МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента

КУРСОВА РОБОТА З ПРОГРАМНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

підготовки здобувачів першого (бакалаврського) рівня вищої освіти

галузі знань 12 Інформаційні технології

за спеціальністю 125 Кібербезпека та захист інформації

Освітня кваліфікація: Бакалавр з кібербезпеки та захисту інформації

Луцьк – 2024

Силабус нормативного освітнього компонента «Курсова робота з програмно-технічного захисту інформації» підготовки бакалаврів, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації

Розробник:
Онищук О. О., кандидат технічних наук, доцент кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

© Онищук О. О., 2024 р.

І. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="6">галузі знань
12 Інформаційні технології
спеціальність
125 Кібербезпека та захист інформації
Освітня кваліфікація:
Бакалавр з кібербезпеки та захисту інформації</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 4-ий</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів 60 / 2</td><td>Семестр 8-ий</td></tr>
<tr><td>Консультації 4 год.</td></tr>
<tr><td>Самостійна робота: 56 год</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></td></tr>
</table>

ІІ. ІНФОРМАЦІЯ ПРО КЕРІВНИКА КУРСОВОЇ РОБОТИ

ПІП	Онищук Оксана Олександрівна
Науковий ступінь	кандидат технічних наук
Вчене звання	доцент
Посада	доцент кафедри комп’ютерних наук та кібербезпеки
Контактна інформація	(096) 6943585,onyshchuk.oksana@vnu.edu.ua
Дні занять	за розкладом http://94.130.69.82/cgi-bin/timetable.cgi?n=700

ІІІ. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

Сучасний етап розвитку науки і техніки зазнає нових та продуктивних змін. Цифровізація суспільства вимагає нових рішень у питаннях захисту інформації. Широке використання сучасних інформаційних технологій, зокрема хмарних технологій, IoT, блокчейн, девайсів та гаджетів вимагають відповідних підходів до кіберзахисту. В свою чергу, це накладає певні вимоги до знань та компетентностей сучасного професіонала з кібербезпеки.

Для забезпечення цілісності, конфіденційності, доступності інформації та ресурсів, з метою мінімізації збитків від розголошення, втрати, несанкціонованого доступу, відмови в обслуговуванні необхідно ретельно вибирати заходи та засоби захисту інформації.

Системи захисту інформації потребують ретельного планування, моделювання та проектування перед впровадженням у життя. Сучасний теоретичних та практичних стан розвитку науки та техніки дозволяє ці процеси автоматизувати, дослідити та перевірити їх працездатність перед використанням у реальному житті.

Значну роль у розвитку навичок самостійної творчої роботи здобувачів вищої освіти відіграє виконання ними курсових робіт, оскільки це дозволяє шляхом розв’язування конкретних реальних проблем залучати їх до науково-дослідної роботи, виховувати у них відповідальність за виконану роботу. Виконання курсових робіт є

складовою науково-дослідної роботи здобувачів вищої освіти, що включається в навчальний процес і сприяє закріпленню, поглибленню і узагальненню знань, отриманих ними під час навчання і застосуванню цих знань до комплексного вирішення конкретних практичних проблем. Написання та захист системи курсових робіт є важливим підготовчим етапом для виконання бакалаврських і магістерських робіт. Підготовка до написання курсової роботи повинна навчити студента користуватися довідковою літературою Держстандартів, типовими проектами у відповідних галузях. Матеріали курсової роботи можуть бути використані для подальшої дослідницької навчально-наукової роботи студента.

Курсова робота з розробки програмно-технічного захисту інформації є обов'язковим компонентом освітньо-професійних програми «Кібербезпека та захист інформації» для здобуття освітнього рівня бакалавр спеціальностей 125 Кібербезпека та захист інформації, виконання якої повинно здійснюватися відповідно до стандартів програмно-технічного захисту систем та інформації, захисту програмного забезпечення, на основі національних і міжнародних стандартів.

Написання курсової роботи з розробки програмно-технічного захисту інформації спрямоване на підвищення рівня формування у студентів знань та умінь, які дадуть теоретичний і практичний фундамент розуміння принципів функціонування та використання в професійній діяльності програмно-технічного захисту інформації та сучасних систем технічного захисту.

