056
5. Мирошниченко Е. А. Технологии программирования: учебное пособие / , 2008. - 128 с.
6. Ефимов А.И., Пальчун Б.П. О технологической безопасности компьютерной инфосферы// Вопросы защиты информации. - 1995.- №3(30).
7. Белкин П.Ю. Новое поколение вирусов. Принципы работы и методы защиты// Защита информации. - 2017.- №2.-С.35-40
8. Зегжда Д.П., Шмаков Э.М. Проблема анализа безопасности программного обеспечения// Безопасность информационных технологий. - 1995.- №2.- С.28.