Міністерство освіти і науки України
Сумський національний аграрний університет
Факультет економіки і менеджменту
Кафедра обліку і оподаткування

Робоча програма (силабус) освітнього компонента

Інформаційна безпека та захист даних
(обов'язковий / вибірковий)

Реалізується в межах освітніх програм галузей знань 05 «Соціальні та поведінкові науки», 07 «Управління та адміністрування», 12 «Інформаційні технології», 28 «Публічне управління та адміністрування»

на другому (магістерському)рівні вищої освіти

Суми – 2024

Розробник: Сергій ГАРКУША, к.е.н., доцент, доцент кафедри обліку і оподаткування

Розглянуто, схвалено та затверджено на засіданні кафедри обліку і оподаткування	протокол від 06.06.2024 р. .№16
	Завідувач кафедри _____ (підпис) **Микола ГОРДІЄНКО**

Погоджено:

Декан факультету, де реалізується освітня програма _____ (підпис) **Маргарита ЛИШЕНКО**

Рецензія на робочу програму(додається) надана: **Інною НАЗАРЕНКО**

Миколою ГОРДІЄНКОМ

Методист відділу якості освіти, ліцензування та акредитації _____ (підпис) (Надія Тарасік)

Зареєстровано в електронній базі: дата: 21.06. 2024 р.

1. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНІЙ КОМПОНЕНТ

<table>
<tr><td>1.</td><td>Назва ОК</td><td colspan="8">Інформаційна безпека та захист даних</td></tr>
<tr><td>2.</td><td>Факультет/кафедра</td><td colspan="8">Економіки і менеджменту/Обліку і оподаткування</td></tr>
<tr><td>3.</td><td>Статус ОК</td><td colspan="8">Вибіркова навчальна дисципліна</td></tr>
<tr><td>4.</td><td>Програма/Спеціальність (програми), складовою яких є ОК для</td><td colspan="8">Облік і оподаткування/ 071 «Облік і оподаткування»</td></tr>
<tr><td>5.</td><td>ОК може бути запропонований для</td><td colspan="8"></td></tr>
<tr><td>6.</td><td>Рівень НРК</td><td colspan="8">7 рівень</td></tr>
<tr><td>7.</td><td>Семестр та тривалість вивчення</td><td colspan="8">3 семестр, 12 тижнів</td></tr>
<tr><td>8.</td><td>Кількість кредитів ЄКТС</td><td colspan="8">Обсяг навчальної дисципліни становить 5 кредитів ЄКТС – денна форма навчання.
Обсяг навчальної дисципліни становить 5 кредитів ЄКТС – заочна форма навчання.</td></tr>
<tr><td rowspan="3">9.</td><td rowspan="3">Загальний обсяг годин та їх розподіл</td><td colspan="4">денна форма</td><td colspan="4">заочна форма</td></tr>
<tr><td colspan="3">Контактна робота (заняття)</td><td>Самостійна робота</td><td colspan="3">Контактна робота (заняття)</td><td>Самостійна робота</td></tr>
<tr><td>Лекційні</td><td>Практичні /семінарські</td><td>Лабораторні</td><td></td><td>Лекційні</td><td>Практичні /семінарські</td><td>Лабораторні</td><td></td></tr>
<tr><td></td><td>24</td><td>24</td><td>-</td><td>102</td><td>14</td><td>14</td><td>-</td><td>122</td></tr>
<tr><td>10.</td><td>Мова навчання</td><td colspan="8">українська</td></tr>
<tr><td>11.</td><td>Викладач/Координатор освітнього компонента</td><td colspan="8">к.е.н., доцент Гаркуша Сергій Анатолійович</td></tr>
<tr><td>11.1</td><td>Контактна інформація</td><td colspan="8">м. Суми, вул. Г. Кондратьєва, 160, факультет Економіки і менеджменту, кафедра Обліку і оподаткування (ауд. 109е), serhii.harkusha@snau.edu.ua</td></tr>
<tr><td>12.</td><td>Загальний опис освітнього компонента</td><td colspan="8">Освітній компонент «Інформаційна безпека та захист даних» – дає здобувачам вищої освіти розуміння теоретичних, організаційно-правових та практичних засад інформаційної безпеки та захисту даних.
Інформаційна безпека являє собою комплекс певних заходів технічного, організаційного плану. Всі вони стосуються заощадження, захисту інформаційних даних, а також різного устаткування, що буде потрібне для обробки цієї інформації, запису, зберігання, передачі. Під таким комплексом прийнято розглядати інноваційні технології, способи і встановлені стандарти, що відповідають за успішне управління інформацією і тим самим забезпечують її надійний захист від сторонніх осіб.</td></tr>
<tr><td>13.</td><td>Мета освітнього компонента</td><td colspan="8">є засвоєння основних понять та категорій комп’ютерної безпеки, вивчення принципів побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій</td></tr>
<tr><td>14.</td><td>Передумови вивчення ОК, зв'язок з іншими освітніми компонентами ОП</td><td colspan="8">передумови відсутні</td></tr>
<tr><td>15.</td><td>Політика академічної доброчесності</td><td colspan="8">Документи стосовно академічної доброчесності наведені на сторінці сайту: https://academiq.org.ua та https://snau.edu.ua/viddil-zabezpechennya-yakosti-osviti/zabezpechennya-yakosti-osviti/akademichna-dobrochesnist/</td></tr>
</table>

