Міністерство освіти і науки України
Національний педагогічний університет імені М.П. Драгоманова

«ЗАТВЕРДЖЕНО»
Проректор з наукової роботи
професор Г.М.Торбін
«24» грудня 2020 р.

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

освітньо-наукової програми доктор філософії PhD
(назва освітнього рівня)

галузі знань 01 Освіта/Педагогіка
(шифр і назва галузі знань)

спеціальності 011 Освіта, педагогічні науки
(код і назва спеціальності)

Київ 2020

Робоча програма розроблена на підставі навчальної програми «*Захист інформаційних ресурсів»,* затвердженої на засіданні Вченої ради НПУ імені М. П. Драгоманова «24» грудня 2020 року, протокол № 6.

Розробники програми: Франчук В.М., кандидат педагогічних наук, професор

Керівник проектної групи _____ Франчук В. М.
(підпис)

Завідуючий відділом аспірантури _____ Боднар К. А.
(підпис)

Предмет вивчення навчальної дисципліни – процес формування у здобувачів вищої освіти умінь захисту інформаційних ресурсів, методи та техніки його організації та проведення, що дозволяє розвивати в аспірантів навички використання програмних засобів і навички роботи в комп'ютерних системах, розуміння тенденцій розвитку захисту інформаційних ресурсів, та здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, здатність до роботи в команді для захисту інформаційних ресурсів.

Міждисциплінарні зв'язки: «Економіко-математичні методи та моделі», «Інформатика», «Дослідження операцій».

Мета: Метою курсу є формування в аспірантів теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції, до свідомого, активного та вмілого використання нових інформаційних технологій у навчально-виховному процесі.

Завданнями вивчення дисципліни є:

- розкрити місце і значення дисципліни в загальній і професійній діяльності;
- з'ясувати психолого-педагогічні аспекти засвоєння предмету, взаємозв'язки курсу з іншими навчальними дисциплінами, зокрема з інформатичними дисциплінами;
- навчити аспірантів ефективно захищати під час навчально-виховного процесу інформаційні ресурси;
- навчити майбутніх фахівців орієнтуватися у засобах захисту навчальних комп'ютерних систем, свідомо обирати тип, склад та конфігурацію обчислювальної техніки у відповідності до конкретних вимог навчального процесу, психофізіологічних особливостей учнів;
- Продемонструвати ефективність використання методів захисту інформаційних ресурсів при організації навчального процесу.
- Розглянути криптографічні та стеганографічні методи захисту даних.

Основні результати навчання та компетентності, які вони формують:

№ з/п	Результати навчання	Компетентності
1.	**ПРН 1_** Здатність до критичного мислення, розуміння широкого кола філософсько-світоглядних питань, використання набутого особистісно-професійного досвіду для вирішення наукових та фахових завдань; аналізу міждисциплінарних явищ та процесів; реалізації власного аксіологічного та наукового потенціалу. **ПРН 2_** Здатність до застосування методів наукового пізнання, проведення	**ЗК 2_Методологічна** Здатність до розуміння сучасної методології освіти; здатність до застосування методів наукового пізнання; проведення науково-дослідної діяльності; розробка та впровадження дослідницьких проектів,

	науково-дослідної діяльності, розробки та впровадження дослідницьких проектів, здійснення наукового дослідження та інтерпретація його результатів, ефективного висвітлення, поширення знань щодо наукових досліджень.	«start-up»; методологічно та технологічно грамотно здійснювати наукове дослідження, інтерпретувати його результати; ефективно висвітлювати, поширювати знання щодо наукових досліджень та інновацій
2.	**ПРН 8_** Здатність представляти в усній і письмовій формах перед фаховою і нефаховою аудиторією результати власної дослідницької діяльності. **ПРН 9_** Здатність виявляти та формувати нові ідеї та актуальні наукові проблеми, здійснювати проектування наукової роботи, визначати проблематику, гіпотезу, мету, завдання, об'єкт та предмет дослідження, складати робочий план теоретичного та експериментального дослідження у сфері освітніх, педагогічних наук. **ПРН 10_** Здатність вибудовувати алгоритм наукового дослідження у сфері освітніх, педагогічних наук, використовувати методологічні принципи наукового дослідження, організувати та проводити педагогічне спостереження і педагогічний експеримент, використовувати теоретичні та емпіричні методи наукового дослідження, визначати порядок проведення дослідження і його етапи. **ПРН 11_** Здатність застосовувати методи математичної статистики для обробки і аналізу отриманих експериментальних даних та об'єктивної оцінки результатів дослідження.	**ЗК 6_Підприємницька** Здатність визначати підприємницькі можливості власного дослідницького проекту, результатів наукового пошуку, участі у проектній діяльності, прогнозувати вплив власного дослідження на розвиток громади, регіону, країни.
3.	**ПРН 15_** Розуміння особливостей становлення особистості у процесі виховання і самовиховання та здатність використовувати сучасні виховні	**ФЗК 1_Педагогічна** Здатність оперувати науковою термінологією педагогічної науки та

