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

# БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

| | |
|---|---|
| **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 Викладач** | Вітер Михайло Богданович, к.ф.-м.н., доцент. e-mail викладача: mbviter@gmail.com |
| **Доступ до матеріалів** | http://vstup.ntu.edu.ua/sam_dis_ipz.pdf |
| **Кафедра** | інформаційних систем і технологій<br>Тел. кафедри: +38 (044) 280-70-66<br>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 для забезпечення безпеки програм та даних, набуття ключових фахових компетентностей, теоретичних знань і практичних навичок з безпеки програм та даних у різних сферах професійної діяльності.

– **Завдання** навчальної дисципліни – формування у студентів чіткого уявлення про сучасні технології, методи та організаційні та програмно -технічні засоби забезпечення безпеки програм та даних, отримання теоретичних знань, вмінь та практичних навичок щодо використання технологій, методів і засобів для реалізації заходів безпеки програм та даних.

**Мова викладання**: українська.

## 2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Безпека програм та даних» покликана допомогти студенту отримати:

**знання** основних понять, методів, засобів, моделей та алгоритмів для реалізації засобів безпеки програм та даних;

**розуміння** принципів застосування технологій захисту програм та даних;

**уміння** вільно орієнтуватись у сучасних підходах, методах та засобах захисту програм та даних, методах, особливостях і програмно-апаратному інструментарію аналізу програм та даних, ускладнювати структуру програм та алгоритми обробки даних для посилення безпеки програм та даних, використовувати криптографічні алгоритми захисту програм і даних, аналізувати шляхи впровадження і протидіяти впровадженню і маскуванню різних типів програмних закладок, протидія хисту програм та данихти комп'ютерним вірусам (яки спеціальному класу програмних закладок), використовувати сучасне програмне забезпечення для реалізаії безпечного функціонування програм та даних при обробці інформації;

**здатність** використовувати можливості сучасних підходів, інструментарію і програмних засобів для реалізації заходів для безпечного функціонування програм та обробки даних.

## КОМПЕТЕНТНОСТІ

### Загальні компетентності

К01. Здатність до абстрактного мислення, аналізу та синтезу.

К02. Здатність застосовувати знання у практичних ситуаціях.

К03. Здатність спілкуватися державною мовою як усно, так і письмово.

К06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

### Спеціальні (фахові, предметні) компетентності

.

К13. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

К14. Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування.

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

К20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.

К29. Здатність розробляти і застосовувати програмне забезпечення для підвищення якості, безпеки, рівня автоматизації та інтелектуалізації транспортних процесів і систем.

К31. 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.

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

ПР13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.

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.:** | **64** |
| Лекції | 16 |
| Лабораторні роботи | 48 |
| Практичні заняття | – |
| **Самостійна робота, у т.ч.:** | **56** |
| Підготовка до аудиторних занять | 16 |
| Підготовка до контрольних заходів | 4 |
| Виконання курсової роботи | – |
| Опрацювання питань програми, які не викладаються на лекціях | 32 |
| Підготовка до заліку | 4 |
| **Всього:** | **120** (4 кредити) |
| **Форма підсумкового контролю** | **Залік** |

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

| Найменування |
|---|
| Опорний конспект лекцій |
| Навчальні посібники |
| Силабус |

| |
|---|
| Програмне забезпечення: C++, Java |
| Комплект контрольних завдань для поточного оцінювання навчальних досягнень |
| Засоби підсумкового контролю (комплект завдань для підсумкового контролю) |

## 3. ОРГАНІЗАЦІЯ НАВЧАННЯ

| Назви тем | Кількість годин | | | |
|---|---|---|---|---|
| | усього | у тому числі | | |
| | | лекції | Лабор. | самостійна робота |
| **Тема 1. Статичні і динамічні методи аналізу програм**. | | | | |
| 1. Загальні відомості, метод експериментів з “чорною скринькою”, програмні відлагоджувальні засоби | 15 | 2 | 6 | 7 |
| **Тема 2. Особливості аналізу ряду типів програм і даних та допоміжний програмно-апаратний інструментарій аналізу програм** | | | | |
| 2. Специфіка аналізу оверлейних програм, графічних програм Windows, програм паралельного коду. ProcMon, утиліти управління процесами ProctssExplorer. | 15 | 2 | 6 | 7 |
| **Тема 3. Штучне ускладнення структури програм і алгоритмів обробки даних.** | | | | |
| 3. Динамічна зміни коду програми та штучного ускладнення програм для убезпечення їх від аналізу. | 15 | 2 | 6 | 7 |
| **Тема 4. Криптографічний захист програм та даних.** | | | | |
| 4. Симетричні та асиметричні крипто-алгоритми, їх особливості. Електронний цифровий підпис. Обмін крипто ключами, алгоритм Діффі-Хеллмана. | 15 | 2 | 6 | 7 |
| **Тема 5. Моделі взаємодії програмних закладок з системою, що перебуває під атакою** | | | | |
| 5. Моделі “спостерігача”, “перехоплення” та ”спотворення” | 15 | 2 | 6 | 7 |
| **Тема 6. Методи протидії впровадженню програмних закладок та їх маскуванню** | | | | |
| 6. Аналіз уразливостей та маскування програмних закладок під різні типи програмного забезпечення | 15 | 2 | 6 | 7 |
| **Тема 7. Підміна системного програмного забезпечення для впровадження закладок** | | | | |
| 7. Засоби і прийоми для впровадження закладок через підміну програмного забезпечення та способи протидії. | 15 | 2 | 6 | 7 |
| **Тема 8. Комп’ютерні віруси як особливий клас програмних закладок** | | | | |
| 8. Засоби і методи захисту від програмних закладок. Антивірусний моніторинг та | 15 | 2 | 6 | 7 |

