

НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ТРАНСПОРТНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ:

Завідувач кафедри інформаційних систем і технологій

проф. В.В. Гавриленко _____
_____ 2020 р.

**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**

Рівень вищої освіти	Перший (бакалаврський)
Спеціальність	121 Інженерія програмного забезпечення Інженерія програмного забезпечення
Освітня програма	http://vstup.ntu.edu.ua/osvitprog/FTIT/121IPZ_2020.pdf
Тип дисципліни	Обов'язкова
Форма навчання	Денна
Семестр	6-й семестр навчального плану
Розробник	Аль-Аморі Алі Нурддинович, д.тех.н., професор e-mail
Викладач	викладача:
Доступ до матеріалів	http://vstup.ntu.edu.ua/sam_dis_ipz.pdf
Кафедра	інформаційних систем і технологій Тел. кафедри: +38 (044) 280-70-66 Веб-сайт кафедри: http://kist.ntu.edu.ua/
Гарант освітньої програми	к.ф.-м. н., доцент Вітер Михайло Богданович

1. АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни – вивчення технологій, методів та засобів захисту інформації у комп'ютерних системах, набуття ключових фахових компетентностей, теоретичних знань і практичних навичок з технологій захисту інформації у комп'ютерних системах у різних сферах професійної діяльності.

Завдання навчальної дисципліни – формування у студентів чіткого уявлення про сучасні технології, методи та підходи, програмно -технічні засоби захисту інформації у комп'ютерних системах, отримання теоретичних знань, вмінь та практичних навичок щодо використання технологій, методів і засобів захисту інформації у комп'ютерних системах.

Мова викладання: українська.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

У результаті вивчення навчальної дисципліни студент повинен отримати:
знання основних понять, методів, засобів, моделей та алгоритмів захисту інформації у комп'ютерних системах;

розуміння принципів та теоретичних основ застосування технологій захисту інформації;

уміння вільно орієнтуватися у сучасних підходах, технологіях і інструментарії захисту інформації у комп'ютерних системах; здійснювати оцінку наявних ресурсів та реалізовувати комплексних захист інформації у комп'ютерних системах, використовуючи симетричні та асиметричні алгоритми шифрування, цифровий підпис, здійснювати розподіл та управління криптоключами, застосовувати програмне забезпечення та технічні засоби для виявлення вторгнень; реалізовувати багаторівневий захист інформації у комп'ютерних системах та здійснювати управління засобами захисту інформації

здатність використовувати теоретичні знання і практичні навички для реалізації комплексної системи захисту інформації у комп'ютерних системах за допомогою сучасних технологій, здійснювати аналіз захищеності та можливих ризиків для комп'ютерних систем, оптимального розподілу наявних ресурсів для побудови багаторівневого захисту інформації.

КОМПЕТЕНТНОСТІ

Загальні компетентності

- K01. Здатність до абстрактного мислення, аналізу та синтезу.
- K02. Здатність застосовувати знання у практичних ситуаціях.
- K03. Здатність спілкуватися державною мовою як усно, так і письмово.
- K06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові, предметні) компетентності

- K13. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.
- K14. Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування.
- K18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).
- K19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.
- K20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.
- K31. Здатність застосовувати на практиці сучасні інформаційні технології відповідно до розв'язуваних прикладних завдань.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

ПР01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПР05. Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об'єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.

ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних обчислювальних засобів інженерії програмного забезпечення.

ПР09. Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення

ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

ПР27. Вміти розробляти і застосовувати програмне забезпечення для підвищення якості, безпеки, рівня автоматизації та інтелектуалізації транспортних процесів і систем.

ПР29. Вміти вибирати та застосовувати на практиці сучасні інформаційні технології відповідно до розв'язуваних прикладних завдань.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Види робіт за навчальним планом	Години
Аудиторні заняття, у т.ч.:	48
Лекції	16
Лабораторні роботи	32
Практичні заняття	–
Самостійна робота, у т.ч.:	57
Підготовка до аудиторних занять	12
Підготовка до контрольних заходів	4
Виконання курсової роботи	–
Опрацювання питань програми, які не викладаються на лекціях	37
Підготовка до екзамену	4
Всього:	105 (3,5 кредити)
Форма підсумкового контролю	Екзамен

ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Найменування
Опорний конспект лекцій

Навчальні посібники
Силабус
Програмне забезпечення: C++, Java, Python
Комплект контрольних завдань для поточного оцінювання навчальних досягнень
Засоби підсумкового контролю (комплект завдань для підсумкового контролю)