		Для здобувачів освіти є неприйнятним під час виконання завдання та теоретичного опитування використання джерел інформації (усні (підказки), письмові (роботи інших осіб), друковані (книги, посібники), електронні (телефони, планшети) За використання заборонених пристроїв і джерел інформації під час контролю знань здобувач позбавляється подальшого права здавати матеріал, що може призвести до виникнення академічної заборгованості. За списування під час виконання окремих завдань здобувачу вищої освіти знижується оцінка або не зараховується завдання залежно від часу виявлення та ступеня порушення академічної доброчесності.
16.	Посилання на курс в Moodle	https://cdn.snau.edu.ua/moodle/course/view.php?id=5305

2. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ ТА ЇХ ЗВ'ЯЗОК З ПРОГРАМНИМИ РЕЗУЛЬТАТАМИ НАВЧАННЯ

Результати навчання за ОК: Після вивчення освітнього компонента студент очікувано буде здатен…»	Як оцінюється РНД
ДРН 1. Здатність до розмежування існуючих підходів до визначення поняття політика інформаційної безпеки.	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 2. Володіти правилами безпеки при роботі із комп'ютерними мережами	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 3. Знати криптографічні методи захисту інформації	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 4. Знати будову та принципи дії комп'ютерних вірусів і шкідливих програм	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 5. Вміти встановлювати та використовувати антивірусні програми та забезпечувати безпеку використання WWW за допомогою web-браузерів	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 6. Вміти розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки	Виконання завдань, експрес-опитування, тестування й обробка результатів

3. ЗМІСТ ОСВІТНЬОГО КОМПОНЕНТА (ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ)

Тема. Перелік питань, що будуть розглянуті в межах теми	Розподіл в межах загального бюджету часу (денна/заочна)				Рекомендована література
	Аудиторна робота			Самостійна робота	
	Лк	П.з / семін. з	Лаб. з.		
Тема 1. **Теоретичні основи інформаційної безпеки.** Поняття інформаційної безпеки. Основні складові інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Концепція керування безпекою інформаційних технологій. Елементи безпеки. Процес керування безпекою інформаційних технологій. Моделі інформаційної безпеки. Архітектура інформаційної безпеки. Аналіз моделей моніторингу.	2/2	2/2		16/20	Основні джерела: 1, 2, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: 1
Тема 2. **Інформаційна система персональних даних.** Суб'єкти відносин, пов'язаних із персональними даними. Об'єкти захисту. Загальні вимоги до обробки персональних даних. Особливі вимоги до обробки персональних даних. Права суб'єкта персональних даних. Повідомлення про обробку персональних даних. Використання персональних даних. Підстави для обробки персональних даних. Збирання персональних даних. Порядок доступу до персональних даних. Відстрочення або відмова у доступі до персональних даних. Забезпечення захисту персональних даних.	2/2	2/2		16/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела1, 5, 6, 7, 8, 9, 10, 11, 12; Програмне забезпечення: -
Тема 3. **Апаратні засоби захисту інформації.**	4/2	4/2		14/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9