2. Мета освітнього компонента. Метою написання курсової роботи з розробки програмно-технічного захисту інформації є дослідження і розв'язок задач проектування та реалізації захисту програмного забезпечення за допомогою технічних засобів; дослідження сутності, задач, принципів та сучасних технологій проектування систем кібербезпеки для комплексного захисту інформації; дослідження методологічних та законодавчих основ організації, планування, проектування, впровадження, експлуатації та супроводу систем кібербезпеки; основних аспектів практичної діяльності по їх проектуванню, розробка, реалізація та забезпечення функціонування; проведення оцінки ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників; освоєння сучасних комп'ютерних технологій проектування систем захисту інформації з використанням графічних програмних середовищ візуального моделювання UML і особливостей проектування систем за допомогою CASE-засобів для задоволення потреб науки, бізнесу та підприємств у різних галузях. Основним результатом виконання курсової роботи з розробки програмно-технічного захисту інформації є програмний продукт.

3. Завдання курсової роботи з розробки програмно-технічного захисту інформації:

Завданнями написання курсової роботи з розробки програмно-технічного захисту інформації є формування спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері професійної діяльності та інформаційних технологій, формування оригінального мислення та проведення досліджень у області програмно-технічного захисту інформації, критичне осмислення проблем кібербезпеки та інформаційних технологій загалом.

Для формування спеціалізованих умінь/навичок та розв'язання проблем необхідно: оволодіння етапами проектування програмно-технічного захисту інформації та систем кіберзахисту; розуміти головні задачі та сервісів кібербезпеки; оволодіння методологічними та законодавчими основами організації, планування, проектування, впровадження, експлуатації та супроводу програмно-технічного захисту інформації та систем кібербезпеки; формування здатності інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; вивчення основних принципів, засад та методів організаційного та програмно-технічного захисту інформації, систем захисту в кіберпросторі; оволодіння методами та технологіями розробки супроводжувальної робочої документації для програмно-технічного захисту інформації; оволодіння методами оцінки ефективності програмно-технічного захисту інформації та систем кіберзахисту.

Для формування здатності розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності необхідно: освоєння сучасних комп'ютерних технологій програмно-технічного захисту інформації та систем захисту інформації з використанням графічних програмних середовищ візуального моделювання UML і особливостей проектування систем за допомогою CASE-засобів.

Курсова робота повинна бути результатом самостійних досліджень здобувача вищої освіти, які:

– сприяють розвитку ініціативності здобувачів у їх виробничій і дослідницькій діяльності;

– розвивають творчий підхід до вирішення проблем кібербезпеки;

–поглиблюють, систематизують та закріплюють компетентності, отримані під час навчання;

– перевіряють вміння здобувача самостійно освоїти та використовувати сучасні організаційні заходи, інформаційні технології, бази знань, програмно апаратні, комунікаційні засоби управління;

– розвивають у здобувача навички ведення самостійного науково практичного пошуку, оволодіння методикою дослідження й експерименту в ході вирішення проблем і питань, поставлених до виконання;

– закріплюють знання і навички виконання графічних робіт та інших конструкторських документів відповідно до вимог і правил, встановлених державними стандартами (ДСТУ 3008-2015), Єдиною системою конструкторської документації (ЄСКД), Єдиною системою проектної документації (ЄСПД), іншими чинними нормативно-технічними документами; – сприяють набуттю вміння аналізувати отримані результати досліджень, формулювати висновки та положення.

За всі відомості, що викладені в курсовій роботі, порядок використання в ході підготовки фактичного матеріалу та іншої інформації, пропозиції, топології, технології, обґрунтованість і вірогідність висновків та положень, що захищаються, несе відповідальність безпосередньо автор – здобувач вищої освіти.

Керівник курсової роботи надає здобувачу вищої освіти допомогу у виборі теми роботи, проводить консультації з проблемних питань, що виникають у процесі проектування, надає допомогу в пошуку методичної та технічної документації, науково-технічної літератури, а також проводить систематичний контроль за виконанням курсової роботи.

Пояснювальна записка курсової роботи повинна містити розроблені здобувачем вищої освіти топології, моделі, схеми, алгоритми, структури баз даних, функціональні та структурні схеми, лістинги програми чи програмного комплексу, інші види

технічного опису особистих фахових науково-технічних рішень.