	системи та технології, реалізовувати ціннісно-смисловий підхід до виховання дітей і молоді **ПРН 21_** Вміти ефективно здійснювати педагогічну взаємодію з різними соціальними групами; забезпечувати ефективний прямий та зворотній зв'язок, контакт з батьками через організацію різних форм роботи; налагоджувати професійну комунікацію із загальноосвітніми навчальними закладами, забезпечуючи наступність і перспективність освіти.	вибудовувати ієрархію наукових понять за рівнями їх узагальнення; розуміти системність, взаємозв'язок та цілісність різних педагогічних явищ і процесів, багатогранність практичної спрямованості педагогіки; орієнтуватися у сучасній нормативно-правовій базі розвитку освіти, тенденціях освітньої політики в Україні; розглядати педагогічні явища, розвиток освіти та науки у їх історичній ретроспективі; застосовувати компаративний аналіз щодо вивчення педагогічних проблем у зарубіжному та вітчизняному контекстах; узагальнювати інноваційний педагогічний досвід у власному науковому дослідженні.
4.	**ПРН 27_** Вміти свідомо застосовувати у роботі наукові й практичні здобутки різних систем освіти; розбиратися у специфіці систем освіти різних країн світу, визначати вплив на сучасні освітні перетворення, робити висновки для практичного застосування у власній педагогічній діяльності шляхом використання на заняттях, в управлінській діяльності, іграх та інших видах роботи з дітьми різного віку.	**ФСК 2_** Здатність до диференціації педагогічної діяльності відповідно до специфіки професійних категорій; застосування педагогічних технологій у неперервній педагогічній освіті; впровадження інноваційних процесів у професійну освіту;

		розробки науково-методичного супроводу професійної підготовки; здатність здійснювати прогностичні, планувально-організаційні функції в управлінні закладом освіти; визначати стратегічні лінії розвитку закладу освіти; передбачати можливі ризики зовнішнього і внутрішнього характеру та завчасно уникати їх негативного впливу.

Примірний тематичний план

На вивчення курсу «Захист інформаційних ресурсів», який вивчається на ІІІ курсі у 5 семестрі, відводиться 3 кредити або 90 навчальні години, з яких 50 годин відведено на самостійну навчально-пізнавальну роботу студентів, а 40 години – на аудиторні заняття, які проводяться у формі лекційних занять (20 год.), лабораторних робіт (20 год.).

Опис дисципліни

<table>
<tr><th>Загальні характеристики дисципліни</th><th colspan="2">Навчальне навантаження з дисципліни</th><th>Методи навчання і форми контролю</th></tr>
<tr><td>Галузь знань
(шифр, назва)</td><td colspan="2">Кількість кредитів – 3</td><td rowspan="6">Методи навчання: словесні – лекція, пояснення, бесіда; практичні – виконання практичних завдань, розробка схем, таблиць; самостійне вивчення теоретичного матеріалу, конспектування джерел та їх аналіз, розробка структурно-логічних схем, таблиць.</td></tr>
<tr><td rowspan="2">Спеціальність 012 Дошкільна освіта
(код, назва)</td><td colspan="2">Загальна кількість годин -</td></tr>
<tr><td>Денна</td><td>Заочна (вечірня)</td></tr>
<tr><td rowspan="3">Освітній рівень (доктора філософії)</td><td colspan="2">Лекції:</td></tr>
<tr><td>20</td><td>20</td></tr>
<tr><td colspan="2">Семінарські (практичні) заняття:</td></tr>
<tr><td>Нормативна/вибіркова</td><td>-</td><td>-</td></tr>
<tr><td rowspan="5">Рік вивчення дисципліни за навчальним планом –ІІІ
Семестр V</td><td colspan="2">Лабораторні заняття:</td><td rowspan="5">Форми поточного контролю – усне опитування, виконання завдань, перевірка самостійної роботи.</td></tr>
<tr><td>20</td><td>20</td></tr>
<tr><td colspan="2">Індивідуальна робота:</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота:</td></tr>
</table>

	50		Модульний контроль – письмова модульна контрольна робота.
Тижневе навантаження (год.) - аудиторне: 2 - самостійна робота 5	*50*	*50*	Форма підсумкового контролю Залік
	Співвідношення аудиторних годин і годин СРС:		
Мова навчання - українська	*40/50*	*40/50*	

Змістовий модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах.

