Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

вибіркової навчальної дисципліни

СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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	4 семестр, 2 курс
Обсяг дисципліни	Загальний обсяг: 135 годин, 4,5 кредитів Аудиторних занять: 68, з них 34 лекції, 34 практичні роботи Самостійна робота: 63 години Консультації: 4 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 національних та міжнародних стандартів інформаційної та кібербезпеки. Дисципліна ознайомить студентів з різними видами стандартів, на основі яких забезпечується захист персональних даних користувачів різних систем, захист даних у платіжних системах, під час передачі інформації у різних мережах, під час обробки та зберігання інформації споживачів хмарних послуг. Вивчення дисципліни включає детальний аналіз стандартів, які регламентують використання криптографічних механізмів та протоколів електронного цифрового підпису. Навчальна програма включає вивчення послідовності розробки і впровадження системи управління інформаційною безпекою, включаючи підготовку та управління документацією системи; розробки системи захисту інформації на основі критерії оцінки безпеки, функціональних вимог та вимог довіри до безпеки. У результаті вивчення дисципліни студенти отримають практичні навички щодо впровадження вимог стандартів у різних системах, ознайомляться з процедурами сертифікаційного аудиту.
Мета вивчення дисципліни	Метою вивчення навчальної дисципліни є формування знань, вмінь та навичок, необхідних для того, щоб підготовлені фахівці здійснювали професійну діяльність на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних, у галузі інформаційної та кібербезпеки.
Що буде вивчатися	1. Державні стандарти України. Основні положення стандартизації. Державні стандарти України ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення, ДСТУ

	3396.1- 96 Захист інформації. Технічний захист інформації. Порядок проведення робіт, ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Гармонізація стандартів. 2. Міжнародні організації з розробки стандартів. Міжнародна організація зі стандартизації (ISO). Інститут стандартів інженерів з електротехніки та електроніки (IEEE-SA). Національний інститут стандартів і технології (NIST). Рада з питань стандартів Асоціації з аудиту та контролю інформаційних систем (ISACA). Інститут SANS. 3. Імплементація стандартів. Сертифікати відповідності стандартам. Аудит ІС на відповідність стандартам. 4. Стандарти серії ISO/IEC 15408. Критерії оцінки безпеки ІТ. Функціональні вимоги безпеки. Вимоги довіри до безпеки. 5. Стандарти серії ISO 27000. Специфікація СУІБ (системи управління інформаційною безпекою). Стандарт управління кібербезпекою ISO 27032. Практика впровадження оптимізованої системи управління безперервністю бізнесу (BCMS) на основі стандарту ISO 22301. 6. Система контролю та управління ІТ підприємства на основі COBIT. 7. Британський стандарт 7799, частина 3 – рекомендації BSI Group щодо управління ризиками інформаційної безпеки. 8. CSF NIST. Стандарти NIST серії 800. NIST SP 800-30 (оцінка ризиків ІБ). NIST SP 800-60 (критичність інформаційних ресурсів). NIST SP 800-61 (інциденти інформаційної безпеки). 9. EEE 802.11-2020 – стандарт безпеки бездротових локальних мереж, контроль доступу (MAC) та функції фізичного рівня (PHY). 10. Впровадження засобів захисту інформації для споживачів та постачальників хмарних послуг на основі стандарту ISO/IEC 27017. 11. Стандарт безпеки даних платіжних карт PCI DSS. Стандарт FINRA для забезпечення захисту даних користувачів при здійсненні фінансових операцій. 12. Стандарти для ЕЦП. Криптографічні механізми та протоколи електронного цифрового підпису. Стандарти ISO/IEC 9796, ISO/IEC 14888, ISO/IEC 18014 (інфраструктура відкритих ключів), ISO/IEC 11770 (управління ключами), ISO/IEC 9798 (криптографічні протоколи автентифікації та ідентифікації). Стандарти CWA. Стандарти ETSI. Основні положення сертифікації ключів та сертифікації атрибутів X.509. ДСТУ 4145. 13. Стандарт HIPAA – Акт про мобільність та підзвітність медичного страхування та його роль для захисту даних пацієнтів. 14. Загальний регламент про захист даних (General Data Protection Regulation, GDPR).
Результати навчання	1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. 2. Уміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. 3. Уміти готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. 4. Уміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

	5. Уміти реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. 6. Уміти застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. 7. Уміти 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 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. ДСТУ ISO/IEC 27000:2017. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою (ISO/IEC 27000:2016, IDT).

2. NIST (National Institute Of Standards And Technology). 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication 800-12).

3. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с. – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf .

4. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

5. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2009. – 716 с.

6. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник / О.К.Юдін. – Київ : НАУ, 2011. – 639 с.

7. Cyber Security Standards [Електронний ресурс]. – Режим доступу: https://www.itgovernance.co.uk/cybersecurity-standards

8. IT Security Standards and Best Practices [Електронний ресурс]. – Режим доступу: https://www.infosec.gov.hk/en/useful-resources/it-security-standards-and-best-practices

Затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол No 7 від 5.01.2021 р.

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