Заклад вищої освіти
«Міжнародний науково-технічний університет
імені академіка Юрія Бугая»

Кафедра комп'ютерних наук та інженерії програмного забезпечення

СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Силабус навчальної дисципліни

на 2021/2022 навчальний рік

Реквізити навчальної дисципліни		
Рівень вищої освіти	Другий (магістерський)	
Галузь знань	12 «Інформаційні технології»	
Спеціальність	122 «Комп'ютерні науки»	
Освітня програма	«Комп'ютерні науки»	
Статус дисципліни	Нормативна	
Форма навчання	Денна	
Рік підготовки, семестр	І курс, 2 семестр	
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	3 кредити/90 годин	
Семестровий контроль/ контрольні заходи	Модульний контроль	
Мова викладання	Українська	
Формат навчальної дисципліни	Змішаний (blended)	
Викладач(і)		**МОСКАЛЕНКО АРТЕМ ОЛЕКСІЙОВИЧ** **Посада:** завідувач кафедри комп'ютерних наук та інженерії програмного забезпечення **Науковий ступінь:** кандидат технічних наук **Вчене звання:** - **Профайл викладача:** https://istu.edu.ua/комп'ютерні_науки_та_інженерія_програмного_забезпечення **Телефон:** +380664495928 **E-mail:** a.moskalenko@istu.edu.ua
Розміщення курсу	**Код курсу Google classroom:** e6y527b **Посилання Meet:** https://meet.google.com/lookup/ewxspe46db	

Програма навчальної дисципліни

1. Опис навчальної дисципліни

Метою навчальної дисципліни «Системи інформаційної безпеки» є ознайомлення здобувачів вищої освіти з сучасними методами та засобами забезпечення інформаційної безпеки, порядком проектування, впровадження та супроводження комплексної системи захисту інформації, системою управління інформаційною безпекою, підготовка фахівців, здатних аналізувати, обирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки та цілісності даних відповідно до розв'язувальних прикладних завдань.

Предмет вивчення навчальної дисципліни: сучасні методи та засоби забезпечення інформаційної безпеки, комплексна система захисту інформації, система управління інформаційною безпекою.

Компетентності у відповідності до освітньо-професійної програми:

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК8. Здатність працювати в команді.

ЗК9. Здатність оцінювати та забезпечувати якість виконуваних робіт.

СК3. Здатність збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

СК10. Здатність використовувати програмні інструментами для організації командної роботи над проєктом.

СК12. Здатність оцінювати якість ІТ-проєктів, комп'ютерних і програмних систем різного призначення, володіти методологіями, методами і технологіями забезпечення та вдосконалення якості ІТ-проєктів, комп'ютерних та програмних систем на основі міжнародних стандартів оцінки якості програмного забезпечення інформаційних систем, моделей оцінки зрілості процесів розробки інформаційних та програмних систем.

СК15. Здатність аналізувати, вибирати та застосовувати методи і засоби забезпечення інформаційної безпеки в комп'ютерних системах різного призначення.

СК16. Здатність оцінювати та забезпечувати надійність, функційну та інформаційну безпечність комп'ютерних систем на всіх етапах життєвого циклу.

Програмні результати навчання у відповідності до освітньо-професійної програми:

ПРН3. Аналізувати проміжні результати розробки або дослідження з метою з'ясування їх відповідності вимогам; розробляти тести та використовувати засоби верифікації, щоб переконатися у якості прийнятих рішень.

ПРН4. Аналізувати предметну область розробки або дослідження, використовуючи наявну документацію, консультації з стейкхолдерами; розробляти документацію, що фіксує як функціональні, так і нефункціональні вимоги до розробки чи дослідження.

ПРН7. Володіти принципами, техніками та засобами розробки або дослідження, що використовуються у предметній області розробки або дослідження; створювати прототипи програмного забезпечення, щоб переконати-ся, що воно відповідає вимогам до розробки; виконувати його тестування і статичний аналіз, щоб переконатися у відповідності завданню розробки або дослідження.

ПРН9. Демонструвати здатність участі у колективній роботі, використання інструментів колективної розробки чи дослідження.

ПРН14. Знати, аналізувати, вибирати, кваліфіковано застосовувати методи і засоби забезпечення інформаційної безпеки при створенні та супроводі комп'ютерних систем.

ПРН15. Визначати вимоги до надійності, функційної та інформаційної безпечності комп'ютерних систем, методи забезпечення їх надійності, розробляти програми та методики випробувань, оцінювати надійність та якість комп'ютерних систем.

