МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра _____«Захист інформації»_____
(найменування кафедри)

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

_____ АНТИВІРУСНІ ТЕХНОЛОГІЇ_____
(назва навчальної дисципліни)

Освітня програма: _____«Безпека інформаційних і комунікаційних систем»_____
(назва освітньої програми)

Спеціальність: _____125 Кібербезпека_____
(найменування спеціальності)

Галузь знань: _____12 Інформаційні технології_____
(найменування галузі знань)

Ступінь вищої освіти: _____Бакалавр_____
(назва ступеня вищої освіти)

Затверджено на засіданні кафедри
_____«Захист інформації»_____
(найменування кафедри)

Протокол №__ _ від _____ квітня _2020_ р.

м. Запоріжжя _2020_

<table>
<tr><th colspan="2">1. Загальна інформація</th></tr>
<tr><td>Назва дисципліни</td><td>Антивірусні технології (код н/д ОПП - ППН 09).
Цикл підготовки - професійна. Нормативна частина.</td></tr>
<tr><td>Рівень вищої освіти</td><td>Перший (бакалаврський) рівень</td></tr>
<tr><td>Викладач</td><td>Корольков Роман Юрійович, ст. викладач</td></tr>
<tr><td>Контактна інформація викладача</td><td>роб. (0617)698-4-91, моб. +3(097)764-81-54,
email: romankor@zntu.edu.ua
roman_korol@me.com</td></tr>
<tr><td>Час і місце проведення навчальної дисципліни</td><td>Згідно розкладу занять викладачів кафедри
https://zp.edu.ua/kafedra-zahistu-informaciyi</td></tr>
<tr><td>Обсяг дисципліни</td><td>Загальна кількість годин – 210 год., у т.ч. 72 години аудиторних занять і 138 годин самостійної роботи студента.
Кількість кредитів ECTS – 7.
<table>
<tr><th></th><th>Семестр – 6</th><th>Семестр – 7</th><th>Разом</th></tr>
<tr><td>Кредитів ECTS</td><td>3</td><td>4</td><td>7</td></tr>
<tr><td>Лекцій</td><td>14</td><td>30</td><td>44</td></tr>
<tr><td>Лабораторних</td><td>14</td><td>14</td><td>28</td></tr>
<tr><td>Самостійна робота</td><td>62</td><td>76</td><td>138</td></tr>
<tr><td>Вид контролю</td><td>залік</td><td>екзамен</td><td></td></tr>
</table></td></tr>
<tr><td>Консультації</td><td>Згідно з графіком консультацій
https://zp.edu.ua/kafedra-zahistu-informaciyi</td></tr>
<tr><th colspan="2">2. Пререквізити і постреквізити навчальної дисципліни</th></tr>
<tr><td colspan="2">Передумови для вивчення дисципліни “Антивірусні технології” базуються на знанні таких дисциплін: “Технології програмування” (код н/д ОПП - ППН 01), “Основи криптографії та стеганографії” (код н/д ОПП - ППН 07).
Знання, здобуті при вивченні дисципліни “Антивірусні технології” є обов'язковими для вивчення дисципліни: ППН 11 “Проектування, впровадження та супровід комплексних систем захисту інформації”.</td></tr>
<tr><th colspan="2">3. Характеристика навчальної дисципліни</th></tr>
<tr><td colspan="2">Ця дисципліна відноситься до дисциплін циклу професійної підготовки. Знання основ дисципліни “Антивірусні технології” на даний час є одним із важливих показників рівня кваліфікації фахівця з інформаційної безпеки.
Студенти при вивченні дисципліни повинні сформувати вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп’ютерних вірусів, захищати інформацію персонального комп’ютера та розроблене програмне забезпечення, розробляти індивідуальні системи управління доступом і захистом інформації.
Перелік компетентностей, яких набуває студент при вивченні дисципліни:
Загальні компетентності:
КЗ 1. Здатність застосовувати знання в практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності:
КФ 4. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах
КФ 7. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 13. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.
Програмні результати навчання:</td></tr>
</table>

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 5. 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 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 19. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 22. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 33. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

4. Мета вивчення навчальної дисципліни

Мета вивчення дисципліни "Антивірусні технології" – сформувати уявлення про комп'ютерні віруси, середовище їх існування та поширення, а також опанувати сучасні антивірусні програми та системи.

