ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
підпис
«02» _____ 2021 р.

СИЛАБУС

Навчальна дисципліна: **Стандарти і політики кібербезпеки**

Освітньо-професійна програма: **Кібербезпека**

Рівень вищої освіти: **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Чешун Віктор Миколайович
Профайл викладача	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	cheshunvictor@gmail.com
Контактний телефон	+3 8 097 218-79-57
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6583
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/3927472324 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2020-2021, семестр ІІ (зимово-весняний)
Розклад занять	Лекції: вівторок, 1 пара, 1-210 Практичні заняття: вівторок, 3 пара, 4-502а
Консультації	Очні: вівторок, 6 пара, 4-502а Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	2	5	150	72	36	-	36	-	78	-	-	+	-

Анотація дисципліни

Дисципліна „Стандарти і політики кібербезпеки” - складова професійної підготовки бакалаврів зі спеціальності „Кібербезпека”, є однією зі спеціальних профілюючих дисциплін.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, тренінгові, навчання у співпраці, моделювання, застосування інформаційно-комп’ютерних технологій.

Пререквізити: основи інформаційної безпеки; англійська мова.

Кореквізити: мережеві операційні системи; захист інформації в інформаційно-комунікаційних системах; управління інформаційною безпекою.

Мета і завдання дисципліни

Мета дисципліни. Формування системи знань міжнародних та національних стандартів, передових практик і політик інформаційної та кібербезпеки, розуміння предметної області щодо правил синтезу і реалізації політик безпеки як базису для дисциплін-кореквізитів і подальшої професійної діяльності із здатністю розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

Предмет дисципліни. Міжнародні та національні стандарти інформаційної та кібербезпеки, політики інформаційної та кібербезпеки.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 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.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

результати навчання:

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* набуті знання для розуміння предметної області та розуміння професії, *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; *приймати участь* у розробці, впровадженні та оцінці стратегії і політик інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації із застосуванням різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів, сучасних принципах, способах та методах теорії захищених систем; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел інформації (державних та міжнародних стандартів тощо) для ефективного рішення спеціалізованих задач професійної діяльності; *застосовувати* державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів і для підготовки пропозицій до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; *застосовувати* здобуті знання міжнародних та національних стандартів, сучасних методів і моделей політик інформаційної безпеки та/або кібербезпеки, розуміння принципів і навички синтезу на їх основі політик безпеки для вирішення задач управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); *застосовувати* знання державної та іноземних мов для вивчення міжнародних та національних стандартів, а також *використовувати* термінологію цих стандартів з метою забезпечення ефективності професійної комунікації.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема практичного заняття*	Самостійна робота студента		
				Зміст	Години	Літера-тура
1	*2*	*3*	*4*	*5*	*6*	*7*
1	1	Концепція, стратегія та політика інформаційної безпеки	**ПЗ1.** Синтез елементарної політики безпеки	Опрацювання теоретичного матеріалу, підготовка до ПЗ №1	4	[1] с.8-15; [3] с.1-16; [10] с.127-135; [14]
2	1	Розробка, реалізація та підтримка політики інформаційної безпеки	**ПЗ1.** Синтез елементарної політики безпеки (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №1	4	[3] с.17-34, 57-108; [4] с.1-16 [10] с.127-135; [14]
3	1	Типові політики інформаційної безпеки – рівень операційних систем	**ПЗ2.** Дослідження--настроювання політик безпеки операційних систем	Опрацювання теоретичного матеріалу, підготовка до ПЗ №2	4	[1] с.151-165; [18]
4	1	Типові політики інформаційної безпеки – безпека WEB-ресурсів і серверів	**ПЗ2.** Дослідження--настроювання політик безпеки операційних систем (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №2	4	[4] с.139-180; [18]
5	1	Типові політики інформаційної безпеки – мережева безпека Cisco	**ПЗ3.** Дослідження політик безпеки провідних фірм ІТ-галузі	Опрацювання теоретичного матеріалу, підготовка до ПЗ №3	5	[1] 59-140, 227-250; [4] с.121-138: [18]
6	2	Класифікація джерел загроз безпеці інформації і вразливостей безпеки і розробка політики	**ПЗ3.** Дослідження політик безпеки провідних фірм ІТ-галузі (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №3	4	[1] с.15-36; [2] с.66-95; [4] с.73-89; [6] с.251-287
7	2	Галузеві політики інформаційної безпеки	**ПЗ4.** Дослідження галузевих політик інформаційної безпеки установ і підприємств регіону	Опрацювання теоретичного матеріалу, підготовка до ПЗ №4	4	[2] с.54-145; [11]; [12]; [13]
8	2	Регулятивні складові інформаційної безпеки.	**ПЗ4.** Дослідження галузевих політик інформаційної безпеки установ і підприємств регіону (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №4	5	[1] с.8-15, 140-150
9	2	Дискреційна, мандатна і рольова моделі політики інформаційної безпеки	**ПЗ5.** Синтез базових видів політик безпеки: дискреційної, мандатної, рольової	Опрацювання теоретичного матеріалу, підготовка до ПЗ №5	5	[1] с.140-150; [10] с.136-155