Результати навчання за дисципліною (РН):

РН 1. Принципи та основи побудови захищених інформаційних систем, організація захисту персональних даних.

РН 2. Захист програмного забезпечення та даних, мережевого трафіку та контроль доступу з використанням існуючих механізмів та засобів.

РН 3. Проектування, впровадження та супроводження комплексної системи захисту інформації у відповідності до вимог керівних документів.

РН 4. Управління інформаційною безпекою з використанням сучасних технологій та методів.

2. Пререквізити та постреквізити

Пререквізити: базові знання в галузі інформаційних технологій.

Постреквізити: «Криптографічні методи захисту інформації в ІС», «Мережева безпека», «Переддипломна практика», «Дипломне проектування».

3. Зміст навчальної дисципліни

ЗМІСТОВНИЙ МОДУЛЬ №1. БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Тема 1. Основні поняття безпеки інформаційних систем.

Тема 2. Криптографічний захист інформації.

Тема 3. Безпека програм та даних.

Тема 4. Мережева та Веб безпека.

ЗМІСТОВНИЙ МОДУЛЬ №2. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Тема 5. Етапи проектування комплексної системи захисту інформації.

Тема 6. Порядок впровадження комплексної системи захисту інформації.

Тема 7. Супроводження комплексної системи захисту інформації.

Тема. 8. Система управління інформаційною безпекою.

4. Навчальні матеріали та ресурси

Основні:

1. Програмні технології захисту інформації: конспект лекцій для студентів за напрямом підготовки 6.050103 «Програмна інженерія» факультету інформаційних технологій УжНУ / Розробник: к.т.н. Поліщук В.В. – Ужгород: 2018. – 80 с.

2. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.

4. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

Додаткові:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/ show/80.

2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Дер спецзв'язку // 2015 - Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/ publish/article?art id=46074.

3. Вербіцький О.В. Вступ до криптології Львів: Науково-технічна література, 1998. — 248 с.

4. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

7. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

11. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

12. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

13. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

14. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Інформаційні ресурси:

Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/.

Навчальний контент

5. Методика опанування навчальної дисципліни

№ тижня	Тема	Заняття	Результат навчання	Контрольний захід
ЗМІСТОВНИЙ МОДУЛЬ №1. БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ				
1	**Т №1.** Основні поняття безпеки інформаційних	**Л №1.** Основні поняття безпеки інформаційних систем	РН №№ 1-2	МК №1
2		**ПЗ №1.** Дослідження моделей	РН №№ 1-2	МК №1,

	систем	розмежування прав доступу		захист ПЗ №1
3	**Т №2.** Криптографічний захист інформації	**Л №2.** Криптографічні методи та засоби захисту інформації	РН № 2	МК №1
4		**ПЗ №2.** Дослідження можливостей Bouncy Castle Crypto package	РН № 2	МК №1, захист ПЗ №2
5	**Т №3.** Безпека програм та даних	**Л №3.** Безпека програм та даних	РН № 2	МК №1
6		**ПЗ №3.** Дослідження можливостей сучасного антивірусного програмного забезпечення	РН № 2	МК №1, захист ПЗ №3
7	**Т №4.** Мережева та Веб безпека	**Л №4.** Мережева та Веб безпека	РН № 2	МК №1
8	**Презентація та захист індивідуального завдання Модульний контроль №1**			
ЗМІСТОВНИЙ МОДУЛЬ №2. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ				
9	**Т №5.** Етапи проектування комплексної системи захисту інформації	**Л №5.** Етапи проектування комплексної системи захисту інформації	РН № 3	МК №2
10	**Т №6.** Порядок впровадження комплексної системи захисту інформації	**Л №6.** Порядок впровадження комплексної системи захисту інформації	РН № 3	МК №2
11	**Т №7.** Супроводження комплексної системи захисту інформації	**Л №7.** Супроводження комплексної системи захисту інформації	РН № 3	МК №2
12		**ПЗ №4.** Розробка технічного завдання на створення комплексної системи захисту інформації	РН № 3	МК №2, захист ПЗ №4
13		**ПЗ №5.** Розробка технічного завдання на створення комплексної системи захисту інформації	РН № 3	МК №2, захист ПЗ №5
14	**Т №8.** Система управління інформаційною безпекою	**Л №8.** Система управління інформаційною безпекою	РН № 4	МК №2
15		**ПЗ №6.** Розробка технічного завдання на створення комплексної системи захисту інформації	РН № 4	МК №2, захист ПЗ №6
16	**Презентація та захист індивідуального завдання Модульний контроль №2**			

6. Самостійна робота здобувача вищої освіти

Основними видами самостійної роботи здобувачів вищої освіти з навчальної дисципліни «Системи інформаційної безпеки» є: самостійне опрацювання навчального матеріалу, підготовка до аудиторних занять (практичних занять, підсумкових контролів, захисту проектних завдань), виконання проектних завдань.