Пояснювальну записку курсової роботи можна умовно поділити на такі змістові частини: вступна частина; основна частина; додатки. Вступна частина пояснювальної записки проекту включає титульну сторінку, реферат, зміст та перелік умовних позначень. До основної частини відносять такі структурні елементи: вступ, три розділи, висновки, перелік посилань у вигляді списку використаної літератури. Пояснювальна записка повинна мати таку структуру:

– титульна сторінка;
– завдання на курсову роботу;
– реферат (анотація);
– зміст;
– скорочення та умовні познаки;
– вступ;
– три розділи;
– висновки;
– перелік джерел посилання;
– додатки (за необхідності).

Об'єм та зміст кожного структурного елементу визначається здобувачем вищої освіти залежно від тематики дослідження. Вимоги та основний зміст кожного структурного елементу наведено нижче. Слід зауважити, що слід дотримуватися рівності об'єму розділів. Змінювати порядок структури пояснювальної записки не дозволяється. Всі наведені елементи структури є обов'язковими, окрім додатків.

4. Результати навчання.

Загальні компетентності.

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні)компетентності.

СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання.

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту зметою оперативного відновлення функціонування інформаційної системи.
РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом

інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

IV. ЕТАПИ НАПИСАННЯ КУРСОВОЇ РОБОТИ ТА ОРІЄНТОВНІ ТЕРМІНИ ЇХ ВИКОНАННЯ

№ п/п	Зміст проведених робіт	Термін виконання у % до загального терміну виконання	Форма звітності
1.	Вибір тематичного напрямку та узгодження теми курсової роботи	10%	Закріплення теми курсової роботи за здобувачем
2.	Розробка технічного завдання, визначення методів та засобів реалізації поставленої задачі	15%	Роздруковане технічне завдання за підписом викладача
3.	Аналіз теоретичних матеріалів за напрямком дослідження, вивчення предметної області	10%	Оформлення розділу 1 курсової роботи в електронному вигляді, оформлення в ел. вигляді списку використаної літератури
4.	Розробка структури системи, функціональних модулів, топології	35%	Структурна та функціональна модель системи. Оформлення розділу 2 курсової роботи.

5.	Розробка алгоритмів роботи системи, програмних модулів, проведення налаштування системи	15%	Розробка тестового прикладу та опис порядку дій користувача в ел. вигляді.
6.	Оформлення пояснювальної записки, підготовка презентаційних матеріалів	15%	Роздрукована пояснювальна записка та готова презентація

Робота над курсовою роботою розпочинається з глибокого вивчення теоретичних питань, важливих наукових відкриттів, передових досягнень, перспективних напрямків розвитку моделей, методів та засобів побудови систем кібербезпеки, що відповідають тематиці роботи, відповідних чинних керівних документів, методик побудови. Це вимагає ознайомлення і використання в ході виконання курсової роботи значної кількості літературних джерел, праці у бібліотеках та використання Internet.

Інформаційні джерела здобувач вищої освіти добирає самостійно. В разі необхідності в доборі літератури допомагає керівник. Використані літературні джерела оформлюються відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічні посилання. Загальні положення та правила складання».

Для оформлення графічної частини в ході виконання відбираються необхідні матеріали для розробки моделей, схем і алгоритмів, що найбільш повно відбивають обсяг і зміст проекту. Всі принципові положення, розрахунки, конструктивні рішення, ескізи, креслення узгоджуються з керівником до того, як вони будуть оформлені остаточно.

Виконання вказівок керівника щодо обсягу, правильності розрахунків і якості виконання курсової роботи є обов'язковими до виконання. Успішність і своєчасність виконання курсової роботи досягається завдяки максимально чіткій організації проекту здобувача вищої освіти як у період розробки, так і під час підготовки проекту до захисту.

Здобувач вищої освіти зобов'язаний періодично звітувати про виконану роботу перед керівником. Керівник систематично контролює і спрямовує роботу здобувача, оцінює результати моделювання, проектування і прийняті рішення, дає поради з окремих питань, вказує на недоліки викладу текстового матеріалу та порядку компонування графічної частини.

Курсова робота оцінюється комплексним рейтинговим показником. Критерії оцінювання представлено у таблиці.