10	2	Початок стандартизації, веселкова серія стандартів інформаційної безпеки	**ПЗ5.** Синтез базових видів політик безпеки: дискреційної, мандатної, рольової (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №5	4	[9] с.6-14; [10] с.156-163
11	2	Розвиток веселкової серії стандартів інформаційної безпеки	**ПЗ6.** Синтез і аудит політики безпеки в розрізі положень веселкової серії стандартів інформаційної безпеки	Опрацювання теоретичного матеріалу, підготовка до ПЗ №6	4	[9] с.6-14; [10] с.156-163
12	2	Перші міжнародні стандарти Європи в галузі безпеки - ITSEC	**ПЗ6.** Синтез і аудит політики безпеки в розрізі положень веселкової серії стандартів інформаційної безпеки (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №6	4	[10] с.164-169
13	2	Федеральні та Канадські критерії безпеки (стандарти FCITS і CTCPEC)	**ПЗ7.** Синтез і аудит політики безпеки на основі стандартів інформаційної безпеки ITSEC, FCITS і CTCPEC	Опрацювання теоретичного матеріалу, підготовка до ПЗ №4	4	[10] с.169-174
14	2	Загальні критерії безпеки інформаційних технологій (стандарт ICO/МЕК 15408)	**ПЗ7.** Синтез і аудит політики безпеки на основі стандартів інформаційної безпеки ITSEC, FCITS і CTCPEC (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №7	5	[10] с.175-183; [16]
15	2	Національні стандарти Германії (BSI) та Великобританії (BS 7799) в міжнародній стандартизації інформаційних технологій	**ПЗ8.** Синтез і аудит політики безпеки на основі стандартів ISO/IEC 13335, 15408 та 27xxx	Опрацювання теоретичного матеріалу, підготовка до ПЗ №8	4	[5]; [7] с.257-289; [8] с.56-58; [9] с.14-30
16	3	Серії міжнародних стандартів інформаційної безпеки ISO/IEC 13335, 15408 та 27xxx (27k)	**ПЗ8.** Синтез і аудит політики безпеки на основі стандартів ISO/IEC 13335, 15408 та 27xxx (презентація результатів)	Опрацювання теоретичного матеріалу, підготовка до презентації--захисту роботи за тематикою ПЗ №8	4	[3] с.35-46; [6] с.407-409; [9] с.34-43; [17]
17	3	Об'єкти і суб'єкти інформаційної безпеки України	Підсумкове заняття**.** Дискусійне обговорення теорії та практик застосування політик і стандартів інформаційної безпеки	Опрацювання теоретичного матеріалу, підготовка до дискусійного обговорення питань теорії та практик застосування політик і стандартів інформаційної безпеки	5	[2] с.135-146; [11]; [12]; [13]; [14]
18	3	Стандартизація питань інформаційної безпеки в Україні	Підсумкове заняття**.** Тестування	Опрацювання теоретичного матеріалу, підготовка до ТК	5	[2] с.135-157; [11]; [12]; [13]; [14]

* лекції і практичні заняття проводяться щотижня по 2 години.