| | | | | |
|---|---|---|---|---|
| програмні пастки. Організаційні та адмінзаходи для безпеки програм та даних. | | | | |
| **Усього годин за рік** | **120** | **16** | **48** | **56** |

## ЛАБОРАТОРНІ РОБОТИ

| № | Назва теми | Кількість годин |
|---|---|---|
| 1 | Вивчення програмних засобів шифрування та криптоаналіз для шифруЦезаря. | 6 |
| 2 | Афінний шифр і його використання для шифрування програм та даних. | 6 |
| 3 | Криптоаналіз на основі афінного перетворенняа. | 6 |
| 4 | Криптоаналіз шифру ключової перестановки. | 6 |
| 5 | Алгоритм CRC та хеш-функціяна його основі. | 8 |
| 6 | Генератори псевдовипадкових послідовностей та їх використання для захисту програм та даних. | 7 |
| 7. | Алгоритм шифрування RSA. | 9 |
| | **Всього** | **48** |

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА


1. Анин Б.Ю. Защита информации в компьютерной системе. - СПб.: БХВ - Санкт-Петербург, 2000. т, 384с.
2. Антоненко В.М., Рогушина Ю.В. Сучасні інформаційні системи і технології. Навчальний посібник. - К.: КСУ МП, 2005. - 131 с.
3. Антонюк А.О. Основи захисту інформації, в автоматизованих системах. Навч. посібн. - К.: Видави, дім “КМ Академія”, 2003. - 244 с.
4. Баричев С., Криптография без секретов. - М.: 1998.
5. Вертузаев М.С.,Юрченко О.М. Захист інформації в комп’ютерних системах від несанкціонованого доступу: Навч. посібник /За редаг. С.Г. Лаптева.- К.:Вид-во Європ. Університету, 2001.- 321 с.
6. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. -М.: Энергоатомиздат, 1994, в 2-х томах.
7. Герасименко В. А. Основы защиты информации: Учебник для вузов-/ Б. А. Герасименко, А. А. Малюк. — М.: Изд-во ООО «Ин-комбук», 1997. - 537 с.
8. Додж М., Кината К., Стинсон К. Эффективная работа с Excel 97. - СПб.: Питер, 1998.- 1072с.
9. Романец Ю.В., Тимофеев П. А., Шаньгин В.Ф. Защита информации вкомпьютерных системах и сетях. - М.: Радио и связь, 1999. 328с.

10. 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.
11. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2008. - 448 с.
12. Проскурин В. Г. Защита программ и данных М. : Издательский центр «Академия», 2012. - 208 с.
13. Янушкевич Д.А. Національна та міжнародна стандартизація. – Х.: ХНАДУ, 2010. – 237 с.

**Електронні ресурси**

14. http://eprint.iacr.org/2005/007
15. http://www.rsa.com/rsalabs/node.asp?id=2092
16. http://www.sagemath.org/
17. http://www.secg.org/download/aid-780/sec1-v2.pdf
18. http://www.win.tue.nl/hashclash/rogue-ca/
19. *http://www.cisco.com/go/sdn*
20. *http://www.s-terra.com/index.htm*
21. *http://www.elvis.ru/solutions_system.shtml*

## 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:** залік

**РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ ЗА МОДУЛІ**

<table>
<tr><td colspan="7">Поточне оцінювання змістових модулів</td><td>Залік</td><td>Сума</td></tr>
<tr><td rowspan="2"></td><td>ЗМ1</td><td>ЗМ2</td><td>МК1</td><td>ЗМ3</td><td>ЗМ4</td><td>МК2</td><td rowspan="5">40</td><td rowspan="5">100</td></tr>
<tr><td>10</td><td>10</td><td rowspan="4">10</td><td>10</td><td>10</td><td rowspan="4">10</td></tr>
<tr><td>Присутність на лекціях</td><td>2</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td>Присутність на ЛР</td><td>2</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td>Виконання та захист ЛР</td><td>6</td><td>6</td><td>6</td><td>6</td></tr>
</table>

**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 розкриту відповідь 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.

**Залік** (максимальна оцінка за залік – 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 розкриту відповідь 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, –одержує 0 балів.

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

**ШКАЛА ОЦІНЮВАННЯ**

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою |
|---|---|---|
| | | для заліку, курсового проекту (роботи), практики |
| 90 – 100 | A | відмінно |
| 82-89 | B | добре |
| 74-81 | C | |
| 64-73 | D | задовільно |
| 60-63 | E | |
| 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,