Програмою навчальної дисципліни «Системи інформаційної безпеки» передбачено виконання двох проектних завдань у першому та другому змістовних модулях відповідно.

Проектне завдання виконується командою у складі від трьох до п’яти здобувачів. На протязі першого тижня вивчення кожного із змістовних модулів дисципліни під керівництвом викладача здійснюється розподіл здобувачів по проектним командам. Розподіл здійснюється з урахуванням побажання здобувачів вищої освіти. Далі у кожній команді відбувається розподіл ролей. На наступному етапі кожна проектна команда обирає тематику проектного завдання. Тематика проектного завдання обирається або з переліку, запропонованого викладачем, або за пропозиціями проектних команд. Для кожної проектної команди на протязі першого тижня складається Картка планування проекту. Проектні завдання виконуються командою на протязі вивчення кожного із змістовних модулів дисципліни під керівництвом викладача та із залученням, за необхідності, відповідних фахівців галузі. Завершальним етапом виконання проектного завдання є презентація та захист проекту членами команди.

Політика та контроль

7. Політика навчальної дисципліни

Організація освітнього процесу

Згідно графіку навчального процесу, за розкладом занять, який розміщено на офіційному сайті МНТУ.

Правила відвідування занять

Здобувачі вищої освіти мають відвідувати аудиторні заняття згідно з розкладом, без запізнень. Освітня діяльність та відвідування здобувачами вищої освіти занять регламентується «Положенням про організацію освітнього процесу в МНТУ» та «Правилами внутрішнього розпорядку для студентів МНТУ».

Пропущені заняття відпрацьовуються в часи самостійної підготовки та у встановлені викладачем терміни.

Відвідування лекцій, практичних занять, а також відсутність на них, не оцінюється. Проте, здобувачам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал та демонструються різноманітні методи розв’язування прикладних задач, розвиваються навички та вміння в області забезпечення безпеки інформаційних систем.

Правила поведінки на заняттях

Норми етичної поведінки учасників академічної спільноти визначені у Кодексі академічної етики ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила захисту практичних робіт

Звіти з практичних робіт, оформлені у відповідності до вимог методичних рекомендацій, повинні бути захищені не пізніше наступного практичного заняття. Звіт з останнього практичного заняття повинен бути захищений до дня захисту індивідуального завдання.

Захист звітів з практичних робіт може проводитись: безпосередньо під час поточного практичного заняття, на наступному практичному занятті, у час, що відведений для консультацій.

Правила захисту проектних завдань

Проектні завдання, виконані та оформлені у відповідності до вимог методичних рекомендацій, повинні бути захищені не пізніше останнього заняття (модульного контролю) із відповідного змістовного модулю дисципліни.

Презентація та захист проектних завдань, як правило, відбувається у повному складі проектної команди, крім випадків, визначених положеннями МНТУ.

Захист проектних завдань може проводитись: під час проведення практичних занять, на останньому занятті (модульному контролі) із відповідного змістовного модулю дисципліни, у час, що відведений для консультацій.

Процедура оскарження результатів контрольних заходів оцінювання

Після отримання коментарів від викладача з аргументацією щодо оцінки, здобувач вищої освіти має право в індивідуальному порядку задати всі питання, які його/її цікавлять стосовно результатів контрольних заходів оцінювання. Якщо здобувач вищої освіти категорично не погоджуються з оцінкою, він/вона мають також навести аргументи щодо своєї позиції.

