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

СИЛАБУС
нормативної навчальної дисципліни
ОСНОВИ КОМП'ЮТЕРНОЇ ВІРУСОЛОГІЇ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека,
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник	Булатецький Віталій Вікторович, кандидат фізико-математичних наук, доцент
Контактна інформація	bulatetska.lesya@vnu.edu.ua
Семестр, курс	4 курс, 7 семестр
Обсяг дисципліни	Загальний обсяг: 150 годин, 7 кредитів Аудиторних занять: 64, з них 30 лекції, 34 лабораторні роботи Самстійна робота: 82 годин Консультації: 4 год.
Форма контролю	Залік
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi
Мова навчання	Українська
Анотація дисципліни	Силабус навчальної дисципліни "Основи комп'ютерної вірусології" складено відповідно до освітньо-професійної програми "Інформаційна безпека" 2020 р., першого рівня вищої освіти за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології. Дисципліна "Основи комп'ютерної вірусології" належить до переліку вибіркових навчальних дисциплін. Однією з важливих проблем, зберігання даних є проблеми надійності, захищеності, тривалого зберігання інформації. Посилити захист персональних комп'ютерів від комп'ютерних вірусів можна, якщо на підставі поглибленого знання теоретичних основ комп'ютерної вірусології, буде розроблена система послідовних практичних дій, що попереджають зараження вірусом або передбачають використання ефективних методів захисту. В даному курсі вивчаються основні типи шкідливого програмного забезпечення (ШПЗ) та засоби боротьби із ним.
Мета вивчення дисципліни	Ознайомлення студентів із структурою сучасних комп'ютерних вірусів та подібного програмного забезпечення, з їх класифікацією та з методами боротьби із ними.
Що буде вивчатися	1. Хронологія появи та статистика розвитку шкідливого

	та руйнуючого програмного забезпечення. (ШПЗ, РПЗ) 2. Різні підходи до визначення «комп'ютерного вірусу», переваги та недоліки. Інші види ШПЗ. 3. Методи аналізу алгоритму роботи ШПЗ. 4. Класифікації ШПЗ. 5. Класифікації та види антивірусного програмного забезпечення. Огляд найпоширенішого ПЗ даного типу. 6. Методи боротьби з ШПЗ засобами операційної системи. 7. Особливості операційних систем щодо стійкості до ПЗ. 8. Огляд основних типів ШПЗ
Результати навчання	1. Здатність застосовувати знання у практичних ситуаціях. 2. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. 4. Вміти аналізувати структуру шкідливого програмного забезпечення, підбирати, налагоджувати та використовувати програмне забезпечення для боротьби з шкідливим програмним забезпеченням.

Політика оцінювання

Політика щодо академічної доброчесності. 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). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

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

Політика щодо оскарження оцінювання. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку

у встановленому порядку. Проте якщо опротестування безпідставне, можливе зменшення оцінки.

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, 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 навчання може відбуватись в он-лайн формі за погодженням з керівником курсу та деканом факультету.

Бонуси. Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освітим буде нараховано додаткові бали за вчасно здані роботи, за відсутність пропусків без поважних причин.

Підсумковий контроль

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль, який нараховується за якісне виконання лабораторних робіт, виконання контрольних, колоквіумів та тестових робіт, до лекційних матеріалів курсу. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 100 балів. Якщо за результатами семестру накопичено не менше 60 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. Крім того, на заліку пропонується студенту перездати, або доздати 1 тему (лабораторну, контрольну, чи колоквіум), якщо йому до якогось конкретного результату не вистачає декілька балів. В іншому випадку студент складає залік; максимальна кількість балів, яку можна отримати 100 балів.

Рекомендована література та інтернет-ресурси

1. Безруков Н.Н. Компьютерная вирусология. - К.: УРЕ, 1991.
2. Коваленко М. М. Комп'ютерні віруси і захист інформації. — К.: Наук. думка, 1999. — 268 с.
3. Гломозда, Д. Комп'ютерна вірусологія : навчальний посібник / Д. Гломозда. – Київ : ВПЦ НаУКМА, 2012. – 116 с.
4. Ахрамович В.М. Інформаційна безпека. Навчальний посібник / В.М. Ахрамович— К. : ДАСОА, 2008.-- 324 с.: іл. – Бібліограф.: 321с.
5. Моисеенков И. Безопасность компьютерных систем. // Компьютер Пресс, 1991, N 10-12.
6. Семьянов П., Зегжда Д. Анализ средств противодействия исследованию программного обеспечения. // Компьютер Пресс, 1993, N11.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 7 від 5.01.2021 р.

Завідувач кафедри: _____(Гришанович Т. О.)