Волинський національний університет імені Лесі Українки Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека
Форма навчання	Денна
Розробник (викладач)	Сачук Юрый Володимирович, кандидат фізико-математичних наук
Контактна інформація	yurii.sachuk@vnu.edu.ua
Семестр, курс	4 семестр, II курс
Обсяг дисципліни	Загальний обсяг: 4,5 кредити / 135 годин. Аудиторних годин: 68; з них: лекцій – 34 год., лабораторних – 34 год. Самостійної роботи: 58 год. Консультації: 9 год.
Форма контролю	Екзамен
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна «Діагностика шкідливого програмного забезпечення» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Спрямована на вивчення різного напряму шкідливого ПЗ, класифікації та особливості; виявлення (діагностику), контрзаходи та можливість захисту від нього. Передбачає ознайомлення з юридичними аспектами у випадках поширення, створення та використання шкідливого ПЗ.
Мета вивчення дисципліни	Мета дисципліни: розглянути різні види шкідливого ПЗ та їх класифікацію відповідно до напрямів: операційна система, мережа Інтернет, мобільні пристрої, персональні дані в електронній формі та ін; визначити способи діагностики та захисту від шкідливого ПЗ. Вирішувати задачі професійного напряму: виявлення шкідливого програмного коду або його слідів, аналіз функцій виявлених програм, аналіз способів установки та управління, формування висновку та алгоритму дій захисту (контрзаходів).

Що буде вивчатись	Основні поняття: діагностика комп'ютера та шкідливе програмне забезпечення. Класифікація шкідливого програмного забезпечення. Інфекційне шкідливе ПЗ: віруси, стелси, троянські програми та ін. Інтернет-загрози та їх розповсюдження. Соціальна інженерія, прихований майнінг. Загрози для мобільних телефонів та операційних систем. Рекламне ПЗ, клавіатурні логери, додзвонювачі. Шпигунські програмні засоби, здирницькі програми, шкідливі плагіни. Аналіз впливу обфускації коду на виявлення шкідливого програмного забезпечення та аналіз програмного коду на наявність можливих загроз. Юридичні аспекти та відповідальність за створення, розповсюдження та використання шкідливого ПЗ. Антивіруси: технології, індустрія, практичне застосування. Захист електронних фінансів. Засоби захисту в мережі. Система виявлення та запобігання вторгнень, їх класифікація. Контрзаходи: моніторингові програмні продукти. Загальні правила для захисту від шкідливого ПЗ та зовнішніх атак. Моделювання процесу захисту від шкідливого ПЗ на основі контролю доступу до ресурсів.
Результати навчання	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. **ПРН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **ПРН 4.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **ПРН 17.** Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. **ПРН 20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. **ПРН 53.** Вирішувати задачі аналізу програмного коду на наявність

	можливих загроз.

Оцінювання

Оцінювання навчальних досягнень з дисципліни “Діагностика шкідливого програмного забезпечення” здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та модульний контроль (оцінюються модульні контрольні роботи у вигляді тестів або письмово або у вигляді індивідуальних завдань). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 60 балів.

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 75 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів. Оцінка за семестр, у випадку складання екзамену, є сумою балів поточного контролю та балів, отриманих під час екзамену.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми.

Під час модульного та підсумкового контролю студентам заборонено користуються такими засобами як мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання мають бути виконані у встановлений термін. Несвоєчасно виконані завдання оцінюються на нижчу оцінку. Виключенням можуть бути завдання, які не вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, то він (вона) вивчає матеріал самостійно, використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу, у випадку розміщення його на платформі дистанційного навчання Moodle, виконує всі домашні завдання. Прозвітуватися про виконання завдань

можна, використовуючи дистанційний курс, прикріпивши виконанні завдання у відповідні комірки та попередити викладача про здане завдання, або під час консультацій або надіслати виконане завдання на корпоративну пошту викладача. Зворотній зв'язок з викладачем для з'ясування всіх питань: використання форуму, чату дистанційного курсу, корпоративної пошти університету або відповідної бесіди у певному месенджері.

Перескладання модульного контролю (письмового чи тестування) заборонено.

Рекомендована література

1. Казіміров В.О. Метод захисту від загрозливих програм, заснований на реалізації контролю доступу до файлових об'єктів / В.О. Казіміров, С.В. Мостовий, В.С. Орленко // «Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020. – Частина 2. С. 45-49
2. Михайлов А. В. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. – М.: Диалог-МИФИ, 2012. – 148 с.
3. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин. - М.: ДМК Пресс, 2012. – 576 с.
4. Захист інформаційних ресурсів: навчально-методичний посібник до курсу – Захист інформаційних ресурсів‖ / укл. С. О. Троян. – Умань : [б.в.], 2012. –120 с.
5. Проскурин В. Г. Защита программ и данных: учебное пособие / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М.: Академия, 2011. – 198 с.

Додаткова література (інтернет-джерела)

1. Діагностика комп'ютера. [Електронний ресурс]. – Режим доступу до ресурсу: http://pkpartner.lviv.ua/services/diagnostics/#diagnostics
2. Шкідливе програмне забезпечення. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/zagrozu/project-updates
3. Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=2897-17.
4. Шкідливі програми, їх типи, принципи дії і боротьби з ними. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.slideshare.net/Tania0408/ss-117466015
5. Шкідливі програми та віруси-вимагачі: у чому різниця? [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.vpnmentor.com/blog/ шкідливі-програми-та-віруси-вимагачі/

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 15.09.2021р.

Завідувач кафедри:  (Гришанович Т. О.)