МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Силабус навчальної дисципліни
«Інформаційна безпека електронного бізнесу»

Галузь знань	17 Електроніка, автоматизація та електронні комунікації
Спеціальність	172 Електронні комунікації та радіотехніка
Освітня програма	Інформаційно-мережна інженерія
Освітній рівень	Перший (бакалаврський)
Статус дисципліни	Вільного вибору
Мова викладання, навчання та оцінювання	Українська
Курс / семестр	Четвертий / восьмий
Кількість кредитів ЄКТС	4
Розподіл за видами занять навчання та годинами навчання	Лекції – 12 (24 годин)
	Лабораторні роботи – 5 (20 годин)
	Практичні заняття – 2 (4 годин)
	Консультації – 4 (8 годин)
	Самостійна робота – 64 години
Форма підсумкового контролю	Залік
Кафедра	Інформаційно-мережної інженерії
Викладач	Золотарьов Вадим Анатолійович, доцент, к.т.н.

Мета вивчення дисципліни: засвоєння теоретико-методологічних засад, інформаційної та інфокомунікаційної складової і організаційно-правового механізму функціонування платіжного ринку та платіжних систем.
Цілями вивчення дисципліни формування у студентів базових знань щодо принципів функціонування кібербезпеки інформаційної безпеки та створення системи захисту, специфіки побудови підприємств електронного бізнесу.

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
ПРН-20. Вміння аналізувати та виявляти інформаційні загрози; забезпечувати конфіденційність особистої та службової інформації за допомогою нормативно-правової бази у галузі інформаційної безпеки; технічних та програмних засобів забезпечення інформаційної безпеки**.**	**ЗК9.** Навики здійснення безпечної діяльності. **ФК20.** Здатність застосовувати технології технічних та програмних засобів захисту інформації в мережах зв'язку.

Зміст навчальної дисципліни

Тема 1. Електронний бізнес. Законодавство України в сфері е-бізнесу. Поняття і принципи функціонування е-бізнесу. Сучасні види та моделі е-бізнесу. Переваги та недоліки створення е-бізнесу і е-комерції. Функціональні форми електронного бізнесу. Сучасні виклики і загрози цифровій трансформації компанії. Кіберстійкість електронного бізнесу. Управління кіберстійкістю в електронному бізнесі

Тема 2. Загальні вимоги до захисту інформації підприємств е-бізнесу (Організаційні, технічні та криптографічні заходи. Заходи з охорони приміщень. Технічний захист ІКС. Засоби захисту мереж)

Тема 3. Комерційна таємниця на підприємствах е-бізнесу. Поняття про комерційну таємницю. Загальні відомості про віднесення інформації до службової таємниці. Облік електронних носіїв інформації про діяльність, віднесеної до службової таємниці. Друкування і розмноження документів про діяльність, віднесену до службової таємниці. Формування

виконаних документів у справи. Користування документами, віднесених до комерційної таємниці.

Тема № 4. Безпека даних в ІКС підприємств у-бізнесу (Захист даних у стані спокою. Захист даних , що передаються. Захист даних, що використовуються. Основні підходи до забезпечення безпеки корпоративних баз даних).

Тема № 5 Безпека електронних документів в ІКМ підприємств е-бізнесу (Основні критерії безпеки системи електронного документообігу. Резервне копіювання. Безперервне резервне копіювання. Безпека електронної пошти)

Тема № 6. Методи ідентифікація та аутентифікації користувачів в інфокомунікаційних системах інноваційного підприємства (Ідентифікація, автентифікація та авторизація користувачів у мережі. Багатофакторна авторизація).

Тема № 7 Розмежування повноважень користувачів в ІКС підприємства у-бізнесу .**(**Концепція контролю доступу. Управління доступом користувача. Розмежування повноважень Дискреційний і мандатний доступ. Рольовий доступ. Відповідальності користувача Контроль доступу до систем та прикладних програм).

Тема № 8 Безпека платіжних систем (Загальна схема інформаційних потоків платіжної системи з описом захисту інформації на кожній її ланці. Система керування криптографічними ключами. Вимоги до паролів. Автентифікація користувачів.)

Тема 9 Кіберзагрози вебзастосунків (Порушення контролю доступу. Криптографічні збої. Ін'єкційні атаки. Небезпечний дизайн. Невірна конфігурація безпеки. Вразливі та застарілі компоненти. Помилки ідентифікації та автентифікації. Помилки цілісності програмного забезпечення та даних. Ведення журналу безпеки і моніторинг збоїв. Підробка запитів на боці сервера)

Тема 10 Захист вебзастосунків (Валідація введення. Аутентифікація та авторизація. Безпечні комунікації. Криптографічний захист. Обробка помилок та ведіння журналу. Регулярні оновлення безпеки. Принцип найменших привілеїв. Рамки безпеки для вебзастосунків. Інструменти для забезпечення безпеки вебзастосунків)

Тема 11 Забезпечення кібербезпеки інтернету речей Загрози безпеці IoT. Модель вразливості IoT. Нормативно-правове забезпечення безпеки IoT.

Тема № 12 Інноваційні технології в кібербезпеці е-бізнесу (Штучний інтелект у кібербезпеці, Архітектура «Нульової довіри». Використання блокчейну. Безперевне вдосконалення захисту хмарних технологій та віртуалізація робочих місць. Розвиток квантової криптографії. Інтеграція Security by Design та автоматизація кібербезпеки

Форми та методи оцінювання

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів.

Підсумковий контроль включає семестровий контроль, який проводиться у формі заліку.

Максимально можлива кількість балів за поточний контроль упродовж семестру для дисципліни, форма контролю якої залік – 100 та мінімально можлива кількість балів – 60.

Поточний контроль включає наступні контрольні заходи: захист звітів з лабораторних робіт; самостійна робота за темами.

Детальніша інформація щодо системи оцінювання та накопичування балів з навчальної дисципліни наведена у робочому плані з навчальної дисципліни.