Основи апаратного захисту. Класифікація технічних засобів зняття інформації. Основні групи технічних засобів ведення розвідки. Радіомікрофони. Основні методи прослуховування телефонних ліній. Телефонні радіо транслятори. Системи прослуховування повідомлень. Використання телефонної лінії для прослуховування приміщень. Спеціальні пристрої прослуховування. Системи і пристрої відео контролю. Пристрої дистанційного управління, відеодетектор руху. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Основні стаціонарні засоби захисту інформації. Пошукове устаткування.					Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Тема 4. **Програмні засоби, що містять небезпеку.** Основні означення і критерії загроз. Найпоширеніші загрози доступності. Деякі приклади загроз доступності. Шкідливе програмне забезпечення. Основні загрози цілісності. Основні загрози конфіденційності.	4/2	4/2		14/18	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Тема 5. **Криптографічний захист інформації.** Криптографічні методи захисту. Основи крипто аналізу. Стеганографія.	4/2	4/2		14/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Тема 6. **Безпека в комп'ютерних мережах.** Короткі відомості про комп'ютерні мережі. Використання міжмережевих екранів. Політика безпеки під час роботи в мережі.Архівування та зберігання облікової інформації. Захист інформації та попередження шахрайства у сфері облікового	4/2	4/2		14/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -

забезпечення					
Тема 7. **Захист інформації в глобальних мережах.** Короткі відомості про глобальні комп'ютерні мережі. Характер проведення атак у глобальних мережах. Захист під час використання WWW (WorldWideWeb). Захист електронних листів та поштових систем	4/2	4/2		14/20	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Всього	24/14	24/14		102/122	

4. МЕТОДИ ВИКЛАДАННЯ ТА НАВЧАННЯ

ДРН	**Методи викладання** (робота, що буде проведена викладачем під час аудиторних занять, консультацій)	**Методи навчання** (які види навчальної діяльності має виконати студент самостійно)
ДРН 1. Здатність до розмежування існуючих підходів до визначення поняття політика інформаційної безпеки.	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)
ДРН 2. Володіти правилами безпеки при роботі із комп'ютерними мережами	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)
ДРН 3. Знати криптографічні методи захисту інформації	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)
ДРН 4. Знати будову та принципи дії комп'ютерних вірусів і шкідливих програм	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)
ДРН 5. Вміти	Словесні: монологічні	Дослідницький метод

встановлювати та використовувати антивірусні програми та забезпечувати безпеку використання WWW за допомогою web-браузерів	(пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	(здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)
ДРН 6. Вміти розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формулюють проблеми, висувають і перевіряють гіпотези, самостійно формулюють висновки)

5. ОЦІНЮВАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ

5.1. Діагностичне оцінювання (зазначається за потреби)

5.2. Сумативне оцінювання

5.2.1.Для оцінювання очікуваних результатів навчання[1]

*здобувачів денної форми навчання*передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання
1.	Дискусії	10 / 10%	Кожного практичного заняття
2.	Виконання завдань	60 / 60%	Кожного практичного заняття
3.	Експрес-опитування	20 / 20%	Кожного практичного заняття
4.	Стандартизовані тести	10 / 10%	Кожного практичного заняття

Для оцінювання очікуваних результатів навчання*здобувачів заочної форми навчання* передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання
1.	Виконання завдань	50 / 50%	Кожного практичного заняття
2.	Експрес-опитування	20 / 20%	Кожного практичного заняття
3.	Тест множинного вибору	30 балів / 30%	Відповідно до графіку освітнього процесу

