Одеський національний університет імені І. І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра комп'ютерних систем та технологій

Силабус курсу

ОПП22 «Технології захисту інформації»

Обсяг	Загальна кількість кредитів – 4, годин – 120 змістовних модулів - 2
Семестр, рік навчання	6 / 3
Дні, час, місце	Згідно розкладу занять
Викладач (-і)	Шугайло Юрій Борисович - кандидат фізико-математичних наук, доцент кафедри комп'ютерних систем та технологій Стукалов Сергій Анатолійович, старший викладач кафедри комп'ютерних систем та технологій
Контактний телефон	+380632758554
E-mail	sstukalov@onu.edu.ua
Робоче місце	кафедра комп'ютерних систем та технологій/ факультет математики, фізики та інформаційних технологій
Консультації	Згідно розкладу консультацій

КОМУНІКАЦІЯ

Спілкування в аудиторіях (Zoom-конференції при дистанційній формі навчання) під час проведення лекцій та виконання лабораторних робіт згідно розкладу.

Проведення консультацій згідно розкладу (Zoom-конференції при дистанційній формі навчання).

У позааудиторний час спілкування через email: sstukalov@onu.edu.ua

АНОТАЦІЯ КУРСУ

Предмет вивчення дисципліни «Технології захисту інформації» є основи сучасного захисту інформації у комп'ютерних системах, політика безпеки, критерії захищеності комп'ютерних систем, основи криптографічного захисту інформації, захист інформації від несанкціонованого доступу.

Пререквізити і постреквізити курсу: вивчення дисципліни «Технології захисту інформації» базується на знаннях студентами курсів «Алгоритмізація та програмування», «Дискретна математика», «Організація баз даних та знань». Знання, здобуті студентами, можуть бути використаними при подальшому вивченні дисциплін «Комп'ютерні мережі», «Проектування інформаційних систем», а також при написанні кваліфікаційних та магістерських робіт.

Мета курсу - формування теоретичних знань щодо можливих небезпек, загроз і ступеня ризику втрат інформації, а також практичних навичок щодо

забезпечення захисту інформації та програмного забезпечення. Ознайомлення із сучасними підходами до збереження та захисту інформації, зі складом і змістом технологічних процедур, протоколів і операцій криптографії, криптоаналізу, стеганографії, що використовуються для вирішення проблем політики безпеки та захисту інформаційних ресурсів.

Завдання дисципліни:

- вивчення і поглиблення на основі сучасних інформаційних технологій теоретичних знань та практичних навиків у галузі інформаційної безпеки та криптографічних методів захисту інформації;
- підготовка фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації;
- оволодіння методами ідентифікації, аутентифікації, криптографії;
- набуття практичного досвіду з політики та менеджменту в галузі технологій захисту та безпеки інформації.

Очікувані результати

Процес вивчення дисципліни спрямований на формування наступних компетентностей:

ІК. Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов..

Загальні компетентності:

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК12. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові) компетентності:

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

В результаті вивчення навчальної дисципліни здобувач вищої освіти повинен знати:

- об'єкти програмного забезпечення, на які можливі атаки та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;
- принципи функціонування систем захисту, призначення привілеїв, зберігання паролів та автентифікації користувачів в операційних системах WINDOWS та LINUX, методи з несанкціонованого проникнення до інформації, привласнення привілеїв адміністратора тощо;

- методи несанкціонованого з’йому та навмисного пошкодження інформації та засоби протидії цим спробам;
- методи побудови захисту окремих програмних продуктів;
- основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання.

Вміти:

- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп’ютерної системи з метою перешкоди призначення невиправданих привілеїв;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.

ВІДПОВІДНІСТЬ ЦІЛЯМ СТАЛОГО РОЗВИТКУ ДО 2030 РОКУ

ЦСР 4 «Справедлива якісна освіта та заохочення можливості навчання впродовж усього життя для всіх». Вивчення курсу та засвоєння технологій захисту інформації запобігають діям, направленим на спотворення інформації, що сприяє підвищенню якості освіти та розвитку критичного мислення.

ЦСР 9 «Інновації та інфраструктура». Оволодіння навичками захисту інформації дозволяє істотно розширити доступ до інформаційних технологій забезпечення загального безперешкодного доступу до інтернету.

ЦСР 17 «Партнерство заради сталого розвитку». Захист інформації на всіх рівнях сприяє повномасштабному функціонуванню банку технологій і механізму розвитку науки та інновацій, забезпечує високу ефективність інформаційно-комунікативних технологій.

ОПИС КУРСУ

Форми і методи навчання

Курс буде викладений у формі лекцій (36 год.) та лабораторних занять (36 год.), організації самостійної роботи студентів (48 год.).

Підготовка здобувачів здійснюється в межах лекційного курсу, також передбачено перелік додаткових питань, які виносяться на самостійну роботу. Практичні навички студенти отримують при виконанні лабораторного практикуму у спеціалізованій лабораторії.

Під час викладання дисципліни застосовуються наступні методи навчання: словесні (лекція, пояснення), наочні (лекція-візуалізація). Студенти мають змогу отримати консультації (очні, дистанційні, змішаної форми в залежності від формату проведення занять та графіку навчального процесу).

