Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

вибіркової навчальної дисципліни

МОДЕЛІ ОРГАНІЗАЦІЇ РОЗМЕЖУВАННЯ РОЛЕЙ ТА ПРАВ В ІНФОРМАЦІЙНИХ 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)	Прус Руслана Богданівна, кандидат технічних наук
Контактна інформація	prus.ruslana@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	8 семестр, 4 курс
Обсяг дисципліни	Загальний обсяг: 195 годин, 6,5 кредитів Аудиторних занять: 60, з них 30 лекції, 30 практичні роботи Самостійна робота: 129 годин Консультації: 6 год.
Форма контролю	Залік
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Мова навчання	Українська
Анотація дисципліни	Дисципліна забезпечує поглиблене вивчення трьох основних принципів безпеки: доступності, цілісності та конфіденційності. Дисципліна ознайомить студентів з механізмами, що використовуються для забезпечення контролю доступу, а також з процедурами забезпечення доступу суб'єкта до ресурсів та контролю можливостей організації взаємодії суб'єкта з ресурсом. Під час вивчення дисципліни студенти аналізують широкий спектр проблем мережевої безпеки. Студенти вивчають, як засоби контролю доступу захищають ресурси від несанкціонованого перегляду, модифікації чи знищення та слугують основним засобом забезпечення конфіденційності, цілісності та запобігання несанкціонованому доступу і витоку інформації. В основі дисципліни лежить вивчення елементів контролю доступу, таких як компоненти розмежування доступу та автентифікація, загрози безпеки пов'язані з порушенням контролю доступу, соціальна інженерія, фізична безпека, віддалений контроль доступу, шифрування та інфраструктура відкритих ключів, криптографія, моніторинг безпеки інформації
Мета вивчення дисципліни	У результаті вивчення дисципліни "Моделі організації розмежування ролей та прав в інформаційних системах" студенти зможуть визначати інструменти, необхідні для забезпечення безпеки уразливих ресурсів в IT-інфраструктурі організації; визначати компоненти контролю доступу як частину системи захисту інформації; визначати ризики, загрози та уразливості в інформаційних системах та IT-інфраструктурах.

Що буде вивчатися	1. Стандарти, процедури та політика контролю доступу. Контроль та розмежування доступу як частина забезпечення інформаційної безпеки. 2. Несанкціонований доступ та загрози безпеки пов’язані із порушенням правил розмежування доступу. Оцінка ризиків. 3. Впровадження механізмів ідентифікації та автентифікації. Однофакторна та багатофакторна автентифікація, біометрія. Токени, доступ до системи та мережі, списки/матриці контролю доступу. Синхронізовані за часом одноразові паролі. Автентифікація в автономному режимі та автентифікація пристроїв. Технологія єдиного входу (Single Sign-On). Впровадження SSO: kerberos. 4. Управління мережевими архітектурами. Порівняння мережевих архітектур, одностороння довіра, двостороння довіра та перехідна довіра. Типовий проект DMZ. 5. Цикл управління ідентифікацією. Управління особистими даними. Авторизація 6. Механізми контролю доступу до інформаційних систем. Планування фізичної безпеки та контролю доступу. Впровадження систем контролю доступу. Імплементація рішень контролю доступу для віддаленої роботи. Інфраструктура відкритих ключів, шифрування та криптографія. 7. Моделі розмежування доступу. Мандатне розмежування доступу для забезпечення конфіденційності. Модель Белла-ЛаПадула (Bell-LaPadula). 8. Моделі розмежування доступу для забезпечення цілісності. Модель Біба (Biba). Модель Кларка-Вільсона (Clark-Wilson). Політика Chinese Wall. 9. Дискреційне розмежування доступу та аналіз захищеності. Модель Take-Grant. Модель Харрисона, Руззо та Ульмана. 10. Моделі розмежування доступу на основі ролей (RBAC). Стандарт NIST RBAC. Розподіл обов'язків у RBAC. Генерація обмежень у RBAC. Ієрархія ролей. Обмежений користувальницький інтерфейс (CUI), типи інтерфейсів. Контроль доступу на основі перегляду (VBAC). Контроль доступу на основі атрибутів (ABAC). 11. Контроль доступу в операційних системах. 12. Контроль доступу до мережі. IEEE 802.1X. Віддалений доступ до телемереж. IPSec VPN. SSL/TLS VPN
Результати навчання	1. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. 2. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. 3. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 4. Вміти вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. 5. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в

	інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 6. Вміти вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). 7. Вміти забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

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 викладачем 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 залік пропонується студенту перездати або доздати 1 тему (практичну, тест чи контрольну), 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 тесту.

Рекомендована література

1. Samarati P. Access Control: Policies, Models, and Mechanisms [Електронний ресурс] / [P. Samarati, S. de Capitani di Vimercati]. – Режим доступу: https://link.springer.com/chapter/10.1007/3-540-45608-2_3

2. Гарасимчук О.І. Комплексні системи санкціонованого доступу: навчальний посібник / О.І. Гарасимчук, В.Б. Дудикевич, В.А. Ромака. – Львів: Видавництво Львівської політехніки, 2010. – 212 с.

3. Голубченко О.Л. Політика інформаційної безпеки / О.Л. Голубченко. – Луганськ: Вид-во СНК ім. В. Даля, 2009. – 300 с.

4. Горбатий І.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи : навчальний посібник / І.В. Горбатий, А.П. Бондарєв. – Львів : Видавництво Національного університету "Львівська політехніка", 2016. – 336 с.

5. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. – К. : Вид. група BHV, 2009. – 608 с.

6. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту [Електронний ресурс]. – Режим доступу: https://security.ukrnet.net

7. Корченко О.Г. Системи захисту інформації: Монографія / О.Г. Корченко. – К: НАУ, 2004. – 264 с.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол No 7 від 5.01.2021 р.

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