5. Завдання вивчення дисципліни

У результаті вивчення навчальної дисципліни "Антивірусні технології" студенти повинні
знати:

- загальні відомості про захист програм та даних;
- класифікацію загроз безпеці комп'ютерних систем та міри протидії;
- принципи побудови, класифікацію та особливості комп'ютерних вірусів;
- способи поширення та структури комп'ютерних вірусів;
- особливості та призначення руткітів;
- програмні та технічні засоби сучасних персональних комп'ютерів як середовища існування та поширення комп'ютерних вірусів;

вміти:

- виявляти існуючі та потенційні загрози у сфері програмного захисту інформації;
- виявляти та усувати шкідливі програми з використанням сучасних антивірусних програмам;
- використовувати світовий досвід щодо програмного захисту інформації для його впровадження в Україні.

6. Зміст навчальної дисципліни

Навчальна дисципліна складається с 3 змістових модулів:
Змістовий модуль 1. Аналіз та класифікація шкідливого програмного забезпечення.
Змістовий модуль 2. Боротьба з небезпечним програмним забезпеченням.
Змістовий модуль 3. Захист від несанкціонованого доступу.

7. План вивчення навчальної дисципліни

№ тижня	Назва теми	Форми організації навчання	Кількість годин
1-2	Хронологія появи та статистика розвитку шкідливого та руйнуючого програмного забезпечення.	лк лб сам.р.	2 2 10
3-6	Комп'ютерні віруси. Основні поняття та визначення. Файлові віруси. Завантажувальні віруси. Файлово-	лк лб сам.р.	4 4 16

	завантажувальні віруси. Резидентні віруси. Поліморфні віруси. Стелс-віруси. Макро-віруси. Spyware. Ad- ware. Maleware. Троянські коні. Черви. Мережеві хробаки. Інші види вірусів.		
7-10	Потенційно небезпечне програмне забезпечення.	лк лб сам.р.	4 4 18
11-14	Елементи захисту від шкідливого програмного забезпечення.	лк лб сам.р.	4 4 18
15-18	Розвиток технологій міжмережевих екранів. Нові покоління міжмережевих екранів. Обхід міжмережевих екранів.	лк лб сам.р.	8 4 22
19-22	Класифікації та види антивірусного програмного забезпечення. Огляд най-поширенішого ПЗ даного типу.	лк лб сам.р.	8 4 18
23-26	Методи боротьби з шкідливим ПЗ засобами операційної системи.	лк лб сам.р.	8 4 20
27-30	Особливості операційних систем щодо стійкості до шкідливого ПЗ.	лк лб сам.р.	6 2 16
		Разом	210

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Теорія появи шкідливого ПЗ. Ранні шкідливі ПЗ. Еволюція шкідливого ПЗ.	8
2	Файлові віруси. Завантажувальні віруси. Файлово-завантажувальні віруси. Резидентні віруси. Поліморфні віруси. Стелс-віруси. Макро-віруси. Spyware. Ad- ware. Maleware. Троянські коні. Черви. Мережеві хробаки. Інші види вірусів.	12
3	Поняття хакер. Поняття руткіт. Руткіти рівня користувача. Руткіти рівня ядра. Шкідливі програми для мобільних пристроїв.	10
4	Класифікації шкідливого ПЗ. За середовищем існування. За деструктивними діями. За способом поширення. За операційними системами. Інші класифікації.	8
5	Потенційно небезпечне програмне забезпечення. Термінологія і теорія. Як Spyware потрапляють на комп'ютер користувача. Ознаки зараження. Боротьба з потенційно небезпечними програмами.	12
6	Елементи захисту від шкідливого програмного забезпечення. Новітні технології боротьби з шкідливим програмним забезпеченням.	12
7	Розвиток технологій міжмережевих екранів. Фільтрація пакетів. Міжмережеві екрани рівня з'єднання. Міжмережеві екрани прикладного рівня. Міжмережеві екрани з динамічною фільтрацією пакетів. Міжмережеві екрани інспекції станів. Міжмережеві екрани рівня ядра. Персональні міжмережеві екрани. Розподілені міжмережеві екрани. Міжмережеві екрани Web- додатків.	16
8	Нові покоління міжмережевих екранів. Основні поняття та визначення. Класифікація нових поколінь міжмережевих екранів.	12
9	Обхід міжмережевих екранів. Вимоги та показники захищеності міжмережевих екранів. Основні поняття та визначення. Основні вимоги до захищеності міжмережевих екранів. Показники захищеності міжмережевих екранів.	14

	Тестування міжмережевих екранів.	
10	Класифікації та види антивірусного програмного забезпечення. Огляд найпоширенішого ПЗ даного типу. Детектори та фаги. Сторожа. Ревізори. Вакцини. Перспективні засоби захисту. Порівняльний аналіз існуючих засобів захисту від вірусів.	14
11	Методи боротьби з шкідливим ПЗ засобами операційної системи. Операційна система MsDos та її утиліти та команди в боротьбі проти вірусів. Внутрішні засоби Windows в бо-ротьбі проти шкідливого ПЗ. Програми сторонніх виробників. Linux-віруси. Mac OS X-віруси.	12
	Особливості операційних систем щодо стійкості до шкідливого ПЗ.	8
	Разом	**138**

