Кібербезпека інформаційних систем

АНОТАЦІЯ

Кібербезпека інформаційних систем (КБІС) – вибіркова навчальна дисципліна, яка забезпечить багатоаспектний розгляд поняття захисту інформації в інформаційних системах з позицій інтересів користувачів, програмістів, операторів, експлуатаційників, адміністраторів обчислювальних систем. Мета викладання дисципліни полягає в навчанні сучасним технологіям в області інформаційних систем, а також створення та експлуатації систем захисту інформації

Особливістю курсу є акцент на: нормативно-правові основи організації інформаційної безпеки; основні загрози інформаційній безпеці, правила їх виявлення, аналізу та визначення вимог до різних рівнів забезпечення інформаційної безпеки; загрози інформаційній безпеці, створювані комп'ютерними вірусами, вивчення особливостей цих загроз та характерних рис комп'ютерних вірусів; вивчення особливостей забезпечення інформаційної безпеки в комп'ютерних мережах і специфіки засобів захисту комп'ютерних мереж а також основні прийоми захисту корпоративних мереж при використанні Internet.

Отримані знання будуть корисними для вирішення проблем забезпечення відмово стійкості та безпеки в інформаційних системах, що прямо пов'язані з питаннями забезпечення їх інформаційної захищеності в першу чергу від кібератак.

metinvest polytechnic

Освітній рівень

МАГІСТР

Кількість кредитів

5,0
(вибіркова)

Мова викладання

УКРАЇНСЬКА, ОКРЕМІ ДЖЕРЕЛА ІНФОРМАЦІЇ - АНГЛІЙСЬКА

Назва кафедри, яка пропонує дисципліну

АВТОМАТИЗАЦІЇ, ЕЛЕКТРО- ТА РОБОТОТЕХНІЧНИХ СИСТЕМ

СУБОТІН Олег
кандидат технічних наук, доцент,
фахівець з комп'ютерно-інтегрованих технологій та автоматизації технологічних процесів
oleg.subotin@mipolytech.education

ВИМОГИ ДО ПОПЕРЕДНЬОГО РІВНЯ ЗНАНЬ

- Базові знання зі спеціальності: електроніка та мікропроцесорна техніка, системний аналіз, інформаційні мережі, мережі та протоколи систем автоматизації.
- Математичні знання та навички: диференціальне та інтегральне обчислення, функції багатьох змінних.
- Підготовка з інформатики: використання Microsoft Word, Excel та Visio, базові знання з алгоритмізації та програмування.

РЕЗУЛЬТАТИ НАВЧАННЯ

- Знати міжнародні та державні нормативно-правові засади захисту інформації в комп'ютерних системах.
- Знати основні загрози та положення по формуванню структури системи захисту інформації на підприємстві (установі, організації).
- Знати основи безпечної міжмережевої взаємодії і підключення до глобальних телекомунікаційних мереж.
- Вміти організовувати і забезпечувати захист інформації в приміщеннях з комп'ютерної технікою і каналах зв'язку.
- Вміти аналізувати вразливості, створювати моделі загроз в автоматизованій системі.
- Вміти створювати типові рішення по захисту корпоративної мережі в умовах несанкціонованого доступу за допомогою спеціальних програмних і технічних засобів, використовуючи процедури дистанційної реєстрації подій, резервування даних на сервері, перевірки захищеності комп'ютера і паролів, контроль змін в системних файлах, систему аутентифікації тощо.

МЕТОДИ І ФОРМИ НАВЧАННЯ

Освітній процес будується як комбінація лекцій та самостійного вивчення навчального матеріалу на платформі Moodle – з одного боку, та практичних занять з опануванням навичок розв'язання задач та програмної обробки їх результатів – з іншого. Практичні заняття передбачають розбір теоретичних та практичних питань з вивчення критеріїв, методів та засобів забезпечення інформаційної безпеки та шляхи запобігання комп'ютерним інцидентам з ураженням інформації.

Окрім роботи на цих заняттях здобувачу необхідно буде виконати та захистити поточні або модульні контрольні роботи.