Порядок подання апеляційних скарг на результати підсумкового контролю визначено у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила призначення заохочувальних та штрафних балів

Заохочувальні бали		**Штрафні бали**	
Критерій	**Бал**	**Критерій**	**Бал**
Участь у міжнародних, всеукраїнських або інших заходах (конкурсах) за тематикою навчальної дисципліни	3 бали	Порушення термінів виконання та захисту звітів з практичних робіт (за кожну роботу)	-2 бали
Опитування на лекційному занятті (опитування на одному занятті)	2 бали	Порушення термінів виконання, презентації та захисту проектних завдань (за кожне завдання кожному члену проектної команди)	-4 бали
Вдосконалення навчально-матеріальної бази кафедри	≤ 5 балів		
Участь у роботі наукового гуртка кафедри за тематикою навчальної дисципліни	5 балів	Злісне невиконання мір техніки безпеки при проведенні навчальних занять (за кожний випадок)	-5 балів

Політика дедлайнів та перескладань

Усі завдання виконуються у зазначені дати та час. Здобувачі несуть відповідальність за управління своїм часом, щоб завдання та проекти могли бути подані до встановленого терміну.

Політика перескладань визначена у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Загальна оцінка після перескладання (ліквідації академічної заборгованості) знижується на 10%.

Політика щодо академічної доброчесності

Обов’язкове дотримання академічної доброчесності та недопущення плагіату під час виконання завдань.

Дотримання умов «Положення про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ЗВО «МНТУ» та Кодексу академічної етики.

Списування під час виконання контрольних робіт та модульних тестів заборонені (у т.ч. із використанням мобільних девайсів).

Плагіат у творчих роботах та презентаціях – заборонений.

8. Види контролю та рейтингова система оцінювання результатів навчання

Рейтингова система оцінювання результатів навчання здобувачів вищої освіти

здійснюється відповідно до:

– Положення про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»;

– умов і критеріїв, визначених у цьому силабусі.

Система оцінювання та вимоги

Система оцінювання навчальної дисципліни	Оцінювання упродовж кожного змістовного модуля здійснюється за 100 бальною системою (до 40 балів за поточний контроль, до 60 балів за модульний контроль).
Практичні заняття	Максимальна кількість балів за кожне практичне заняття – 10 балів. 0 балів – не виконання відповідного завдання без поважних причин. 1 бал – виконання відповідних завдань без оформлення звіту з кількома помилками. 2 бали - виконання відповідних завдань без оформлення звіту з незначною кількістю помилок. 3 бали - виконання завдання та оформлення звіту з кількома негрубими помилками. 4 бали - виконання завдання та оформлення звіту з незначною кількістю помилок. 5-6 балів - виконання завдання, оформлення та захист звіту з незначною кількістю грубих помилок. 7-8 балів - виконання завдання, оформлення та захист звіту з кількома негрубими помилками. 9-10 балів – виконання завдання, оформлення та захист звіту з незначною кількістю помилок. При здійсненні оцінювання враховуються наявні штрафні бали для даного заняття.
Проектні завдання	Максимальна кількість балів за кожне проектне завдання – 10 балів. Кожний член проектної команди оцінюється індивідуально. Складовими частинами індивідуального оцінювання проектного завдання є: ➢ 0-4 балів – презентація та захист проектного завдання командою; ➢ 0-3 балів – виконання індивідуального звіту, оформленого у відповідності до вимог; ➢ 0-3 балів – індивідуальна участь в проекті кожного учасника проектної команди. При здійсненні оцінювання враховуються наявні штрафні бали для даного виду діяльності.
Умови допуску до підсумкового (модульного) контролю	Виконання всіх практичних завдань за відповідним змістовним модулем. Виконання проектного завдання відповідного змістовного модулю. Наявність не менше 20 балів за поточну успішність.

Середньозважений бал за навчальну дисципліну визначається як середній арифметичний бал всіх результатів модульних контролів.

Оцінювання навчальних досягнень здобувачів вищої освіти за всіма видами контролю – здійснюється за національною системою та ECTS.

Шкала оцінювання успішності студентів

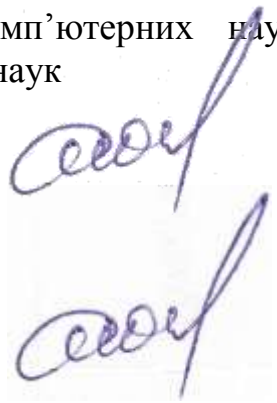
СУМА БАЛІВ	ОЦІНКА ECTS	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		екзамен	**залік**
90-100	A	відмінно	зараховано

82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно	не зараховано
34-0	F	незадовільно	

9. Додаткова інформація з дисципліни (за потреби)

Силабус навчальної дисципліни:
складено завідувачем кафедри комп'ютерних наук та інженерії програмного забезпечення, кандидатом технічних наук

Артемом МОСКАЛЕНКО



«Погоджено»
Гарант освітньої програми

Артем МОСКАЛЕНКО