КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ/
SECURITY OF INFORMATION SYSTEMS AND NETWORKS

SYLLABUS

освітній ступінь	**Бакалавр /** bachelor
галузь знань	**12 Інформаційні технології /** Information Technologies
спеціальність	**125 Кібербезпека**/ Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці /** Security of information and communication systems in economy

Київ 2021

Автори: Пашорін В. І., канд. техн. наук, проф.,

Силабус розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 27 серпня 2021 протокол № 1.

СИЛАБУС

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ/ SECURITY OF INFORMATION SYSTEMS AND NETWORKS

SYLLABUS

освітній ступінь	**Бакалавр /** bachelor
галузь знань	**12 Інформаційні технології /** Information Technologies
спеціальність	**125 Кібербезпека**/ Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці /** Security of information and communication systems in economy

1. **Викладач**:
   1.1. **Лектор**: Пашорін Валерій Іванович,
   - *вчене звання та посада*: канд. техн. наук, професор;
   - *педагогічний стаж* – 20 років;
   - *контактиний телефон:* (044)-531-49-56;
   - *e-mail:* vpashorin@knute.edu.ua
   - *наукові інтереси*: безпека універсальних та спеціалізованих інформаційних систем
   - *стажування та підвищення кваліфікації*: науково-практичний курс серії вебінарів компанії Linkos Group «Інформаційні технології в економіці: інноваційні рішення захисту даних підприємства».

2. **Дисципліна**: «**Безпека інформаційних систем та мереж**»,
   - рік навчання: ІІІ;
   - семестр навчання: 5;
   - кількість кредитів: 6;
   - кількість годин за семестр: 180 год.
     - лекційних: 28 год.
     - лабораторних: 56 год.
     - на самостійне опрацювання: 96 год.
   - кількість аудиторних годин на тиждень:
     - лекційних: 2 год.
     - лабораторних: 4 год.
3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено в аудиторіях: 505, 510, 510а, 514;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
   - всі лабораторні завдання виконуються на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення лабораторних та лекційних занять на базах підприємств-партнерів.
4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** дисципліна базується на знаннях та компетентностях, що набуває здобувач вищої освіти під час вивчення дисциплін «Економічна інформатика», «Іноземна мова за професійним спрямуванням», «Об'єктно-орієнтоване програмування».
   - **постреквізити:** Дисципліна надає студентам необхідні знання та навички, які будуть корисні при проходженні виробничої практики, підготовці до випускного кваліфікаційного проекту та у подальшій професійній діяльності.

5. **Характеристика дисципліни:**
   5.1. **Призначення навчальної дисципліни:** Дисципліна «Безпека інформаційних систем та мереж» є важливою складовою підготовки сучасних фахівців ІТ-сфери. Завданням дисципліни є ознайомлення студентів із законодавчим, організаційним, інженерно-технічним і програмними рівнями безпеки інформаційних систем, засобами і методами управління контролем доступу в комп'ютерних системах, методами ідентифікації і аутентифікації користувачів і ресурсів інформаційних систем, особливостями захисту інформації в локальних і корпоративних мережах, навчити їх реалізовувати практично правила політики безпеки.
   5.2. **Метою викладання дисципліни** є формування теоретичних знань та практичних навичок, необхідних для ефективного використання інформаційних технологій

в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

5.3. **Задачі вивчення дисципліни (відповідно до ОП):** Основними завданнями вивчення дисципліни «Безпека інформаційних систем та мереж» є формування у студентів компетентностей та програмних результатів навчання:

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.	1-10
КЗ 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	1-10
КЗ 5	Здатність до пошуку, оброблення та аналізу інформації.	1-10
Фахові компетентності за освітньою програмою		
КФ 4	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	1-10
КФ 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	1-10
КФ 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	1-10
КФ 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	1-10
КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	1-10
Програмні результати навчання за освітньою програмою		
14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	1-10
16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.	1-10
17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик,	1-10

	навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	
19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	1-10
20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	1-10
21	Вирішувати задачі забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	1-10
24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно - телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	1-10
27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	1-10
28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	1-10
31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.	1-10
32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.	1-10
34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	1-10
36	Виявляти небезпечні сигнали технічних засобів.	1-10
37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.	1-10

42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.	1-10

5.4. **Зміст навчальної дисципліни:** відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

5.5. План вивчення дисципліни та оцінювання:

Тема	Робочий час студента	Бали
Тема 1. Основні положення теорії безпеки інформаційно-телекомунікаційних систем	18	10
Тема 2. Шкідливе програмне забезпечення і захист від руйнуючих програмних дій	18	10
Тема 3. Правове забезпечення кібербезпеки	18	10
Тема 4. Адміністративне та організаційне забезпечення інформаційно-телекомунікаційних систем	18	10
Тема 5. Інженерно–технічне забезпечення інформаційно-телекомунікаційних систем	18	10
Тема 6. Апаратні та програмні засоби захисту	18	10
Тема 7. Основи криптографічного захисту інформації	18	10
Тема 8. Технології безпеки на основі фільтрації та моніторингу мережевого трафіку	18	10
Тема 9. Протоколи захисту в телекомунікаційних мережах	18	10
Тема 10. Безпечна робота в комп'ютерних мережах	18	10

6. Список рекомендованих джерел

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник. Чернівці.- Видавничий дім «Родовід», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ, 2013. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: навч. посібник. – К., 2013. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах/Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №3.160 С.
10. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова*

// Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.
11. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
12. A.Menezes, P. van Oorshot, S.Vanstone. Handbook of Applied Cryptography. CRC Press Inc, 2015, 780 p.
13. Г.В.Кузнецов, В.В.Фомичов, С.О.Сушко. Математичні основи криптографії: Ч.1. Дніпропетровськ: Національний гірничий університет, 2014,391с.
14. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К. КНТ. 2012, 160с.

Internet-ресурси

15. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*
16. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*
17. Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*
18. IEEE computer society. SWEBOK – режим доступу: *http://www.computer.org/portal/web/swebok/htmlformat*
19. Process Models in Software Engineering – режим доступу: *http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE-Encyc.pdf*
20. Technical writing for software engineers – режим доступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*

7. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)

Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється з використанням 365 Office);
- захист лабораторних робіт (проходить під час кожної лабораторної роботи);
- перевірка ходу виконання індивідуального завдання (фінальний проект);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції та заслуховування доповідей на обрані студентами теми.

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного

теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3. **Правила поведінки під час занять:** обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)

8.4. **За порушення академічної доброчесності** студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти КНТЕУ (Наказ КНТЕУ від 02.02.2018 №377. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MTEyNDI=/f78c64a74cbbe5b4238729782d707efa.pdf)