5.2.2. Критерії оцінювання для *здобувачів денної форми* навчання

Компонент	**Незадовільно**	**Задовільно**	**Добре**	**Відмінно**
Дискусії	*0-3 балів*	*4-6 балів*	*7-8 балів*	*9-10 балів*
	Пасивна участь у дискусії	Участь у дискусії, необґрунтовані відповіді	Активна участь у дискусії, продемонстровано навички критичного мислення	Активна участь у дискусії, продемонстровано навички критичного мислення, системність знань та креативність
Виконання завдань	*<35 балів*	*36-44 балів*	*45-53 балів*	*54-60 балів*
	Завдання не виконано	Завдання виконане, але деякі питання не розкриті, мають місце неточності	Завдання виконане, але мають місце незначні неточності	Завдання виконане, всі питання розкриті
Експрес-опитування	*0-11 балів*	*12-14 балів*	*15-17 балів*	*18-20 балів*
	Відсутні знання по теоретичним питанням	Низький рівень знань теоретичних питань	Володіння понятійно-категоріальним апаратом, фаховою термінологією , теоретичними знаннями, незначні неточності у відповідях на питання	Володіння понятійно-категоріальним апаратом, фаховою термінологією , теоретичними знаннями
Стандартизовані тести	*0-5 балів*	*6 балів*	*7-8 балів*	*9-10 балів*
	Вірно вирішено менше 60 % тестів	Вірно вирішено 60 -74 % тестів	Вірно вирішено 75 - 89 % тестів	Вірно вирішено 90 і більше % тестів

[1]Здобувачі вищої освіти мають право на перерахування результатів навчання набутих у неформальній/інформальній освіті відповідно до Положення про порядок визнання результатів, здобутих шляхом неформальної та/або інформальної освіти (http://surl.li/ummfb)

Критерії оцінювання для здобувачів *заочної форми* навчання

Компонент	**Незадовільно**	**Задовільно**	**Добре**	**Відмінно**
Виконання завдань	*<29 балів*	*30-36 балів*	*37-44 балів*	*45-50 балів*
	Завдання не виконано	Завдання виконане, але деякі питання не розкриті, мають місце неточності	Завдання виконане, але мають місце незначні неточності	Завдання виконане, всі питання розкриті
Експрес-опитування	*0-11 балів*	*12-14 балів*	*15-17 балів*	*18-20 балів*
	Відсутні знання по теоретичним питанням	Низький рівень знань теоретичних питань	Володіння понятійно-категоріальним апаратом, фаховою термінологією , теоретичними знаннями, незначні неточності у відповідях на питання	Володіння понятійно-категоріальним апаратом, фаховою термінологією , теоретичними знаннями
Тест множинного вибору	*0-17 балів*	*18-21 балів*	*22-26 балів*	*27-30 балів*
	Вірно вирішено менше 60 % тестів	Вірно вирішено 60 -74 % тестів	Вірно вирішено 75 - 89 % тестів	Вірно вирішено 90 і більше % тестів

5.3. Формативне оцінювання:

Для оцінювання поточного прогресу у навчанні та розуміння напрямів подальшого удосконалення передбачено

№	**Елементи формативного оцінювання**	**Дата**
1	Настанови викладача в процесі виконання завдань	Кожного практичного заняття
2	Усне опитування	Кожного практичного заняття
3	Спостереження за ходом вирішення завдань, обговорення та усні коментарі викладача	Кожного практичного заняття
4	Контроль за виконанням завдань	Кожного практичного заняття
5	Перевірка тестів і обговорення результатів тестування	На наступну пару після проведення тестування

6. НАВЧАЛЬНІ РЕСУРСИ (ЛІТЕРАТУРА)