3. ОРГАНІЗАЦІЯ НАВЧАННЯ

Назви змістових модулів і тем лекцій	Кількість годин			
	усього	у тому числі		
		лекції	Лабор.	самостійна робота
Тема 1. Проблеми інформаційної безпеки				
1. Основні поняття інформації, її захисту та безпеки.	13	2	4	7
2. Аналіз загроз інформаційної безпеки.	13	2	4	7
Тема 2. Технології захисту даних				
3. Симетричні та асиметричні криптосистеми шифрування, цифровий підпис	14	2	4	8
4. Основні поняття автентифікації та авторизації. Адміністрування користувачів.	13	2	4	7
Тема 3. Багаторівневий захист корпоративних мереж				
5. Захист інформації при роботі з мережевими ресурсами.	13	2	4	7
6. Захист відділеного доступу. Протоколи централізованого контролю віддаленого доступу.	13	2	4	7
Тема 4. Технологія виявлення вторгнень та управління засобами захисту інформації				
7. Аналіз цілісності системи захисту інформації	13	2	4	7
8. Комп'ютерні віруси і проблеми антивірусного захисту	13	2	4	7
Усього годин за рік	105	16	32	57

ЛАБОРАТОРНІ РОБОТИ

№	Назва теми	Кількість годин
1	Шифри простої заміни, шифр Цезаря.	4
2	Шифр Віженера (індивідуальний зсув кожної літери).	6
3	Шифри складної заміни, парний шифр.	5
4	Шифри підстановки (квадрат Полібія).	5
5.	XOR-кодування. (Схема С. Р. Вернама)	6

6.	Шифри перестановки. Постовпцова транспозиція	6
	Всього	32

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Антонюк А.О. Основи захисту інформації, в автоматизованих системах. Навч. посібн. - К.: Видави, дім “КМ Академія”, 2003. - 244 с.
2. Вертузаев М.С.,Юрченко О.М. Захист інформації в комп’ютерних системах від несанкціонованого доступу: Навч. посібник /За редак. С.Г. Лаптева.- К.:Вид-во Європ. Університету, 2001.- 321 с.
3. Герасименко В. А. Основы защиты информации: Учебник для вузов-/ Б. А. Герасименко, А. А. Малюк. — М.: Изд-во ООО «Ин-комбук», 1997. - 537 с.
4. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навчальний посібник/За заг. ред. М.Я. Азарова. - Ірпінь: Академія ДПС України, 2003. - 466 с.
5. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2008. - 448 с.
6. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб, пособие для вузов / П.Ю. Белкин, О. О.Михальский, А. С. Першаков. - М.: Радио и связь, 1999. - 168 с.
7. Столлингс В. Криптография и защита сетей: теория и практика. - М.: Вильямс. - 2001.
8. Чижухин Г.Н. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учеб. Пособие'. - Пенза: Изд-во Пенз. гос. ун-та, 2001. - 164 с.; 19 ил., 5 табл., библиогр. 8 назв.
9. Шаньгин В.Ф. Защита компьютерной информации. – М.: Изд. ДКМ Пресс, 2010. - 544 с.
- 10.Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: Изд. Форум-Инфра, 2008. - 418 с.
11. José Luis Gómez Pard. Introduction to Cryptography with Maple Springer-Verlag. Berlin Heidelberg, 2013. -, 705 p

Електронні ресурси

http://www.nsa.gov/ia/programs/suiteb_cryptography/
<http://www.rsa.com/rsalabs/node.asp?id=2125>
<http://www.dtc.umn.edu/odlyzko/doc/future.of.factoring.pdf>
http://www.gutenberg.org/wiki/Main_Page
http://www.citforum.ru/internet/infsecure/its2000_01.shtml
http://www.3dnews.ru/software/microsoft_security_essentials/
<http://www.cyberguru.ru/networks/network-security/botnet.html>

4. ПОРЯДОК ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Методи поточного контролю: поточне тестування, індивідуальне та фронтальне опитування, перевірка індивідуальних завдань.

Методи модульного контролю: письмова контрольна робота.

Методи підсумкового контролю: екзамен

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ ЗА МОДУЛІ

Поточне оцінювання змістових модулів							Екзамен	Сума
	ЗМ1	ЗМ2	МК1	ЗМ3	ЗМ4	МК2	40	100
	10	10	10	10	10	10		
Присутність на лекціях	2	2		2	2			
Присутність на ЛР	2	2		2	2			
Виконання та захист ЛР	6	6		6	6			

Модульна оцінка (максимальна кількість балів – 30) складається із:

- присутності студента на лекціях (максимальна кількість балів – 4);
- присутності на лабораторних заняттях (максимальна кількість балів – 4);
- виконання та захисту лабораторних робіт (максимальна кількість балів – 12);
- модульної контрольної роботи (максимальна кількість балів – 10).