Умовні позначення: ПЗ – практичне заняття, ТК – тестовий контроль

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально- методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і практичні заняття згідно з розкладом, не запізнюватися на заняття, контрольні точки виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних занять студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

Оцінювання результатів навчання студентів

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

Аудиторна робота		**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Практичні заняття (мінімальна кількість оцінок - 5)	Тестовий контроль 1	Залік за рейтингом
Тема	1-2	1-2	
Ваговий коефіцієнт	0,75	0,25	

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: здатність обрати вірний підхід у виконанні завдань і обґрунтувати зроблений вибір; правильність та самостійність виконання завдань (своєї складової загального завдання при застосуванні рольового розподілу відповідальності для ефективного рішення спеціалізованих задач професійної діяльності за предметом дисципліни), якість отримуваних результатів; вільне володіння студентом спеціальною термінологією і застосовуваними методами дисципліни, здатність критично осмислювати основні теорії, принципи, методи і поняття; уміння обґрунтувати прийняті рішення.

Оцінку, отриману на практичному занятті, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

Впродовж семестру студент має отримати на практичних заняттях щонайменше чотири позитивні оцінки, щоб виконати програму дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Оцінювання реферативної роботи. Оцінка, яка виставляється за реферативну роботу, складається з таких елементів: якість розкриття теми реферату; своєчасність захисту реферату; засвоєння студентом теоретичного матеріалу з дисципліни, вільне володіння студентом спеціальною термінологією дисципліни і уміння фахово обґрунтувати прийняті рішення та зроблені висновки; проявлені в роботі здатність виконувати пошук, оброблення, аналіз та синтез інформації з різних джерел інформації (державних та міжнародних стандартів тощо), а також здатність критично осмислювати основні теорії, принципи, методи і поняття дисципліни; якість оформлення реферативної складової роботи і презентації.

Оцінки за реферативну роботу викладач оголошує одразу після захисту і проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
1	*2*
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в

установленому порядку, але обов’язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незарахо-вано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

Питання для самоконтролю студентів

1. Види політик інформаційної безпеки.
2. Параметри політики безпеки.
3. Управління параметрами безпеки на основі політики.
4. Правила и взаємодія параметрів безпеки.
5. Адміністрування параметрів політики безпеки.
6. Політики диспетчера списку мереж.
7. Настройка параметрів політики безпеки.
8. Управління інформаційною безпекою та управління ризиками .
9. Ролі інформаційної безпеки.
10. Домени кібербезпеки.
11. Використання вимог по стандартизації до систем і процесів управління інформаційною безпекою.
12. Концепція та основні поняття зі стандарту COBIT.
13. Процесна модель COBIT.
14. Стандарти та специфікацій в області інформаційної безпеки.
15. Основні поняття і історія. Нормативна база. Канадські критерії оцінки безпеки надійних комп'ютерних систем.
16. Впровадження системи управління інформаційною безпекою згідно вимог міжнародніх стандартів.
17. Впроваджувати процесний підхід до створення СУІБ організації згідно вимог ISO IEC 27001 та 27002.
18. Організація системного захисту інформації на базі міжнародного стандарту ISO/IEC 27002 13.
19. Забезпечення безпеки інформаційних мереж та систем на базі міжнародного стандарту ISO/IEC 27002 15.
20. Організація захисту та створення безпечного зовнішнього середовища за стандартом ISO/IEC 17799 32.
21. Розробка політики інформаційної безпеки за стандартом ISO/IEC 17799 48.
22. Оцінка безпеки інформаційних технологій за стандартом ISO/IEC 15408 55.
23. Федеральні критерії оцінки безпеки надійних комп'ютерних систем.
24. Предмет інформаційної безпеки. Завдання інформаційної безпеки.
25. Тенденції та їх витоки трансформації процесів організації та проведення локальних та регіональних міждержавних конфліктів та війн.
26. Відображення цих процесів у національних та міжнародних нормативно-правових, доктринальних та стратегічних актах.
27. Основні функції системи забезпечення інформаційної безпеки України.
28. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
29. Основні положення політики забезпечення інформаційної безпеки України.
30. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.
31. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
32. Загрози інформаційній безпеці України.
33. Джерела загроз інформаційній безпеці України.
34. Стан інформаційної безпеки України.
35. Завдання і забезпечення інформаційної безпеки України.
36. Класифікація загроз інформаційній безпеці.
37. Методики оцінки ризиків інформаційної безпеки.
38. Методи обробки ризиків інформаційної безпеки.