6.1. Основні джерела

6.1.1. Підручники, посібники

1. Вишня Б.В. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.URL:https://er.dduvs.in.ua/bitstream/123456789/4206/1/Основи%20інформаційної%20безпеки%20навчальний%20посібник%2006.2019%20%283%29.pdf
2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник Київ: НА СБ України, 2020. 256 с.URL:http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf
3. Електронна бухгалтерія: підручник для здобувачів вищої освіти /В.Я. Плаксієнко, І.М. Назаренко, К.С. Жадько, С.А. Гаркуша /Зазаг. редакцією В.Я. Плаксієнка. – Київ: «Центр учбової літератури». 2021. 298 с.
4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова.К.: Видавництво Ліра-К, 2021. 412 с.URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf
5. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.URL:https://er.dduvs.in.ua/bitstream/123456789/5717/1/ПОСІБНИК%20ОУІБ%20.pdf

6.1.2. Інші джерела

6. Методичний комплекс «Інформаційна безпека та захист даних» в програмі MOODLE. URL :https://cdn.snau.edu.ua/moodle/course/view.php?id=5475
7. Інформаційна безпека та захист даних : конспект лекцій для здобувачів вищої освіти спеціальності 071 «Облік і оподаткування» денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. Суми, 2023. 102 с.
8. Інформаційна безпека та захист даних : методичні рекомендації щодо проведення практичних занять для здобувачів вищої освіти спеціальності 071 «Облік і оподаткування» денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. Суми, 2023. 54 с.
9. Інформаційна безпека та захист даних : методичні рекомендації для самостійної роботи для здобувачів вищої освіти спеціальності 071 «Облік і оподаткування» денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. Суми, 2023. 60 с.

6.2. Додаткові джерела

1. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. Суми : Сумський державний університет, 2021. 99 с.URL:https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf;jsessionid=B24CA3148C2AE0D463CDBA60D4C17C24
2. Гаркуша С.А. Діджиталізація обліково-управлінських процесів. *Сучасний стан та перспективи економічного розвитку України: теорія, методологія, практика : колективна монографія* / Кол. авторів. Полтава: ПП «Астрая», 2023. С. 95-104. URL: http://www.economics.in.ua/2023/04/collectivemonograph.html
3. Гаркуша С.А. Захист бухгалтерської інформації автоматизованих інформаційних систем. *Економіка, облік, фінанси та право: виклики сучасного інформаційного суспільства*: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 22 грудня 2021 р.): Полтава: ЦФЕНД, 2021. Ч. 1. С. 31-32.
4. Гаркуша С.А. Захист інформації та попередження шахрайства у сфері облікового забезпечення. *Економіка та суспільство.* 2021. № 33. URL:

https://economyandsociety.in.ua/index.php/journal/article/view/902. DOI: 10.32782/2524-0072/2021-33-34

5. Захист прав, свобод та безпеки людини в інформаційному суспільстві: навчальний посібник/ Пилипчук В.Г., Брижко В.М., Дзьобань О.П., Довгань О.Д., Золотар О.О., Ткачук Т.Ю., за заг.ред. В.Г. Пилипчука.- Київ-Одеса : Фенікс, 2021, 273 с. URL: http://ippi.org.ua/zakhist-prav-privatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu

6. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 6 (червень). 261с URL: http://ippi.org.ua/sites/default/files/2021-6.pdf

7. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і праваНАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 5(травень). 304с. - URL: http://ippi.org.ua/sites/default/files/2021-5.pdf

8. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с. URL: http://ippi.org.ua/natsionalnabezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi

9. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.URL:https://dspace.nau.edu.ua/bitstream/NAU/57731/1/Інформаційна%20безпека_курс%20лекцій_2022.pdf

10. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони/ збірник документів і матеріалів / Упорядники: Беланюк М.В., Доронін І.М., Лебединська О.В., Радзієвська О.Г., Пилипчук В.Г., Шамара О.В., Фурашев В.М. – К.: Видавничий дім «АртЕк». 2020. 756 с. URL: http://ippi.org.ua/sites/default/files/verstka_zbirnuk_zakoniv.pdf

11. Про захист персональних даних: Закон України від 01.06.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

12. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія / Н. Уханова; за заг. ред. В. Пилипчука.КиївОдеса: Фенікс, 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativniminformatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus

6.3. Програмне забезпечення

1. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: Особистий кабінет. URL: https://cip.gov.ua/cabinet