Зміст навчальної дисципліни

Змістовний модуль 1. Основи технології захисту інформації

Тема 1. Захист інформації та його основні завдання.
Тема 2. Поняття інформаційної безпеки.
Тема 3. Механізми і політики розмежування прав доступу.
Тема 4. Основні програмно-технічні заходи інформаційної безпеки.
Тема 5. Методи та пристрої забезпечення захисту і безпеки.
Тема 6. Моделі захисту інформації.
Тема 7. Паролі і механізми контролю за доступом.

Змістовний модуль 2. Криптографічні основи захисту інформації.

Тема 8. Шифрування даних.
Тема 9. Алгоритми з секретним ключем.
Тема 10. Алгоритми з відкритим ключем.
Тема 11. Протоколи аутентифікації.
Тема 12. Цифрові підписи.
Тема 13. Основні види атак, принципи криптоаналізу.
Тема 14. Напрями розвитку сучасної криптографії.
Тема 15. Механізми та протоколи керування ключами інформаційної системи..

Перелік рекомендованої літератури

Основна

1. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.
2. Остапов С. Е Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: Вид. ХНЕУ, 2013. 476 с.
3. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
4. Семенов С.Г. Захист інформації в комп'ютерних системах та мережах: навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014. 251 с.
5. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. 138 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. 510 с..

ОЦІНЮВАННЯ

Поточний контроль здійснюється за результатами виконання 2 контрольних робіт за змістовними модулями, захисту індивідуального завдання. Оцінюється також активність студента в процесі занять: усне опитування на лекції, написання звітів до лабораторних робіт, їх захист, розв'язання практичних задач. Підсумковий контроль - іспит.

Критерії оцінювання виконання самостійної роботи

Результати індивідуального завдання представляються у вигляді доповіді (7-10 хв), що супроводжується презентацією (5-7 слайдів).

Критеріями оцінювання є: повнота представленого матеріалу, якість доповіді та презентації, відповідей на запитання викладача та однокурсників.

Критерії оцінювання виконання лабораторних робіт

Студент повинен виконати всі лабораторні роботи. За виконання розрахунків та оформлення роботи згідно вимог методичних вказівок до лабораторних робіт нараховується 8 балів за кожну роботу. При захисті роботи, за кожну правильну відповідь на запитання додається 2 бали. За неповну відповідь, відповідь, що містить несуттєві помилки додається 1 бал. За неправильну відповідь, або її відсутність бали не додаються. Максимальна кількість балів за лабораторну роботу не повинна перевищувати 15 балів. При виставленні підсумкової оцінки береться середня арифметична оцінка за всіма лабораторними роботами.

Критерії оцінювання підсумкового контролю

Підсумковий семестровий контроль (іспит) проводиться в усній формі. Екзаменаційний білет містить два теоретичних питання, кожне з яких оцінюється окремо за 20 бальною шкалою.

Критерії оцінювання теоретичного питання:

– повна розгорнута відповідь – 20 балів;

– повна, але не розгорнута відповідь – 17 балів;

– повна, але не розгорнута відповідь, яка містить незначну помилку чи суперечність – 15 балів, за кожну наступну незначну помилку чи суперечність знімається 1 бал;

– неповна відповідь, яка не містить критичних помилок чи суперечностей – 10 балів,

за кожну наступну незначну помилку чи суперечність знімається 1 бал;

– відповідь, що містить критичну помилку чи неточність, або відсутність відповіді оцінюється в 0 балів.

Кількість балів, що здобувач отримав на іспиті, є сумою балів, що були отримані за кожне завдання з екзаменаційного білету.

Кінцева оцінка виставляється за сумою балів поточного та підсумкового контролю.

Поточний контроль, самостійна робота, індивідуальні завдання												**Підсумковий контроль (Іспит)**	**Сума балів**
Змістовний модуль 1 Поточний контроль на лекціях								**Контрольна робота**	**Індивідуальні завдання**	**Виконання і захист лабораторних робіт**	**Разом**		
Т	**Т**	**Т**	**Т**	**Т**	**Т**	**Т**	**Т**						

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td></td><td></td><td></td><td rowspan="4">60</td><td rowspan="4">40</td><td rowspan="4">100</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>5</td><td>2</td><td>15</td></tr>
<tr><td colspan="8">Змістовний модуль 2
Поточний контроль на лекціях</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Т 9</td><td>Т 10</td><td>Т 11</td><td>Т 12</td><td>Т 13</td><td>Т 14</td><td>Т 15</td><td></td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td></td><td>5</td><td>3</td><td>15</td></tr>
</table>

ПОЛІТИКА КУРСУ

Політика щодо дедлайнів та перескладання: Захист звітів з лабораторних робіт здійснюється наступного тижня до початку виконання наступної роботи. Звіти та інші види контролю, які здаються з порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності). Перескладання модулів відбувається за наявності поважних причин (наприклад: лікарняний лист).

Політика щодо академічної доброчесності: Відповідно до діючого законодавства України щодо академічної доброчесності. Списування будь якої форми підчас контрольних робіт або плагіат у індивідуальних завданнях заборонені та тягнуть за собою повторне складання контрольного заходу.

Політика щодо відвідування та запізнень:. Відвідування лекцій та лабораторних занять є обов'язковим компонентом поточного контролю, за який нараховуються бали. За об'єктивних причин (хвороба та т.і.) навчання може відбуватися в дистанційній формі за погодженням із викладачем курсу.

Мобільні пристрої: Використання електронних пристроїв відбувається за згоди та відома викладача.

Поведінка в аудиторії: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчального матеріалу ознайомившись з ним напередодні.