Сумарний показник переводиться у оцінку за затвердженою шкалою оцінювання. Закінчений курсовий проект, підписаний здобувачем вищої освіти і керівником, реєструється на кафедрі та здається керівнику для остаточної перевірки і вирішення питання допуску роботи до захисту перед членами комісії.

Основними формами контролю виконання проекту є – поточний, проміжний і підсумковий. Поточний контроль здійснюється здобувачем вищої освіти особисто, шляхом системної перевірки відповідності стану виконаних робіт графіку виконання роботи і поточних характеристик роботи вимогам технічного завдання.

Проміжний контроль здійснюється керівником курсової роботи, у відповідності до графіку проведення контролю, шляхом перевірки виконаних згідно графіку курсової завдань. Визначені недоліки мають бути усунені до завершення виконання курсової роботи.

Підсумковий контроль містить 2 етапи:

Етап перший – допуск курсової роботи до захисту. Передбачає перевірку курсової роботи керівником і висновок щодо можливості захисту із зазначенням недоліків. У результаті позитивного висновку – недоліки розробник виправляє за бажанням. У разі негативного висновку основні недоліки є обов'язковими до виправлення.

Етап 2 – захист курсової роботи. Проводиться комісією, яка складається із представників кафедри в термін визначений графіком виконання проекту. Підсумковий контроль передбачає:

1. Доповідь здобувача вищої освіти щодо реалізованих в системі проектних рішень.

2. Комплексне тестування всього проекту і окремих модулів на відповідність функціональним і якісним характеристикам.

3. Перевірку складу та якості програмної документації, комплектність проекту у відповідності до пред'явленого опису і технічного завдання. 4. Співбесіда. Для встановлення рівня теоретичних та практичних знань комісія проводить опитування здобувача вищої освіти. Можливі питання: уточнюючі за матеріалами курсової роботи, загальні з освітньої компоненти «Проектування систем кібербезпеки».

На основі результатів підсумкового контролю комісія робить висновок про приймання або неприйняття роботи, з оформленням відповідного акту (рецензії) на виконану роботу і визначенням оцінки за курсову роботу. Захист одного здобувача має відбутися протягом 30 хвилин. Для повідомлення (доповіді) здобувачу вищої освіти надається 10-12 хвилин. Доповідь містить, як правило, коротку узагальнену інформацію, яка викладена у вступі, висновках до підрозділів і розділів, у загальному висновку. Повідомлення здобувача вищої освіти щодо результатів курсової роботи повинне супроводжуватися електронною презентацією. Послідовність захисту курсової роботи:

− голова комісії по захисту курсових проектів (робіт) надає слово здобувачу вищої освіти для доповіді;

− здобувач вищої освіти доповідає про результати своєї роботи;

− члени комісії по черзі задають уточнюючі питання здобувачу вищої освіти;

− здобувач вищої освіти відповідає на кожне питання конкретно, коротко, змістовно, спокійно, стримано, етично;

− присутні на захисті здобувачі та викладачі також можуть задати здобувачу вищої освіти запитання, на які він повинен дати відповідь; Після захисту члени комісії самостійно ставлять студенту оцінку за 100- бальною системою оцінювання. При цьому враховують: загальну ерудицію; теоретичну підготовку з дисципліни; технічний рівень виконаного проекту, об'єм роботи здобувача вищої освіти.

Після захисту всіх здобувачів, зазначених у графіку на даний день, проводиться закрите засідання комісії по захисту курсових проектів (робіт), на якому обговорюються результати захисту. За підсумками відкритого голосування членів комісії здобувачу виставляється середньозважена оцінка. Виставлені оцінки оголошуються здобувачам і виставляються в екзаменаційну відомість та залікову книжку здобувача.

V. ВИБІР ТЕМИ КУРСОВОЇ РОБОТИ

Основою курсової роботи є тема, питання дослідження та розробка системи програмно-технічного захисту інформації, які викладені в завданні, що видається керівником в установленому порядку. Тематика курсових робіт повинна бути актуальною, відповідати сучасному стану та перспективам розвитку науки і техніки. Перелік тем курсових проектів складається на початку семестру з урахуванням сучасного стану інформаційних технологій та кібербезпеки, затверджується в установленому порядку. Кількість тем повинна перевищувати кількість студентів, які виконують курсову роботу.

