Чернівецький національний університет імені Юрія Федьковича

(повне найменування закладу вищої освіти)

Інститут фізико-технічних і комп'ютерних наук

(назва інституту/факультету)

Кафедра комп'ютерних систем та мереж

(назва кафедри)

СИЛАБУС

навчальної дисципліни

Кібербезпека (Cybersecurity Cisco)

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

вибіркова

(обов'язкова чи вибіркова)

Освітньо-професійна програма – *" Комп'ютерна інженерія технологій інтернету речей та кіберфізичних систем"*

Спеціальність *123 – Комп'ютерна інженерія*

(шифр і назва спеціальності)

Галузь знань *12 – Інформаційні технології*

(шифр і назва галузі знань)

Рівень вищої освіти – *другий (магістерський)*

(вказати: перший (бакалаврський)/другий (магістерський)/третій (освітньо-науковий))

Інститут фізико-технічних і комп'ютерних наук

(назва факультету / інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання – *українська*

(мова, на якій читається дисципліна)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ, кандидат техн. наук,

(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Профайл викладача (-ів) https://csn.chnu.edu.ua, https://csn.chnu.edu.ua/employees/ivanushhak-nataliya-myhajlivna/

Контактний тел. +(38) 0372 50 94 32 (кафедра КСМ) – Іванущак Н.М.

E-mail: n.ivanuschak@chnu.edu.ua

Сторінка курсу в Moodle https://moodle.chnu.edu.ua/course/view.php?id=1357

Консультації *on-line: середа з 17.00 до 18.00*

1. Анотація дисципліни

Курс «Кібербезпека (Cybersecurity Cisco)» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань засобів захисту інформації, Забезпечує оволодіння студентами загальними тафаховими компетентностями і досягнення ними програмних результатів навчання; використання програмно-апаратних методів для побудови систем захисту.

1.1. Мета навчальної дисципліни: надання студентам систематизованих знань для побудови комплексної системи захисту інформації, отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп'ютерних системах і мережах та усунення проблем безпеки шляхом розробки та впровадження захисних заходів. Окрім цього, засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування комплексної системи захисту інформації.

1.2. Завдання навчальної дисципліни «Кібербезпека (Cybersecurity Cisco)» - надання студентам необхідної теоретичної та практичної підготовки для того, щоб вміти: використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності; аналізувати та виявляти загрози інформації, а також проводити реалізацію алгоритмів шифрування та дешифрування даних; аналізувати наслідки кібератак; знати різні категорії вразливостей програмного та апаратного забезпечення і систем безпеки; Описати принципи конфіденційності, цілісності та доступності відносно стану даних та заходів протидії загрозам в області кібербезпеки; Прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству організації та дестабілізуючі чинники в роботі систем управління; Описати тактику, методи та процедури, які використовуються кіберзлочинцями; Описати, як технології, продукти і процедури використовуються для захисту конфіденційності, забезпечення цілісності, забезпечують високу доступність; пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережної інфраструктури; розробляти моделі загроз інформації та моделі порушників інформаційної безпеки; знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей, тощо.

1.3. Пререквізити. Для коректного розуміння і засвоєння матеріалу даного курсу слухачі повинні попередньо пройти курси: криптографія та побудова систем безпеки, захист інформації в комп'ютерних системах, комп'ютерні мережі, комп'ютерний захист фінансової інформації. Доцільно також мати певні уявлення з архітектури комп'ютерів, основ баз даних, програмування.

2. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

2.1. Знати: найновіші досягнення в галузі захисту інформації; характеристики основних підсистем ідентифікації та аутентифікації; характеристики основних механізмів доступу; характеристики підсистем захисту основних класів операційних систем; основні принципи формування політики безпеки підприємства; основні канали витоку інформації та методи боротьби з ним; критерії захищеності автоматизованих систем; характеристики основних стандартних профілів захищеності автоматизованих систем; основні характеристики захищених протоколів передавання даних.

2.2. Вміти: критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформацій-них та інформаційно-телекомунікаційних (автоматизованих) системах; вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); 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; здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; 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; вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

2.3. Набути компетентностей:

Z - загальних

Z1. Здатність до абстрактного мислення, аналізу і синтезу.

