Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

вибіркової навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЇ В БАНКІВСЬКИХ СИСТЕМАХ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Сачук Юрій Володимирович, кандидат фізико-математичних наук
Контактна інформація	Yurii.sachuk@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	4 курс, 7 семестр
Обсяг дисципліни	Загальний обсяг: 150 годин, 5 кредитів Аудиторних занять: 64, з них 30 лекції, 34 практичні роботи Самостійна робота: 82 годин Консультації: 4 год.
Форма контролю	Залік
Час занять	Тижневих годин - 4 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіка
Мова навчання	Українська
Анотація дисципліни	Дисципліна присвячена вивченню умов побудови та функціонування банківської системи, забезпечення безпеки у всіх сферах банківської діяльності, зокрема забезпечення складовою – безпека економічної інформації. В процесі вивчення дисципліни розглядаються особливості захисту інформаційних систем у банківських установах.
Пререквізити дисципліни	Знання основ побудови системи захисту інформації та кібербезпеки; порядок дій при виявленні кібератак; оцінка ризиків інформаційної безпеки; знання елементів криптографічного та технічного захисту інформації.
Постреквізити дисципліни	Отримані знання можуть виявитися корисними у професійній діяльності майбутніх спеціалістів та під час вивчення багатьох інших дисциплін по спеціальності.

Мета вивчення дисципліни	Метою вивчення дисципліни "Захист інформації в банківських системах " є вивчення основних аспектів інформаційно-технічної безпеки комерційних банків України; Міжнародна платіжна система SWIFT.
Що буде вивчатися	Протягом курсу будуть вивчатись такі поняття, як: Cash Trapping; використання накладок (скімерів) на термінальному обладнанні, яке дозволяє під час здійснення розрахунку зчитувати та передавати дані платіжної картки; автентифікація клієнтів Інтернет-Банкінгу; авторизація платіжних документів.
Результати навчання	1. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики безпеки. 2. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. 3. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

Політика оцінювання

Політика щодо академічної доброчесності. 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). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку, визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.
Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене икладачем для більш оперативного зв’язку зі студентами.

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

Політика щодо оскарження оцінювання. Якщо здобувач вищої освіти не згоден з оцінюванням його знань, він може опротестувати виставлену викладачем оцінку у встановленому порядку. Проте якщо опротестування безпідставне, можливе зменшення оцінки.

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми навчання відвідування занять є обов’язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту. За об’єктивних причин навчання може відбуватись в онлайн формі за погодженням з керівником курсу та деканом факультету.

Бонуси. Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освіти буде додано додаткові бали за вчасно здані роботи, за відсутність пропусків без поважних причин.

Підсумковий контроль. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль, який нараховується за якісне виконання практичних робіт, виконання контрольних, тестових робіт до лекційних матеріалів курсу. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 100 балів. Якщо за результатами семестру накопичено не менше 60 балів і студент погоджується із цим результатом,

то оцінка за семестр може виставлятися без складання заліку. Крім того, на заліку пропонується студенту перездати або доздати 1 тему (практичну, контрольну чи колоквіум), якщо йому до якогось конкретного результату не вистачає декілька балів. В іншому випадку студент складає залік. Максимальна кількість балів, яку можна отримати - 100. Залік проходить у вигляді загального тесту.

Рекомендована література

1. А.О.Корченко, Л.М.Скачек, В.О.Хорошко Банківська безпека: Підручник / КорченкоА.О., Скачек Л.М, Хорошко В.О. /За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 – с.185.
2. Кравченко А.М., Орєхов А.А., Гаркунов А.Г. Особливості захисту інформаційних систем у банківських установах // Сучасний захист інформації. – 2013. – №2. – С. 53-55.
3. Кібальник Л.О., Напора І.Ю Впровадження політики інформаційної безпеки банківських установ // Причорноморські економічні студії. – 2016. – Вип. 12-2. – С. 119-122.
4. О.А. Курченко, А. В. Головатенко, Л.Ю. Карасевич Підвищення ефективності системи управління захистом персональних даних клієнтів банку // Сучасний захист інформації. – 2014. – №1. – С. 32-37.
5. Жарій Я. В. Актуальні проблеми фінансово-інформаційної безпеки банківської системи України / Я. В. Жарій, Л. В. Дохтаренко // Вісник Чернігівського державного технологічного університету. Серія : Економічні науки. - 2013. - № 1. - С. 231-239.

Затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 7 від 5.01.2021 р.

в. о. завідувача кафедри: _____(Гришанович Т. О.)