Тема 1. Основні поняття з галузі захисту інформаційних ресурсів.

Актуальність проблеми комп'ютерної безпеки, цілісність даних, конфіденційність даних, доступність даних, розголошення даних, витік даних, захист даних, порушенням режиму доступу, несанкціонований доступ, об'єкт злочину, блокування даних, модифікація даних, одержання захищуваних даних, фільтрація даних, канал витоку даних, помилка, прорахунок, вразливість інформаційної системи, види загроз, джерела загроз, контроль безпеки, види атак, вторгнення, політика безпеки, класифікація навмисних загроз безпеки комп'ютерних систем.

Тема 2. Засоби парольної ідентифікації та адміністрування.

Ідентифікація, засоби парольної ідентифікації в операційних системах, в програмних додатках, в мережевих сервісах, способи захисту від перебирання паролів, варіанти заміни традиційних паролів, способи створення складних паролів.

Тема 3. Архівування та резервне копіювання даних.

Стискування, архівація даних, архіватор, ступінь стискування, коефіцієнт стискування, методи стискування файлів, резервне копіювання, технології резервного копіювання.

Тема 4. Захист вмісту зовнішньої пам'яті.

Перспективні розробки у сфері зберігання вмісту запам'ятовуючих пристроїв, технології захисту оптичних дисків від несанкціонованого копіювання, діагностика та профілактика жорстких магнітних дисків, технології захисту флеш-накопичувачів, засоби відновлення пошкодженого і втраченого вмісту запам'ятовуючих пристроїв, гарантоване вилучення вмісту запам'ятовуючих пристроїв.

Тема 5. Захист програмного забезпечення.

Вразливості програмного забезпечення та засоби боротьби з ними, дослідження вихідних текстів програмного забезпечення, захист програм встановлених на жорсткому диску, захист програм від вивчення.

Тема 6. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм.

Комп'ютерні віруси і засоби боротьби з ними, історія комп'ютерних вірусів, класифікація комп’ютерних вірусів, антивірусні програми, типи антивірусних програм, методи розпізнавання шкідливих об'єктів, захист

комп'ютера від шпигунських програм.

Тема 7. Поширені види мережевих атак і способи захисту від них.

Мережеві атаки, види мережевих атак, сегментація мереж, міжмережеві екрани, списки управління доступом (ACL), загрози використання глобальної мережі Інтернет, методи захисту.

Тема 8. Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.

Актуальні проблеми використання безпровідних мереж, типи загроз безпеці в безпровідних мережах, способи захисту даних в безпровідних мережах.

Змістовий модуль 2. Криптографічні та стеганографічні методи захисту даних.

Тема 9. Основні поняття криптографії. Коротка історія криптографії.

Поняття криптології, криптографії. Ключ, шифрування, зашифровування, розшифровування, криптостійкість, криптоаналіз, методи криптоаналізу, криптографічні методи захисту даних.

Тема 10. Популярні алгоритми шифрування даних.

Алгоритми шифрування, асиметричні криптографічні алгоритми, симетричні криптографічні алгоритми.

Тема 11. Використання електронного підпису.

Криптосистеми з відкритим ключем, електронний (цифровий) підпис, технології застосування систем електронного цифрового підпису, генерація ключів.

Тема 12. Програмно-апаратні засоби шифрування даних.

Реалізації криптозахисту на апаратному рівні. Архітектура апаратних засобів криптозахисту. Організація інтерфейсу для роботи з прикладними програмами.

Тема 13. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи.

Поняття стеганографії, історія стеганографії, стеганографічні методи і системи.

Тема 14. Деякі проблеми і перспективи використання криптографічних засобів захисту даних.

Проблеми шифрування великих повідомлень, сучасні способи вирішення проблеми розподілу ключів, системи біометричної аутентифікації, перспективи використання криптографічних засобів захисту даних.

Форма підсумкового контролю успішності навчання

Політика щодо дедлайнів та перескладання. Роботи, які здано з порушенням термінів без поважних причин, буде оцінено на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності). Перескладання модуля відбувається за наявності поважних причин.

