КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(протокол № 16 від «28» 01 2021 р.)
Ректор
_____ А.А. Мазаракі

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ/ SECURITY OF INFORMATION SYSTEMS AND NETWORKS

ПРОГРАМА / COURSE SUMMARY

Київ 2020

Автори: В.І. ПАШОРІН, кандидат технічних наук, професор
кафедри інженерії програмного забезпечення та кібербезпеки,
Т.В. САВЧЕНКО, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки
М.В. САШНЬОВА, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного
забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «15» вересня 2020 р., протокол №4.

Рецензенти: С.Л. РЗАЄВА, кандидат технічних наук, доцент
О.О. РУДЕНКО, Front-endTeamLeadatAstoundCommerce
О.А. ХАРЧЕНКО, декан факультету інформаційних технологій, кандидат технічних наук, доцент
В.М. КОРОЛЬЧУК, доктор психологічних наук, професор
В.А. ОСИКА, декан факультету торгівлі та маркетингу, доктор технічних наук, професор

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ/ SECURITY OF INFORMATION SYSTEMS AND NETWORKS

ПРОГРАМА / COURSE SUMMARY

ВСТУП

Дисципліна «Безпека інформаційних систем та мереж» є обов'язковою дисципліною навчального плану підготовки студентів денної форми навчання освітнього ступеня «бакалавр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» спеціалізації «Безпека інформаційних і комунікаційних систем в економіці» та вибірковою для студентів денної форми навчання освітнього ступеня «бакалавр» галузі знань 12 «Інформаційні технології» спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютері науки», 126 «Інформаційні системи та технології» спеціалізацій «Інженерія програмного забезпечення», «Комп'ютері науки» та «Інформаційні системи та технології» та освітнього ступеня «магістр» галузі знань 05 Соціальні та поведінкові науки спеціальностей 051 «Економіка» та 053 «Психологія», спеціалізацій «Цифрова економіка» та «Психологія», галузі знань 07 «Управління та адміністрування», спеціальності 076 «Підприємництво, торгівля та біржова діяльність», спеціалізацій «Категорійний менеджмент у ритейлі» та «Товарознавство і комерційна логістика».

Програму підготовлено відповідно до Стандартів вищої освіти України із зазначених спеціальностей та відповідних освітньо-професійних програм підготовки бакалаврів та магістрів КНТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для ефективного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

Предметом дисципліни є вивчення основних положень та принципів забезпечення інформаційної безпеки автоматизованих інформаційних систем і мереж та практичне опанування сучасних методів їх захисту.

Задачі вивчення дисципліни полягають у тому, щоб ознайомити студентів із законодавчим, організаційним, інженерно-технічним і

програмними рівнями безпеки інформаційних систем, засобами і методами управління контролем доступу в комп'ютерних системах, методами ідентифікації і аутентифікації користувачів і ресурсів інформаційних систем, особливостями захисту інформації в локальних і корпоративних мережах, навчити їх реалізовувати практично правила політики безпеки.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- організація комп'ютерних мереж;
- безпека операційних систем;
- захист систем електронних комунікацій;
- архітектури комп'ютера;
- основ кібербезпеки;
- об'єктно-орієнтованого програмування;
- комп'ютерної дискретної математики;
- економічної інформатики (стандартне програмне забезпечення персональних комп'ютерів);
- технологія Java;
- правове забезпечення інформаційної безпеки держави;
- іноземної мови за професійним спрямуванням;

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google;
- налаштування операційних систем.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека інформаційних систем», як обов'язкова компонента освітньої програми «Безпека інформаційних і комунікаційних систем в економіці» та вибірковою компонентою освітньої програми «Інженерія програмного забезпечення», «Комп'ютері науки» та «Інформаційні системи та технології», «Цифрова економіка», «Психологія», «Категорійний менеджмент у ритейлі» та «Товарознавство і комерційна логістика», забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідними освітньо-професійними програмами:

«Безпека інформаційних і комунікаційних систем в економіці» (ОС бакалавр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.	2-6
КЗ 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	1-6
КЗ 5	Здатність до пошуку, оброблення та аналізу інформації.	3-6
Фахові компетентності за освітньою програмою		
КФ 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	3
КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	3-6
Програмні результати навчання за освітньою програмою		
ПР 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	1-6
ПР 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах(АС)організації(підприємства)відповідно до вимог нормативно-правових документів.	2, 3
ПР 17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних	2-5

	інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	
ПР 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	2-6
ПР 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	4-6
ПР 21	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.	1-6
ПР 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	4
ПР 28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	1-6
ПР 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	1-6
ПР 37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.	4-6

«Психологія» (ОС магістр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК2	Здатність проведення досліджень на	2-6

	відповідному рівні.	
ЗК3	Здатність генерувати нові ідеї (креативність).	1-6
ЗК4	Уміння виявляти, ставити та вирішувати проблеми.	3-6
Фахові компетентності за освітньою програмою		
СК1	Здатність здійснювати теоретичний, методологічний та емпіричний аналіз актуальних проблем психологічної науки та / або практики.	3
СК3	Здатність обирати і застосувати валідні та надійні методи наукового дослідження та/або доказові методики і техніки практичної діяльності.	3-6
СК6	Здатність ефективно взаємодіяти з колегами в моно- та мультидисциплінарних командах.	1-6
Програмні результати навчання за освітньою програмою		
ПР1	Здійснювати пошук, опрацювання та аналіз професійно важливих знань із різних джерел із використанням сучасних інформаційно-комунікаційних технологій.	1-6
ПР2	Вміти організовувати та проводити психологічне дослідження із застосуванням валідних та надійних методів.	2, 3
ПР8	Оцінювати ступінь складності завдань діяльності та приймати рішення про звернення за допомогою або підвищення кваліфікації.	2-5
ПР13	Здійснювати адаптацію та модифікацію існуючих наукових підходів і методів до конкретних ситуацій професійної діяльності.	2-6

«Цифрова економіка» (ОС магістр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК4	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).	2-6
ЗК8	Здатність проводити дослідження на	1-6

	відповідному рівні.	
Фахові компетентності за освітньою програмою		
СК4	Здатність використовувати сучасні інформаційні технології, методи та прийоми дослідження економічних та соціальних процесів, адекватні встановленим потребам дослідження.	3
СК8	Здатність оцінювати можливі ризики, соціально-економічні наслідки управлінських рішень.	3-6
Програмні результати навчання за освітньою програмою		
6	Оцінювати результати власної роботи, демонструвати лідерські навички та уміння управляти персоналом і працювати в команді.	1-6
8	Збирати, обробляти та аналізувати статистичні дані, науково-аналітичні матеріали, необхідні для вирішення комплексних економічних завдань.	2, 3
10	Застосовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення у соціально-економічних дослідженнях та в управлінні соціально-економічними системами.	2-5
16	*Розробляти й аналізувати моделі діджиталізації економічних процесів та здійснювати їх програмну реалізацію у цифровому просторі.*	*2-6*

«Категорійний менеджмент у ритейлі» (ОС магістр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК1	Здатність до адаптації та дії в новій ситуації.	2-6
ЗК5	Визначеність і наполегливість щодо поставлених завдань і взятих обов’язків.	1-6
Фахові компетентності за освітньою програмою		
СК3	Здатність до ефективного управління діяльністю	3