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.	http://elartu.tntu.edu.ua/handle/123456789/18299
2.	Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Видання друге, перероб. та доп. – Одеса : ОНАЗ ім. О.С. Попова, 2019. − 320 с.	metod.onat.edu.ua/download/686
3.	Douglas J. Landoll Information Security Policies, Procedures, and Standards: A Practitioner's Reference / Douglas J. Landoll. – Boca Raton : CRC Press Taylor & Francis Group, 2016. – 246 p.	https://www.pdfdrive.com/information-security-policies-procedures-and-standards-a-practitioners-reference-e186540593.html
4.	Practical Information Security: A Competency-Based Education Course / [Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, Ahmad Al-Omari]. – Cham, Switzerland : Springer International Publishing AG, 2018. – 328 p.	https://www.pdfdrive.com/practical-information-security-a-competency-based-education-course-e188074398.html
5.	Mair D. Information Security Standards / Dougal Mair, Shahn Harris (Lateral Security - IBM sub-contractor), Dougal Mair (ITS). – V1.4-draft. – Hillcrest : The University of Waikato, 2019. – 80 p.	https://www.waikato.ac.nz/ict-self-help/policy/UOW-Framework-Information-Security.pdf
6.	Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.	https://www.pdfdrive.com/fundamentals-of-information-systems-security-e186521700.html
7.	Галатенко В. А. Стандарты информационной безопасности / В. А. Галатенко – М.: Национальный открытый университет "ИНТУИТ", 2016. – 308 с.	https://obuchalka.org/20191004114420/standarti-informacionnoi-bezopasnosti-galatenko-v-a-2016.html
8.	Михнев И. П. Информационная безопасность: учебное пособие / И. П. Михнев; Волгоградский институт управления. – Волгоград: Изд-во Волгоградского института управления – филиала РАНХиГС, 2019. – 82 с.	https://drive.google.com/drive/u/4/folders/0AOwk3E6vGowtUk9PVA
9.	Сычев Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. - Москва: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2017. - 207 с.	https://ru.pdfdrive.com/Стандарты-информационной-безопасности-Защита-и-обработка-конфиденциальных-документов-d189593258.html
10.	Вострецова Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
11.	Про національну безпеку України: Закон України [Електронний ресурс] / Затверджено Указом Президента України від 21 червня 2018 року № 2469^Ш – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19. – Назва з екрану.	https://zakon.rada.gov.ua/laws/show/2469-19
12.	Стратегія кібербезпеки України [Електронний ресурс] / Указ Президента України від 15.01.2016 р. № 96/2016 – Режим доступу:. https://zakon5.rada.gov.Ua/laws/show/96/2016#n11. – Назва з екрану.	https://zakon5.rada.gov.Ua/laws/show/96/2016#n11
13.	Стратегія національної безпеки України [Електронний ресурс] / Указ Президента України від 06.05.2015р. № 287/2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015. – Назва з екрану.	https://zakon.rada.gov.ua/laws/show/287/2015

14.	ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. МЕТОДИ ЗАХИСТУ. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.	https://metrology.com.ua/ntd/skachat-dstu-gost-gost-r/dstu/dstu-iso-iec-27032-2016/