Політика щодо академічної доброчесності. Письмові роботи викладач перевіряє на наявність плагіату і допускає до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час модульних робіт та екзаменів заборонено (у т. ч. із використанням мобільних девайсів). Мобільні

пристрої дозволено використовувати лише під час онлайн- тестування (наприклад, у програмі MOODLE).

Політика щодо відвідування. Відвідування занять є обов'язковим компонентом освітнього процесу. За об'єктивних причин (наприклад, хвороба, міжнародне стажування, участь в представленні соціального проєкту) навчання може відбуватися в онлайн-формі за погодженням із керівником курсу.

Залік є формою підсумкового контролю результатів навчання студентів і має на меті перевірку системності засвоєння програмового матеріалу, цілісності бачення навчального курсу, рівня осмислення знань та набуття умінь, їх комплексного застосування у практичній діяльності, діагностування ефективності самостійної навчальної роботи студентів.

Відмітка «зараховано» виставляється студенту при умові набору більше 60 рейтингових балів, а саме: регулярного відвідування лекційних і лабораторних занять або їх негайному відпрацюванні, своєчасного складання усіх видів поточного контролю з позитивними результатами; поглибленні набутих знань у процесі самостійної роботи; засвоєнні змісту навчального курсу в обсязі, передбаченому галузевим стандартом вищої освіти.

Якщо студент з поважних причин, що підтверджено документально, був відсутній на заняттях, він має право на одне перескладання з можливістю отримання максимальної кількості балів. Термін перескладання визначається викладачем.

Якщо впродовж семестру студент пропустив значну кількість занять, не має оцінок за виконання модулів, у відповідних графах «Відомості обліку успішності» виставляється «1», у графі «залік» виставляється «не зараховано», а у графі «екзамен» – відмітка про не допуск до нього.

Рейтинговий регламент Інституту. Шкала відповідності

За шкалою ECTS	**За шкалою університету**	**Визначення**	**Оцінка за національною шкалою**	
			Екзамен	**Залік**
A	90 – 100	Відмінно	5 (відмінно)	Зараховано
B	80 – 89	Дуже добре	4 (добре)	
C	70 – 79	Добре		
D	65 – 69	Задовільно	3 (задовільно)	
E	60 – 64	Достатньо		
FX	35 – 59	Незадовільно з можливістю повторного складання	2 (незадовільно)	Не зараховано
F	1 – 34	Незадовільно з обов'язковим повторним курсом		

Засоби діагностики успішності навчання

Видом контролю навчальних досягнень студентів під час вивчення курсу є залік. За результатами роботи на лабораторних заняттях, виконання завдань для самостійного опрацювання, підготовки та виступу з доповіддю на заняттях, модульних тестів, студенти накопичують певну кількість балів, відповідно до якої відбувається оцінювання їх навчальних досягнень.

Побудова програми за кредитно-модульною схемою спрямована на максимальну індивідуалізацію процесу навчання. Структура програми дібрана так, щоб надати студентам можливість навчатись в індивідуальному темпі та орієнтуватись на певні рівні вимог щодо засвоєння навчального матеріалу.

Контроль знань студентів здійснюється за модульно-рейтинговою системою. Навчальна діяльність студентів протягом семестру оцінюються за 100-бальною системою. Робота в семестрі поділяється на змістові модулі.

Накопичення балів протягом семестру відбувається так:

№ з/п	Вид діяльності	Кількість балів за дидактичну одиницю	Кількість лекцій, практичних робіт тощо	Загальна кількість балів
1	2	3	4	5
1	Відвідування та активність під час лекцій та лабораторних	5	5	25
2	Виконання лабораторних робіт	10	7	70
3	Виступ з повідомленням на занятті	8	2	16
4	Модульні тести	10	1	10
Формула переведення балів у бали за модульно-рейтинговою системою 100*А/121, де А – кількість набраних студентом балів.				**121**
Залік				100
Оцінка за курс (середній бал)				100

Засоби діагностики успішності навчання:

- ✓ теоретичні запитання та практичні завдання до лабораторних робіт;
- ✓ комплекс тестових завдань для модульного (підсумкового) контролю рівня навчальних досягнень студентів;
- ✓ індивідуальні завдання студентам;
- ✓ комплексна контрольна робота.

Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

- ✓ Мультимедійний проєктор – демонстрація презентацій.
- ✓ Комп’ютери з доступом до Інтернету.

Рекомендована література:

1. Баричев С.Т., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: Горячая линия-Телеком, 2001. 152 с.

2. Биячуев Т.А. Безопасность корпоративных сетей. Под ред. Л.Г. Осовецкого. СПб: СПб ГУ ИТМО, 2004. 161 с.