Здобувачам вищої освіти надається право вибору теми курсової роботи самостійно з урахуванням тематики магістерської кваліфікаційної роботи. Студент може запропонувати свою тему курсової роботи з обґрунтуванням необхідності її розробки. До обов'язків керівника входить:

- видача завдання на курсову роботу;
- надання здобувачу допомоги у складанні календарного плану на весь період розробки, у підборі необхідної основної літератури, довідкових даних та інших матеріалів;
- проведення систематичних консультацій, передбачених розкладом;
- перевірка виконаної роботи (по частинах і в цілому);

Згідно Положення про організацію навчального процесу у вищих навчальних закладах тематика курсових проектів (робіт) повинна тісно пов'язуватися з практичними потребами конкретного фаху. Тематика курсової роботи з розробки програмно-технічного захисту інформації повинна відповідати професійним завданням, зафіксованим в освітній програмі. Тематика курсової роботи з розробки програмно-технічного захисту інформації повинна бути актуальною, відповідати сучасним тенденціям та перспективам розвитку комп'ютерних наук. Назва курсової роботи повинна бути короткою та відповідати меті дослідження. У темі не бажано використовувати термінологію популярного характеру. Основним результатом курсової роботи повинен бути програмний продукт прикладного характеру.

Перелік тем курсової роботи з розробки програмно-технічного захисту інформації формується випусковою кафедрою та оновлюється кожного навчального року. Запропоновані теми курсових робіт не повинні бути шаблонними, передбачати вирішення взаємопов'язаних між собою питань, узгоджуватись з інтересами та здібностями студента.

Здобувачі вищої освіти мають право запропонувати свою тему з обґрунтуванням її доцільності та актуальності, або самостійно вибрати із переліку запропонованих. Вибираючи тему дослідження, здобувач вищої освіти повинен насамперед, орієнтуватися на власну зацікавленість тією чи іншою науковою проблемою, на актуальність, елементи новизни і перспективність обраної теми також рекомендується використати досвід та матеріали, отримані під час виконання індивідуального завдання, виконаного при проходженні навчальних та виробничих практик.

VI. АПРОБАЦІЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Апробація являє собою різновид наукової діяльності у формі проведення перевірок результатів дослідження. Мета полягає у встановленні придатності результатів для реалізації конкретних завдань.

Види апробації:

- участь в бесідах та круглих столах на кафедрі з обговоренням результатів роботи;

- представлення доповідей на Днях науки факультету інформаційних технологій і математики;
- публікації в рецензованих журналах результатів проведеного наукового дослідження;
- представлення доповідей в рамках наукових конференцій чи семінарів та публікація тез;
- оприлюднення пропозицій у практичній діяльності підприємства, організації та установи.

VII. ПРОЦЕДУРА ДОПУСКУ КУРСОВОЇ РОБОТИ ДО ЗАХИСТУ

Основною формою контролю освітнього компонента «**Курсова робота з розробки програмно-технічного захисту інформації**» є залік, що проводиться у вигляді публічного захисту.

Допуск здобувача вищої освіти до захисту курсової роботи здійснює науковий керівник. Критерієм допуску є:

- наявність електронного варіанту текстової частини курсової роботи у форматі *.doc* або *.docx* оформленого згідно вимог;
- наявність електронного варіанту працюючої програмної розробки (згідно задачі, поставленої у роботі), поданого у вигляді інсталятора для однієї або кількох із поширених сучасних операційних систем;
- наявний переплетений друкований примірник текстової частини курсової роботи, оформлений згідно вимог, завізований керівником;
- відповідність змісту текстової частини темі курсової роботи;
- наявність в додатках текстової частини курсової роботи технічного завдання та інструкції користувачу для використання програмної розробки;
- наявність відеоролика-представлення програмної розробки;
- дотримання академічної доброчесності під час написання курсової роботи, відповідно до нормативних документів.

Здобувач не допускається до захисту курсової роботи у випадках:

- недотримання критеріїв допуску;
- порушення термінів подачі роботи на кафедру без поважних причин;
- порушень академічної доброчесності.