Додаткова

15.	Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.	https://drive.google.com/file/d/1-ZmFMuTkL5VnBgh1bXNfD6nODchxWI4U/view?usp=sharing
16.	Common Criteria for Information Technology. Security Evaluation. Part 1: Introduction and general model. - April 2017. – Version 3.1, Revision 5. – 106 p.	https://www.pdfdrive.com/common-criteria-for-information-technology-security-evaluation-part-1-e57968654.html
17.	Barry L. Williams Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0 / Barry L. Williams. – Boca Raton : CRC Press Taylor & Francis Group, 2013. – 155 p.	https://www.pdfdrive.com/information-security-policy-development-for-compliance-isoiec-27001-nist-sp-800-53-hipaa-standard-pci-dss-v20-and-aup-v50-e157745645.html
18.	Бармен С. Разработка правил информационной безопасности: пер. с англ. / Скотт Бармен– М.: Издательский дом "Вильямс", 2002. – 208 с.	http://www.dut.edu.ua/ru/lib/112/category/1298/view/828
19.	Sari Stern Greene. Security Program and Policies: Principles and Practices / Sari Stern Greene. – Second Edition, Second Printing. – Indianapolis, Indiana 46240 USA Pearson Education Inc., Second Printing - July 2015. – 638 p.	https://www.seu1.org/files/level8/IT409/Security%20Policies%20and%20Procedures.pdf
20.	Nieles M. An Introduction to Information Security / Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri; Computer Security Division - Information Technology Laboratory. – NIST Special Publication 800-12, Revision 1. – Gaithersburg : National Institute of Standards and Technology, 2017. – 101 p.	https://www.pdfdrive.com/an-introduction-to-information-security-e52588024.html
21.	Cybersecurity: Geopolitics, Law, and Policy / Amos N. Guiora; Professor of Law at the S.J. Quinney College of Law, University of Utah, USA. – New York : Taylor & Francis Books, 2017. – 177 p.	https://www.pdfdrive.com/cybersecurity-geopolitics-law-and-policy-e167545127.html
22.	Информационная безопасность: учебное пособие / [Ясенев В. Н., Дорожкин А. В., Сочков А. Л., Ясенев О. В]; под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.	http://www.unn.ru/books/met_files/infbezop.pdf
23.	Information Security Standard: Information Technology Resource Management. Virginia Information Technologies Agency (VITA), 2016. – 183 p.	https://www.pdfdrive.com/information-security-standard-e60350584.html
24.	Humphreys E. Implementing the ISO/IEC 27001:2013 ISMS Standard / Edward Humphreys. – Second Edition. – Norwood : Artech house, 2016. –239 p.	https://www.pdfdrive.com/implementing-the-isoiec-27001-2013-isms-standard-e58196796.html
25.	Calder A. IT Governance: An International Guide to Data Security and ISO27001/ISO27002 / Alan Calder, Steve Watkins. – Sixth edition. – London/Philadelphia/New Delhi : KoganPage, 2015. – 359 p.	https://www.pdfdrive.com/it-governance-an-international-guide-to-data-security-and-iso27001-iso27002-e185943941.html
26.	Johnson R. Security Policies and Implementation Issues / Robert Johnson. – 2-nd Edition – Burlington :Jones & Bartlett Learning, 2015. – 492 p.	http://www.homeworkgain.com/wp-content/uploads/edd/2019/07/20190214010138pdf.pdf
27.	Гладун А.Я. Таксономія стандартів інформаційної безпеки /	http://dspace.nbuv.gov.ua/bitstr