Z2. Здатність вчитися і оволодівати сучасними знаннями.

Z3. Здатність застосовувати знання у практичних ситуаціях.

Z6. Навички міжособистісної взаємодії.

Z7. Вміння виявляти, ставити та вирішувати проблеми.

Z8. Здатність працювати в команді.

Р - фахових

Р1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

Р2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

Р3. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.

Р4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

Р5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

Р6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

Р7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

Р8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

Р9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

Р10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

Р11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

Р15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

ПРН - програмовані результати навчання за загальними та загально-професійними фаховими компетентностями

N1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.
N2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.
N3. Знати новітні технології в галузі комп'ютерної інженерії.
N6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.
N8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.
N9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.
N10. Вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати, типове для спеціальності обладнання.
N13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.
N14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.
N19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

3. Опис навчальної дисципліни
3.1. Загальна інформація

Назва навчальної дисципліни *ППВ5 Кібербезпека (Cybersecurity Cisco)*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсум-кового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	**5**	**7**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Екзамен**
Заочна	**5**	**7**	**4**	**120**	**2**	**4**	**-**	**-**	**4**	**112**	**-**	**Екзамен**

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 0,33 ((15+15)/90);
для заочної форми навчання – 0,07 ((4+4)/112).

3.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Напрями забезпечення кібербезпеки												
Тема 1. Основні положення забезпечення кібербезпеки.	14	2	-	2	-	10	13	1	-	1	-	12
Тема 2. Технологічні аспекти забезпечення кібербезпеки інформаційних систем	16	2	-	2	-	10	15	0	-	-	-	14
Тема 3. Кібербезпека - загрози, вразливості та атаки	16	2	-	2	-	10	15	1	-	1	-	14
Тема 4. Захист домену кібербезпеки.	14	2	-	2	-	10	17	0	-	-	-	16
Разом за змістовим модулем 1	60	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Технологічні рішення щодо забезпечення конфіденційності, цілісності та доступності												
Тема 5. Мистецтво захисту таємниць.	18	2	-	2	-	15	18	1	-	1	-	18
Тема 6. Мистецтво забезпечення цілісності даних.	26	2	-	2	-	15	20	0	-	-	-	18
Тема 7. Концепція п'яти дев'яток.	16	3	-	3	-	20	22	1	-	1	-	20
Разом за змістовим модулем 2	60	7	-	7	-	50	60	2	-	2	-	56
Усього годин	120	15	-	15	-	90	120	4	-	4	-	112

3.2.1. Теми семінарських або практичних, або <u>лабораторних</u> занять

№	Назва теми
1.	Комунікація у кібер-світі
2.	Вивчення аутентифікації, авторизації та обліку
3.	Налаштування транспортного режиму VPN
4.	Брандмауери на сервері та ACL на маршрутизаторі
5.	Вивчення шифрування файлів і даних
6.	Використання перевірок цілісності файлів та даних
7.	Резервування маршрутизаторів і комутаторів

3.2.2. Тематика індивідуальних завдань

В даному курсі виконання індивідуальних завдань не передбачено.*

* ІНДЗ – може бути рекомендовано в окремих випадках для студентів, які успішно освоїли основний навчальний матеріал, з метою поглибленого вивчення чи удосконалення матеріалів певного змістового модуля, або в цілому для навчальної дисципліни за рішенням кафедри чи викладача.

3.2.3. Самостійна робота

№ з/п	Назва теми
1	Дії у кіберпросторі та напрями забезпечення кібербезпеки України
2	Забезпечення цілісності баз даних
3	Впровадження заходів аварійного відновлення
4	Укріплення захисту серверів та мереж
5	Домени кібербезпеки.
6	Розуміння етики роботи у кібербезпеці, цивільний захист та безпека праці.
7	Організаційний рівень безпеки та підготовки фахівців з кібербезпеки

3.3. Форми і методи навчання

Форми навчання – це проблемні й оглядові лекції, лабораторні заняття, заняття із застосуванням комп'ютерної та телекомунікаційної техніки, інтерактивні заняття з навчанням одних студентів іншими, інтегровані заняття, проблемні заняття, відеолекції, відеозаняття і відеоконференції засобами Google Meet, Zoom, заняття з використанням системи електронного навчання Moodle.