Модульна контрольна робота МК1 та МК2 складається з 4 питань теоретичного курсу та 1 практичного завдання. Максимальна кількість балів за кожне питання:

- за повністю розкритою відповіддю на питання та вірно виконане завдання студент одержує 2 бали;
- якщо у відповіді не повністю розкрито сутність питання та допущені невірні тлумачення, студент одержує 1 бал;
- якщо студент не надав відповідь на питання, повністю не виконано завдання, або допущено принципові помилки, – студент одержує 0 балів.

Екзамен (максимальна оцінка за екзамен – 40 балів). Завдання до заліку складається з трьох питань теоретичного курсу та 1 практичного завдання.

Максимальна кількість балів за кожне питання та завдання:

- за повністю розкритою відповіддю на питання та вірно виконане завдання студент одержує 10 балів;
- якщо студент дав відповідь на питання і виконав завдання, допустивши не принципові помилки, студент одержує 7 балів;
- якщо у відповіді не повністю розкрито сутність питання та допущені невірні тлумачення, студент одержує 3 бали;
- якщо студент не надав відповідь на питання, не виконав завдання, або виконав завдання з принциповими помилками, тоді він одержує 0 балів.

Підсумкова оцінка з дисципліни визначається як сума балів за всі види навчальної діяльності.

ШКАЛА ОЦІНЮВАННЯ

Сума балів за всі види навчальної	Оцінка ECTS	Оцінка за національною шкалою
		для заліку, курсового проекту (роботи), практики

діяльності		
90 – 100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	
60-63	E	задовільно
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

5. ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Форми організації освітнього процесу, види навчальних занять і оцінювання результатів навчання регламентуються [Положенням про організацію освітнього процесу в Національному транспортному університеті](#) та [Положенням про систему внутрішнього забезпечення якості вищої освіти](#).

Інформація про мету, завдання, структуру і порядок вивчення навчальної дисципліни надається здобувачам на початку семестру у вигляді **навчально-методичного комплексу (НМК)**, склад якого регламентується [Переліком навчально-методичного забезпечення дисциплін](#).

Політика виставлення оцінок: кожна оцінка виставляється відповідно до розроблених викладачем та заздалегідь оголошених студентам критеріїв, а також мотивується в індивідуальному порядку на вимогу студента; у випадку не виконання студентом усіх передбачених навчальним планом видів занять (лабораторних робіт, курсової роботи) до заліку він не допускається; пропущені заняття обов'язково мають бути відпрацьовані.

Відвідування є обов'язковим (за винятком випадків, коли існує поважна причина, наприклад, хвороба чи дозвіл працівників деканату). У деяких випадках можливе зарахування окремих тем, модулів дисципліни, що регламентується [Тимчасовим положенням про порядок визнання результатів навчання, набутих студентами Національного транспортного університету у неформальній/інформальній освіті](#).

Порядок зарахування пропущених занять. Відпрацювання пропущеного заняття з лекційного курсу здійснюється шляхом підготовки і захисту реферату за відповідною темою у вигляді презентації відповідно до графіку консультацій викладача. Відпрацювання пропущеного лабораторного заняття здійснюється шляхом самостійного виконання завдання і його захисту відповідно до графіку консультацій викладача.

Політика академічної доброчесності. Плагіат та інші форми нечесної роботи неприпустимі. Всі індивідуальні завдання та курсову роботу студент має виконати самостійно із використанням рекомендованої літератури й отриманих знань та навичок. Цитування в письмових роботах допускається тільки із відповідним посиланням на авторський текст. Недопустимі підказки і списування у ході захисту лабораторних робіт, на контрольних роботах, на іспиті. Дотримання академічної

доброчесності студентів і викладачів регламентується [Положенням про систему забезпечення академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти в Національному транспортному університеті](#) та вимогами [Антикорупційної програми](#).

Норми академічної етики – дисциплінованість; дотримання субординації; чесність; відповідальність; робота в аудиторії з відключеними мобільними телефонами – задекларовані у [Кодексі етики академічних взаємовідносин та доброчесності Національного транспортного університету](#).

При виконанні лабораторних робіт студент може користуватися ноутбуками. Проте під час лекційних занять та обговорення завдань лабораторних робіт не слід використовувати ноутбуки, смартфони, планшети чи комп'ютери. Це відволікає викладача і студентів групи та перешкоджає навчальному процесу. Якщо ви використовуєте свій ноутбук чи телефон для аудіо- чи відеозапису, необхідно заздалегідь отримати дозвіл викладача. Повага один до одного дає можливість ефективніше досягати поставлених командних результатів.

Конфліктні ситуації мають відкрито обговорюватись в академічних групах з викладачем, необхідно бути взаємно толерантним, поважати думку іншого. Для запобігання конфліктних ситуацій в НТУ є можливість скористатися «Скринькою довіри» відповідно до [Положення про функціонування у Національному транспортному університеті «Скриньки довіри» з питань запобігання виникненню конфліктних ситуацій](#),