

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ»



Ступінь освіти
Освітня програма

магістр
С1.01 Економіка
D1 Облік і
оподаткування
D2 Фінанси,
банківська
справа,
страхування та
фондовий ринок

Тривалість викладання

3 чверть

Заняття:

Весняний семестр

лекції:

2 години

практичні заняття:

3 година

Мова викладання

українська

Сторінка курсу в СДО НТУ «ДП»: <https://do.nmu.org.ua/course/view.php?id=4525>

Кафедра, що викладає економіки та економічної кібернетики



Викладач:

Пістунов Ігор Миколайович

Професор, доктор. техн. наук, професор

кафедри економіки та економічної

кібернетики

Персональний сайт

<http://pistunovi.inf.ua/>

Е-mail:

pistunov.i.m@nmu.one

pistunovi@gmail.com

1. Анотація до курсу

Інтернет-комерція, торгівля в Інтернеті це – комерційна діяльність в Інтернеті, коли процес покупки / продажу товарів або послуг (весь цикл комерційної / фінансової транзакції або її частина) здійснюється електронним чином із застосуванням Інтернет-технологій.

Водночас зі зростання кількості послуг зростає й небезпека, оскільки значна кількість чинників можуть викликати втрати, збитки при проведенні електронних операцій.

Студентам пропонується набір простих, але дієвих прийомів із забезпечення безпеки електронної комерції, а також ряд корисних програм, які зменшать вразливість сайтів.

Знання програмування не потрібні, потрібно тільки бажання захистити свій бізнес.

2. Мета та завдання курсу

Мета дисципліни – формування системи знань і практичних навичок в оцінюванні стану безпеки електронної комерції, набуття навичок в організаційному та програмному плані забезпечення безпеки в державних органах, комерційних та фінансових організаціях, а також для приватних користувачів.

Завдання курсу:

Засвоєння термінології та понять засад безпеки електронної комерції
Виконувати прикладні дослідження у сфері визначення стану безпеки електронної комерції
Розробляти та реалізовувати засобів безпеки для фінансових установ
Розробляти та реалізовувати засобів безпеки для фінансових установ
Розробляти та реалізовувати засобів безпеки для комерційних організацій
Розробляти та реалізовувати засобів безпеки для приватних користувачів

3. Результати навчання

Засвоєння теоретичних і практичних знань з основ захисту електронного бізнесу від ворожого впливу.

4. Структура курсу

РОЗДІЛ 1. ОЦІНКА СТАНУ БЕЗПЕКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ 1.1. Види загроз електронної комерції 1.2. Розрахунок міри захищеності інформаційної системи електронної комерції 1.3. Розрахунок початку кібератаки 1.4. Страхування електронної комерції
РОЗДІЛ 2. ЗАХОДИ БЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОГО УПРАВЛІННЯ 2.1. Безпека взаємовідносин державних установ з іншими суб'єктами засобами електронної комунікації 2.2. Модель потенційного порушника 2.3. Особливості розкриття комп'ютерних злочинів 2.4. Зарубіжний досвід технологій створення захищеного простору суб'єкта підприємницької діяльності 2.4.1. Сполучені Штати Америки 2.4.2. Велика Британія 2.4.3. Німеччина 2.4.4. Україна 2.4.5. Цензура в Інтернеті 2.4.6. Міжнародні організації із протидії кіберзлочинам
РОЗДІЛ 3. ЗАХОДИ БЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ 3.1. Безпека платіжних систем 3.2. Шифрування, як захист систем «Клієнт-Банк» 3.3. Шахрайства з використанням банків
Розділ 4.. ЗАХОДИ БЕЗПЕКИ КОМЕРЦІЙНИХ ОРГАНІЗАЦІЙ 4.1. Програмні заходи безпеки. Захист окремих елементів мережевого обміну даними 4.1.1. Інструменти безпеки від Google 4.2. Електронні злочини в Інтернеті та способи їх уникнення 4.3. Програма кодування текстових повідомлень PortablePGP
Розділ 5. ЗАХОДИ БЕЗПЕКИ ПРИВАТНИХ КОРИСТУВАЧІВ 5.1. Шахрайство у фінансовій сфері 5.2. Інші види шахрайства 5.3. Методи захисту від шахрайства в Інтернеті 5.3.1. Організаційні заходи безпеки 5.3.2. Заходи безпеки при налаштуванні браузера 5.3.3. Програма Password Safe
ПРАКТИЧНІ ЗАНЯТТЯ
Завдання 1. Оцінка стану безпеки електронної комерції Завдання 2. Засвоєння заходів безпеки для органів державного управління Завдання 3. Засвоєння заходів безпеки для фінансових установ Завдання 4. Засвоєння заходів безпеки для комерційних організацій Завдання 5. Засвоєння заходів безпеки для приватних користувачів

5. Технічне обладнання та/або програмне забезпечення

Персональні комп'ютери з браузером та можливістю доступу до Інтернету

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
75-89	добре
60-74	задовільно
0-59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови у процесі здавання лабораторних робіт, якщо набрана у суму кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи.

Теоретична частина відсутня.

6.3. Критерії оцінювання підсумкової роботи

Середнє з балів, отриманих за виконання практичних завдань.

6.4. Критерії оцінювання лабораторної роботи

З кожної лабораторної роботи здобувач вищої освіти отримує завдання, ківі виконує самостійно і представляє результати в електронному вигляді.

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2. Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

З 24.02.2022 реалізація освітньої діяльності відбувається в умовах правового режиму воєнного стану. Наявна низка небезпек: повітряні тривоги, ризики припинення енергозабезпечення, мобільного та Інтернет-зв'язку. Згідно з наказами по університету у 2025-2026 навчальному році освітня діяльність здобувачів другого (магістерського) рівня вищої освіти всіх форм навчання здійснюється з використанням дистанційних технологій через синхронні та асинхронні комунікації.

Відвідування онлайн лекцій та практичних занять реалізується через приєднання до «команди» Microsoft Teams. Під час повітряної тривоги заняття перериваються і продовжуються лише за умов перебування учасників освітнього процесу у захищених приміщеннях. Викладачем (за технічної та безпекової можливості) здійснюється запис заняття для підтримки асинхронного формату навчання.

У випадках відсутності енергозабезпечення, мобільного та Інтернет-зв'язку викладачем забезпечується асинхронний формат навчання та комунікація зі здобувачами за допомогою каналів зв'язку, що функціонують.

Про причини неможливості взяти участь в онлайн заняттях, ускладненні доступу до матеріалів на дистанційних платформах НТУ «ДП» тощо здобувач вищої освіти має повідомити викладача в особистих повідомленнях чатів Microsoft Teams, або листом на корпоративну е-пошту НТУ «ДП», або через старосту чи представника адміністрації факультету.

7.6. Бонуси

Немає

8 Рекомендовані джерела інформації

Базові

1. Пістунов І.М. Безпека електронної комерції [Електронний ресурс]: навч. посібн. / І.М. Пістунов, Є.В. Кочура ; Нац. гірн. ун-т. – Електрон. текст. дані. – Д. : НГУ, 2014. – 125 с. Гриф МОН України (№1/11-6641 від 06.05.14)

Додаткові

1. Опис електронного шахрайства // history.lohotron.in.ua

2. Енциклопедія шахрайств та лохотронів – history.lohotron.in.ua