Методи: проблемний виклад матеріалу, частково-пошукові та дослідницькі лабораторні практикуми, презентації, консультації і дискусії, робота в інтернет-класі: електронні лекції, лабораторні роботи, дистанційні консультації та ін., спрямовані на активізацію і стимулювання навчально-пізнавальної діяльності студентів.

Підходи до навчання: використовуються студентоцентрований, проблемно-орієнтований, діяльнісний, комунікативний, професійно-орієнований, міждисциплінарний підходи.

Реалізація навчального процесу здійснюється під час лекційних, лабораторних занять, самостійної позааудиторної роботи з використанням сучасних інформаційних технологій навчання, консультацій з викладачами.

Для **формувань уміння та навичок** застосовуються такі **методи навчання**:

- вербальні/словесні *(лекція, пояснення, розповідь, бесіда, інструктаж);*
- наочні *(спостереження, ілюстрація, демонстрація);*
- практичні *(проведення експерименту, практики);*
- пояснювально-ілюстративний або інформаційно-рецептивний, який передбачає пред’явлення готової інформації викладачем та її засвоєння студентами*;*
- репродуктивний *(виконання лабораторних завдань за зразком);*
- метод проблемного викладу матеріалу на лекційних заняттях.

3.4. Технічне й програмне забезпечення/обладнання.

Комп’ютери в комп’ютерних класах 8 к. ЧНУ кафедри КСМ з наступною конфігурацією:

- Motherboard Asus Prime H310M-A R2.0
- CPU Intel Pentium Gold G5400 (BX80684G5400) s1151 BOX
- SSD Apacer AS350 Panther 240GB 2.5" SATAIII TLC (AP240GAS350-1)

- Memory HyperX DDR4-2400 8192MB PC4-19200 Fury Black (HX424C15FB2/8)
- Case GameMax ET-207 400 Вт
- Keyboard Defender Element HB-520 PS/2 Black (45520)
- Mouse 2E MF107 USB Black (2E-MF107UB
- Monitor 21.5" Philips.

Програмне забезпечення: ліцензійні пакети Windows 10, MS Office sotfware 79P-05726 OfficeProPlus 2019 UKR OLP NL Acdmc Non-specific No Level (Word, Excel, Power Point, Access); хмарний сервіс Google Colab, програмне забезпечення Cisco Packet Tracer.

4. Система контролю та оцінювання

4.1. Розподіл максимально можливої кількості балів, які отримують студенти за виконання всіх видів навчальної діяльності

Поточне тестування та самостійна робота									Підсумковий тест (залік)	Сума балів
Змістовий модуль 1					Змістовий модуль 2				30	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
5	5	5	5	10	10	10	10	10		

Змістовий модуль 1. Напрями забезпечення кібербезпеки

Т1. Основні положення забезпечення кібербезпеки (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т2. Технологічні аспекти забезпечення кібербезпеки (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т3. Кібербезпека - загрози, вразливості та атаки (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т4. Захист домену кібербезпеки (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

М1 – модульна контрольна робота №1 (10 балів)

Змістовий модуль 2. Технологічні рішення щодо забезпечення конфіденційності, цілісності та доступності

Т5. Мистецтво захисту таємниць (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

Т6. Мистецтво забезпечення цілісності даних (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

Т7. Концепція п'яти дев'яток (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

М2 – модульна контрольна робота №2 (10 балів).

4.2. Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
80 – 89	**B**	добре	
70 – 79	**C**		
60 – 69	**D**	задовільно	
50 – 59	**E**		
35 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 – 34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

4.3. Засоби оцінювання

Засобами оцінювання результатів навчання студента є: завдання для виконання лабораторних робіт, тести, а також модульні контрольні роботи.

4.4. Форми поточного та підсумкового контролю

Формами поточного контролю рівня знань є усна та письмова відповідь студента при захисті виконаних лабораторних робіт, кількість отриманих балів при виконанні тестового завдання, а також письмова відповідь при написанні модульних контрольних робіт.