3. Блэк У. Інтернет: протоколы безопасности. Учебный курс. СПб.: Питер, 2010. 288 с.

4. Болотов А.А., Гашков А.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 328 с.

5. Бормотов СВ. Системное администрирование на 100 % (+CD). СПб.: Питер, 2006. 256 с.

6. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. М.: ПАИМС, 2000. — 36 с.

7. Гордейчик СВ., Дубровин В.В. Безопасность беспроводных сетей. — М.: Горячая линия-Телеком, 2008. 288 с.

8. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996. 130 с.

9. Зубов А.Ю. Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.

10. Касперски К. Восстановление данных. Практическое руководство: Пер. с англ. СПб.: БХВ-Петербург, 2006. 352 с.

11. Касперски К., Рокко Е. Искусство дизассемблирования. Наиболее полное руководство в подлиннике. СПб: БХВ-Петербург, 2008. 891 с.

12. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. — М.: Издательская группа "БДЦ-пресс", 2006. 304 с.

13. Митник К. Искусство вторжения: Пер. с англ. Семенова А.В. М.: АйТи, ДМК Пресс, 2005. 280 с.

14. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Лань, 2000. 256 с.

15. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999. 200 с.

16. Низамутдинов М.Ф. Тактика защиты н нападения на Web-приложения. СПб.: БХВ-Петербург, 2005. 432 с.

17. Норткат С, Новак Дж. Обнаружение нарушений безопасности в сетях. – М.: Издательский дом "Вильяме", 2003. 448 с.

18. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. М. ДМК пресс, 2001. 400 с.

19. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М: ДМК, 2000. 448 с.

20. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студ. высш. учеб. Заведений. М. : Издательский центр "Академия", 2006. 240 с.

21. Практическая криптографія: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. М.: СОЛОН-Пресс, 2002. 256 с.

22. Скляров Д. Искусство защиты и взлома информации. СПБ.: БХВ-Петербург, 2004. 288 с.

23. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам'янець-Подільський: ПП Буйницький О А, 2011. 704 с

24. Фленов М.Е. PHP глазами хакера. СПб.: БХВ-Петербург, 2005. 304 с.

25. Форд Дж. Ли. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. М.: КУДИЦ-ОБРАЗ, 2002. 272 с.

26. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов. М.: Издательство "Русская Редакция"; СПб.: Питер, 2007. 432 с.

27. Хоффман Л.Дж. Современные методы защиты информации. М.: Сов. Радио, 1980. 246 с.

28. Чирилло Дж. Обнаружение хакерских атак. Для профессионалов. СПб.: Питер. 2002. 864 с.

29. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире . СПб.: Питер, 2003. 368 с.

30. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. М: Издательско-торговый дом "Русская Редакция", 2003. 416 с.

Електронні ресурси та web-сайти

31. Громов В.И. Васильев Г.А. Энциклопедия компьютерной безопасности. Режим доступа: http://kiev-security.org.ua/b/1.shtml. —Название с экрана.

32. Зиммерман Филипп. Кодирование с открытым ключом для всех. Руководство пользователя PGP. — Режим доступа: http://lib.metromir.ru/book2571. — Название с экрана.

33. Иллюстрированный самоучитель по защите информации. — Режим доступа: http://www.inattack.ru/program/525.html. — Название с экрана.

34. Иллюстрированный самоучитель по теории операционных систем. — Режим доступа: http://www.soft-info.ru/downloads/1230999291. — Название с экрана.

35. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака через Internet. — Режим доступа: http://www.rus-linux.net/lib.php?name=/MyLDP/BOOKS/books#lin-ru. — Название с экрана.

36. Наказ Міністерства транспорту та зв'язку України від 27.04.2005 "Про затвердження порядку проведення державної реєстрації електронних інформаційних ресурсів".— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0528-05. — Назва з екрана.

37. Руководство по информационной безопасности. — Режим доступа: http://unix1.jinr.ru/ faq_guide/security/jet/secplant. — Название с экрана.

38. Стандарты и спецификации в области информационной безопасности. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт. Режим доступа: http://www.intuit.ru/department/security/secbasics/5. — Название с экрана.

39. Техника восстановления данных с лазерных дисков или практическое знакомство с сессиями. — Режим доступа: http://hack-tools.ucoz.com. — Название с экрана.

40. Ферри Д. Секреты супер-хакера. — Режим доступа: http://www.domknig.net/book-2697.html. — Название с экрана.