	суб'єктів господарювання в сфері підприємництва, торгівлі та/або біржової діяльності.	
СК4	Здатність до вирішення проблемних питань і прийняття управлінських рішень у професійній діяльності.	3-6
СК5	Здатність до ініціювання та реалізації інноваційних проектів в підприємницькій, торговельній та/або біржовій діяльності.	1-6
СК7	*Здатність до формування та управліннясортиментомтоварнихкатегорійіззастосуванням сучаснихінформаційних систем.*	*1-6*
СК8	*Здатність розробляти цінову, асортиментну та комунікаційну стратегію підприємств ритейлу.*	*1-6*
Програмні результати навчання за освітньою програмою		
1	Вміти адаптуватися та проявляти ініціативу і самостійність в ситуаціях, які виникають в професійній діяльності.	1-6
5	Вміти професійно, в повному обсязі й з творчою самореалізацією виконувати поставлені завдання у сфері підприємництва, торгівлі та/або біржової діяльності.	2, 3
6	Вміти розробляти та впроваджувати заходи для забезпечення якості виконуваних робіт і визначати їх ефективність.	2-5
10	Вміти вирішувати проблемні питання, що виникають в діяльності підприємницьких, торговельних та/або біржових структур за умов невизначеності та ризиків.	2-6
11	Впроваджувати інноваційні проекти з метою створення умов для ефективного функціонування та розвитку підприємницьких, торговельних та/або біржових структур.	1-6
12	*Здійснювати моніторинг та формувати асортимент товарних категорій у ритейлі із застосуванням сучасних інформаційних технологій*	*1-6*

«Товарознавство і комерційна логістика» (ОС магістр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК3	Здатність мотивувати людей та рухатися до спільної мети.	2-6
ЗК4	Здатність спілкуватися з представниками	1-6

	інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).	
Фахові компетентності за освітньою програмою		
СК1	Здатність розробляти та реалізовувати стратегію розвитку підприємницьких, торговельних та/або біржових структур.	3
СК3	Здатність до ефективного управління діяльністю суб'єктів господарювання в сфері підприємництва, торгівлі та/або біржової діяльності.	3-6
Програмні результати навчання за освітньою програмою		
4	Застосовувати бізнес-комунікації для підтримки взаємодії з представниками різних професійних груп.	1-6
10	Вміти вирішувати проблемні питання, що виникають в діяльності підприємницьких, торговельних та/або біржових структур за умов невизначеності та ризиків.	2-6

«Інформаційні системи та технології» (ОС бакалавр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ 2	Здатність застосовувати знання у практичних ситуаціях.	2-6
КЗ 3	Здатність до розуміння предметної області та професійної діяльності.	1-6
Фахові компетентності за освітньою програмою		
КС 3	Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп'ютерно-інтегрованих систем та системної мережної структури, управління ними.	3-6
КС 10	Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем,	1-6

	технологій та інфокомунікацій, сервісів та інфраструктури організації.	
Програмні результати навчання за освітньою програмою		
ПР 3	**Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.	1-6

«Інженерія програмного забезпечення» (ОС бакалавр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
К01	Здатність до абстрактного мислення, аналізу та синтезу.	2-6
К02	Здатність застосовувати знання у практичних ситуаціях.	1-6
Фахові компетентності за освітньою програмою		
К13	Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.	3-6
К14	Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування.	1-6
К15	Здатність розробляти архітектури, модулі та компоненти програмних систем.	1-6
К16	Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.	1-6
К18	Здатність аналізувати, вибирати і	1-6

	застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).	
К20	Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення.	1-6
К23	Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.	1-6
К26	Здатність до алгоритмічного та логічного мислення.	1-6
Програмні результати навчання за освітньою програмою		
ПР01	Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.	1-6
ПР03	Знати основні процеси, фази та ітерації життєвого циклу програмного забезпечення.	1-6
ПР05	Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об’єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.	1-6
ПР09	Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.	1-6
ПР11	Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання.	1-6
ПР14	Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.	1-6
ПР19	Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.	1-6

ПР20	Знати підходи щодо оцінки та забезпечення якості програмного забезпечення.	1-6

«Комп'ютерні науки» (ОС бакалавр 2020 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Фахові компетентності за освітньою програмою		
СК14	Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.	3-6
Програмні результати навчання за освітньою програмою		
ПР 16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	1-6

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1.Основні положення теорії інформаційної безпеки

Основні терміни та визначення інформаційної безпеки. Актуальність інформаційної безпеки. Інформаційна безпека в умовах функціонування глобальних мереж. Цілі і завдання інформаційної безпеки. Види можливих порушень в роботі інформаційної системи. Розголошування. Витік інформації. Несанкціонований доступ до системи або мережі. Загрози інформації. Основні поняття і класифікація загроз. Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденційності. Порушники інформаційної безпеки. Класифікація порушників. Методика вторгнення. Умови, що сприяють неправомірному оволодінню інформацією. Канали витоку інформації та перехоплення даних. Модель безпеки: структура і компоненти. Засоби забезпечення безпеки інформаційних систем і мереж.