Формами підсумкового контролю рівня знань є усна та письмова відповідь студента при здачі іспиту або підсумкове тестування у системі Cisco Networking Academy.

4.5. Політика дисципліни

Визначається системою вимог викладача щодо рівня знань і засвоєння матеріалу студентом при вивченні дисципліни, та ґрунтується на засадах академічної доброчесності з урахуванням норм законодавства України щодо академічної доброчесності та Статуту, положень Університету, й інших нормативних документів, які регламентують організацію освітнього процесу при вивченні дисципліни.

Вимоги стосуються заохочень і нарахування додаткових балів за активну участь у дискусіях щодо аналізу і обговорення тематичного матеріалу на лекціях і лабораторних заняттях, ґрунтовної підготовки до занять, відсутності пропусків без

поважних причин, виявлення поглиблених знань під час захисту звітів з лабораторного практикуму і модульного контролю.

5. Перелік питань до підсумкового модуль-контролю (іспиту)

1. Класифікація загроз інформації та методи боротьби з основними загрозами. Необхідність комплексного підходу до захисту інформації.
2. Формування політики безпеки.
3. Найбільш небезпечні загрози сучасних комп'ютерних систем і мереж.
4. Оцінка ризиків підприємства. Вартість та ціна інформації.
5. Класифікація технічних каналів витоку інформації.
6. Методи та способи захисту інформації від витоку технічними каналами. Активні та пасивні способи захисту.
7. Основні засоби технічної розвідки.
8. Класифікація систем за ступенем безпеки на основі «Помаранчевої книги». Поняття безпечної системи згідно з TCSEC.
9. Класифікація автоматизованих систем (АС) та стандартні функціональні профілі захищеності оброблювальної інформації від НСД.
10. сновні завдання захисту ОС. Принципи керування доступом сучасних універсальних ОС. Аутентифікація, авторизація та аудит. Протокол «виклик-відповідь».
11. Основні завдання захисту ОС. Принципи керування доступом сучасних універсальних ОС. Аутентифікація, авторизація та аудит. Протокол Kerberos.
12. Основні захисні механізми UNIX. Принципові недоліки захисту UNIX від НСД.
13. Основні захисні механізми Windows NT/2000/XP. Принципові недоліки захисту Windows NT/2000/XP від НСД.
14. Методи підсилення захисту універсальних операційних систем від НСД. Вимоги до додаткових засобів захисту.
15. Захист інформації від комп'ютерних вірусів.

6. Рекомендована література

6.1. Базова (основна)

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г.Даник, П.П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. − 228 с. ISBN 978-617-582-064-3
2. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.
3. Бурячок В. Л. Інформаційний та кіберпростори : проблеми безпеки,методи та засоби боротьби. Навчальний посібник / В. Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко - К. : ДУТ- КНУ, 2016.-178 с.
4. Кавун С. В. Інформаційна безпека : навч. посіб. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : ХНЕУ, 2008. – 352с. – Бібліогр.: с. 338-349. – ISBN 978-966-676-281-1

6.2. Допоміжна

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І. Вернадського. – К., 2019. – No6 (червень). – 71с.
2. Даник Ю. Г. Основи кібернетичної безпеки: монографія / Ю. Г. Даник, Р. В. Грищук; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.
3. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю.Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування та експлуатації складних інформаційних систем: зб. наук.праць. – Житомир: ЖВІНАУ, 2012. – Спецвипуск 2. – С. 5-1
4. Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – No 2. –С. 61 – 68.
5. Указ Президента України від 15 березня 2016 року No 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України".
6. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – No 45. – Ст.403.
7. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – No 45. – Ст.403.

7. Інформаційні ресурси

1. Cisco -Україна. URL: https://www.cisco.com
2. Annual Threat Reports. URL: https://www.fireeye.com/current- threats/annual-threat-report.html
3. European union agency for cybersecurity. URL: https://www.enisa.europa.eu .
4. Cybersecurity Essentials. Інтернет-ресурс Академії CISCO, netacad.com.