	А.Я. Гладун, К.О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64	eam/handle/123456789/150729/07-Hladun.pdf?sequence=1
28.	Shojaie B. Implementation of Information Security Management Systems based on the ISO/IEC 27001 / Bahareh Shojaie. - Dissertation with the aim of achieving a doctoral degree at the Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universit¨at Hamburg. February 20, 2018. 147 p.	https://ediss.sub.uni-hamburg.de/volltexte/2018/9005/pdf/Dissertation.pdf
29.	Нестеров С. А. Основы информационной безопасности: Учебное пособие. / С. А. Нестеров – 3-е изд., стер. – СПб.: Издательство «Лань», 2017. – 324 с.	https://ru.pdfdrive.com/Основы-информационной-безопасности-e188335575.html
30.	Stephen Sakawa Kibwage. Role-Based Access Control Administration of Security Policies and Policy Conflict Resolution in Distributed Systems / Stephen Sakawa Kibwage. – A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems Graduate School of Computer and Information Sciences. – Nova Southeastern University, 2015. – 111 p.	https://www.pdfdrive.com/role-based-access-control-administration-of-security-policies-and-policy-conflict-resolution-in-e96324096.html
31.	Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. – New York : Springer, 2014. – 360 p.	https://www.pdfdrive.com/cyber-development-cyber-democracy-and-cyber-defense-challenges-opportunities-and-implications-for-theory-policy-and-practice-e188268326.html
32.	Кондратенко Ю. В. Візуальний аналіз політик безпеки в ERP-системах / Ю. В. Кондратенко, І. Г. Зотова, В. В. Грицюк // Збірник наукових праць Центру воєнно-стратегічних досліджень НУ оборони України ім. Івана Черняховського. – 2018. – № 1. – С. 68-73.	http://nbuv.gov.ua/UJRN/Znpcvsd_2018_1_13
33.	Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet / Clare Stevens // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 129-152.	https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1675258
34.	Овсянніков В. В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки / [В. В. Овсянніков, С. В. Дехтяр, С. А. Паламарчук, Ю. О. Черниш, О. В. Шемендюк]. // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 3(24). – С. 187-193.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=sitsbo_2015_3_35
35.	Кібальник Л. О. Впровадження політики інформаційної безпеки банківських установ / Л. О. Кібальник, І.Ю. Напора // Гроші, фінанси і кредит. – 2016. – Випуск 12-2. – С. 119-122.	http://bses.in.ua/journals/2016/12-2_2016/23.pdf
36.	Борсуковський Ю. В. Аналіз сучасних вимог до створення парольних політик корпоративних користувачів Ю. В. Борсуковський, В. Л. Бурячок, П. М. Складанний // Сучасний захист інформації. – 2016. – № 3. – С. 72-76.	http://journals.dut.edu.ua/index.php/dataprotect/article/view/709
37.	Борсуковський Ю. В. Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів / Ю. В. Борсуковський // Сучасний захист інформації. – 2016. – № 4. – С. 5-9.	http://journals.dut.edu.ua/index.php/dataprotect/article/view/1241

38.	Борсуковський Ю. В Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації на підприємстві / Ю. В. Борсуковський // Сучасний захист інформації. – 2018. – № 1. – С. 74-81.	http://journals.dut.edu.ua/index.php/dataprotect/article/view/1797
39.	Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. – 2017. – № 1. – С. 10-14.	http://journals.dut.edu.ua/index.php/dataprotect/article/view/1405
40.	Дикий О. В. Стандарти інформаційної безпеки: компаративне дослідження / О. В. Дикий, М. О. Флюнт // Право та державне управлінняю – 2019. – № 2 (35), том 1. – С. 80-87.	http://www.pdu-journal.kpu.zp.ua/archive/2_2019/tom_1/16.pdf
41.	Dunn M. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Myriam Dunn Cavelty, Andreas Wenger // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 5-32.	https://www.tandfonline.com/doi/pdf/10.1080/13523260.2019.1678855
42.	Hend K. Alkahtani. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions / Hend K. Alkahtani // Computer and Information Science. – Vol. 12, No. 2; 2019. – ISSN 1913-8989, E-ISSN 1913-8997. – Published by Canadian Center of Science and Education. – P. 117-125.	https://pdfs.semanticscholar.org/6653/6d70cf96b5a7a45edbb35d001c7917db9959.pdf?_ga=2.45767788.971915258.1601500221-216281436.1597350674

Інформаційні ресурси

1. Інформаційне забезпечення у сфері технічного регулювання ДП "Укрметртестстандарт". Каталог НД України on-line. [Електронний ресурс]. – Режим доступу: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3731&Itemid=154&lang=uk. – Назва з екрану.

2. Метрология и стандартизация - ГОСТ, ДСТУ и ... [Електронний ресурс]. – Режим доступу: https://metrology.com.ua/. – Назва з екрану.

Електронний університет:

3. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khnu.km.ua.

4. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище викладача(ів))

Погоджено

Гарант освітньої програми _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище)

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Ю.П. Кльоц (Ініціали, прізвище)