Список рекомендованих джерел:

Основний: 1,2,3,4

Додатковий: 13

Internet-ресурси:15,20

Тема 2.Правове забезпечення інформаційної безпеки

Структура законодавства по захисту інформації. Основні нормативні керівні документи, що стосуються державної таємниці. Нормативно-довідкові документи. Призначення і завдання у сфері забезпечення інформаційної безпеки на рівні держави. Міжнародні стандарти інформаційної безпеки. Державний стандарт України із захисту інформації.

Список рекомендованих джерел:

Основний: 1,2,3,4

Додатковий: 7,8,9,10,11

Internet-ресурси: 20

Тема 3.Адміністративне та організаційне забезпечення інформаційної безпеки

Організаційний захист. Політика безпеки. Програма безпеки. Управління ризиками. Стандарти інформаційної безпеки. Критерії оцінювання захищеності інформаційної системи. «Критерії оцінки довірених комп'ютерних систем» («Помаранчева книга»). Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. Аналіз засобів порушення інформаційної безпеки.

Список рекомендованих джерел:

Основний: 1,2,3,4

Додатковий: 7,8,9,10,11,14

Internet-ресурси:20

Тема 4.Програмно–технічне забезпечення інформаційної безпеки

Інженерно-технічний рівень інформаційної безпеки. Технічні засоби для несанкціонованого доступу до інформації. Засоби протидії несанкціонованому доступу до інформації. Канали витоку інформації. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. Програмні засоби захисту. Ідентифікація і аутентифікація. Управління доступом. Реєстрація подій і аудит. Функціональне призначення та реалізація парольного захисту. Паролі в ОС Windows. Мережева аутентифікація в Windows. Апаратні засоби аутентифікації.

Список рекомендованих джерел:

Основний: 1,2,3,4,5

Додатковий: 10,11,14

Internet-ресурси:18,19

Тема 5. Основи криптографічного захисту інформації.

Основні терміни та поняття криптографії. Історія та законодавча база криптографії. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інші.

Багатоалфавітні системи шифрування: Бьюфорта, Віженера та інші. Сучасні криптосистеми та їх особливості. Основні типи алгоритмів шифрування. Електронний цифровий підпис. Управління ключами та сертифікація ключів. Стеганографічні методи захисту інформації

Список рекомендованих джерел:

Основний: 2,3,4,5

Додатковий: 9,12,13

Internet-ресурси: 20

Тема 6.Захист від руйнуючих програмних дій.

Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Програмні закладки. Програми - шпигуни і логічні бомби. Троянські програми. Черв'яки і інші шкідливі програми. Визначення видів захисту від вірусів. Антивірусні програми. Корпоративні антивіруси. Правила використання стороннього програмного забезпечення. Спам і засоби боротьби з ним.

Список рекомендованих джерел:

Основний: 3,4,5

Додатковий: 14

Internet-ресурси:18,20

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник. Чернівці.- Видавничий дім «Родовід», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ, 2013. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: навч. посібник. – К., 2013. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. Антонюк А., Жора В. Моделювання доступу та каналів витоку вінформаційних системах/Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №3.160 С.
10. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
11. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
12. A.Menezes, P. vanOorshot, S.Vanstone. HandbookofAppliedCryptography. CRC PressInc, 2015, 780 p.
13. Г.В.Кузнецов, В.В.Фомичов,С.О.Сушко. Математичні основи криптографії: Ч.1. Дніпропетровськ: Національний гірничий університет, 2014,391с.
14. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К. КНТ. 2012, 160с.

Internet-ресурси

15. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*

16. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*

17. Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*

18. IEEE computer society. SWEBOK – режимдоступу: *http://www.computer.org/portal/web/swebok/htmlformat*

19. Process Models in Software Engineering – режимдоступу: *http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE-Encyc.pdf*

20. Technical writing for software engineers – режимдоступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

**Курсивом зазначені джерела, що є в бібліотеці КНТЕУ*