9. Система та критерії оцінювання курсу

У процесі вивчення навчальної дисципліни « Антивірусні технології » використовуються наступні види контролю:

1. Поточний контроль – здійснюється протягом семестру шляхом опитування на семінарських (практичних) заняттях, перевірки виконання тестових завдань, виконання лабораторних робіт, модульних контрольних робіт тощо. За змістом він включає перевірку ступеню засвоєння студентом навчального матеріалу, який охоплюється темою лекційного та семінарського заняття, уміння самостійно опрацьовувати навчально-методичну літературу, здатність осмислювати зміст теми, уміння публічно та письмово представити певний матеріал, а також виконання завдань самостійної роботи.
2. Підсумковий семестровий контроль – здійснюється у формі тестування відповідно до графіка освітнього процесу шляхом визначення ступеню засвоєння студентом навчальної дисципліни за результатами виконання обов’язкових завданнь поточного (модульного) контролю.

Для оцінювання студентів використовується система накопичування балів. Згідно з «Положення про організацію освітнього процесу в Національному університеті «Запорізька політехніка» підсумкова оцінка з дисципліни виставляється за 100-бальною шкалою з наступним переведенням у національну шкалу та шкалу ECTS.

Бали нараховуються за виконання завдань аудиторної роботи, лабораторних робіт, контрольних (модульних) завдань, тестів.

Форми семестрового контролю:

1. Семестровий (диференційований) залік – вид підсумкового контролю, під час якого засвоєння студентом навчального матеріалу з дисципліни оцінюється на підставі результатів поточного контролю протягом семестру. Семестровий залік планується за відсутності екзамену і не передбачає обов'язкової присутності студентів на заліковому заході (заліковій контрольній роботі), залік виставляється за результатами поточного контролю.
2. Семестровий екзамен – форма підсумкового контролю засвоєння студентом теоретичного та практичного матеріалу з навчальної дисципліни за семестр, що проводиться як контрольний захід. Оцінка рівня роботи студента протягом семестру під час навчальних занять та самостійної роботи здійснюється у межах 60 балів. Вага екзамену у підсумковій оцінці складає 40 балів.

Відповідність національної шкали оцінювання академічної успішності шкалі ECTS.

За шкалою ECTS	За 100-бальною шкалою	За національною шкалою	Визначення
A	90 - 100	відмінно	***відмінно*** - відмінне виконання з незначною кількістю помилок
B	85-89	добре	***дуже добре*** - вище від середнього рівня, але з деякими поширеними помилками
C	75-84		***добре*** - в цілому правильне виконання, але з помилками
D	70-74	задовільно	***задовільно*** – виконання в повному обсязі, але зі значною кількістю недоліків

E	60-69		***достатньо*** - виконання задовільняє мінімальні критерії
FX	35-59	незадовільно з можливістю повторного складання	***незадовільно*** – недостатньо: необхідно доопрацювати
F	1-34	незадовільно з обов'язковим повторним курсом	***незадовільно*** - необхідна серйозна подальша робота з повторним вивченням курсу

10. Політика курсу

Вивчення курсу "Антивірусні технології" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та лабораторних заняттях, самостійної роботи та виконання індивідуальних завдань.

При вивченні навчальної дисципліни студенти зобов'язані:

1. Відвідувати навчальні заняття, передбачені розкладом.
2. Вчасно інформувати про неможливість відвідувати заняття.
3. Відповідально, сумлінно і творчо ставитися до виконання навчальних завдань.
4. Систематично й глибоко оволодівати знаннями, вміннями, практичними навичками, професійною майстерністю та підвищувати загальний культурний рівень.
5. Діяти у професійних і навчальних ситуаціях із позицій академічної доброчесності та професійної етики:
    1) усвідомлювати значущість норм академічної доброчесності;
    2) самостійно виконувати навчальні завдання;
    3) коректно покликатися на джерела інформації у разі запозичення ідей, тверджень, відомостей;
    4) оцінювати приклади людської поведінки відповідно до норм академічної доброчесності;
    5) давати моральну оцінку власним вчинкам, співвідносити їх із моральними та професійними нормами, та ін.

Викладач та всі здобувачі, що вивчають цей курс, зобов’язуються дотримуватись Закону України про освіту, Закону України про вищу освіту, Статуту та Правил внутрішнього розпорядку Університету, «Положення про організацію освітнього процесу в Національному університеті «Запорізька політехніка»», етичних норм, та розуміють, що за їх порушення несуть особисту відповідальність.