Волинський національний університет
імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки
СИЛАБУС
навчальної дисципліни циклу професійної підготовки
Технології захисту інформації

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Освітня програма	Комп'ютерні науки та інформаційні технології (2021 р.)
Форма навчання	Денна
Розробник	Глинчук Людмила Ярославівна, кандидат фізико-математичних наук, доцент
Контактна інформація	hlynchuk.ludmila@vnu.edu.ua
Семестр, курс	4 курс, 8 семестр;
Обсяг дисципліни	Загальний обсяг: 120 годин, 4 кредитів Аудиторних занять: 50, з них 20 лекції, 30 лабораторні роботи Самостійна робота: 62 годин Консультації: 8 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	Як навчальна дисципліна «Технології захисту інформації» забезпечує володіння принципами побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації; основними принципами побудови комплексних систем захисту інформації, розробки механізмів захисту інформації; механізмами захисту, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій; основами стенографічного захисту інформації та особливостями побудови інфраструктури відкритих ключів.
Мета вивчення дисципліни	Основною метою викладання дисципліни є навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій (ІС та Т), вивчення студентами основ стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів (ІВК).
Що буде вивчатися	1 Категорії інформаційної безпеки з точки зору інформації та інформаційних систем 2 Абстрактні моделі захисту інформації. Огляд найпоширеніших методів "злому" 3 Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації

	4 Класифікація криптоалгоритмів 5 Системи шифрування даних, які передаються в мережах 6 Засоби управління криптографічними ключами 7 Сучасна ситуація у сфері інформаційної безпеки. Рівні мережних атак 8 Апаратні та програмні засоби захисту інформації в мережах 9 Термінали захищеної інформаційної системи. Отримання пароля на основі помилок
Результати навчання	ПРН9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук. ПРН10. Використовувати інструментальні засоби розробки клієнт-серверних застосувань, проектувати концептуальні, логічні та фізичні моделі баз даних, розробляти та оптимізувати запити до них, створювати розподілені бази даних, сховища та вітрини даних, бази знань, у тому числі на хмарних сервісах, із застосуванням мов веб-програмування. ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних. ПРН18. Знати принципи представлення числової, текстової, графічної, звукової інформації у пам'яті комп'ютера, оперувати даними, представленими у різних системах числення, володіти алгоритмами обробки даних різного роду.

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 лектора 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 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 он-лайн формі за погодженням з керівником курсу та деканом факультету.

Бонуси. Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освітим буде нараховано 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 лабораторних робіт, виконання контрольних, колоквіумів та 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 (лабораторну, 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 балів.

Рекомендована література та інтернет-ресурси

Основна

1. . Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.
2. Венбо М. Современная криптография: теория и практика : пер. С англ. / М.Венбо – М. : Издательский дом "Вильямс", 2005. – 768 с.
3. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998. – 248 с.
4. Горбатов В. С. Основы технологии PKI / В. С.Горбатов, О. Ю. Полянская – М. : Горячая линия – Телеком, 2004. – 248 с
5. Гребенчук В. Г. Цифровая стеганография / В. Г. Гребенчук, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.
6. Грибунин В. Г. Цифровая стеганографія / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Прес, 2002. – 272 с.
7. Зима В. М. Безопасность глобальніх сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – 2-е изд. – СПб. : БХВ- Петербург, 2003. – 368 с.
8. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
9. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.
10. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. Т.II. Информационная безопасность. – К. : Арий, 2008. – 344 с.
11. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров – М. : ДМК, 2000. – 448 с.
12. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.
13. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. :ООО "Компания СМИТ", 2006. – Т. 2. – 252 с.
14. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. / В. Столлингс; пер. с англ. – М. : Издательский дом "Вильямс", 2001. – 672 с.
15. Хайнс Б. Руководство по безопасности Windows Server 2008 / Б. Хайнс, Б. Курри, Д. Стин, Р. Харриссон. – Microsoft, 2008. – 326 с.
16. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.
17. Чмора А. Л. Современная прикладная криптографія / А. Л. Чмора. – М. : Гелиос АРВ, 2001. – 256 с.
18. Щеглов А. Ю. Защита компьютерной информации от несанк- ционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.

Ресурси мережі Інтернет

19. http://bezopasnost.biz.
20. http://dstszi.gov.ua.
21. Журнал "Информационные технологии. Аналитические материалы" [Электронный ресурс]. – Режим доступа : http://it.ridne.net.
22. Історія розвитку інформаційних технологій в Україні
[Електронний ресурс]. – Режим доступу : http://www.icfcst.kiev.ua/ MUSEUM/IT_u.html.
23. Нормативные акты Украины [Электронный ресурс]. – Режим доступа : www.nau.kiev.ua.
24. Центр информационных технологий [Электронный ресурс]. – Режим доступа : http://www.citmgu.ru.
25. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.
26. www.pgpi.org.
27. linuxpage.ru.
28. www.securityfocus.com.
29. www.sysinternals.com.

30. www.zdnet.ru.
31. www.submarine.ru.
32. www.securitylab.ru.
33. http://www.osp.ru.
34. http://zakon1.rada.gov.ua.
35. http://www.cyberguru.ru.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки
протокол № 2 від 15.09.2021__ р.

Завідувач кафедри:  (Гришанович Т. О.)