Результатом виконання курсової роботи є технічні описи, розрахунки, таблиці, моделі, графіки, алгоритми, топології, програми, ескізи, пояснення до них тощо. Ці матеріали оформляються у вигляді пояснювальної записки.

Види, комплектність і оформлення всіх документів курсової роботи повинні відповідати вимогам діючих стандартів, ЄСКД, ЄСДП та інших чинних нормативно-правових документів. Рекомендується оформляти курсову роботу одночасно з роботою над нею.

Кожне висунуте положення повинне бути обґрунтоване розрахунками, фактичним матеріалом і посиланнями на літературні джерела, науково-технічні звіти тощо. Не допускаються посилання на усні вказівки керівників, консультантів, викладачів та інших осіб.

За прийняті в курсовій роботі рішення і за правильність усіх даних відповідає здобувач вищої освіти – автор проекту.

Матеріали курсової роботи подаються українською мовою. В окремих випадках, коли здобувач не має атестації з української мови, йому надається право написання проекту іншою мовою у встановленому порядку.

Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності.

Здобувач вищої освіти має право висловити побажання щодо призначення науковим керівником конкретного викладача і, за умови існування такої можливості, кафедра погоджує запропоновану кандидатуру. Крім того, може враховуватись принцип наступності наукового керівництва студентською науковою та курсовою роботою на попередніх курсах навчання.

Науковий керівник допомагає здобувачу сформулювати актуальну тему курсової роботи, з врахування його наукових та практичних інтересів, видає кожному студенту індивідуальне завдання, затверджує план-графік виконання курсової роботи, надає різноманітні консультації щодо змісту та оформлення роботи, контролює дотримання регламенту її підготовки та дотримання здобувачем академічної доброчесності. Науковий керівник контролює підготовку здобувача до захисту курсової роботи, надає консультації, щодо формування презентації та виступу. Приймає участь у роботі комісії з попереднього захисту.

Здобувач освіти зобов'язаний вчасно звернутися до керівника курсової роботи для надання консультації з приводу вибору та формулювання теми курсової роботи, складання плану написання курсової роботи з зазначенням термінів, вчасно виконувати всі етапи плану написання курсової роботи, дотримання академічної доброчесності згідно ст. 42 Закону України «Про освіту», Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки та Положення про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників ВНУ імені Лесі Українки. На кожному етапі написання курсової роботи здобувач вищої освіти зобов'язаний подавати результати роботи на розгляд керівнику і відповідно до його зауважень уточнювати, доповнювати і в разі потреби їх доопрацьовувати.

Політика щодо академічної доброчесності

Дотримання студентами академічної доброчесності при написанні **«Курсова робота з розробки програмно-технічного захисту інформації»** регламентується ст. 42 Закону України «Про освіту», Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки, Положенням про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників ВНУ імені Лесі Українки.

У разі виявлення науковим керівником у роботі студента одного або кількох видів порушень академічної доброчесності, а саме: академічного плагіату, самоплагіату, фабрикації, фальсифікації, обману до нього можуть бути застосовані види відповідальності, передбачені Кодексом академічної доброчесності Волинського національного університету імені Лесі Українки, зокрема: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми; відрахування з університету; позбавлення академічної стипендії; позбавлення наданих університетом пільг з оплати навчання.

У випадку, якщо порушення виявлені не менш, як за три-чотири тижні до захисту курсової роботи, студенту надається можливість виправити порушення. Якщо порушення виявлені менше, як за два-три тижні до захисту, курсова робота не допускається до захисту, студент отримує оцінку «незадовільно» з можливістю повторного захисту.

Політика щодо дедлайнів та перескладання

Терміни підготовки курсової роботи оголошуються на початку семестру і регламентуються календарним планом.

Курсова робота повинна виконуватись відповідно до затвердженого календарного плану. На кафедрі складається графік консультацій наукових керівників, в якому вказується час і місце їх проведення. Консультації з керівником повинні проводитися не менше, як 1 раз в тиждень. В процесі виконання завдання курсової роботи, здобувач вищої освіти зобов'язаний відвідувати консультації згідно розкладу і звітувати відповідно до графіку про стан готовності курсової роботи. У випадку неявки на 3 контрольні точки перевірки, зазначених в індивідуальному завданні, науковий керівник зобов'язаний довести цю інформацію до відома завідувача кафедри та декана факультету через службову записку.