Доступні індивідуальні та групові консультації, які проводяться з метою допомоги студентам у виконанні їх самостійних завдань та роз'яснення окремих розділів теоретичного та практичного матеріалу.

Підсумковий контроль з даної дисципліни відбувається у формі заліку. Залік виставляється лише по сукупності виконання контрольних точок та підсумкового тестового або розрахункового завдання.

ПІДХОДИ ДО ОЦІНЮВАННЯ

Складові оцінювання успішності

Назва і стислий зміст контрольного заходу	Кількість балів
Виконання та захист практичних робіт (6 робіт по 10 балів)	60
Виконання індивідуальних завдань	10
Модульні контрольні роботи (3 роботи по 10 балів)	30
Всього /Підсумкова оцінка (ПО)	**100**

- Модульні контрольні роботи складаються на практичних заняттях за розкладом, графік складання контрольних точок (надання та захисту практичних робіт, індивідуальних завдань) повідомляється викладачем на початку викладання освітнього компоненту, однак вони мають бути захищені не пізніше, як за один тиждень до закінчення семестру (теоретичного навчання) для встановлення поточної успішності (О).
- Підсумкова оцінка (ПО) за освітній компонент здобувачам освіти визначається на момент закінчення сесійного контролю за результатами остаточної оцінки всіх контрольних заходів, в т.ч. тих, які були складені після завершення теоретичного навчання, а в разі не виконання вимог даної робочої програми – у встановлені терміни ліквідації академічної заборгованості. Переведення кількості балів у шкалу ECTS (A, B, C, D, E, F, FX) та інші шкали здійснюється відповідно до регламентів Університету.
- В рамках процедур визнання та перезарахування кредитів, отриманих в рамках формальної освіти, враховуються кредити та оцінка результатів навчання з дисциплін, споріднених за змістом (Положення-про-порядок-визначення-та-перезарахування-кредитів-в-МІП.pdf (metinvest.university)).
- Результати неформальної або інформальної освіти можуть бути визнані відповідно до «Положення про визнання в ТЕХНІЧНОМУ УНІВЕРСИТЕТІ «МЕТІНВЕСТ ПОЛІТЕХНІКА» результатів навчання, набутих у неформальній / інформальній освіті» (Положення-про-НІО.pdf (metinvest.university)).
- Результати участі у науковій роботі (статті, тези виступів, конкурсні наукові роботи тощо) можуть бути визнані в рамках оцінювання окремих індивідуальних завдань і модульних контрольних робот за узгодженням з викладачем.

ЛІТЕРАТУРА

1. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. (Електронний ресурс. Режим доступу: https://ela.kpi.ua/handle/123456789/45723).
2. 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.
4. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
5. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.
6. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510 с.
7. Кузнецов О.О. Захист інформації в інформаційних системах. методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2010.– 316 с.
8. Yi Pan, Yang Xiao. Security in Ad Hoc and Sensor Networks. Computer and Network Security - Vol. 3 // World Scientific Publishing, 2010. – P.403.

АКАДЕМІЧНІ ПОЛІТИКИ

Як член студентської спільноти Технічного університету «МЕТІНВЕСТ ПОЛІТЕХНІКА» Ви маєте дотримуватися певних стандартів та академічної політики:

Академічні політики - Polytechnic (metinvest.university)

- Шахрайство та плагіат заборонені.
- Матеріали в рамках курсу, захищені авторським правом, можуть бути використані лише тільки здобувачами освіти, яким призначено даний курс. зарахованих на курс для цілей, пов'язаних з цим курсом і не можуть поширюватися.
- Спілкування з однокурсниками та викладачем має бути професійним та ввічливим.
- Очікується, що Ви перевірятимете всі Ваші письмові повідомлення, включаючи поштові повідомлення, на коректність змісту та мови.
- Університет прагне підтримувати середовище, вільне від дискримінації або дискримінаційних домагань, спрямованих на будь-яку людину або групу в межах своєї спільноти - здобувачів освіти, співробітників або відвідувачів.