Захист курсової роботи відбувається відповідно до розкладу заліково-екзаменаційної сесії, затвердженої деканом факультету. Курсова робота, матеріали якої здаються із порушенням термінів без поважних причин, не допускаються до захисту. У випадку, коли здобувач освіти не виконав завдання курсової роботи у зазначені терміни, він має можливість представити курсову роботу до захисту під час ліквідації академічної заборгованості.

Ліквідація академічної заборгованості здійснюється шляхом повторного виконання та захисту курсової роботи за новою темою (у випадку грубих порушень академічної доброчесності), або після виправлення недоліків у даній курсовій роботі та її повторного захисту. Студент може бути допущений до повторного захисту курсової роботи у встановлений термін ліквідації академічної заборгованості. Інші випадки (хвороба, відрядження тощо) регламентуються Положенням про організацію навчального процесу на першому (бакалаврському) та другому (магістерському) рівнях у Волинському національному університеті імені Лесі Українки.

VIII. ПІДСУМКОВИЙ КОНТРОЛЬ

Підсумковою формою контролю освітнього компонента **«Курсова робота з розробки програмно-технічного захисту інформації»** є залік, що проводиться у вигляді публічного захисту. Захист курсової роботи проводиться перед комісією у складі не менше двох викладачів кафедри за участю керівника курсової роботи. Дата захисту передбачається графіком підсумкового семестрового контролю на факультеті.

Захист курсової роботи включає в себе короткий виступ студента з презентацією, його відповіді на запитання членів комісії. У виступі студента відображаються актуальність теми, завдання курсової роботи, її основні результати та демонстрація роботи програмного продукту. Студент повинен продемонструвати вміння відповідати на питання з предметної області курсової роботи, вести наукову дискусію.

Після закінчення процедури захисту комісія ухвалює рішення щодо підсумкової сумарної оцінки за курсову роботу з урахуванням орієнтовних критеріїв. Результати захисту в той же день оголошуються здобувачам вищої освіти. Диференційована оцінка за курсову вноситься в заліково-екзаменаційну відомість, індивідуальний навчальний план (залікову книжку) студента за підписами членів комісії і враховується під час визначення розміру стипендій разом з іншими підсумковими оцінками. У разі отримання підсумкової сумарної оцінки менше 60 балів за 100-бальною шкалою або у випадку, якщо курсова робота не була допущена до захисту, у заліково-екзаменаційній відомості робиться відповідний запис про академічну заборгованість з курсової роботи.

Критерії оцінювання «Курсової роботи з розробки програмно-технічного захисту інформації»

Критерій	Максимальна кількість балів	Примітка
Своєчасність затвердження теми та завдання на курсову роботу	5	Бали не нараховуються у випадку несвоєчасного затвердження теми та завдання.
Якість оформлення пояснювальної записки	20	Бали може бути знижено за порушення вимог до оформлення роботи, невідповідність структури курсової визначеним вимогам та ін.
Алгоритмічна, математична та функціональна складність розробленого проекту програмно-технічного захисту інформації для кібербезпеки	55	Оцінюється якість та коректність побудованих моделей, правильність оформлення алгоритмів та складність структури системи.
Якість підготовленої доповіді та рівень захисту курсової роботи	20	Бали може бути знижено за відсутність презентації (5 балів), некоректні відповіді на питання 10 балів.

VI. ШКАЛА ОЦІНЮВАННЯ

Оцінка в балах за всі види навчальної діяльності	**Оцінка**
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
1–59	Незараховано (з можливістю повторного складання)

IX.Рекомендована література та інтернет-ресурси

Основна

1. Конституція України. Режим доступу: https://zakon.rada.gov.ua/go/254к/96-вр
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах», від 05.07.1994 № 81/94-ВР (Зі змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
5. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
6. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
7. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. 8. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01– 01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).
8. ISO/IEC 27002:2022 (en). Information security, cybersecurity and privacy protection – Information security controls// Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en
9. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
10. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
11. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
12. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.
13. Закон України «Про інформацію» № 2657-ХИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650.Система управління якістю відповідає ДСТУ ISO 9001:2015
14. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).
15. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).
16. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
17. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
18. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
19. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
20. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. 22. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. 23. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
21. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

22. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.
23. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.
24. Lobanchykova, N.M., Pilkevych, I.A., Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. // Joint Proceedings of the Workshops on Quantum Information Technologies and Edge Computing (QuaInT+doors 2021), Zhytomyr, Ukraine, April 11, 2021. Edited by Serhiy O. Semerikov. (CEUR-WS.org). Pp. 83-96. http://ceur-ws.org/Vol-2850/paper6.pdf
25. Ihor Pilkevych, Oleg Boychenko, Nadiia Lobanchykova, Tetiana Vakaliuk, Serhiy Semerikov. Method of Assessing the Influence of Personnel Competence on Institutional Information Security // Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, CEUR Workshop Proceedings, Khmelnytskyi, Ukraine, March 24–26, 2021. Edited by Tetiana Hovorushchenko, Oleg Savenko, Peter Popov, Sergii Lysenko. Pp. 266-275. http://ceur-ws.org/Vol-2853/paper33.pdf
26. N Lobanchykova, S Kredentsar, I Pilkevych and M Medvediev. Information technology for mobile perimeter security systems creation// Journal of Physics: Conference Series, Volume 1840, 012051, XII International Conference on Mathematics, Science and Technology Education (ICon-MaSTEd 2020) 15-17 October 2020, Kryvyi Rih, Ukraine. DOI: 10.1088/1742- 6596/1840/1/012022.
27. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с.
28. Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World/ Joseph Menn.– New York: PublicAffairs, 2019.– 270.

Допоміжна література

29. Грайворонський М.В. Безпека інформаційно-комунікаційних систем/ М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009.– 608с. 41. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с. Режим доступу: Комплексні системи захисту інформації /
30. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. / 2017 (vntu.edu.ua)
31. Akhmetov, B., Lakhno, V. (2018). System of decision support in weaklyformalized problems of transport cybersecurity ensuring, Journal of Theoretical and Applied Information Technology, 96 (8), pp. 2184-2196.
32. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1 (2-85), pp. 4-15.
33. Akhmetov, B., Lakhno, V., Malyukov, V., Sarsimbayeva, S., Zhumadilova, M., Kartbayev, T. (2019). Decision support system about investments in smart city in conditions of incomplete information, International Journal of Civil Engineering and Technology, 10 (2), pp. 661-670/
34. Інформаційні ресурси в Інтернеті
35. Стандарти інформаційної безпеки: http://www.is-standard.com 52. Інформаційна безпеки: науковий журнал: http://www.nbuv.gov.ua/portal/natural/Ibez/index.html

36. Центр інформаційної безпеки: http://www.bezpeka.com
37. Журнал «Інформаційні технології. Аналітичні матеріали»: http://it.ridne.net/taxonomy/term/14
38. Положення про організацію освітнього процесу в Волинському національному університет https://ed.vnu.edu.ua/wp-content/uploads/2024/09/%D0%9D%D0%90%D0%9A%D0%90%D0%97-%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D0%BE%D1%81%D0%B2%D1%96%D1%82.-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%83-2024_25-%D0%BD.%D1%80.-.pdf
39. Кодекс академічної доброчесності ВНУ ім. Лесі Українки http://ra.vnu.edu.ua/wp-content/uploads/2023/06/Kodeks-akademichnoyi-dobrochesnosti.pdf
40. Положення про систему запобігання та виявлення академічного плагіату в науковій та навчальні діяльності ЗО, докторантів, науково-педагогічних і наукових працівників ВНУ ім. Лесі Українки https://ra.vnu.edu.ua/akademichna_dobrochesnist/

41. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
42. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія /Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016 – 636 с.
43. Kevin Mitnick. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big./ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, 2017 – 320 с.
44. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.
45. Лобанчикова Н.М. Основи побудови автоматизованих систем управління : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, І. І. Сугоняк, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 174 с.
46. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території .Сучасний захист інформації, 2020.Вип №1(41). С.42 – 48. 36. Матвійко А.В. Управління ІТ-проектами. – Львів: Новий світ-200, 2017. – 550 с.
47. Kevin Mitnick. Ghost In The Wires: My Adventures as the World's Most Wanted Hacker/ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, Back Bay Books, 2012 – 448 с.